

ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE FORMACIÓN DE TECNÓLOGOS

IMPLEMENTACION DE UN SISTEMA BIOMÉTRICO DE AUTENTIFICACIÓN PARA EL CONJUNTO RESIDENCIAL “CONDE 4”

**TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE
TECNÓLOGO SUPERIOR EN REDES Y TELECOMUNICACIONES**

Lizbeth Mishell Ludeña Rosero

`lizbeth.ludena@epn.edu.ec`

Jessenia Patricia Rivera Campoverde

`jessenia.rivera@epn.edu.ec`

DIRECTOR: Ing. Fanny Paulina Flores Estévez, MSc.

`fanny.flores@epn.edu.ec`

CODIRECTOR: Ing. Mónica de Lourdes Vinueza Rhor, MSc.

`monica.vinueza@epn.edu.ec`

Quito, noviembre 2021

CERTIFICACIÓN

Certificamos que el presente trabajo fue desarrollado por las Srtas. Ludeña Rosero Lizbeth Mishell y Rivera Campoverde Jessenia Patricia como requerimiento parcial a la obtención del título de TECNÓLOGO SUPERIOR EN REDES Y TELECOMUNICACIONES, bajo nuestra supervisión:



Ing. Fanny Flores Estévez, MSc.
DIRECTOR(A) DEL PROYECTO

Ing. Mónica Vinueza Rhor, MSc.
CODIRECTOR(A) DEL PROYECTO

DECLARACIÓN

Nosotras Ludeña Rosero Lizbeth Mishell con CI: 171840322-1 y Rivera Campoverde Jessenia Patricia con CI: 175473787-0 declaramos bajo juramento que el trabajo 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 144 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.

Entregamos toda la información técnica pertinente, en 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.



Lizbeth Mishell Ludeña Rosero



Jessenia Patricia Rivera Campoverde

DEDICATORIA

Este proyecto de titulación fue desarrollado con esfuerzo, dedicación, perseverancia, paciencia y mucho amor, debido a que la finalización del mismo fue un proceso largo y complicado dedico este trabajo:

A **DIOS**, por guiar mi mente y camino para sobrepasar la incertidumbre y por constantemente darme fuerzas para finalizar este proyecto.

A mi **MADRE y HERMANA, Margarita Rosero y Erika Ludeña**, quienes estuvieron conmigo apoyándome y motivándome durante todo el desarrollo de este trabajo, a ellas quienes son el motor principal de mi vida y las merecedoras de todos mis logros, a ellas que a pesar de las dificultades jamás me han dejado sola.

A mis **AMIGOS**, por brindarme apoyo, fortaleza e inspiración.

Y a todos aquellos quienes incondicionalmente formaron parte de este proceso e hicieron posible con sus consejos y empuje día tras día, el cumplimiento de una meta académica en mi vida.

Lizbeth Ludeña

AGRADECIMIENTO

“El conocimiento no es una vasija que se llena, sino un fuego que se enciende”. Plutarco.

Agradezco esencialmente a la Escuela Politécnica Nacional (EPN) y a la Escuela de Formación de Tecnólogos (ESFOT), por brindarme la oportunidad de aprender de todos sus profesionales y por permitirme crecer tanto a nivel personal como académico. Quedo agradecida por el aprendizaje obtenido, por la ayuda y confianza que la institución y sus maestros han depositado en mí.

A la **Directora, Ing. Fanny Flores**, por colaborar con la investigación y desarrollo de este proyecto de titulación, por ser maestra, guía y amiga durante todo el proceso y por brindar su tiempo, dedicación y esfuerzo a la finalización exitosa de este proyecto.

A la **Co-Directora, Ing. Mónica Vinuesa**, por su aportación y valoración constructiva al desarrollo y entrega del proyecto.

A todos los Maestros, quienes con sus conocimientos y enseñanzas tanto a nivel personal como profesional aportaron a mi formación académica y durante todo el periodo dentro y fuera de la institución fueron inspiración, apoyo y motivación.

Al **Presidente y Secretaria** del Conjunto Residencial “Conde 4”, **Sr. Renan Sarchí y Sra. Grecia Falconi**, por brindarnos la oportunidad de realizar el proyecto en sus instalaciones a cargo, por facilitarnos los medios para la implementación y por depositar su confianza en el desarrollo y finalización exitosa del proyecto.

Lizbeth Ludeña

DEDICATORIA

Este documento está dedicado a mi familia por ser el pilar fundamental de mi desarrollo personal y profesional, por ser la guía e impulso necesario para seguir por el camino correcto y cumplir mis metas. Además de haberme inculcado el amor a Dios para hoy poder agradecerle el estar aquí cumpliendo un sueño que parecía inalcanzable.

Jessenia Rivera

AGRADECIMIENTO

En primer lugar, agradezco a la Escuela Politécnica Nacional de manera muy especial a la ESFOT por permitirme continuar con mis estudios, por día con día demostrarme a mí que soy capaz y que logré alcanzar una meta.

Ing. Fanny Flores por haber sido la guía y el apoyo en momentos muy difíciles el poder ver más allá de un estudiante con un rendimiento académico y reconocer a una persona que tenía dificultades.

También gracias al Sr. Renan Sarchí y a la Sra. Grecia Falconi por permitirme realizar el trabajo de titulación dentro del Conjunto, por la confianza de que era posible realizar el trabajo de titulación.

Gracias por la confianza brindada fue un trabajo arduo y que al final dio frutos gracias a la perseverancia y la confianza depositada por cada persona que estuvo a nuestro lado gracias a esas personas hoy me siento capaz de hacerlo al final entendí que solo fue cuestión de creer en mí.

Jessenia Rivera

ÍNDICE DE CONTENIDOS

1	INTRODUCCIÓN	1
1.1	Objetivo general.....	2
1.2	Objetivos específicos.....	2
1.3	Fundamentos	2
2	METODOLOGÍA	10
2.1	Descripción de la metodología usada	10
3	RESULTADOS Y DISCUSIÓN	11
3.1	Requerimientos del sistema biométrico	11
3.2	Diseño del sistema de seguridad utilizando biométricos	15
3.3	Implementación del sistema biométrico	23
3.4	Automatización del sistema en cada puerta	34
3.5	Verificación de funcionamiento.....	36
3.6	Manual de Uso y Mantenimiento	43
3.7	Presupuesto	44
4	CONCLUSIONES Y RECOMENDACIONES	45
4.1	Conclusiones.....	45
4.2	Recomendaciones	47
5	REFERENCIAS BIBLIOGRÁFICAS	48
	ANEXOS	51
	Anexo 1: Certificado de Funcionamiento	i
	Anexo 2: Manual de Usuario	iii
	Anexo 3: Manual de Administrador	ix

ÍNDICE DE FIGURAS

Figura 1.1 Biométrico <i>ZKTeco</i> -MB360.....	3
Figura 1.2 Biométrico <i>ZKTeco</i> -MA300.....	3
Figura 1.3 Botón <i>no-touch</i> K11/K2 TLEB 102.....	4
Figura 1.4 Pulsador Dorcas PL3	5
Figura 1.5 Enrutador <i>D-Link</i> N650 DIR-635.....	5
Figura 1.6 Pantalla principal de <i>ZKAccess</i> 3.5	6
Figura 1.7 Especificaciones metraje norma ANSI/TIA 568.0-D.....	8
Figura 1.8 T568-B código de colores	8
Figura 1.9 Etiquetado y ponchado del cable UTP	9
Figura 3.1 Elementos complementarios del sistema biométrico	13
Figura 3.2 Diagrama de flujo del funcionamiento del sistema.....	14
Figura 3.3 Plano con metraje de la infraestructura.....	16
Figura 3.4 Diagrama de conexión para la zona garita.....	18
Figura 3.5 Diagrama de conexión para la zona administrativa	19
Figura 3.6 Diagrama de red.....	22
Figura 3.7 Infraestructura inicial de la zona garita.....	23
Figura 3.8 Reparaciones de la zona garita	24
Figura 3.9 Adecuaciones del área de trabajo	24
Figura 3.10 Creación de la caja de alimentación para la garita	25
Figura 3.11 Creación de la caja de alimentación para la zona administrativa.....	25
Figura 3.12 Instalación de las cajas de alimentación	26
Figura 3.13 Instalación de los biométricos.....	26
Figura 3.14 Instalación del pulsador y botón <i>no-touch</i>	27
Figura 3.15 Proceso de canalización de la zona garita	28
Figura 3.16 Proceso de canalización de la zona administrativa	28
Figura 3.17 Creación del área.....	29
Figura 3.18 Creación del dispositivo	29
Figura 3.19 Creación del nivel de acceso	30
Figura 3.20 Creación del departamento.....	31
Figura 3.21 Creación de usuarios	32
Figura 3.22 Configuración del <i>tag</i>	32
Figura 3.23 Configuración de la huella dactilar.....	33
Figura 3.24 Código QR para la Base de datos	34
Figura 3.25 Configuración de las puertas	36

Figura 3.26	Ingreso de los biométricos al <i>software</i> con las direcciones IP.....	37
Figura 3.27	Comprobación de conexión para el biométrico MA300	37
Figura 3.28	Comprobación de conexión para el biométrico MB360	38
Figura 3.29	Comprobación de conexión del biométrico “zona administrativa”	38
Figura 3.30	Comprobación de conectividad de todos los biométricos.....	39
Figura 3.31	Reporte de funcionamiento.....	40
Figura 3.32	Funcionamiento de huella dactilar en el biométrico MB360	40
Figura 3.33	Comprobación de los biométricos a través del <i>tag</i>	41
Figura 3.34	Comprobación de huella dactilar con el biométrico MA300.....	41
Figura 3.35	Comprobación <i>tag</i> -huella en Administración.....	42
Figura 3.36	Apertura con la huella dactilar en la zona de administración.....	42
Figura 3.37	Comprobación a través del botón <i>no-touch</i>	43
Figura 3.38	Código QR de verificación de funcionamiento	43
Figura 3.39	Código QR para el Manual de Usuario.....	44
Figura 3.40	Código QR para el Manual de Administrador.....	44

ÍNDICE DE TABLAS

Tabla 1.1 Especificaciones técnicas del biométrico MB360	3
Tabla 1.2 Especificaciones técnicas del biométrico MA300	4
Tabla 1.3 Especificaciones técnicas del botón <i>no-touch</i> TLEB 102	4
Tabla 1.4 Especificaciones técnicas del pulsador PL3	5
Tabla 1.5 Especificaciones técnicas del enrutador <i>D-Link</i> N650 DIR-635	6
Tabla 1.6 Descripción del formato de etiquetado clase 1	9
Tabla 3.1 Comparación entre los atributos de los biométricos <i>ZKTeco</i>	12
Tabla 3.2 Planeamiento de la red	22
Tabla 3.3 Características del cable UTP Cat. 5e	27
Tabla 3.4 Presupuesto del proyecto	45

RESUMEN

El presente proyecto de titulación, “Implementación de un sistema biométrico de autenticación para el Conjunto Residencial Conde 4”, está segmentado en dos partes: área garita y área administrativa. En total se utilizó tres biométricos, un pulsador y un botón *no-touch*. Todos los elementos fueron integrados en una sola red para realizar autenticación de usuarios y control de acceso mediante el reconocimiento de huellas dactilares y *tags*, tanto al ingreso como a la salida de ambas zonas.

El documento está conformado por cinco secciones. En la primera sección se presenta el problema de los habitantes, el cual surge a partir de los constantes robos a domicilios en la ciudad Quito sector sur por falta de mecanismos de seguridad para autenticación y control de acceso. Además, en los fundamentos se expone conceptos básicos del proyecto, elección de elementos de *hardware* y *software*, así como también las normativas a ser cumplidas en la implementación. El segundo apartado aborda la metodología usada para alcanzar los objetivos específicos.

En la tercera sección, resultados y discusión, se detalla el procedimiento realizado que partió con la determinación de los requisitos para la elección y compra de los dispositivos, así como también se diseñó planos y diagramas de conexión en base al metraje físico de la infraestructura y la interconectividad de los equipos, respectivamente. Además, se explica el proceso realizado para la implementación en base a las normativas correspondientes y automatización en cada puerta; así mismo, se evidencia la verificación de funcionamiento del sistema como un único conjunto conformado por tres biométricos. Finalmente, se añadió videos y manuales tanto para residentes como para el administrador, estos documentos fueron incorporados como anexos.

En la cuarta sección, conclusiones y recomendaciones, se da a conocer de forma sintetizada cada uno de los procedimientos realizados, siendo estos la identificación del problema, diseño, implementación, automatización y verificación de funcionamiento del sistema.

PALABRAS CLAVE: Sistema biométrico, *hardware*, *software*, *tags*, huellas digitales, TCP/IP.

ABSTRACT

The present degree project, "Implementation of a biometric authentication system for the Complex Residential Conde 4", is segmented into two parts: the guardianship area and the administrative area. In total, three biometrics, a button, and a no-touch button were used. All elements were integrated into a single network to perform user authentication and access control through fingerprint and tags recognition, allowing the entry and exit.

The document contains five sections. The first section details the problem that people have in the residential complex, where the main issue is home robberies in southern Quito due to the lack of security mechanisms for authentication and access control. Additionally, this section includes the hardware and software elements review and the necessary regulations for the implementation. The second section contains the methodology used to achieve the specific objectives.

The third part, results and discussion, gives an overview of the process performed that started with the determination of requirements for choosing the devices, also the design of plans and connection diagrams using infrastructure measures and the interconnectivity equipment are presented. In addition, it explains the process for the implementation based on normative and automatization of each door, the system operation verification as a unique set that has three biometrics. Finally, videos and manuals for residents and administrative, are included in the section of annexes.

In the fourth section, conclusions and recommendations, is released, synthesizing all the processes and giving suggestions for each procedure, including problem identification, design, implementation, automatization, and verification of the system operation.

KEYWORDS: *Biometric system, hardware, software, tags, fingerprints, TCP/IP.*

1 INTRODUCCIÓN

La seguridad dentro de la ciudad de Quito es uno de los problemas más difíciles de afrontar. De acuerdo con un estudio realizado sobre delitos de robo en el Distrito Metropolitano de Quito (DMQ), se obtuvo un total de 1 708 casos de robo a domicilios que representa el 13% del total de denuncias durante el año 2017 [1]. Por lo cual, es importante tomar medidas de protección para evitar ser víctimas de la delincuencia. Con el propósito de mitigar dicha problemática, cada vez resulta más común la implementación de sistemas con autenticación y control de acceso, basados en avances tecnológicos que facilitan y mejoran el nivel de vida.

La necesidad dentro del Conjunto Residencial “Conde 4” ubicado en la ciudad de Quito sector Sur, surge al no contar con un mecanismo de seguridad que proporcione un control de acceso para las personas que habitan dentro del Conjunto, convirtiéndolo en un foco de inseguridad.

Con la finalidad de solventar el problema, se propuso implementar un sistema biométrico dentro de la urbanización. Dicho sistema consta de dos etapas, la primera es la instalación de dos biométricos y un pulsador en la puerta principal de la residencia, en la segunda se colocó un punto de acceso en la zona administrativa, el cual se compone de un biométrico y un botón *no-touch*. Los biométricos utilizan el Protocolo de Control de Transmisión / Protocolo de Internet (TCP/IP) para transmitir, recibir y cargar información al *software*, otros elementos que conforman este medio de comunicación son cables de red y direcciones IP, de esta forma se obtiene un sistema sencillo, funcional y convergente.

El sistema biométrico tiene como propósito brindar seguridad mediante la verificación y autenticación de usuarios, impidiendo que individuos externos ingresen al Conjunto a causar algún tipo de daño, sin dejar de lado el hecho de cuidar y precautelar los bienes materiales de cada uno de los residentes. Adicionalmente, la administración tendrá la potestad de tomar medidas disciplinarias y sancionar cualquier tipo de infracción por inconvenientes ocasionados dentro del Conjunto, asegurando una convivencia pacífica.

La autenticación que maneja el sistema biométrico se basa en la tecnología de la biometría, donde los sensores del lector del biométrico son capaces de identificar huellas dactilares entre otras características físicas. En caso de que la identificación de la huella sea errónea, los residentes no tendrán acceso al Conjunto [2]. Otra posibilidad

para la apertura de las puertas es el uso de *tags*, los mismos que funcionan con la tecnología de Identificación por Radiofrecuencia (RFID) almacenando un código único, siendo el biométrico el encargado de reconocer y comparar la información entre el *tag* y la base de datos del *software* [3].

1.1 Objetivo general

Implementar un sistema biométrico de autenticación para el Conjunto Residencial “Conde 4”.

1.2 Objetivos específicos

- Determinar los requerimientos del sistema biométrico
- Diseñar el sistema de seguridad utilizando biométricos
- Implementar el sistema biométrico con todos los componentes
- Automatizar todos los sistemas en cada puerta
- Verificar el correcto funcionamiento del proyecto

1.3 Fundamentos

Un sistema biométrico es un proceso de reconocimiento automatizado que utiliza la biometría personal; este método de seguridad permite la autenticación de usuarios en base a la identificación de características físicas, como pueden ser: rostros, iris o huellas dactilares [4].

Además, otro método de verificación que se utiliza en un sistema biométrico es el uso de *tags*, donde la tecnología de reconocimiento que se aplica en este tipo de seguridad es sumamente integral e intuitivo con el usuario. Todas estas posibilidades de acceso hacen que esta estructura sea confiable, eficiente y cómoda [4].

ZKTeco es una de las marcas con mayor reconocimiento en la fabricación de equipos para el desarrollo de estos procedimientos, debido a su calidad y economía. La implementación cumple con las funciones de protección, identificación y automatización incorporando *hardware* y *software* [5].

- **Hardware**
 - **Biométrico *ZKTeco*-MB360**

El biométrico *ZKTeco*-MB360 es un dispositivo innovador e inteligente fabricado para administración de usuarios, control de acceso, gestión de eventos, creación de horarios

y entrega de reportes. Este equipo utiliza autenticación mediante la detección de rostros, huellas dactilares, tarjetas RFID, *tags* y claves [6].

ZKTeco-MB360 utiliza TCP/IP para comunicarse a través de una interfaz con el computador, otra alternativa es el uso de un Bus Serie Universal (USB) donde la transferencia de información es manual. En la Figura 1.1 y Tabla 1.1 se presenta el equipo y sus respectivas especificaciones técnicas.



Figura 1.1 Biométrico ZKTeco-MB360 [6]

Tabla 1.1 Especificaciones técnicas del biométrico MB360 [6]

Características	Especificaciones
Capacidad de huellas	1 500
Capacidad de <i>tag</i>	10 000
Capacidad de eventos	100 000
Detección	< 1 (s)
Tipo de comunicación	TCP/IP
Dimensiones	73 x 148 x 34.5 (mm)
Fuente de alimentación	12 (V _{DC}) 1.5 (A)

- **Biométrico ZKTeco-MA300**

El biométrico MA300 maneja el algoritmo 3D *Neuron* para reconocimiento de huellas dactilares y para la identificación de tarjetas o *tags*, los cuales utilizan tecnología RFID. Este equipo es hermético y cuenta con protección IP65; además, funciona con comunicación TCP/IP; estas características hacen que el sistema en el cual se integre este dispositivo sea sumamente preciso, confiable y eficiente [7].

En la Figura 1.2 y Tabla 1.2 se muestra el equipo y sus características técnicas.



Figura 1.2 Biométrico ZKTeco-MA300 [7]

Tabla 1.2 Especificaciones técnicas del biométrico MA300 [7]

Características	Especificaciones
Capacidad de huellas	2000
Capacidad de <i>tag</i>	2000
Capacidad de eventos	100 000
Detección	< 1 (s)
Tipo de comunicación	TCP/IP – USB
Dimensiones	167.5 x 148.8 x 32.2 (mm)
Fuente de alimentación	12 (V _{DC})

- **Botón *no-touch* ZKTeco K11 TLEB 102**

El botón K11/K2 TLEB 102 es un elemento moderno que ocupa un sensor óptico infrarrojo para detectar el movimiento realizado por el usuario; este mecanismo es sensible, por lo cual el accionamiento del sistema es inmediato. La verificación de funcionamiento se realiza con la ayuda de diodos emisores de luz (LED); además, tiene integrado un receptor de radiofrecuencia (RF) que permite la apertura de la puerta a distancia [8].

En la Figura 1.3 y en la Tabla 1.3 se encuentra el equipo y las especificaciones técnicas.



Figura 1.3 Botón *no-touch* K11/K2 TLEB 102 [8]

Tabla 1.3 Especificaciones técnicas del botón *no-touch* TLEB 102 [8]

Características	Especificaciones
Proximidad	0.1 ~ 10 (cm)
Dimensiones	115 x 70 x 29 (mm)
Fuente de alimentación	12 (V _{DC})
Material	Acero inoxidable
LED Indicador	LED AZUL: Reposo LED ROJO: Activación
Frecuencia de trabajo	433 (MHz)

- **Pulsador DORCAS PL3**

Un pulsador es un dispositivo que concede o interrumpe el flujo de electricidad; por lo general, si los bornes se encuentran unidos al pulsador existe el paso de corriente; por el contrario, si ambas piezas se encuentran separadas no existe afluencia de corriente eléctrica [9]. En la Figura 1.4 y Tabla 1.4 se evidencia el elemento y las especificaciones técnicas.



Figura 1.4 Pulsador Dorcas PL3 [9]

Tabla 1.4 Especificaciones técnicas del pulsador PL3 [9]

Características	Especificaciones
Tipo de contacto	Pulsación
Dimensiones	100 x 25 x 36 (mm)
Material	Acero inoxidable
Corriente máxima	12 (V _{AC}) 3 (A)

- **Enrutador *D-Link RangeBooster* N650 DIR-635**

El enrutador *D-Link* DIR-635 tiene un alto rendimiento con todas las tecnologías sea *Ethernet* o inalámbrica; además, cuenta con varios tipos de seguridades como: Privacidad Equivalente por Cable de 64/128 bits (WEP), filtrado por Control de Acceso a Medios (MAC) y por Localizador Uniforme de Recurso (URL).

Este dispositivo de la marca *D-Link* tiene una cobertura máxima de hasta 30 (m) gracias a las tres antenas dipolo de 2 (dBi). Además, maneja varios puertos, los cuales le permiten acceder a diferentes tipos de redes como: la Red de Área Local (LAN) y la Red de Área Amplia (WAN) [10].

En la Figura 1.5 y Tabla 1.5 se presenta el equipo y sus características técnicas.



Figura 1.5 Enrutador *D-Link* N650 DIR-635 [10]

Tabla 1.5 Especificaciones técnicas del enrutador *D-Link* N650 DIR-635 [10]

Características	Especificaciones
Tasa de transferencia	Máximo 100 (Mb/s)
Dimensiones	116.84 x 193.04 x 30.48 (mm)
Fuente de alimentación	5 (V _{DC}) 3 (A)
Puertos	- LAN: 4 puertos 10/100 (Mb/s) - WAN: 1 puerto 10/100 (Mb/s) - USB 2.0
Antena	3 antenas dipolo de 2 (dBi)
Frecuencia de trabajo	3.8 (GHz)

- **Software**

ZKAccess 3.5

El sistema de control de acceso *ZKAccess 3.5* es un *software* de administración que permite la fácil gestión de procesos, sean estos operativos o de seguridad dentro de la aplicación. Además, proporciona dos métodos de trabajo, el primero es un sistema personal donde el administrador organiza departamentos y gestiona usuarios; el segundo método conocido como sistema de equipo, permite realizar todas las configuraciones pertinentes para la comunicación entre el sistema y los equipos interconectados [11].

En la Figura 1.6 se muestra la pantalla principal con sus respectivos íconos.



Figura 1.6 Pantalla principal de *ZKAccess 3.5* [11]

El administrador de la plataforma tiene la posibilidad de realizar varias actividades, tales como: creación (departamentos, usuarios, reportes, áreas, dispositivos, horarios, días festivos, niveles de acceso y privilegios), configuración (sistema, equipos, usuarios, registros y niveles de acceso) y administración (edición, eliminación y bloqueo de usuarios). El monitoreo en tiempo real es un proceso que debe realizarse estrictamente cuando existe una conexión a internet y con un *software* adicional [11].

Este *software* tiene varios parámetros y funciones, que lo hacen la mejor opción dentro del mercado, centralizando todo el proceso de gestión de los tres dispositivos en una sola aplicación. Algunas de sus características principales son la capacidad de interconectar hasta 100 equipos con una cantidad límite de hasta 30 000 usuarios, ocupa la base de datos *Microsoft Office Access* y se maneja con el sistema operativo (SO) a partir de *Windows 7* de 32 o 64 *bits* [11].

- **Normativas**

Todas las normativas detalladas a continuación pertenecen a: el Instituto Nacional Estadounidense de Estándares (ANSI), la Asociación de Industrias Electrónicas (TIA) y al Instituto de Ingenieros Eléctricos y Electrónicos (IEEE).

- **ANSI/TIA 568.0-D**

Par Trenzado no Blindado (UTP) categoría 5e: Se designa aplicar a los cables de 100 (Ω) con características de transmisión especificadas de hasta 100 (MHz).

Cableado horizontal: Es el área compuesta por cables, terminaciones, canalización, cables de equipos y cordones de conexión que son necesarios para llevar un servicio hasta el puesto de trabajo.

Área de trabajo: Con este estándar, se define como el espacio en el que el usuario final interactúa con los equipos terminales.

Conexión cruzada horizontal: Es el conjunto de equipos finales que usa la conexión a través del tendido, empleando en ambos extremos *patch cords* de máximo 10 (m). Esta especificación de la norma se encarga de conectar el cableado horizontal de máximo de 90 (m) con equipos terminales a partir de dispositivos de capa 2 [12], como se muestra en la Figura 1.7.

Topología: El estándar exige que sea tipo estrella para el cableado horizontal.

Conectores de telecomunicaciones: En las áreas de trabajo se utilizan conectores modulares conocidos como RJ45 para la terminación de cables horizontales de cobre.

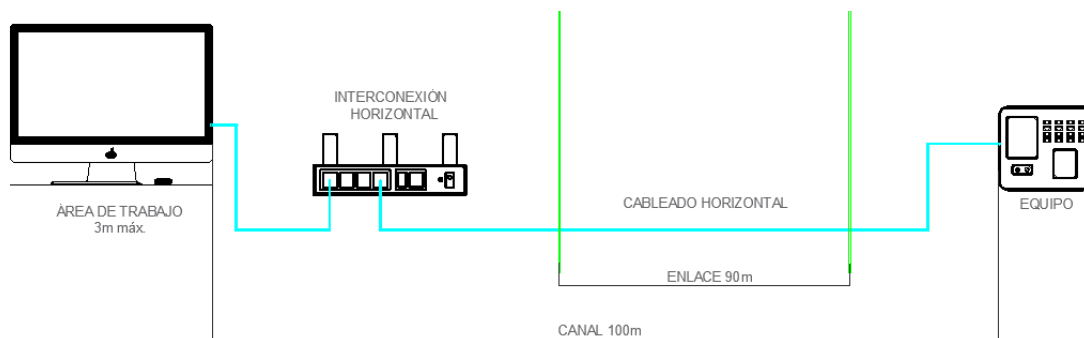


Figura 1.7 Especificaciones metraje norma ANSI/TIA 568.0-D [12]

- **Estándar de terminación T568-B:** Define el código de colores que se debe usar para el ponchado en cada una de las terminales del cableado horizontal [12], tal como se muestra en la Figura 1.8.

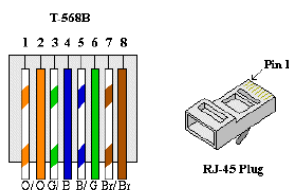


Figura 1.8 T568-B código de colores [12]

- **ANSI/TIA 570-A**

Área de trabajo: Los conectores de telecomunicación se colocarán dependiendo del usuario final; por lo general, se coloca cerca a la salida eléctrica que alimenta el sistema de telecomunicaciones dentro de 1 (m). La altura para la instalación de la salida de telecomunicaciones depende del tipo de muebles que posea o de las necesidades del usuario final, tomando un valor mínimo de referencia de 30 (cm) sobre el suelo ya terminado.

Canalización: En la selección del tipo de canalización se debe considerar el soporte de la pared y verificar que el ambiente sea seco [13].

- **ANSI/TIA 606-A**

Esta norma sirve para realizar el etiquetado de los sistemas y cables, tanto del área de trabajo como del cuarto de telecomunicaciones; el etiquetado incluye código de colores y los diferentes terminales del sistema implementado [14].

Clase 1: sirve para identificar el cableado horizontal, y el espacio de telecomunicaciones; la descripción del formato (fs – an) se muestra en la Tabla 1.6.

Tabla 1.6 Descripción del formato de etiquetado clase 1 [14]

Formato	Descripción
f	Denota el piso del edificio con un carácter numérico.
s	Denota el espacio en el que se encuentra con caracteres alfanuméricos
fs	Identificador del espacio de telecomunicaciones con caracteres alfanuméricos.
a	Identifican un panel de conexión con puertos numerados de manera secuencial.
n	Sirve para designar el puerto al que está conectado

La norma **ANSI/TIA 607-B** que especifica la estandarización de los enlaces y puesta a tierra de telecomunicaciones, no fue implementada porque la locación ya contaba con puesta a tierra en la caja de *breakers*.

- **Estándar IEEE 802.3ab**

También conocido como 1000BASE-T, sirve para la transferencia de datos entre equipos a nivel de capa física en redes LAN manejando una velocidad de transmisión de hasta 1 (Gb/s); además, permite trabajar con un sistema de cableado estructurado con cable UTP Cat. 5e. La última versión actualizada es IEEE 802.3cu 2021 [15], la cual emplea una velocidad de hasta 400 (Gb/s).

• **Tecnología Ethernet**

Ethernet es la tecnología de interconexión entre *hardware* y *software* más utilizada en redes LAN; los terminales se comunican entre sí a través del uso de este medio de comunicación, compartiendo información dentro de la red a la cual pertenecen [16].

Cualquier infraestructura realizada con el protocolo IEEE 802.3, mejor conocido como *Ethernet*, debe llevar un correcto etiquetado al igual que el ponchado adecuado con respecto al tipo de dispositivos que se desea conectar.

Las etiquetas utilizadas para el reconocimiento del cableado fueron realizadas en base a la norma ANSI/TIA 606-A Clase 1; por otro lado, la norma utilizada para el ponchado es la T568-B. En la Figura 1.9 se evidencia el ejemplo del etiquetado y ponchado.



Figura 1.9 Etiquetado y ponchado del cable UTP

2 METODOLOGÍA

2.1 Descripción de la metodología usada

Los requerimientos para la implementación del sistema biométrico fueron determinados en base a un análisis previo donde se establecieron las particularidades que debían cumplir los biométricos a ser instalados. En la instalación del sistema se ocuparon componentes como: cerraduras electromagnéticas, soportes, fuentes de alimentación, baterías alternas, botones de salida y *tags*. También se evaluó las necesidades que presentaba el Conjunto con respecto al nivel de seguridad, asimismo otros puntos en consideración con respecto al cableado estructurado fueron la infraestructura de las puertas, los puntos de acceso, el tipo y metraje del cable. Todos los elementos se adquirieron después de realizar un acuerdo con los beneficiarios, en relación al costo de los mismos.

Para el diseño se procedió a plasmar el ambiente físico dentro del *software AutoCAD*; estos planos incluyen la ubicación y distancia entre los puntos de acceso para los biométricos, el sistema de alimentación de los equipos, cableado estructurado y la automatización de las puertas. Además, se incluyó las medidas de la infraestructura. Una vez finalizada la elaboración del plano con todos los datos de metraje, se procedió a seleccionar el sistema de alimentación y reserva para en el caso en que no se cuente con suministro de energía, este funcione sin interrupción. Luego, se realizó la estructuración de la red; conociendo que los biométricos trabajan de forma individual, se decidió que los tres equipos trabajen como un solo sistema formando una topología tipo estrella que sea manejada a través del *software*.

La implementación del sistema biométrico se realizó en base a los diseños elaborados en *AutoCAD*. Para la puesta en marcha se consideró el cumplimiento de las normativas que regulan el sistema de cableado, siendo la de mayor peso la norma ANSI/TIA569-D. Una vez realizada la activación del sistema por completo, fue necesario realizar el registro de huellas y *tags*; para ello, se utilizó el *software ZKAccess 3.5* desde el cual se configuró los biométricos y la base de datos. Todos los elementos del sistema fueron interconectados mediante el cableado estructurado, garantizando que todos los dispositivos se comuniquen y que la información que se transfiera sea íntegra y confiable.

En la puerta del área garita y área administrativa se implementó cerraduras electromagnéticas y un brazo hidráulico que funciona con baterías; la integración de estos elementos permitirá tener un servicio de manera ininterrumpida. Por tanto, el biométrico de ingreso, salida y de la administración con los equipos adicionales pertenecen a una misma red. De esta forma se autoriza o deniega el ingreso y salida del Conjunto Residencial “Conde 4”; además, se proporciona acceso únicamente a personas autorizadas en el área de administración.

Finalmente, instalado el sistema completo con los tres biométricos y sus respectivos elementos complementarios, se procedió a la verificación de funcionamiento de todos los equipos en conjunto; adicionalmente, se informó a los residentes de la operatividad del sistema. Por otro lado, a los funcionarios que controlan el sistema dentro del condominio, se les proporcionó un manual que indique cómo manejar y modificar el sistema en caso de requerir algún cambio o bloquear alguna huella o *tag* de cualquier residente. Además, se brindó recomendaciones en cuanto al mantenimiento de los dispositivos y del sistema, con la finalidad de establecer normas de seguridad para que todos los beneficiarios cuiden de los equipos y de esa forma evitar daños o fallas del sistema.

3 RESULTADOS Y DISCUSIÓN

3.1 Requerimientos del sistema biométrico

Para iniciar el proyecto se solicitó información acerca de la urbanización a la junta directiva del Conjunto Residencial “Conde 4”; gracias a estos datos, se determinó los requisitos para la adquisición de los equipos. En este informe se detalla que existe un total de 189 casas de las cuales solo 164 están habitadas, en las que viven de 2 a 5 personas por cada domicilio; además, se especifica que antes de la implementación del presente proyecto, la seguridad era insuficiente, ya que la única protección con la que se contaba eran candados en las puertas y la presencia del guardia de turno.

Conociendo la necesidad de la residencia y en base a la información obtenida, se realizó un análisis para definir las cualidades de los biométricos, los equipos complementarios, el nivel y tipo de seguridad. La implementación de los dispositivos biométricos tiene como finalidad aumentar el nivel de seguridad, utilizando una protección de biometría, este método es sofisticado y cómodo para la autenticación de usuarios.

Considerando que los biométricos deben tener una capacidad mínima de 820 huellas dactilares, eventos, registros y *tags*; además, se requiere que cuente con comunicación TCP/IP para obtener todos los beneficios que la tecnología basada en dicha comunicación ofrece. Conociendo los parámetros fundamentales, se consideró analizar los siguientes equipos IN01, F18, MB-360, MA-300 y X7, todos de la marca *ZKTeco*.

Teniendo conocimiento de las características de los biométricos y de las necesidades de la urbanización, se puntualizó que los equipos MB-360 y MA-300 son los indicados para la implementación porque cumplen con todos los atributos requeridos. En la Tabla 3.1 se realiza una comparativa de los biométricos mencionadas.

Tabla 3.1 Comparación entre los atributos de los biométricos *ZKTeco* [6] [7] [17] [18] y [19].

Biométricos/ Atributo	Cantidad de huellas	Cantidad de <i>tags</i>	Cantidad de eventos	Tipo de comunicación	Dimensiones
F18	3 000	5 000	30 000	TCP/IP	80 x 183 x 42 (mm)
IN01	3 000	-----	100 000		210 x 157 x 50 (mm)
MB-360	2 000	2 000	100 000		167.5 x 148.8 x 32.2 (mm)
MA-300	1 500	10 000	100 000		73 x 148 x 34.5 (mm)
X7	500	500	-----		88.1 x 88.1 x 34.69 (mm)

Los biométricos *ZKTeco*-MB-360 y *ZKTeco*-MA-300 abastecen la cantidad de usuarios estimados, sus dimensiones son precisas para el lugar de ubicación y cabe recalcar que ambos dispositivos están adaptados para instalaciones en exteriores. La preferencia del primer equipo frente a los no seleccionados se debe a que este agrega otros tipos de seguridades, como el uso de una clave o la lectura facial.

Después de definir los equipos principales, se procedió a determinar los equipos complementarios como baterías, cerraduras electromagnéticas, soportes tipo Z y L, transformadores, tarjetas convertidoras de corriente alterna (AC) a corriente continua (DC) y gabinetes; adicionalmente, se planteó la utilización de un brazo hidráulico, un pulsador, un botón *no-touch* y un enrutador. En la Figura 3.1 se muestran los elementos complementarios.

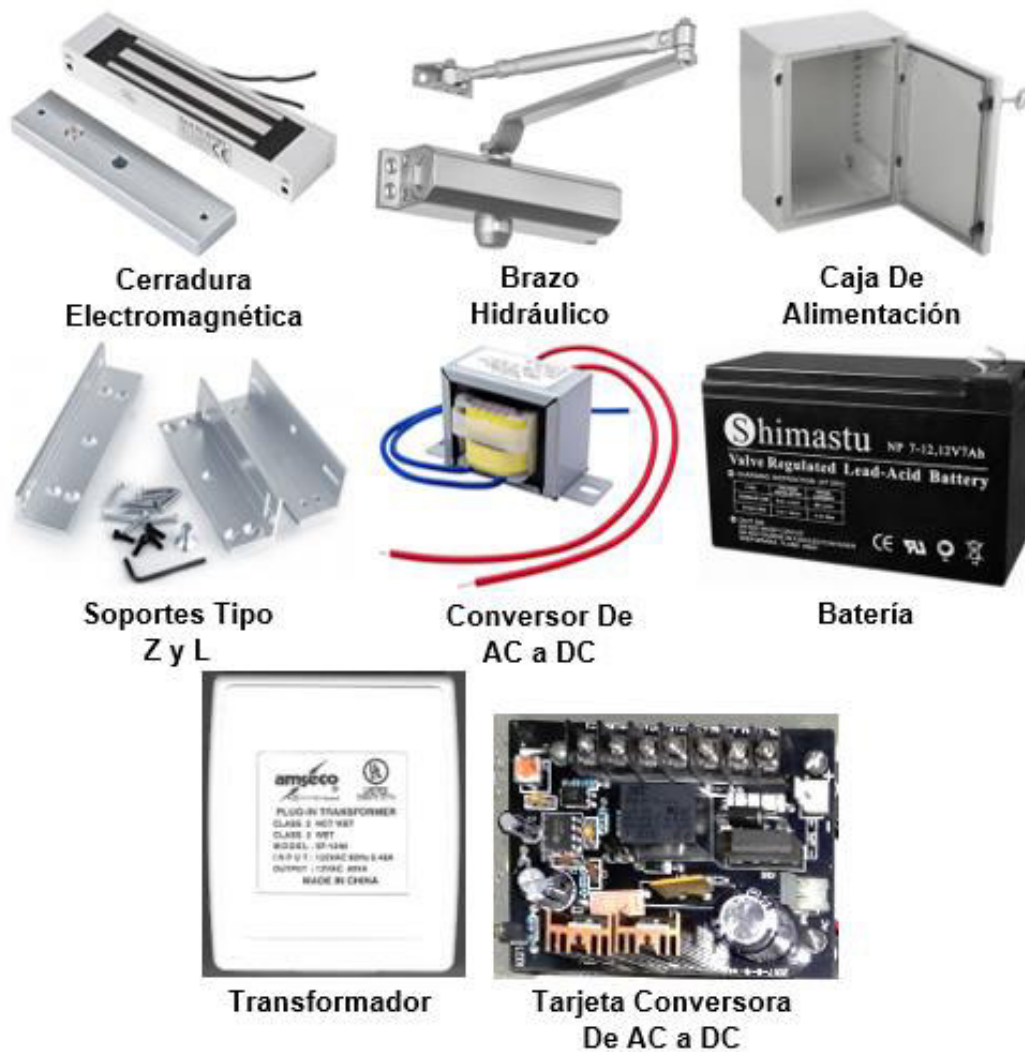


Figura 3.1 Elementos complementarios del sistema biométrico [20]

La implementación del sistema biométrico está segmentada en dos ubicaciones; en la parte interna del área de la garita se colocó el biométrico MB-360 y el MA-300 en la parte externa, la conexión de los biométricos con la cerradura, brazo y elementos del gabinete de esta sección se realizó con 10 (m) de cable UTP cat. 5e. Así mismo, en el área administrativa se instaló el biométrico MA-300 a la entrada de la puerta y con la intención de reducir el contacto del usuario con el dispositivo, en la parte interna se ubicó un botón *no-touch*, para esta interconexión se utilizó 8 (m) de cable.

El nivel de seguridad implementado en las puertas para el control de acceso varía según la necesidad; en la puerta principal existen tres tipos: huellas, *tags* y claves para residentes, la última opción también es válida para visitantes. Por otro lado, la puerta del área administrativa tiene dos tipos de seguridades: huellas dactilares y *tags*. Cabe recalcar que ambas áreas cuentan con tarjetas de administrador.

Adicionalmente, el modelo MB-360 soporta reconocimiento facial; sin embargo, por solicitud de la administración, no se habilitó dicha funcionalidad.

En la Figura 3.2 se evidencia el funcionamiento del biométrico MB-360 en base a lo explicado con anterioridad. La diferencia con el modelo MA-300 es que no existe la posibilidad del ingreso mediante el uso de una clave; cabe recalcar que solo cuando se produzca el acceso correcto, la puerta se abrirá, caso contrario permanecerá cerrada.

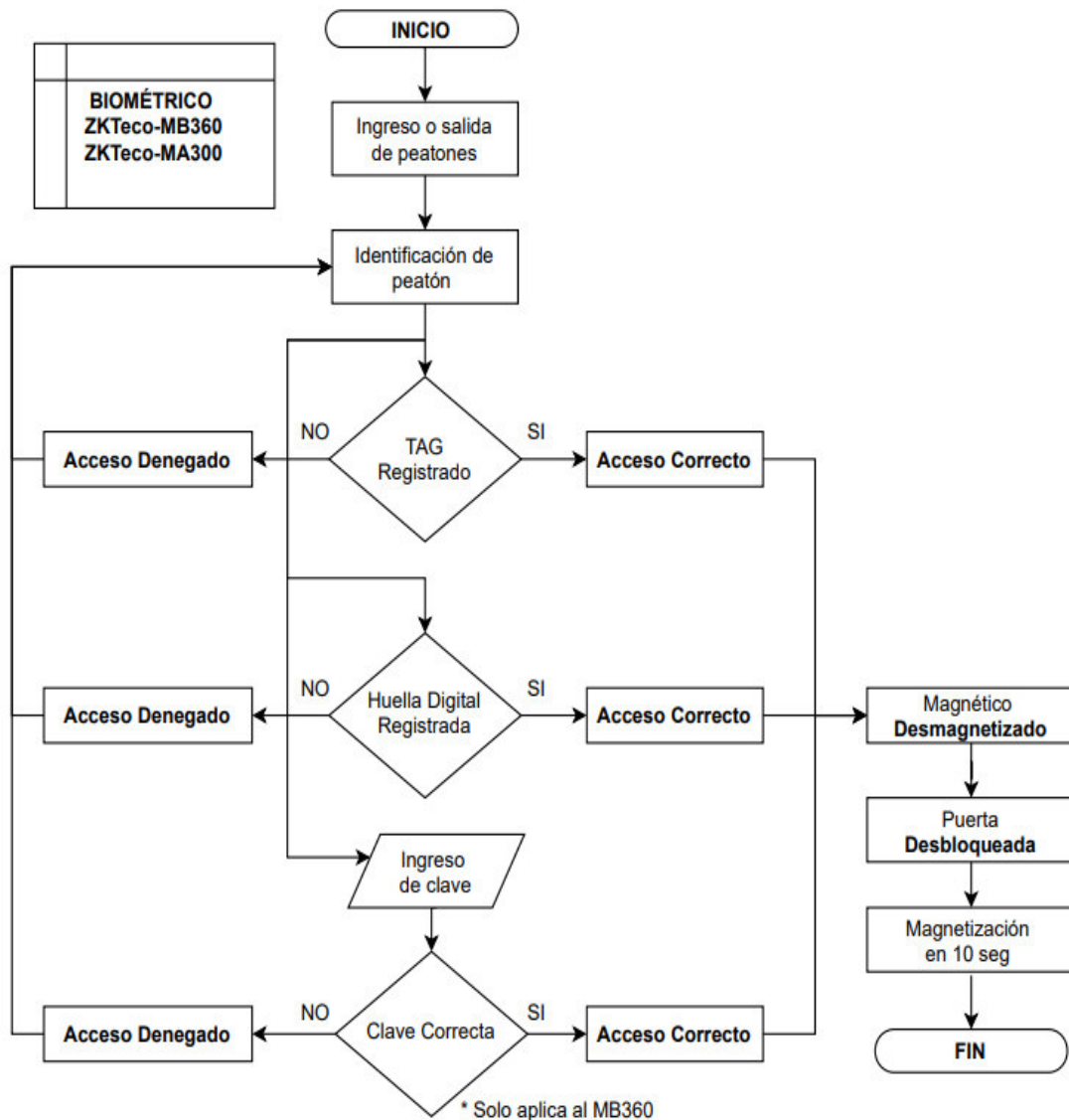


Figura 3.2 Diagrama de flujo del funcionamiento del sistema

3.2 Diseño del sistema de seguridad utilizando biométricos

Primero se procedió a medir la zona de la garita y la zona administrativa con el objetivo de conocer las dimensiones exactas del espacio físico para elaborar el sistema de cableado estructurado, teniendo las siguientes medidas; zona garita 247 x 178 (cm) y zona administrativa 326 x 178 (cm).

La instalación de los biométricos y elementos complementarios, se realizó en base a un plano desarrollado en *AutoCAD* usando una escala de 1:00, en la Figura 3.3 se puede observar el metraje tanto de la infraestructura como de los puntos de acceso.

Ubicación de los puntos de acceso

Una vez adquiridos los equipos y accesorios para la instalación del sistema biométrico, se determinó la altura para la colocación de cada dispositivo, para lo cual se consideró la recomendación del fabricante, que indica que los biométricos no deben estar a una altura menor de 1.15 (m) [21].

En la Figura 3.3, se evidencia las medidas a las cuales fueron instalados los biométricos teniendo; el MB300 a 130 (cm), el MA360 a 150 (cm) y el zona administrativa a 225 (cm) de altura con respecto al suelo. Además, entre los dispositivos de la garita existe una distancia de separación de 150 (cm), la ubicación estratégica de todos los componentes da como resultado un sistema eficiente.

Diagramas de Conexión

En el Conjunto Residencial “Conde 4”, se realizó la implementación del sistema biométrico en dos etapas. La primera consistió en la instalación de dos biométricos en la zona de la garita y en la segunda zona, dedicada al uso administrativo se implementó un biométrico junto con un botón *no-touch*. Ambas zonas tienen como finalidad facilitar el acceso de los residentes.

Es importante hacer énfasis en algunas características; tales como, el uso de 30 (m) de cable UTP Cat-5e y de la norma ASNI/TIA 606-A para el etiquetado del cableado estructurado, mismo que será ubicado en la zona administrativa; asimismo, en las dos zonas se incluyó transformadores de 110 a 12 (V) y baterías, estos elementos en conjunto garantiza la independencia del sistema eléctrico público. Además, en el plano se incluyó la simbología de los elementos para facilitar el reconcomiendo de los mismos.

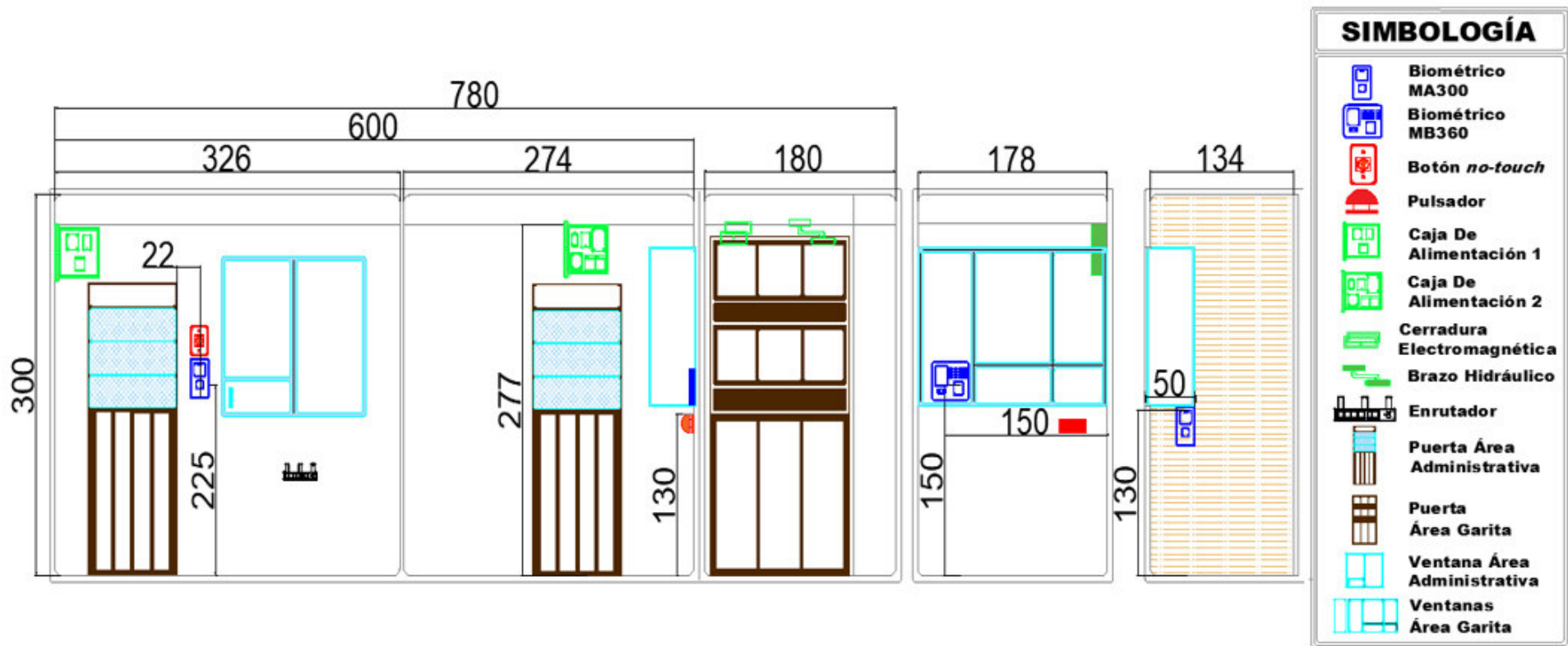


Figura 3.3 Plano con metraje de la infraestructura

Zona de Garita

En esta área se procedió a instalar dos biométricos cuyos modelos son MA300 y MB360 tanto al ingreso, como a la salida del Conjunto, respectivamente. A pesar de las diferentes dificultades presentadas, se logró establecer un sistema convergente y funcional; se determinó que el medio óptimo de conexión y comunicación para estos equipos fue el *software*.

Así para el caso de conexión entre el MA300 y el MB360, se planteó el diagrama de conexión mostrado en la Figura 3.4, en el cual se detalla las entradas y el modo de conexión que se realizó para que funcionen como un sistema.

Así las entradas para el biométrico MA300 y MB360 son:

NC1: Entrada conocida como normalmente cerrada, la cual ayuda a la cerradura electromagnética a formar un campo magnético; para esto necesita un flujo de corriente continua, impidiendo que la puerta se abra, a menos de que se realice un corte de energía a través de la verificación dentro de la lectora de un usuario en particular.

COM1: Conocida como común.

+12 (V): Este pin permite alimentar al biométrico en el caso que sea tipo ingreso (IN); también posee otra entrada con el mismo nombre tipo salida (OUT), esta permite la alimentación de otros dispositivos, recordando que el amperaje es bajo. Esta aclaración es muy importante pues esta razón fue por la cual no se energiza la cerradura con el mismo biométrico.

Tierra (GND): Son las conexiones a tierra del sistema.

Botón (BUT): Esta entrada del biométrico MB360 permitió conectar el pulsador que se encuentra en la parte interna de la garita.

Mientras que el conector tipo **RJ45** sirve para una comunicación tipo TCP/IP, la misma que es usada para enviar todos los datos desde la computadora, con ayuda del *software*, hacia el biométrico.

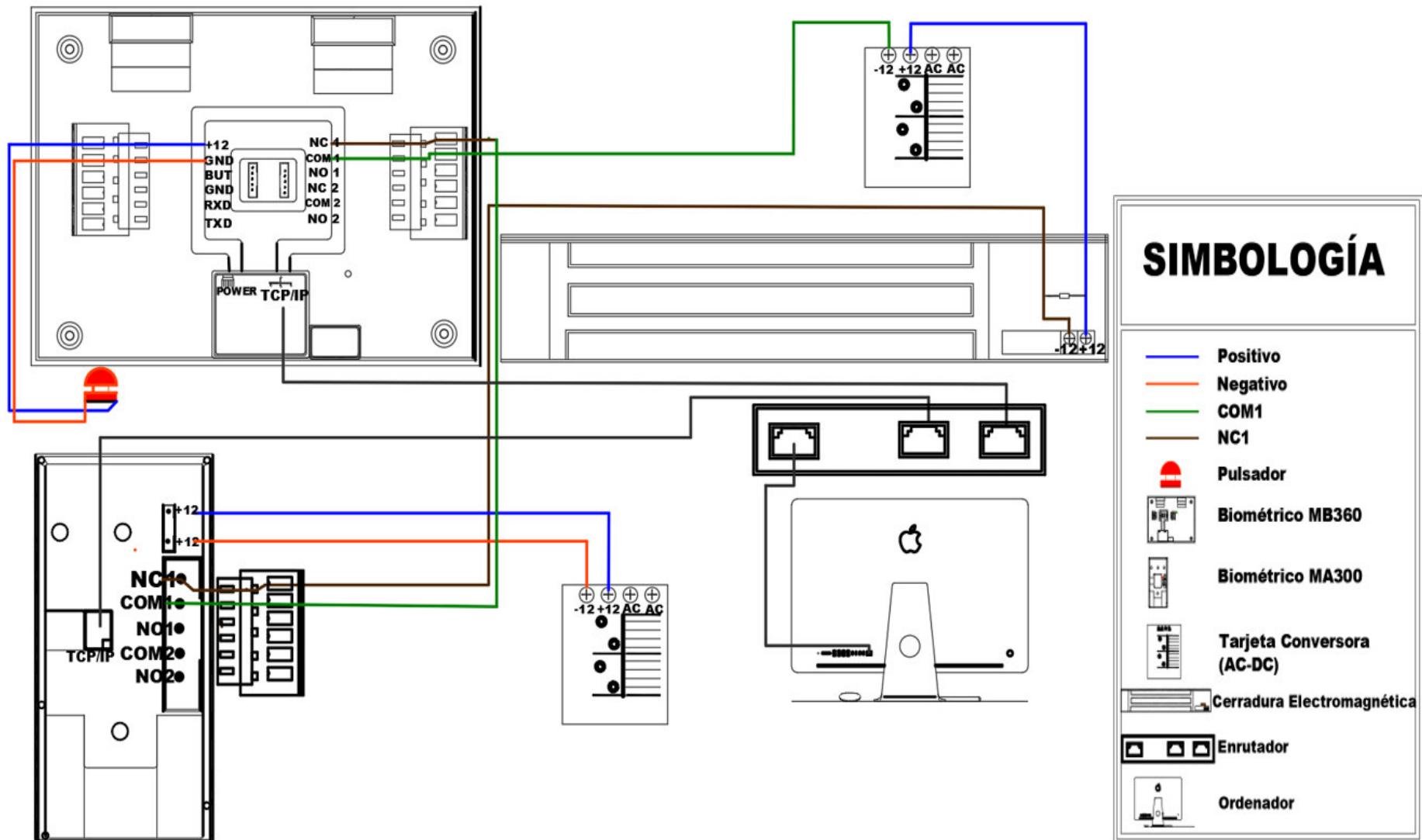


Figura 3.4 Diagrama de conexión para la zona garita

Zona de Administración

En esta zona se utilizó el modelo del biométrico MA300; además, a diferencia del sistema en la zona de la garita, este no utilizó otro biométrico, por el contrario, se usa un botón *no-touch*, el mismo que cuenta con entradas de energía (+12 (V), GND) y entradas de comunicación entre el biométrico y el botón (COM, NC1). El sistema trabaja con la cerradura electromagnética y su propia fuente de alimentación. El diagrama de conexión de la zona administrativa se muestra en la Figura 3.5.

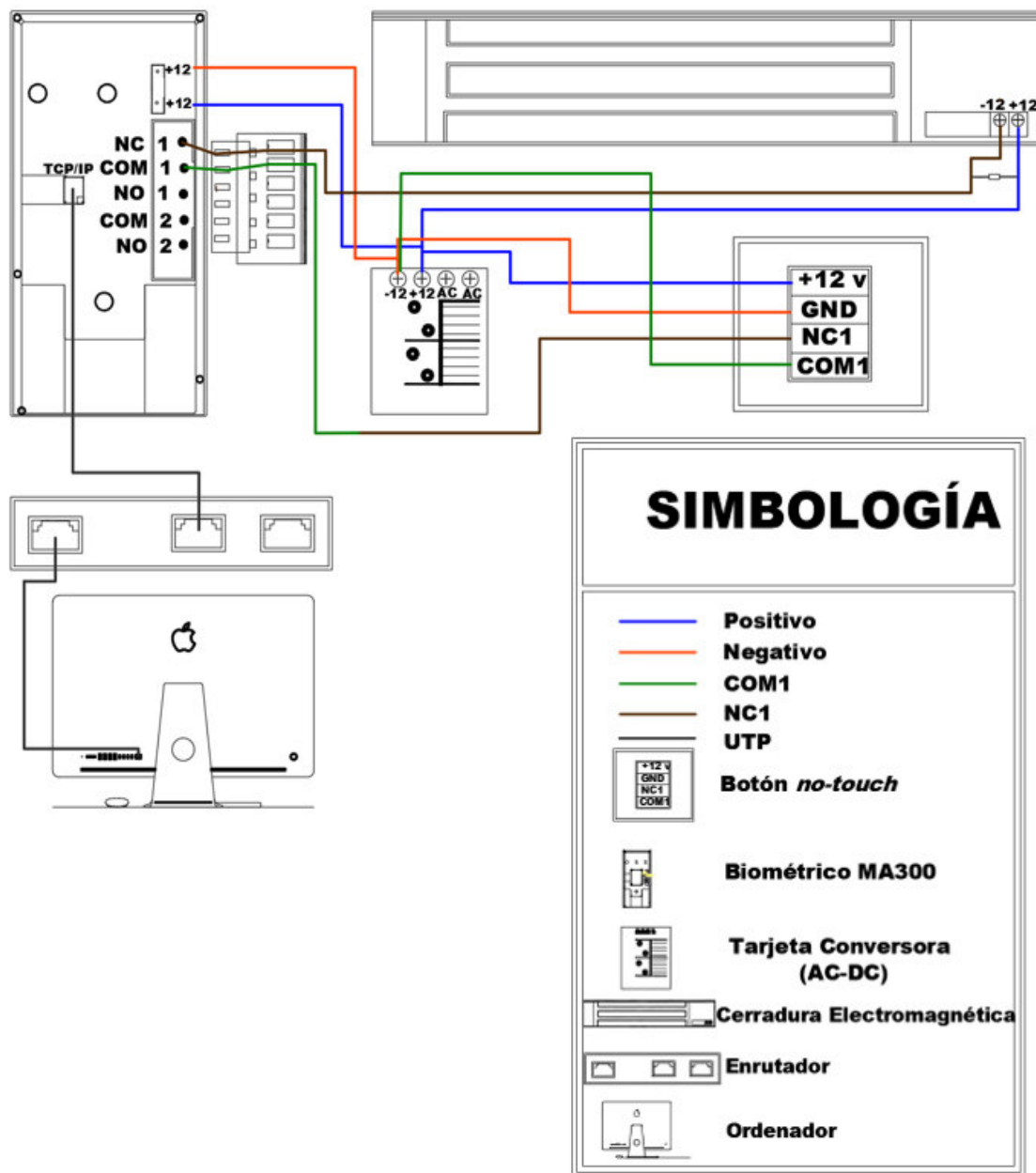


Figura 3.5 Diagrama de conexión para la zona administrativa

Modo de alimentación

La alimentación de energía principal es la fuente eléctrica de corriente alterna; sin embargo, por seguridad y debido a que el biométrico MA300 no posee alimentación autónoma, a diferencia de la MB360, se presenta la necesidad de una fuente de alimentación continua (baterías) para los biométricos.

Por tanto, se diseñaron cajas de alimentación con componentes que trabajan en conjunto para ofrecer alimentación al usuario, no solo de los biométricos sino también para electromagnéticos y pulsadores, las mismas que son para el área de la garita y administrativa.

Dentro de las cajas de alimentación se tiene:

- a. **Transformador:** Toma el flujo de corriente AC y lo convierte en DC.
- b. **Tarjeta convertora:** Convierte la energía, sirve como distribución para los componentes del sistema (biométrico MA300, cerradura electromagnética, botón *no-touch* y pulsador).
- c. **Baterías de 12 (V):** Estos elementos brindan un sistema sin interrupciones, esto es para que en el caso de que se encuentre sin suministro eléctrico, el sistema continúe funcionando sin inconvenientes.

Finalmente, se debió colocar dos tarjetas convertoras y dos baterías del lado de la garita, pues esto permitirá que el sistema se encuentre alimentado en su totalidad; además de que, en caso de corte de suministro eléctrico, el sistema funcione por un rango de tiempo determinado.

Cálculo para durabilidad para las baterías

Es por esta razón que se debe calcular el tiempo durante el cual las baterías entran en funcionamiento [22].

Para realizar el cálculo, se aplica las siguientes expresiones:

$$W_{baterías} = V_{baterías} \times I_{baterías}$$

Ecuación 3.1 Potencia entre voltaje y corriente de la batería

$$W_{consumo} = V_{consumo} \times I_{consumo}$$

Ecuación 3.2 Potencia de consumo del MA300

$$Tiempo = \frac{W_{baterias}}{W_{consumo}}$$

Ecuación 3.3 Relación de potencias

Si las expresiones se toman a consideración con la elaboración del sistema, se obtiene:

Donde:

V : 12 (V) voltaje

I : 5 (A) y (A) corriente

I : 7 (Ah) corriente por hora

$$W_{baterias} = 12 (v) \times 7 (Ah) = 84 W$$

$$W_{consumo} = 12 (v) \times 5 (Ah) = 60 W$$

$$W_{consumo} = 12 (v) \times 1 (Ah) = 12W$$

$$Tiempo = \frac{84}{60} = 1,4 \text{ horas .}$$

$$Tiempo = \frac{84}{1} = 84 \text{ horas}$$

Por tanto, el sistema tiene un periodo de tiempo de 1.4 horas activo; a pesar de que para la cerradura el periodo de tiempo sea mayor, los biométricos pasado el tiempo establecido, se apagarán.

Diagramas de Red

Para que todos los biométricos y todos los demás elementos funcionen adecuadamente, se debió cargar la información de los residentes, para esto se aprovechó la implementación del *software*, el mismo que centraliza todos los elementos y procesos en un solo computador, como se muestra en la Figura 3.6.

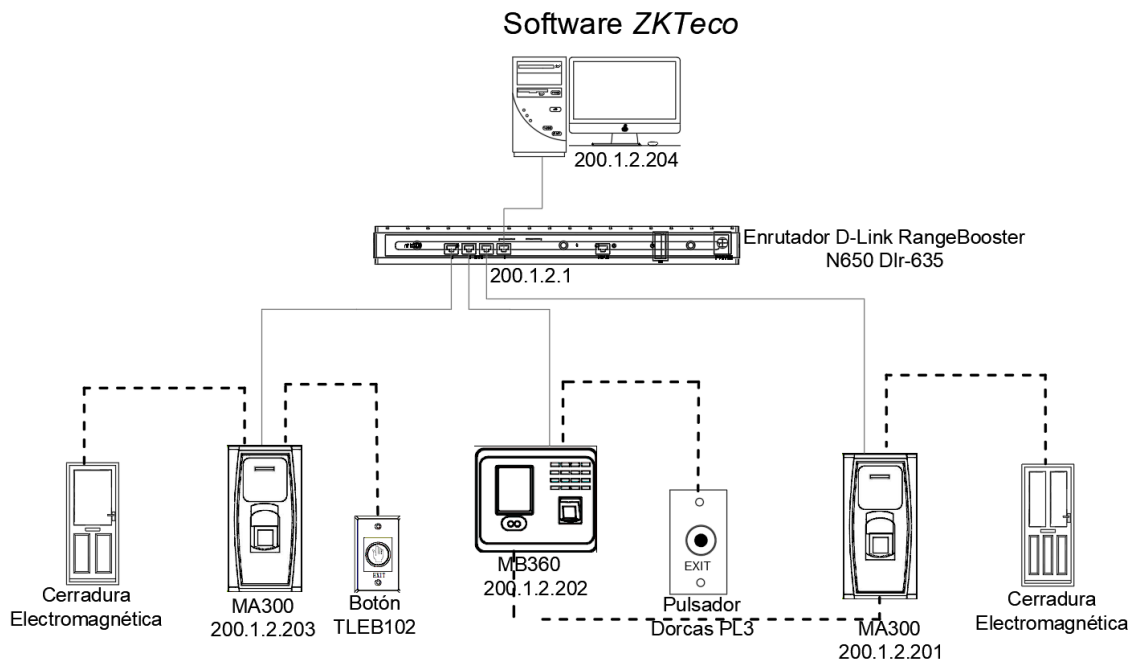


Figura 3.6 Diagrama de red

Para esto, se realizó un planeamiento de red usando la dirección IP 192.168.2.200 con máscara 29, con este valor se obtiene $32 - 29 = 3$, $2^3 = 8$. Por lo tanto, se tiene 8 direcciones IP, la primera dirección de red y la última dirección de *broadcast* dando como resultado la cantidad de 6 direcciones IP para *host* como se muestra en la Tabla 3.2.

Es importante resaltar que, las direcciones IP mostradas en la Figura 3.6 y en la Tabla 3.2, no son las direcciones reales implementadas en el proyecto, por razones de seguridad. Sin embargo, como el sistema forma parte de una intranet que no requiere acceso a internet se utilizó direcciones IP privadas de clase C.

Tabla 3.2 Planeamiento de la red.

Dispositivo	Zona	Dirección IP	Máscara de subred	Gateway
Enrutador	Administración	192.168.2.206	255.255.255.248	N/A
Biométrico MA300	Garita	192.168.2.201	255.255.255.248	192.168.2.206
Biométrico MB360		192.168.2.202		
Biométrico MA300	Administración	192.168.2.203		
PC1		192.168.2.204		
Dir. <i>Broadcast</i>	N/A	192.168.2.207		
Dir. Red		192.168.2.200		

Configuración del Software

El *software* utilizado es *ZKTeco Access 3.5*, descargado de la página del proveedor, facilitó la configuración y administración de cada uno de los dispositivos. El proceso de instalación es intuitivo y no tiene mayor complejidad; gracias al uso de esta aplicación, se consiguió centralizar el sistema en el computador, con este aplicativo es posible crear una lista de acceso, a través de la cual se atribuirá el ingreso y salida de los usuarios.

3.3 Implementación del sistema biométrico

Hardware

La implementación del sistema biométrico se realizó en dos partes, cabe recalcar que en ambos lugares se efectuaron los mismos procedimientos con algunas variaciones.

Previamente a realizar la implementación de los biométricos con sus respectivos componentes en la garita, la zona se encontraba como se muestra en la Figura 3.7.

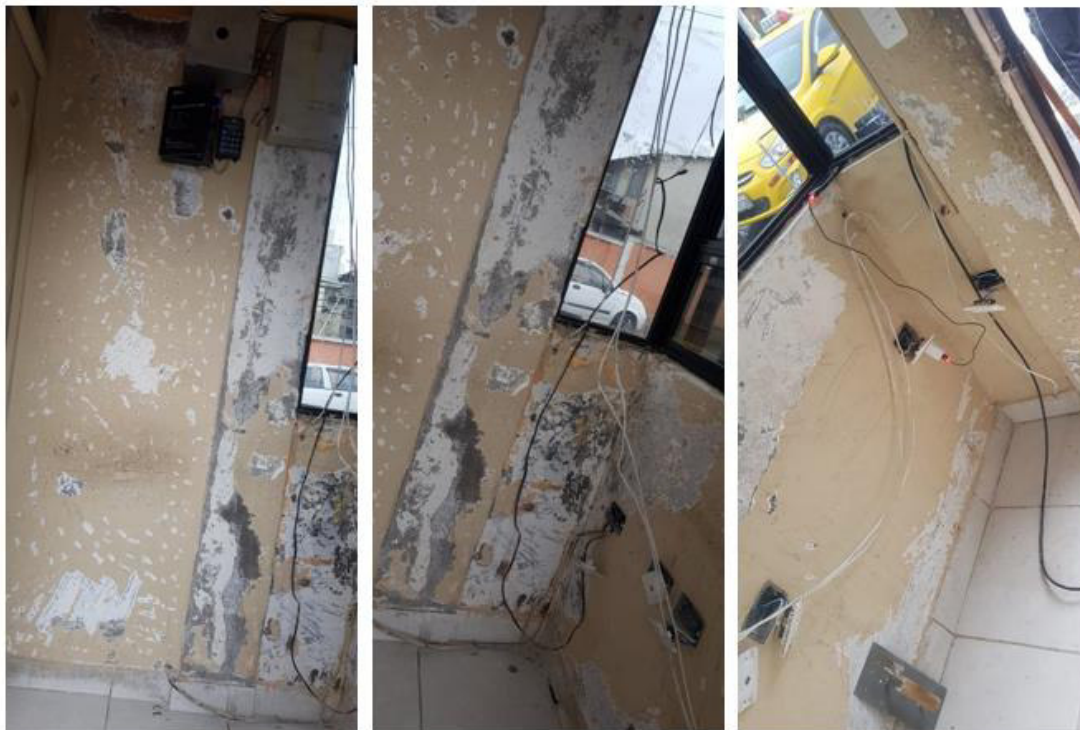


Figura 3.7 Infraestructura inicial de la zona garita

Por cuestiones estéticas y cumplimiento de normativas, el primer paso a ser realizado fue la reparación de la infraestructura; se encementó, empastó y pintó, como se evidencia en la Figura 3.8.



Figura 3.8 Reparaciones de la zona garita

Además, se llevó a cabo la adecuación del espacio; para este proceso se hicieron agujeros en la pared exterior frente a la puerta de ingreso y en el vidrio interno de la garita. Para la zona administrativa se realizó el mismo proceso, dejando un hueco en la pared externa junto a la puerta. Todos los orificios fueron encementados, empastados y pintados posteriormente, estos procedimientos se muestran en la Figura 3.9.

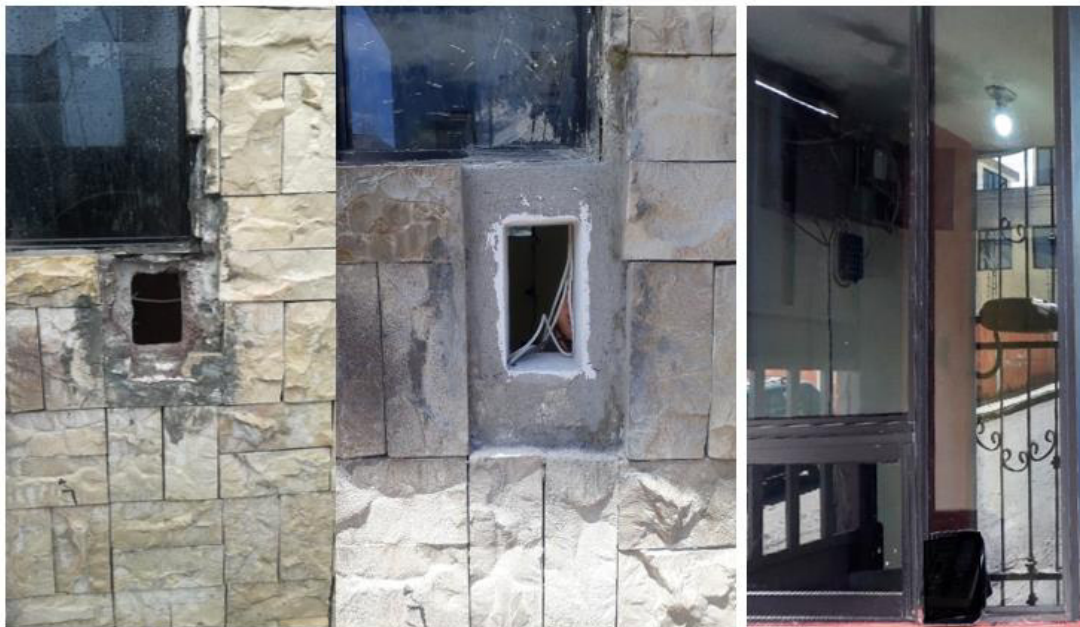


Figura 3.9 Adecuaciones del área de trabajo

Finalizadas las reparaciones y adecuaciones del espacio en la garita, el siguiente paso fue la preparación de la caja de alimentación, en su interior se encuentran: dos baterías de 12 (V), un conversor de AC a DC, un transformador conectado a un enchufe simple y dos tarjetas conversoras de AC a DC. Este proceso se presenta en la Figura 3.10.

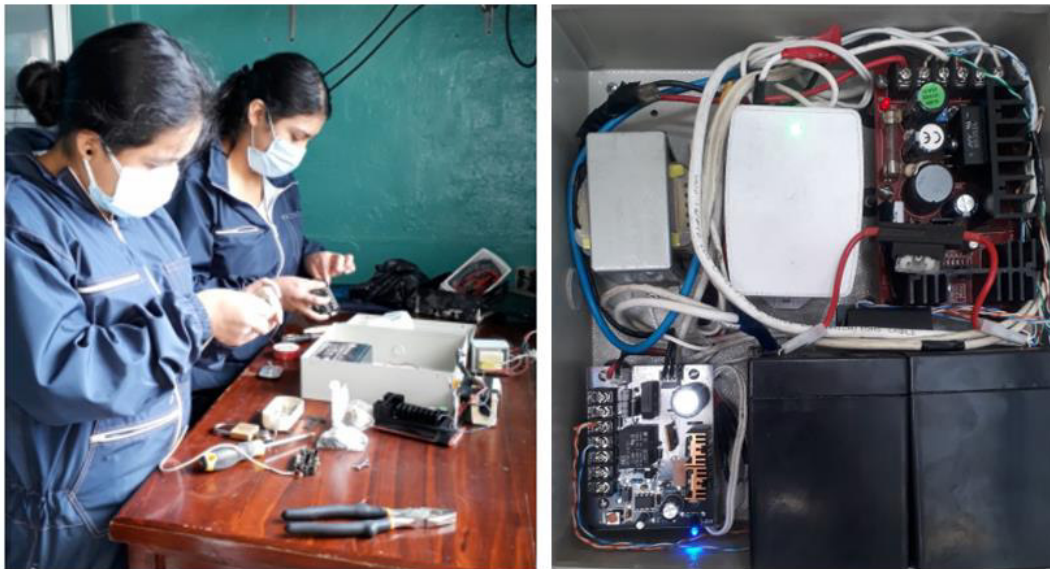


Figura 3.10 Creación de la caja de alimentación para la garita

Para la zona administrativa, la caja de alimentación cuenta con: una batería de 12 (V), un transformador conectado a un enchufe simple y una tarjeta convertora de AC a DC, como se evidencia en la Figura 3.11.

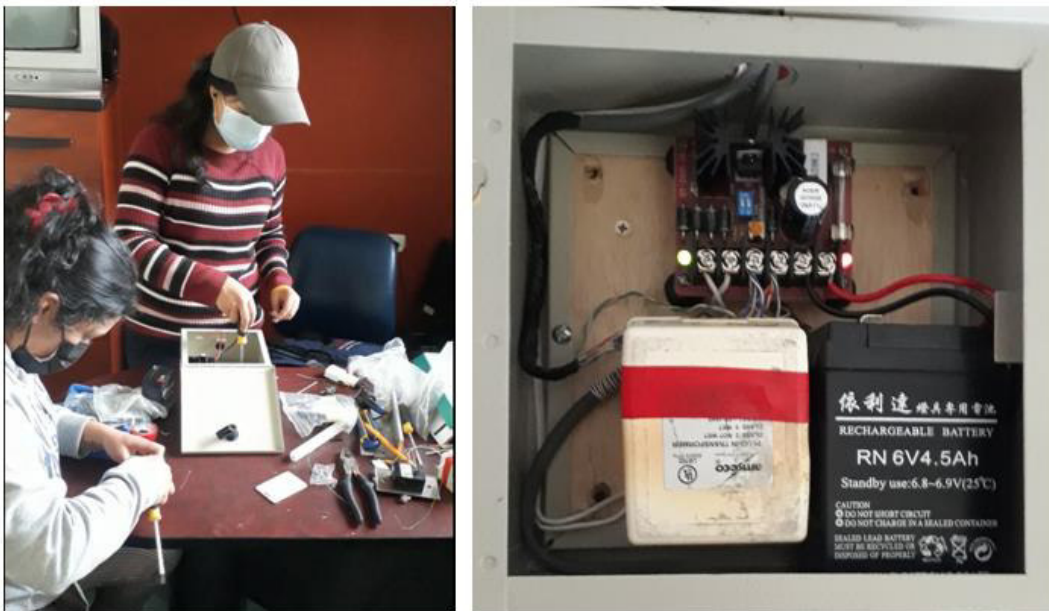


Figura 3.11 Creación de la caja de alimentación para la zona administrativa

Posterior al montaje de los elementos, dentro de cada gabinete se procedió a la instalación; en la garita la caja fue instalada en la parte superior de la pared interna al frente de la puerta de ingreso. En la zona administrativa se colocó en la parte superior de la pared interna junto a la puerta, tal como se evidencia en la Figura 3.12.



Figura 3.12 Instalación de las cajas de alimentación

Completada esta etapa, se colocó los biométricos en los orificios correspondientes, la MB360 en el vidrio y la MA300 en la pared externa en el área de la garita. En la zona administrativa se instaló la MA300, como se puede observar en la Figura 3.13.



Figura 3.13 Instalación de los biométricos

El biométrico MB360 tiene fuente propia; por lo tanto, no tiene conexión con la caja de alimentación; sin embargo, el MA300 está interconectado con la caja en ambas áreas. Cada dispositivo cuenta con su propio cable de red, este a su vez se encuentra individualmente direccionado al enrutador que se encuentra en la zona administrativa.

El pulsador fue instalado en la parte interna en la pared adyacente a la puerta de ingreso en la zona de la garita y el botón *no-touch* fue colocado en la parte interna junto a la ventana que se encuentra junto a la puerta de la zona administrativa. Dichas instalaciones eléctricas se evidencian en la Figura 3.14.



Figura 3.14 Instalación del pulsador y botón *no-touch*

El cableado de la instalación se realizó con cable UTP Cat. 5e, este conductor tiene un calibre de alambre americano (AWG) de 24 AWG; además, dispone de un aislamiento de polietileno con 8 hilos trenzados sin blindaje. Cabe recalcar que este cable soporta las velocidades de transmisión de las tecnologías *Ethernet*, *Fast Ethernet* y *Gigabit Ethernet*, las características técnicas se muestran en la Tabla 3.3.

Tabla 3.3 Características del cable UTP Cat. 5e [23]

Características	UTP Cat. 5e
Hilos / Pares	8 / 4
Frecuencia	100 (MHz)
Pérdida de retorno	20.1 (dB)
Atenuación	22 (dB)
Diafonía de Extremo Cercano (NEXT)	35.3 (dB)
Paradiafonía de suma de potencia next (PSNEXT)	32.3 (dB)
Diafonía de igual nivel de Extremo Lejano (ELFEXT)	23.8 (dB)
Paradiafonía de suma de potencia elfext (PS- ELFEXT)	20.8 (dB)

Todo el cableado realizado fue tendido dentro de canaletas; el proceso de canalización se muestra en la Figuras 3.15 para la garita, donde se ocupó 20 (m) de cable UTP Cat. 5e; por el contrario, en la Figura 3.16 de la zona administrativa se utilizó 10 (m).



Figura 3.15 Proceso de canalización de la zona garita



Figura 3.16 Proceso de canalización de la zona administrativa

Software

Previamente a la creación de los dispositivos y de la base de datos, se realizó la instalación del *software ZKAccess 3.5* en la computadora de la zona administrativa.

A continuación, se detallan los procedimientos efectuados dentro de la aplicación.

- **Creación del Área**

Para la creación del área, se ingresó a la pestaña “Dispositivo” y se seleccionó la opción “Área”. Una vez dentro, se editó el área existente y añadió otra, con la finalidad de disponer del área de ingreso y salida, para posteriormente asignar este parámetro según corresponda en la creación de dispositivos.

La creación del área se realizó completando los campos obligatorios mostrados en la Figura 3.17, los cuales son nombre, ID y área superior.

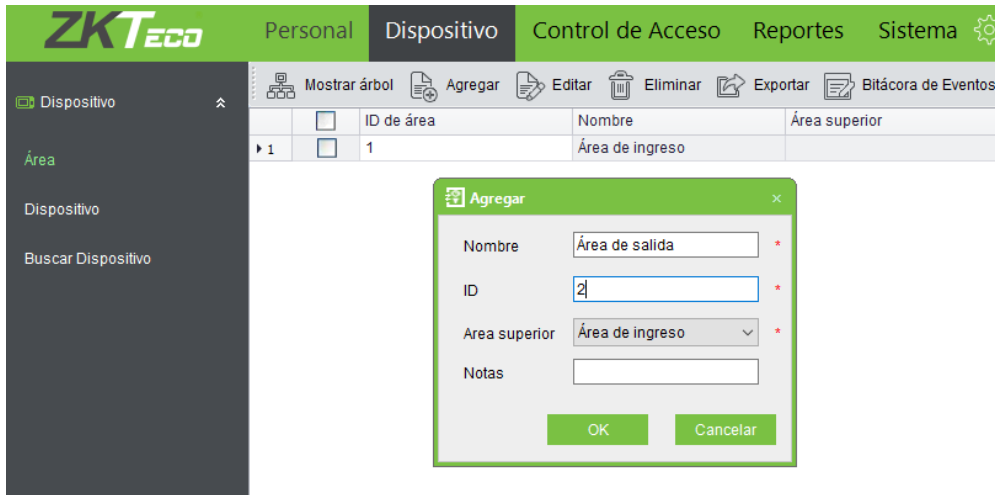


Figura 3.17 Creación del área

- **Creación de Dispositivos**

Una vez seleccionada la opción “Dispositivo” ubicada en la pestaña “Dispositivo”, se procedió a agregar a los tres dispositivos en modo profesional uno a la vez; terminado este proceso, se actualizó la pantalla para que los biométricos se muestren dentro del *software*.

En la creación del dispositivo se llenó los parámetros obligatorios evidenciados con asteriscos rojos, los cuales se pueden visualizar en la Figura 3.18. Es importante enfatizar en la correcta asignación del área, dirección IP y puerto; además, se debe activar la opción “eliminar los datos del dispositivo al agregar” con el fin de evitar la carga automática de información.

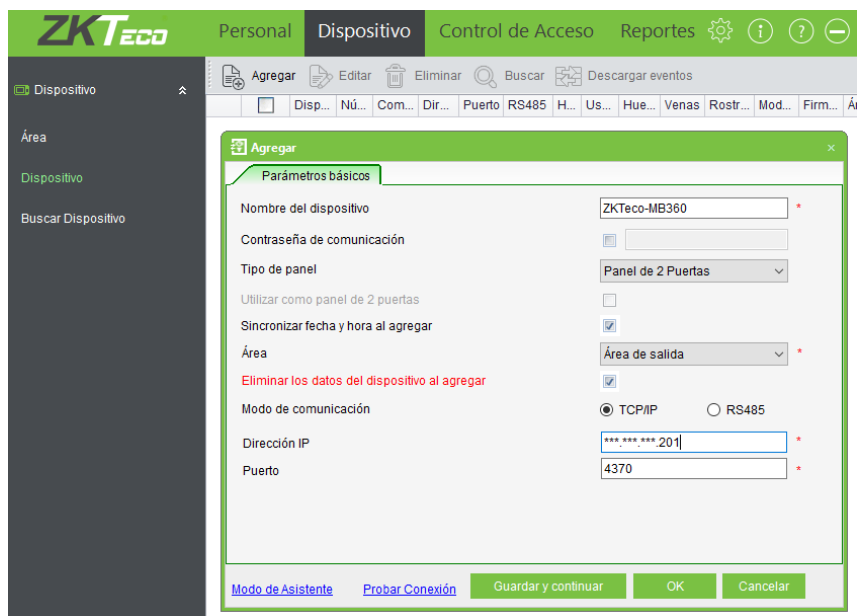


Figura 3.18 Creación del dispositivo

Cabe recalcar que; como se usó dos dispositivos del mismo modelo, para la creación del segundo equipo MA300 se le colocó el nombre de Zona Administrativa y que el establecimiento de los dispositivos tuvo como finalidad la posterior asignación de estos en la correspondiente lista de acceso.

- **Niveles de acceso**

Los niveles de acceso fueron creados tras completar los campos obligatorios mostrados en la Figura 3.19, los cuales son nombre y horario; además, se realizó la selección de puertas y usuarios correspondientes para cada lista. Este procedimiento se llevó a cabo con la finalidad de escoger a quienes van a formar parte de dicho nivel de acceso; es importante recalcar que la aplicación de la lista solo se efectúa sobre las puertas y usuarios que se encuentran en la parte derecha de la imagen. Todo este proceso se realizó en la pestaña “Control de Acceso” en la opción “Niveles de Acceso”.



Figura 3.19 Creación del nivel de acceso

- **Creación del Departamento**

La creación del departamento fue realizada en la pestaña “Personal” en la opción “Departamentos”; una vez dentro de la pantalla, se procedió a agregar un departamento, para lo cual se completó los parámetros nombre, código y departamento superior, los cuales se pueden observar en la Figura 3.20 como campos obligatorios.

La finalidad de la creación del departamento es segmentar a los usuarios en base a la división a la cual pertenecen, en el *software* se realizó este proceso en la creación de usuarios.



Figura 3.20 Creación del departamento

- **Creación de Usuarios**

En la creación de usuarios se realizaron múltiples pasos; primero se ingresó a la pestaña “Personal” en la opción “Usuarios”; una vez dentro, se procedió a agregar al residente. En la pantalla emergente dentro de la “Información personal” se llenó el ID de usuario, nombre, apellido, género y departamento; para estos parámetros se debe tomar en cuenta que el ID debe ser único e irrepetible y que en el apellido se colocó el número de casa del usuario.

El segundo paso realizado fue en “Niveles de Acceso”, en esta opción de la pantalla se seleccionó la lista a la cual va a pertenecer el residente. El procedimiento detallado anteriormente se evidencia en la Figura 3.21.

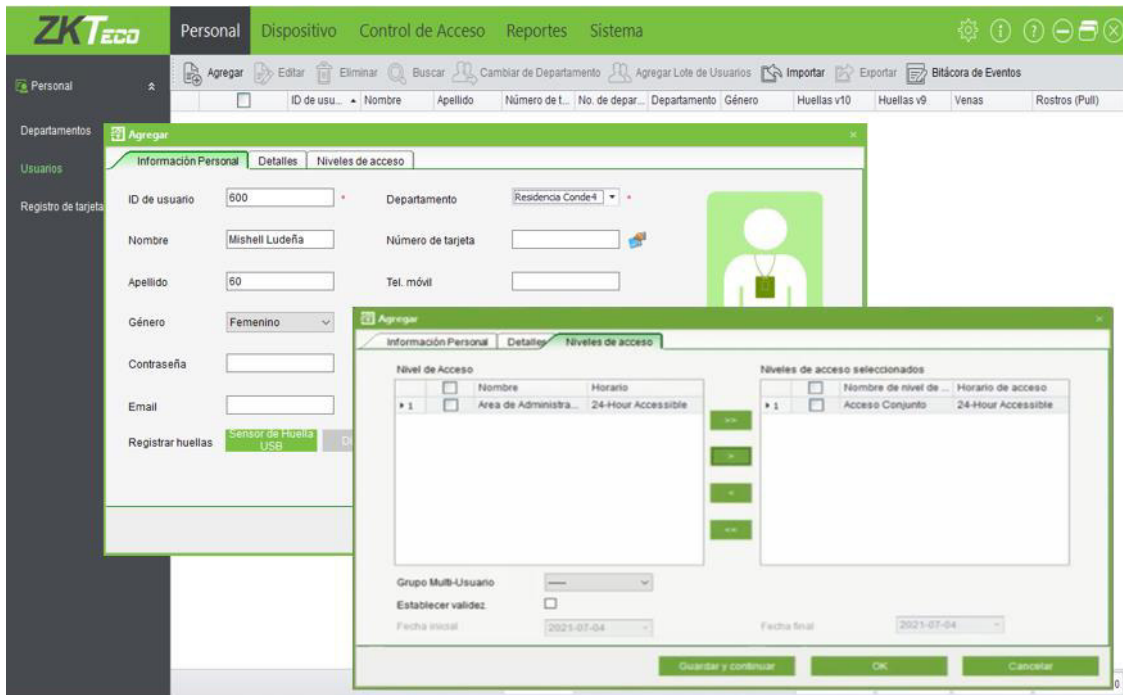


Figura 3.21 Creación de usuarios

- **Configuración de huella dactilar y tag**

Tras la creación del usuario, se realizó la configuración del tag y de la huella dactilar; para este proceso, primero se ingresó en la opción “Usuario” ubicada dentro de la pestaña “Personal”. Una vez dentro, se seleccionó al usuario al cual se le va a registrar dicho tag, luego en la pantalla emergente en la opción “Información Personal”, se ingresó el valor numérico del tag en el campo “número de tarjeta”, como se muestra en la Figura 3.22.

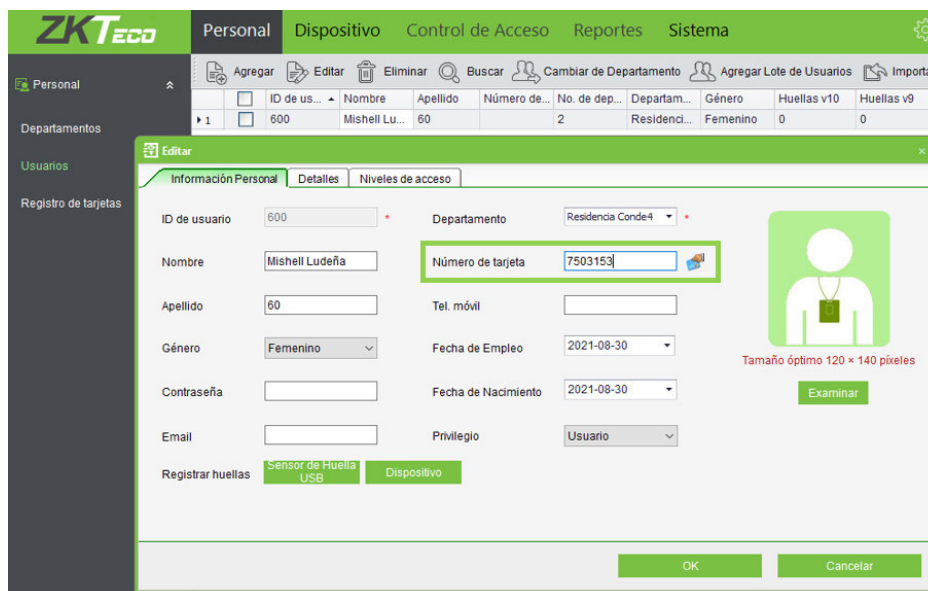


Figura 3.22 Configuración del tag

Para el registro de las huellas dactilares se partió desde el punto anterior, pero para este caso se pulsó sobre la opción “Dispositivo” del campo “Registro huellas”. En la pantalla “Seleccione la puerta”, se escogió el biométrico en la cual se añadió la huella, después en la ventana “Registro de huellas” se seleccionó el dedo que va ser reconocido por el lector de huellas de los diferentes dispositivos tanto para ingreso como salida de los habitantes.

Realizados estos procesos, de forma física el usuario debe ingresar su dedo dentro del lector de huellas del biométrico por tres veces consecutivas, de esta forma el *software* logra vincular la huella con los datos del residente, los mismos que se encuentran ya en el sistema. Este proceso se evidencia en la Figura 3.23.

El registro de las huellas dactilares fue un proceso opcional, debido a que ciertos usuarios no deseaban contar con este tipo de seguridad por razones de salud y físicas. Además, es importante resaltar que todos los procedimientos detallados anteriormente deben ser sincronizados cada vez que el administrador de red realice una modificación de cualquier tipo.

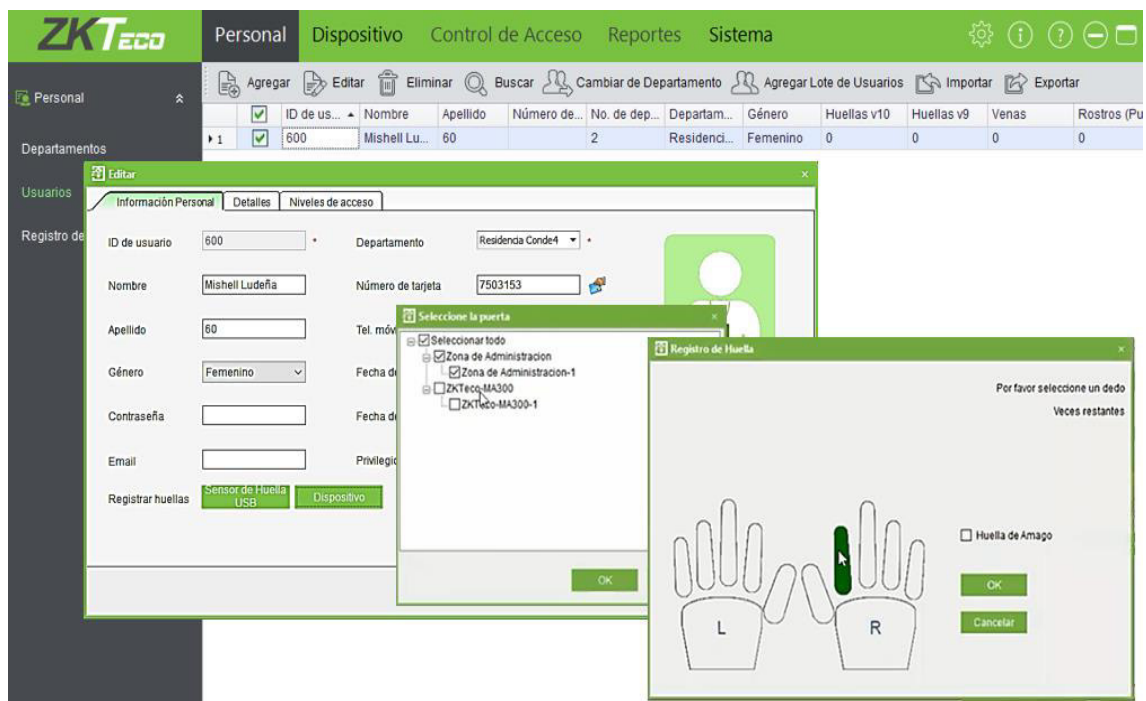


Figura 3.23 Configuración de la huella dactilar

3.4 Automatización del sistema en cada puerta

Se realizó la instalación de cerraduras electromagnéticas y del brazo hidráulico, estos elementos son indispensables para la apertura de la puerta. Así se tiene que, para la zona de la garita fue necesario colocar una cerradura electromagnética de 600 (lb), la misma que fue soldada en la parte superior de la puerta, su complemento fue colocado en el marco de la pared, gracias a la soldadura los soportes de la cerradura son estables, esto permite que el campo electromagnético sea más eficiente; es decir, la cerradura no pierda fuerza al momento de la energización. Para la zona de administración fue necesario colocar una cerradura electromagnética de 300 (lb).

Para que el sistema deje de ser manual; es decir que el usuario ya no ejerza fuerza para abrir la puerta, se utilizó la funcionalidad de los biométricos del envío de señales hacia las cerraduras electromagnéticas. Para ello, el *software* necesitó algunas configuraciones para tiempos de apertura, tiempos de respuesta, creación de lista de acceso mediante la cual se pueda permitir o bloquear la apertura de las puertas.

Además, se elaboró una hoja de Excel en la cual consta los siguientes datos de los residentes: ID de usuario, nombre, apellido, número de tarjeta, género y departamento. Esta información fue cargada a la base de datos *software*, esto con la finalidad de que el sistema este organizado y sea eficiente. Cabe recalcar que, por motivos de confidencialidad dicha información solo se encuentra visible para miembros de la EPN y se puede observar en la Figura 3.24.



Figura 3.24 Código QR para la Base de datos

Comunicación entre biométrico y cerradura electromagnética

El biométrico recopila información de tipo fisiológica, conocida como huella dactilar o también conjunto de números específicos que se encuentran en el *tag*, donde mediante sensores de alta tecnología y códigos de programación, se encargan de obtener la información y compararla con la base de datos que se encuentra cargada dentro de cada biométrico.

En caso de que la verificación coincida, el biométrico se encarga de convertir la información en un pulso eléctrico, el mismo que es enviado al sistema que alimenta la cerradura; este pulso eléctrico corta la energía debido a que se necesita que permanentemente tenga un flujo de corriente y este se interrumpe en el momento de una verificación exitosa.

Con esto, el circuito cerrado que se formó con los diferentes elementos se convierte en un circuito abierto, provocando que los 12 (V) que alimenta a la cerradura electromagnética, no lleguen a la cerradura; por tanto, el campo magnético generado de manera continua se destruye y las piezas de la cerradura pierden contacto.

Una vez que la puerta se abre, el brazo hidráulico permite que la puerta se cierre de manera paulatina; en este caso se colocó al ingreso del Conjunto puesto que la estructura de la puerta es pesada y si esta se cierra de manera abrupta, ocasionaría que la cerradura se rompa o se mueva del lugar donde fue instalada.

Comunicación entre botón *no-touch* y cerradura electromagnética

Para el caso del botón *no-touch*, el procesamiento interno es diferente debido a que este envía un pulso eléctrico que interrumpe el flujo de energía, pero este botón tiene la característica de no necesitar contacto para ser activado, lo que quiere decir que el botón se activa a una proximidad de 20 (cm) como mínimo. Una vez que se realiza la detección de movimiento, los LED's infrarrojos de color rojo, que significa reposo, cambian a color azul, permitiendo que el pulso interrumpe el flujo de corriente y la cerradura se desmagnetice. En este punto, el brazo no se consideró como una opción factible debido a que la estructura de la puerta tiene partes de vidrio, impidiendo realizar la instalación del brazo, además por solicitud de la administración del Conjunto.

Comunicación entre pulsador y cerradura electromagnética.

El pulsador, por defecto, permite el paso de corriente desde la fuente al biométrico, manteniendo así la puerta cerrada. Una vez el pulsador es activado, este emite una señal al biométrico, el cual interrumpe el paso de corriente, eliminando el campo magnético en la cerradura para así desbloquear la puerta y permitir el acceso de los usuarios.

El botón *no-touch* y el pulsador envían la señal al biométrico y esta toma la decisión de cortar el flujo de corriente. Pero adicional a ello, este permite o bloquea el paso de corriente de manera continua hacia la cerradura.

Automatización de puertas

Dentro del *software*, y una vez tendido el cableado, se procedió a la configuración de cada uno de los tiempos, los cuales deben coincidir en los dos dispositivos ubicados en la zona de la garita. Como se observa en la Figura 3.25, para el caso de duración de apertura de la puerta (tiempo que tiene el magnético para perder el campo magnético y la puerta se abra) se configuró un tiempo de 0 (s) y para definir el tiempo de apertura de la puerta se estableció 4 (s). Además de un intervalo de 10 (s) para el retardo del sensor de puerta, el mismo que mide el retardo en la comprobación del sensor de la puerta después de que esta se abre, genera un *beep* para corroborar que la puerta se abrió con éxito.



The image shows a software configuration window titled 'Editar'. It contains various settings for a door device. The settings are organized into two columns. The left column includes: 'Nombre de dispositivo' (Prueba), 'Número de Puerta' (1), 'Nombre de puerta' (Prueba-1), 'Horario default' (24-Hour Accessible), 'Horario apertura programada', 'Modo de verificación', 'Contraseña de amago' (Configuración), 'Contraseña de emergencia' (Configuración), and 'Wiegand' (Configuración Wiegand). The right column includes: 'Tipo de sensor de puerta' (Normalmente Cerrado), 'Puerta Mantenido Abierta' (4 Segundo(1-99)), 'Cerrar al detectar Puerta' (checked), 'Tiempo y asistencia' (checked), 'Duración de apertura de puerta' (0 Segundo(1-10)), 'Intervalo de lectura' (0 Segundo(0-10)), 'Verificaciones fallidas' (3), 'Retardo de sensor de puerta' (10 Segundo(1-99)), and 'Habilitar SRB' (unchecked). At the bottom, there are two checkboxes: 'Aplicar esta configuración a todas las puertas del panel actual' and 'Aplicar esta configuración a todas las puertas de todos los paneles'. There are also 'OK' and 'Cancelar' buttons.

Figura 3.25 Configuración de las puertas

3.5 Verificación de funcionamiento

Una vez que se realizó la implementación del sistema, se realizó la comprobación de que el sistema funcione de manera correcta. La comprobación de todo el sistema se analizó en tres etapas.

- **A Nivel de *software***

Después de la configuración de las IP de manera interna de cada equipo dentro del *software*, se pudo verificar la correcta configuración y asignación del nombre del equipo con su respectiva IP, como se muestra en la Figura 3.26.

	<input type="checkbox"/>	Dispositivo	Número de ...	Comu...	Dirección IP	H...	Área	Usu...	Hue...
1	<input checked="" type="checkbox"/>	Zona de Administra...	AEWD2018...	TCP/IP	192.168.1.203	✓	Area salida	2	2
2	<input type="checkbox"/>	MB360	AEWD2018...	TCP/IP	192.168.1.202	✓	Area salida	185	115
3	<input type="checkbox"/>	MA300	AHGU2052...	TCP/IP	192.168.1.201	✓	Area Ingreso	185	115

Figura 3.26 Ingreso de los biométricos al *software* con las direcciones IP

Para probar que cada dispositivo se encuentra conectado al *software*, se probó la conexión. En la parte inferior de la ventana de creación del dispositivo, existe la opción “Probar conexión”, la cual busca el dispositivo con la dirección IP asignada anteriormente y si el dispositivo concuerda con la dirección IP, entonces el mensaje es “conexión exitosa”, como se muestra en las Figuras 3.27 y 3.28. Aquí se puede presentar un error conocido como falla de puerto, esto se debe a que de alguna manera se reutiliza el número de puerto, lo cual no debe ocurrir.

Figura 3.27 Comprobación de conexión para el biométrico MA300

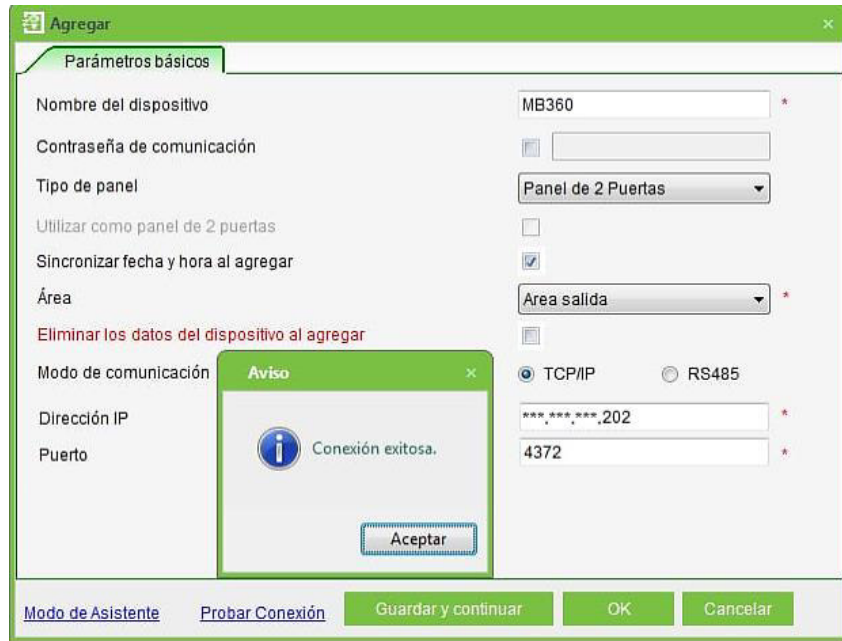


Figura 3.28 Comprobación de conexión para el biométrico MB360

En la Figura 3.29 se muestra la dirección IP del biométrico ubicado en la zona de administración y la comprobación de conexión a través del *software*.

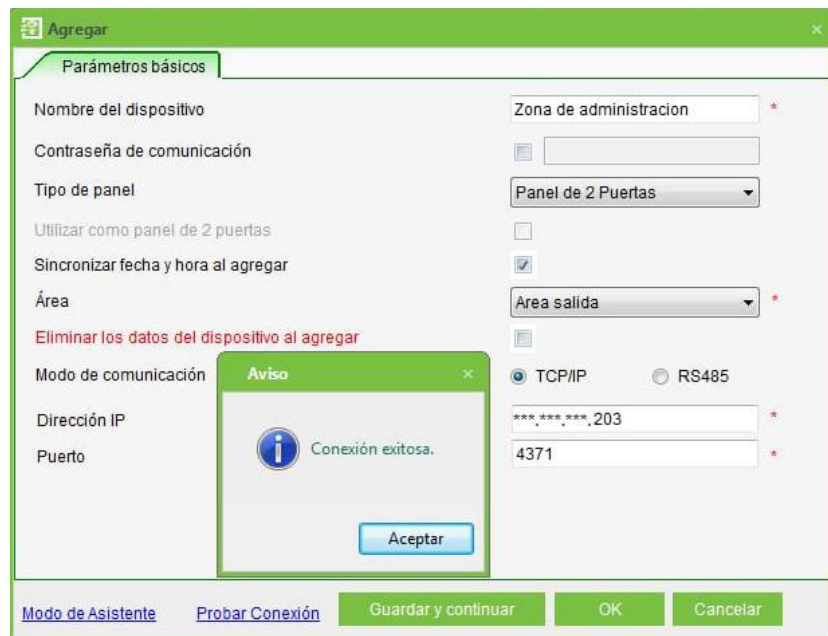


Figura 3.29 Comprobación de conexión del biométrico “zona administrativa”

En este caso, es importante realizar la comprobación de conectividad a cada uno de los dispositivos; es decir que todos se encuentre en red. Para ello, es necesario realizar un *ping* a través de un computador central mediante la consola para verificar que la conexión sea correcta, como se muestra en la Figura 3.30.

Debido a que el *ping* es una petición que se realiza al equipo para conocer si este se encuentra o no conectado a la computadora, si el *ping* es exitoso puedo comenzar a enviar información, asegurando una conexión de extremo a extremo confiable es decir que si envío la información de usuario esta no se va a perder o no sincronizar dentro del equipo. Para el caso del *ping* realizado desde el computador al enrutador al ser exitoso este me permite tener una puerta de acceso que se encargará de distribuir la información para que los diferentes dispositivos se carguen con la información y configuración respectiva.

Una vez realizado esto, se procede a cargar la información y la verificación en cada una de los biométricos. En caso de que el biométrico no identifique la información que se requiere, se emitirá un anuncio de restricción.

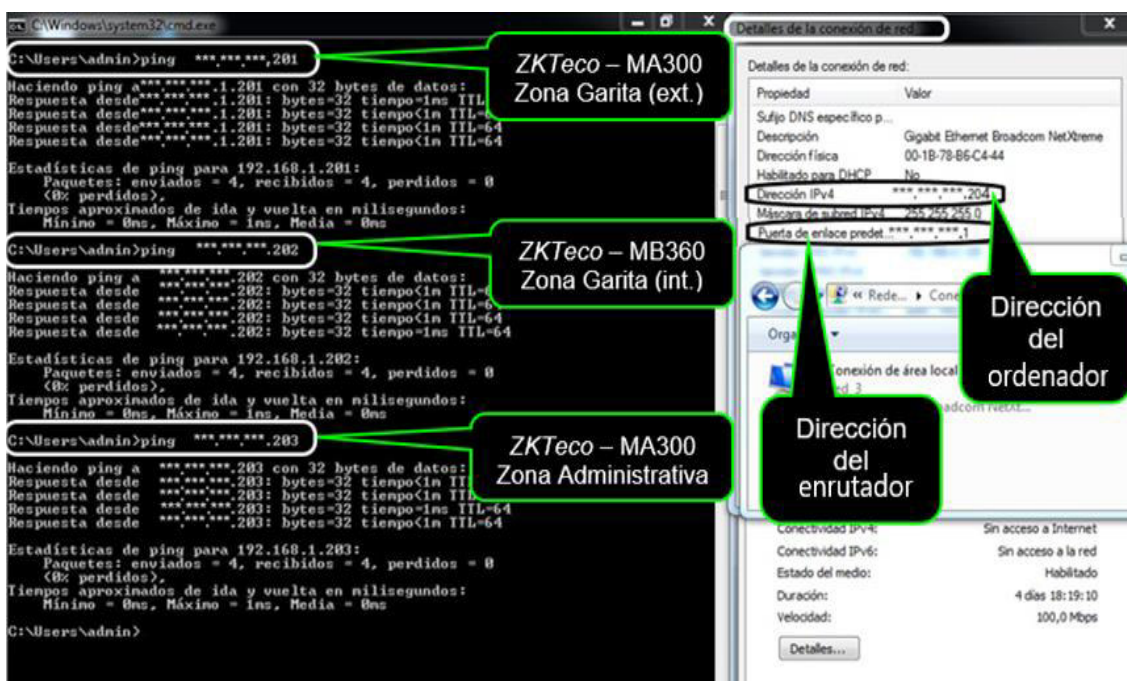


Figura 3.30 Comprobación de conectividad de todos los biométricos

Reporte de ingresos y salidas a través de ZKAccess 3.5

Una vez realizada la comprobación de conectividad dentro del *software*, se procedió al monitoreo de los usuarios que ingresan y salen a través de los biométricos. Como se muestra en la Figura 3.31, se tiene la lista de usuarios que por un periodo de tiempo han ingresado haciendo uso ya sea de la huella dactilar como de *tags*, comprobando así el correcto uso de los biométricos y su trabajo conjunto con el *software*.

	Tiempo	ID	Nombre	Apelli.	Disposit.	Punto d.	Verific.	Estado	Evento	Notas
5	2021-09-06 20:07:42	441	Edwin Delgado	146	MA300	MA300-1	Targeta	Entrada	Apertu...	
6	2021-09-06 20:07:33	441	Edwin Delgado	146	MA300	MA300-1	Targeta	Entrada	Apertu...	
7	2021-09-06 20:07:30	441	Edwin Delgado	146	MA300	MA300-1	Targeta	Entrada	Apertu...	
8	2021-09-06 20:07:22	182	Jessenia Rivera	60	MA300	MA300-1	Huella	Entrada	Apertu...	
9	2021-09-06 20:07:10	182	Jessenia Rivera	60	MA300	MA300-1	Huella	Entrada	Apertu...	
10	2021-09-06 20:07:03	105	Grecia Falconi	34	MA300	MA300-1	Targeta	Entrada	Apertu...	
11	2021-09-06 20:06:54	441	Edwin Delgado	146	MA300	MA300-1	Targeta	Entrada	Apertu...	
12	2021-09-06 20:06:47	441	Edwin Delgado	146	MA300	MA300-1	Targeta	Entrada	Apertu...	
13	2021-09-06 20:06:40	182	Jessenia Rivera	60	MA300	MA300-1	Huella	Entrada	Apertu...	
14	2021-09-06 20:06:35	105	Grecia Falconi	34	MA300	MA300-1	Targeta	Entrada	Apertu...	
15	2021-09-06 20:06:30	105	Grecia Falconi	34	MA300	MA300-1	Targeta	Entrada	Apertu...	

Figura 3.31 Reporte de funcionamiento

- **A nivel de *Hardware***

Zona de la garita

Esta fue el área más importante y crítica de todo el sistema, debido a que por esta puerta los residentes ingresan y salen constantemente del Conjunto. Para probar el funcionamiento del biométrico MB360, se procedió a realizar la comprobación tanto del *tag* como de huellas dactilares, como se puede ver en la Figura 3.32.



Figura 3.32 Funcionamiento de huella dactilar en el biométrico MB360

Mientras que para probar el funcionamiento del biométrico MA300 también se realizó a través del *tag*; para ello, se solicitó al guardia la verificación del funcionamiento del sistema, como se muestra en la Figura 3.33.



Figura 3.33 Comprobación de los biométricos a través del tag

Para la verificación a través de una huella digital, se ingresa el dedo que fue registrado con anterioridad; al reconocer la lectora la información de la huella, se procede a desmagnetizar la cerradura y la puerta se abre, como se muestra en la Figura 3.34.



Figura 3.34 Comprobación de huella dactilar con el biométrico MA300

Zona de administración

Por otro lado, se comprobó el funcionamiento del sistema del lado externo de la administración a través de un tag, como se muestra en la Figura 3.35; dado que el registro concordó con el dispositivo o huella a verificar, la puerta se abrió.



Figura 3.35 Comprobación *tag*-huella en Administración

De igual manera para la verificación a través de la huella dactilar, como se muestra en la Figura 3.36, existió un reconocimiento dactilar exitoso, por tal razón se procedió a la apertura de la puerta.



Figura 3.36 Apertura con la huella dactilar en la zona de administración

En la parte interna, se realizó la comprobación con el botón *no-touch*, como se muestra en la Figura 3.37; donde mediante un pequeño acercamiento sin contacto hacia el dispositivo, se produjo, el corte de energía para que la cerradura se desmagnetice y la puerta se proceda a abrir.



Figura 3.37 Comprobación a través del botón *no-touch*

A continuación, se presenta el código QR en la Figura 3.38 en el cual se detalla, mediante un video, la verificación del sistema y su correcto funcionamiento. Adicionalmente, se describe las áreas donde están ubicados los biométricos y todos los elementos necesarios para la implementación; además, del proceso llevado a cabo para el cumplimiento de cada uno de los objetivos planteados en un inicio.



Figura 3.38 Código QR de verificación de funcionamiento

3.6 Manual de Uso y Mantenimiento

Previo al desarrollo y elaboración de los manuales, se realizó una capacitación a los miembros de la junta directiva del Conjunto; posteriormente, se procedió a entregar los documentos de forma física, en los cuales se explica de manera detallada el funcionamiento, aplicación y mantenimiento de los equipos, así como también el manejo del *software ZKAccess 3.5*. El primer manual es dedicado para el conocimiento y uso exclusivo de los habitantes de la urbanización.

El segundo documento es un manual de administrador, aquí se explica las especificaciones de todas las funciones con las que cuenta el sistema. Además, se realizaron videos donde se explica los manuales, la verificación de conectividad entre los equipos, el funcionamiento del sistema y el manejo del *software*.

En los anexos 2 y 3, se presenta el manual de usuario y el manual de administrador, respectivamente. Adicionalmente, a través de las Figuras 3.39 y 3.40, se puede acceder a los códigos QR de los manuales presentados mediante videos.



Figura 3.39 Código QR para el Manual de Usuario



Figura 3.40 Código QR para el Manual de Administrador

3.7 Presupuesto

En la Tabla 3.4 se detalla el costo de los elementos utilizados para la implementación del proyecto; es importante resaltar que previo a la adquisición de los equipos se llegó a un acuerdo con los beneficiarios en el cual se detalla que no existirá un cobro por mano de obra ni desarrollo intelectual.

Tabla 3.4 Presupuesto del proyecto

Cantidad	Descripción	P. Unitario	P. Total
2	Control de asistencia <i>ZKTeco</i> ZK-MA300	\$ 116,00	\$ 232,00
1	Control de asistencia <i>ZKTeco</i> ZK-MB360	\$ 145,00	\$ 145,00
1	Cerradura electromagnética 600 (lb)	\$ 33,60	\$ 33,60
1	Cerradura electromagnética 400 (lb) ZK-AL-14045	\$ 25,20	\$ 25,20
2	Tarjetas para fuente de alimentación 2 (A) ~ 3 (A) AC – DC	\$ 30,00	\$ 60,00
1	Tarjetas para fuente de alimentación 3 (A) AC – DC	\$ 42,20	\$ 42,20
35	Cable UTP Cat. 5e	\$ 0,46	\$ 16,10
1	Pulsador salida metálico control de acceso	\$ 12,99	\$ 12,99
1	Botón de salida <i>no-touch</i> TLEB102	\$ 16,80	\$ 16,80
2	Transformador de 12 (V)	\$ 2,80	\$ 5,60
3	Batería 12 (V) 4 (A) 22001	\$ 11,00	\$ 33,00
5	Canaleta lisa de 20 x 12 (cm) ca-dxn1001	\$ 2,73	\$ 13,65
1	Caja metálica 24 X 26,5 (cm)	\$ 12,88	\$ 12,88
1	Caja metálica 21 X 20 (cm)	\$ 10,88	\$ 10,88
4	Conectores RJ45	\$ 0,25	\$ 1,00
2	Capuchones para conectores RJ45	\$ 0,25	\$ 0,50
1	Brazo hidráulico de 120 (kg)	\$ 120,00	\$ 120,00
1	Mesa para cerradura de 300 (lb)	\$ 8,63	\$ 8,63
189	<i>Tags</i> de acceso	\$ 0,99	\$ 187,11
1	Enrutador <i>D-Link</i> N650 DIR-635	\$ 8,50	\$ 8,50
		TOTAL	\$ 985,64

4 CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

- Existe una gran variedad de dispositivos que trabajan con tecnología biométrica dentro del mercado, estos se diferencian por sus especificaciones técnicas, funcionalidades, materiales y precios; sin embargo, previamente a la adquisición es fundamental analizar las necesidades de los beneficiarios para de esta forma determinar adecuadamente los elementos a ser instalados.
- Los biométricos tienen acceso a las bases de datos y dan acceso a los diferentes usuarios, dependiendo la dirección IP que estos dispongan. El computador que maneja el *software*, no cuenta con *Dynamic Host Configuration Protocol* (DHCP), sino que se le asignó una dirección IP de manera estática, la misma que pertenece a la red en la que se encuentran los biométricos. En cuanto al *software*

ZKTeco Access 3.5, permitió el ingreso de usuario, centralización y monitoreo del sistema de manera sencilla y eficiente.

- La implementación del sistema biométrico para autenticación de usuarios con lectura de huellas digitales y *tags* proporcionó a la urbanización seguridad y control. Este proceso fue extenso, requirió de una gran precisión en la interconexión de los equipos; finalmente, el proceso de canalización permitió que el tendido de las zonas trabajadas quede estético.
- La automatización del sistema permite que las personas faciliten un proceso; en este caso, lo realizan con los biométricos y el *software* donde a través del computador se monitorea y configura cada función y desempeño del sistema. De ahí la importancia de realizar una correcta instalación y configuración de cada elemento que compone el sistema.
- La etapa de verificación es una de las más críticas pues lo que se busca es que todo el sistema funcione de manera correcta a través de *ZKAccess 3.5*, *software* encargado de centralizar el proceso. Mientras que los cables UTP Cat. 5e permiten la conexión y transmisión de información requerida para el funcionamiento del sistema.
- Los manuales de usuario y propietario sirven como guía; además, son herramientas fundamentales realizadas para minimizar el tiempo de capacitación, reducir daños en los equipos, realizar un correcto mantenimiento al *hardware* y *software*, así como también hacer respetar las políticas de la urbanización. Con todas las recomendaciones presentadas en dichos documentos, se espera que los beneficiarios utilicen y protejan el proyecto adecuadamente, consiguiendo de esta manera un sistema interoperable y eficiente.
- Las normas de cableado estructurado ANSI/TIA 568, ANSI/TIA 569-A, ANSI/TIA 606-A y el estándar de terminación T568-B, permiten establecer una infraestructura adecuada a la necesidad existente sea esto una *intranet* o *extranet*; además, ayudan a garantizar la interoperabilidad de un sistema que es implementado bajo sus especificaciones sea para la estructura del sistema de cables, tipos de conexiones, áreas de trabajo, topología, canalización, conectores, código de colores para el conector y el etiquetado del cable.

4.2 Recomendaciones

- Es recomendable analizar todas las características de los equipos previamente a su adquisición, con la finalidad de no cometer errores futuros en la instalación y evitar pérdidas económicas innecesarias.
- En cuanto a la alimentación del sistema, es importante tomar en cuenta que se debe contar con un juego de dos baterías pues esto permite asegurar que cuando exista una falla de energía, el sistema de biométricos como el de la cerradura electromagnética sigan funcionando sin interrupción. El mismo que, mientras permanezcan activas, permitirá tomar acciones correctivas o buscar nuevas formas de alimentación momentáneas hasta el restablecimiento del flujo eléctrico.
- Previo a la implementación, es recomendable contar con todo el material y los diagramas de conexión de los equipos a ser interconectados. Con estos antecedentes, la instalación se vuelve un proceso sencillo; tener la noción de funcionamiento del sistema también es importante para reconocer y rectificar errores.
- Para el registro de los usuarios es importante definir el número de casa y el nombre del propietario. Además, para conservar el orden es imprescindible dejar un espacio entre usuarios; es decir, para cada domicilio se reservan cinco espacios para el registro de sus integrantes, sea para uso actual o futuro. De esta manera, es posible la reutilización de la base de datos y no un cambio o transcripción total.
- Se debe hacer un correcto registro tanto de huellas de *tags*, pues en caso de que el lector no reconozca, simplemente la puerta no se desmagnetiza e impide el ingreso o salida hacia el Conjunto.
- Es recomendable que antes de realizar los manuales de usuario y administrador, se tenga un conocimiento total del funcionamiento del sistema, debido a que esto facilitará la redacción de dichos documentos; además, de posibilitar la opción de mostrar soluciones a problemas presentados en el manejo de *hardware* y *software*.

5 REFERENCIAS BIBLIOGRÁFICAS

- [1] A. Q. J. Luis, «DSpace.UCE,» 2019. [En línea]. Available: <http://www.dspace.uce.edu.ec/bitstream/25000/18410/1/T-UCE-0005-CEC-182.pdf>. [Último acceso: 19 Julio 2021].
- [2] V. Bjorn, «Springer Link,» 3 Julio 2015. [En línea]. Available: https://bvirtual.epn.edu.ec:2069/10.1007/978-1-4899-7488-4_32. [Último acceso: 19 Julio 2021].
- [3] R. é. T. J. Zhu Zhi-yuan, «IEEE,» 29 Julio 2010. [En línea]. Available: <https://bvirtual.epn.edu.ec:2060/document/5529867/authors#authors>. [Último acceso: 19 Julio 2021].
- [4] R. Muñoz, «Inacorp,» Inacorp del Ecuador S.A, 07 11 2018. [En línea]. Available: <https://inacorpsa.com/2018/11/07/sistemas-biometricos/>. [Último acceso: 15 07 2021].
- [5] Z. Latinoamérica, «ZKTeco,» ZKTeco Latinoamérica , 2021. [En línea]. Available: <https://www.zktecolatinoamerica.com/>. [Último acceso: 15 07 2021].
- [6] Z. Latinoamérica, «MB360 Terminal Multi-biométrica para Gestión de Asistencia y funciones de Control de Acceso,» ZKTeco CO., TLD., 2017.
- [7] Z. Latinoamérica, «MA300 Terminal Biométrica IP Para Control de Acceso en Exteriores,» ZKTeco, Inc., México D.F., 2015.
- [8] Z. Latinoamérica, «K2 Botón de Salida Sin Contanco con Control Remoto,» ZKTeco Co., Ltd., México D.F., 2017.
- [9] Dorcas, «Dorcas Pulsadores,» Montajes Electrónicos Dorcas, S.L. , Valencia, España , 2015.
- [10] D-Link, «RangeBooster M 650 Router,» D-Link Corporation, Taiwan, 2008.
- [11] Z. Latinoamérica, «Manual de Usuario ZKAccess 3.5,» ZKTeco CO., LTD., 2016.

- [12] Btnet, «TIA/EIA-568-B,» Mayo 2001. [En línea]. Available: <https://bibdigital.epn.edu.ec/bitstream/15000/9268/5/Cap%204.pdf>. [Último acceso: 1 Julio 2021].
- [13] C. A. Nelly Flores, «Redes Convergentes,» de *ANSI/TIA/EIA 569-A*, España, ITCA, 2012, p. 254.
- [14] F. A. G. Orozco, «DISEÑO PARA EL MEJORAMIENTO DE LA RED DE COMUNICACIONES ACTUAL EN LA,» de *SEMINARIO DE PROFUNDIZACION EN REDES DE TELECOMUNICACIONES*, Bogotá, 2019.
- [15] IEEE Std, «Estandar IEEE para Ethernet,» *IEEE Std 802.3-2018*, Vols. %1 de %2Pp.1-5600, pp. 2-18, 2018.
- [16] I. D. Guide, «¿Qué es Ethernet (IEEE 802.3)?,» IONOS Digitalguide, 15 Agosto 2018. [En línea]. Available: <https://www.ionos.es/digitalguide/servidores/know-how/ethernet-ieee-8023/>. [Último acceso: 15 Julio 2021].
- [17] Z. Latinoamérica, *Terminal Biométrica IP de Huella Digital*, ZKTeco CO., LTD., 2020.
- [18] OpenCart, «Compteg Solution,» Compteg WebStore, 2021. [En línea]. Available: http://compteg.com/store/index.php?route=product/product&product_id=61. [Último acceso: 29 julio 2021].
- [19] Z. Latinoamérica, *Lector Biométrico para Control de Acceso*, ZKTeco CO., LTD., 2017.
- [20] S. Proaño, *Kit Acceso Dáctilar y Facial*, Quito: Cronte Technology, 2021.
- [21] G. d. U. ZKTEco, «Dispositivo de Control de Acceso Multi-Biométrico,» Julio 2015. [En línea]. Available: https://www.zkteco.com.pe/documentos/control-de-acceso/Multi-Biometrico_pantalla_2.8_Guia%20Rapida.pdf. [Último acceso: 29 Julio 2021].
- [22] Coelectrix, «Calcular la Autonomía de una Batería,» 9 Octubre 2019. [En línea]. Available: <https://coelectrix.com/calcular-la-autonomia-de-una-bateria>. [Último acceso: 1 Agosto 2021].

- [23] Cervi, «Sistema de cableado UTP Cat. 5e,» Cervi.es, 2011. [En línea]. Available: <https://www.cervi.es/ES/3-productos/36--sistemas-de-cableado-y-racks/268-sistema-de-cableado-utp-cat5e.html>. [Último acceso: 2 Agosto 2021].
- [24] INEC, «Encuesta de Victimización y Percepción de Inseguridad 2011,» INEC, 2011. [En línea]. Available: <https://www.ecuadorencifras.gob.ec/encuesta-de-victimizacion-y-percepcion-de-inseguridad-2011/>. [Último acceso: 20 Febrero 2021].
- [25] A. Q. J. Luis, «Análisis espacial de la distribución del delito de robo en el distrito,» Universidad Central de Ecuador, 2019. [En línea]. Available: <http://www.dspace.uce.edu.ec/bitstream/25000/18410/1/T-UCE-0005-CEC-182.pdf>. [Último acceso: 20 Febrero 2021].
- [26] M. A. Aguirre, «Procedimientos de los vigilantes para empresa de seguridad privada,» TresPuntoUno, 28 Diciembre 2018. [En línea]. Available: <https://trespuntouno.com/procedimientos-de-los-vigilantes-para-empresa-de-seguridad-privada/>. [Último acceso: 21 Febrero 2021].
- [27] Research Techsci , «Actualizacion atraves de Sistemas Biometricos,» TechSci Research, 20 Febrero 2015. [En línea]. Available: <https://www.techsciresearch.com/>. [Último acceso: 21 Febrero 2021].
- [28] Conjunto Residencial Conde 4, PDF, 23 Febrero 2004. [En línea]. Available: <https://www.habitatyvivienda.gob.ec/wp-content/uploads/downloads/2019/04/ESTATUTO-DE-CONFORMACION.pdf>. [Último acceso: 28 Febrero 2021].
- [29] A. Q. J. Luis, «Dspace.UCE,» 2019. [En línea]. Available: <http://www.dspace.uce.edu.ec/bitstream/25000/18410/1/T-UCE-0005-CEC-182.pdf>. [Último acceso: 19 Julio 2021].

ANEXOS

ANEXO 1: CERTIFICADO DE FUNCIONAMIENTO



ESCUELA POLITECNICA NACIONAL

Campus Politécnico "J. Rubén Orellana R

Quito, 3 de septiembre de 2021

CERTIFICADO DE FUNCIONAMIENTO DE PROYECTO DE TITULACIÓN

Yo, Fanny Paulina Flores Estévez, docente a tiempo completo de la Escuela Politécnica Nacional y como director de este trabajo de titulación, certifico que he constatado el correcto funcionamiento de la implementación del sistema biométrico de autenticación para el Conjunto Residencial "Conde 4", el cual fue implementado por las estudiantes Lizbeth Ludeña y Jesenia Rivera.

El proyecto cumple con los requerimientos de implementación y parámetros necesarios para que los residentes del "Conde 4" puedan usar los equipos de seguridad para su beneficio y confort.

DIRECTOR

Ing. Fanny Paulina Flores Estévez., Msc.

ANEXO 2: MANUAL DE USUARIO



MANUAL DE USUARIO

SISTEMA BIOMÉTRICO PARA AUTENTIFICACIÓN EN EL CONJUNTO RESIDENCIAL “CONDE 4”

Modelos aplicables:

ZKTeco-MB360 y ZKTeco-MA300

✉ lizbeth.ludena@epn.edu.ec, ✉ jesenia.rivera@epn.edu.ec

TABLA DE CONTENIDO

1. INFORMACIÓN.....	vi
2. EQUIPOS.....	vi
2.1. <i>ZKTeco</i> -MB360.....	vi
2.2. <i>ZKTeco</i> -MA300.....	vii
3. INSTRUCCIONES DE USO	vii
3.1. Reconocimiento dactilar.....	vii
3.2. Reconocimiento del <i>tag</i>	vii
4. PRECAUCIONES	viii

1. INFORMACIÓN

La implementación del sistema biométrico de autenticación para el “Conjunto Residencial Conde 4”, está conformado por el biométrico *ZKTeco-MB360* en la parte interna y el *ZKTeco-MA300* en la parte externa de la puerta principal del Conjunto; además, se colocó un pulsador para uso exclusivo del guardia a cargo.

Al concluir la puesta en funcionamiento del proyecto, se entregó a la directiva del Conjunto, la instalación de los equipos y el *software* con la respectiva base de datos. Los representantes del conjunto supervisaron, aprobaron y verificaron la operatividad de todo el sistema.

A continuación, se describe el uso y los cuidados necesarios para el mantenimiento adecuado de todo el sistema.

2. EQUIPOS

Los biométricos MB360 y MA300 tienen cargada la información de *tags* y huellas digitales, de acuerdo a la configuración realizada dentro del *software ZKAccess 3.5*.

NOTA: Se puede utilizar cualquier opción de reconocimiento para el acceso.

2.1. *ZKTeco-MB360*

En la Figura A2.1 se evidencian las partes principales del equipo.



Figura A2.1 Partes del *ZKTeco-MB360*

2.2. ZKTeco-MA300

En la Figura A2.2 se muestra las partes principales del equipo.



Figura A2.2 Partes del ZKTeco-MA300

3. INSTRUCCIONES DE USO

3.1. Reconocimiento dactilar.

Si el usuario desea ingresar o salir del Conjunto con el uso de su huella dactilar, debe colocar el dedo sobre el lector hasta que el dispositivo identifique su huella.

Nota: Para el reconocimiento de la huella dactilar debe existir el registro previo en el *software*.

3.2. Reconocimiento del *tag*.

Si el usuario desea ingresar o salir del Conjunto con el uso del *tag*, este debe colocar el elemento de forma diagonal al lector del biométrico sin mantener contacto directo con el lector. Por su seguridad se recomienda no hacer mal uso de los *tags*. Ejem. Prestar el *tag* a otra persona.

Nota: Los *tags* son **personales**, el beneficiario es el único responsable a cargo del mismo. Recuerde que este elemento es individual y se encuentra anexo a su nombre en la base de datos. Por lo tanto, la administración determinará la sanción respectiva en caso de detectar un mal uso de este dispositivo.

4. PRECAUCIONES

- **NO** colocar ningún objeto sobre el lector del biométrico.
- **NO** limpiar el vidrio del lector con alcohol o cualquier sustancia líquida.
- **NO** pulsar de forma agresiva el teclado del biométrico.
- **NO** golpear y forzar el biométrico.
- **Evitar** lesiones en los dedos para prevenir inconvenientes con el reconocimiento dactilar.
- **En caso de mal funcionamiento del equipo**, notifique dicho inconveniente al guardia o a la administración.

ANEXO 3: MANUAL DE ADMINISTRADOR



MANUAL DE ADMINISTRADOR


	<input type="checkbox"/>	ID de ...	Nombre	Apellido	Número...	No. de ...	Depart...	Género	Huellas v...	Huellas ...	Venas	Rostros (Pull)
1	<input type="checkbox"/>	1	Garita	Guardia	7503153	1	Conj. H...	Mascu...	1	0	0	0
2	<input type="checkbox"/>	2	Alicia E...	2		1	Conj. H...	Mascu...	1	0	0	0
3	<input type="checkbox"/>	3	Lizbeth ...	2	4700948	1	Conj. H...	Mascu...	1	0	0	0
4	<input type="checkbox"/>	4	David E...	2	4701321	1	Conj. H...	Mascu...	1	0	0	0
5	<input type="checkbox"/>	8	Angel G...	3	125886...	1	Conj. H...	Mascu...	0	0	0	0
6	<input type="checkbox"/>	14	Flor Mol...	5	2159636	1	Conj. H...	Femeni...	0	0	0	0
7	<input type="checkbox"/>	17	Freddy ...	6	8018099	1	Conj. H...	Mascu...	1	0	0	0
8	<input type="checkbox"/>	18	Freddy ...	6	8058285	1	Conj. H...	Mascu...	0	0	0	0
9	<input type="checkbox"/>	20	Julio Es...	7	6687210	1	Conj. H...	Mascu...	1	0	0	0
10	<input type="checkbox"/>	21	Pamela...	7		1	Conj. H...	Femeni...	1	0	0	0
11	<input type="checkbox"/>	22	Odalis ...	7		1	Conj. H...	Femeni...	1	0	0	0
12	<input type="checkbox"/>	23	Lina Es...	7		1	Conj. H...	Femeni...	1	0	0	0
13	<input type="checkbox"/>	38	Mariane...	12	6693334	1	Conj. H...	Mascu...	0	0	0	0
14	<input type="checkbox"/>	47	Anthony...	15		1	Conj. H...	Mascu...	1	0	0	0
15	<input type="checkbox"/>	48	Sebasti...	15		1	Conj. H...	Mascu...	1	0	0	0
16	<input type="checkbox"/>	49	Lorena ...	15		1	Conj. H...	Mascu...	1	0	0	0
17	<input type="checkbox"/>											
18	<input type="checkbox"/>											
19	<input type="checkbox"/>	53	Belen G...	16		1	Conj. H...	Mascu...	1	0	0	0

SISTEMA BIOMÉTRICO PARA AUTENTIFICACIÓN EN EL CONJUNTO RESIDENCIAL “CONDE 4”

Modelos aplicables:
ZKTeco-MB360 y ZKTeco-MA300

✉ lizbeth.ludena@epn.edu.ec, ✉ jesenia.rivera@epn.edu.ec

TABLA DE CONTENIDO

1. ANTECEDENTES	xii
2. EQUIPOS	xii
2.1. <i>ZKTeco</i> -MB360	xii
2.2. <i>ZKTeco</i> -MA300	xiii
2.3. Botón <i>no-touch</i> TLEB 102	xiii
2.4. Pulsador DISCA PL3	xiii
2.5. Enrutador <i>Range Booster</i> N650 DIR-635	xiv
3. DIAGRAMA DE RED	xiv
4. INDICACIONES ESPECÍFICAS DE CONFIGURACIÓN	xiv
4.1. <i>ZKTeco</i> -MB360	xiv
4.2. <i>ZKTeco</i> -MA300	xix
4.3. Enrutador <i>Range Booster</i> N650 DIR-635	xx
5. CONFIGURACIÓN DE USUARIOS EN EL <i>SOFTWARE</i>	xxi
5.1. Ingreso al sistema	xxi
5.2. Menú del sistema	xxii
5.3. Proceso de configuración	xxiv
6. MODOS DE VERIFICACIÓN	xxix
6.1. Huella digital	xxix
6.2. <i>Tag</i>	xxx
7. PRECAUCIONES 	xxx

1. ANTECEDENTES

La implementación del sistema biométrico de autenticación para el “Conjunto Residencial Conde 4”, está conformado por dos áreas ubicadas en la entrada principal del condominio.

En el área de la garita se instaló dos biométricos, la *ZKTeco-MB360* en la parte interna y la *ZKTeco-MA300* en la parte externa; además, se dispuso de un pulsador para uso exclusivo del guardia a cargo. Por otro lado, en el área administrativa se ocupó el biométrico *ZKTeco-MA300* junto con un botón *no-touch* K1-1. Todos los dispositivos se encuentran enlazados en la misma red mediante el uso de un enrutador *Range Booster N650 DIR-635*.

Al concluir la puesta en funcionamiento del proyecto, se entregó a la directiva del conjunto, la instalación de los equipos y el *software* con la respectiva base de datos. Los representantes supervisaron, aprobaron y verificaron la operatividad de todo el sistema.

NOTA: En este manual se describe las actividades que estarían a cargo por parte del administrador, para garantizar un control adecuado de los dispositivos.

2. EQUIPOS

2.1. ZKTECO-MB360

En la Figura A3.1 se evidencia el equipo.



Figura A3.1 *ZKTeco-MB360*

ESPECIFICACIONES

- Capacidad de Huellas **2000**
- Capacidad de Tarjetas **2000**
- Capacidad de Evento **100 000**
- Verificación de usuarios **<1 (s)**
- Comunicación **TCP/IP**
- Control de Acceso **ZKTeco-MA300, pulsador, brazo hidráulico y cerradura electromagnética.**
- Fuente de alimentación **12 (Vdc) 1.5 (A)**
- Dimensiones **167.5 x 148.8 x 32.2 (mm)**
- Peso Total **380 (gr)**

2.2. ZKTECO-MA300

En la Figura A3.2 se observa el biométrico.



ESPECIFICACIONES

- Capacidad de Huellas **1 500**
- Capacidad de Tarjetas **10 000**
- Capacidad de Evento **100 000**
- Verificación de usuarios **<1 (s)**
- Comunicación **TCP/IP**
- Control de Acceso **ZKTeco-MB360, botón *no-touch* y cerradura electromagnética.**
- Fuente de alimentación **12 (Vdc)**
- Dimensiones **73 x 148 x 34.5 (mm)**

Figura A3.2 ZKTeco-MA300

2.3. BOTÓN NO-TOUCH TLEB 102

En la Figura A3.3 se muestra el botón *no-touch*.



ESPECIFICACIONES

- Rango de detección **0.1 ~ 10 (cm)**
- **NO REQUIERE CONTACTO**
- Sensor de reposo **LED AZUL**
- Sensor de actividad **LED ROJO**
- Fuente de alimentación **12 (Vdc)**
- Dimensiones **115 x 70 x 2.9 (mm)**
- Peso **85 (gr)**

Figura A3.3 Botón *no-touch*

2.4. PULSADOR DISCA PL3

En la Figura A3.4 se visualiza el pulsador.



ESPECIFICACIONES

- Fuente de alimentación **12 (Vdc)**
- Dimensiones **100 x 25 x 36 (mm)**
- Peso **80 (gr)**
- Material **acero inoxidable**

Figura A3.4 Pulsador PL3

2.5. ENRUTADOR RANGE BOOSTER N650 DIR-635

En la Figura A3.5 se muestra el enrutador de red.



Figura A3.5 Enrutador

ESPECIFICACIONES

- Fuente de alimentación **5 (Vdc) 3 (A)**
- **QoS** prioriza el tráfico de paquetes
- Puertos: **4LAN, 1WAN, USB, WLAN y POWER**
- Procesador **3.8 (GHz)**
- RAM **256 (MB)**
- Sistema Operativo min **Windows XP**

3. DIAGRAMA DE RED

En la Figura A3.6 se visualiza el diagrama de red de la instalación.

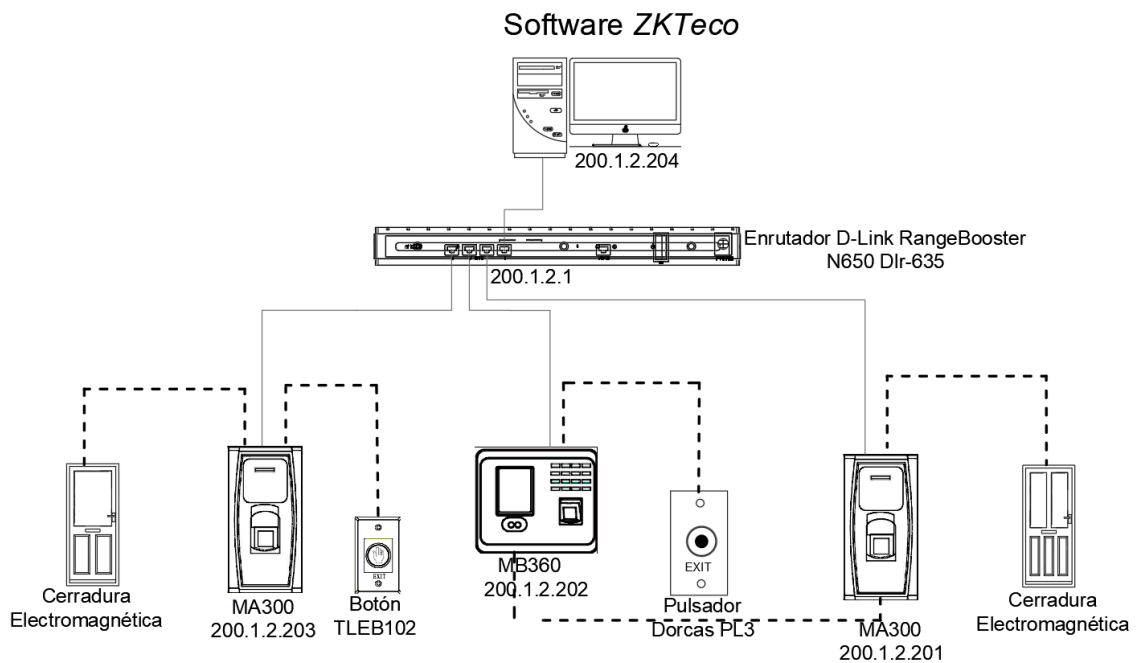


Figura A3.6 Diagrama de red

4. INDICACIONES ESPECÍFICAS DE CONFIGURACIÓN

4.1. ZKTECO-MB360

El biométrico *ZKTeco-MB360* permite la configuración de usuarios tanto de forma manual como a través del *software*.

MENÚ PRINCIPAL

El administrador(a) puede ingresar al “menú” pulsando sobre el “M/OK” del teclado. En la Figura A3.7 se observa la interfaz gráfica del biométrico.



Figura A3.7 Menú Principal

- **Usuarios:** Permite añadir, modificar y eliminar datos de los usuarios.
- **Privilegios:** Permite otorgar cierto tipo de acceso (administrador o usuario).
- **Red:** Permite configurar el medio conexión entre el equipo y el computador (*ethernet* y *serial*).
- **Sistema:** Permite el acceso a las configuraciones de fecha, hora, control de asistencia, huellas, actualización y reinicio.
- **Personalizar:** Permite observar parámetros tales como altavoces, interfaz de usuario y configuraciones de teclado.
- **Datos:** Permite generar respaldos, eliminar y restablecer los datos del dispositivo.
- **Acceso:** Permite configurar los eventos, otorgar accesos a grupos y verificar usuarios múltiples.
- **Gestión USB:** Permite cargar y descargar la base de datos con el uso de un micro USB.
- **Búsqueda de eventos:** Permite indagar en la base de datos del dispositivo para encontrar información específica sobre cierto usuario.
- **Mensaje:** Permite añadir, modificar y eliminar mensajes mostrados al público en pantalla.
- **Código de trabajo:** Permite añadir, modificar y eliminar el código de trabajo del equipo.

Nota: De ser activada esta opción, el ingreso al sistema será únicamente con la verificación de dicho código.

- **Autodiagnóstico:** Posibilita un análisis automático de todo el sistema de forma independiente.
- **Información del sistema:** Permite verificar la capacidad, los datos y el *firmware* del equipo en uso.

NOTA: Para más información consulte el “Manual de usuario del equipo ZKTeco-MB360”.

CONFIGURACIÓN MANUAL DE USUARIOS

- REGISTRO DE USUARIOS

En caso de requerir añadir nuevos usuarios, se debe seguir el siguiente procedimiento.

1. Pulsar sobre: “**M/Ok**” > **Usuarios** > **Nuevo Usuario**. Este proceso de evidencia en la Figura A3.8.

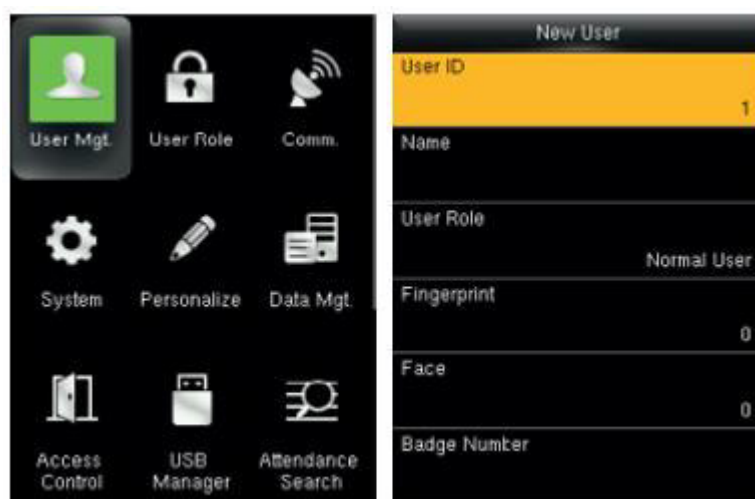


Figura A3.8 Registro de usuarios

2. Colocar: **ID del usuario y nombre de usuario** (número secuencial que tiene el usuario, el cual es único; cada casa tiene 5 espacios disponibles para ingreso de *tag* o huellas).
3. A continuación, si se desea registrar una huella digital dentro del ID ya creado, escoger la opción **HUELLA** > **Seleccionar el dedo** > **Registrar la huella (3 veces insertar el dedo)** > **Esperar la verificación de la huella**.

NOTA: Es recomendable utilizar el dedo pulgar o índice para el registro de la huella dactilar, en casos donde el usuario presente problemas de salud como

presión arterial alta o cualquier otra afección cardiaca, es aconsejable que realice el registro con el dedo medio, anular o meñique.

En la Figura A3.9 se puede observar un ejemplo del registro de huella.



Figura A3.9 Registro de la huella en el biométrico

4. Por otro lado, si se desea registrar un *tag*, escoger la opción **Número de tarjeta** > **Acercar el tag al lector** > **Esperar verificación del tag**. En la Figura A3.10 se puede observar la verificación correcta del *tag* tras la lectura realizada por el equipo.

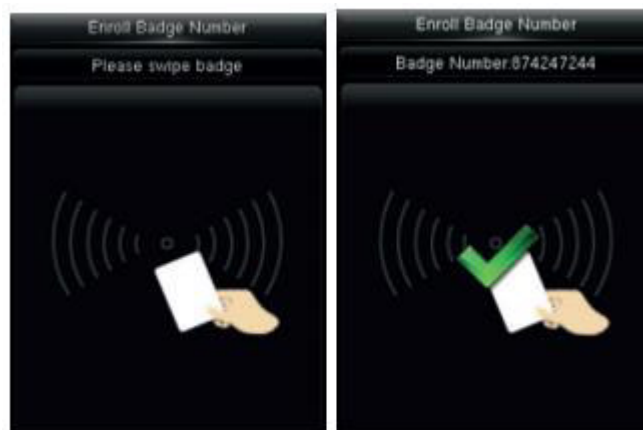


Figura A3.10 Registro del *tag* en el biométrico

- EDICIÓN DE USUARIOS

Para modificar algún parámetro de configuración de un usuario, se debe seguir el siguiente procedimiento.

1. Pulsar sobre: “M/Ok” > **Usuarios** > **Seleccionar usuario**
2. Escoger **Editar** > **Modificar el parámetro deseado**

En la Figura A3.11 se puede visualizar la edición de los parámetros ya configurados para el usuario.

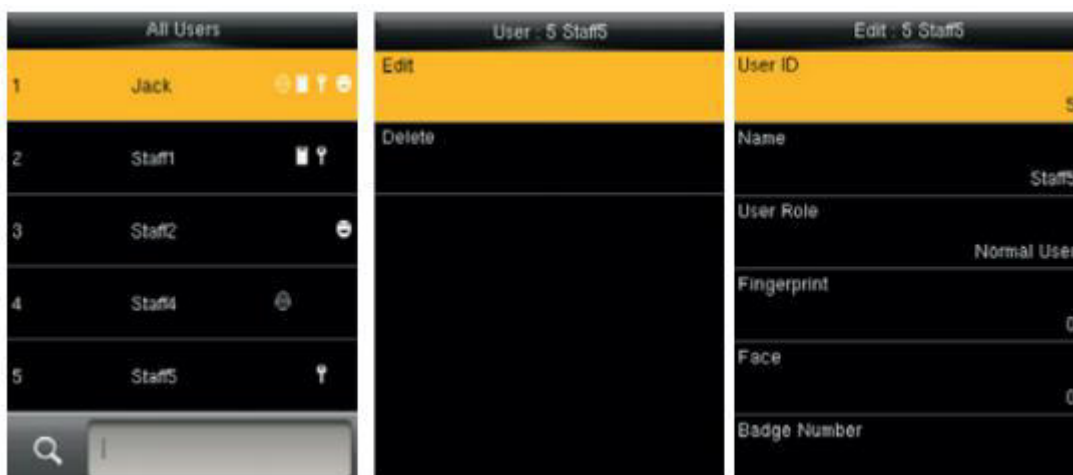


Figura A3.11 Edición de los parámetros

- ELIMINACIÓN DE USUARIOS

En caso de que el residente deje el Conjunto de forma permanente o de cometer alguna equivocación en la configuración, se debe realizar el proceso de eliminación de usuarios esto para no mantener información innecesaria ni afectar la base de datos, este proceso se muestra en la Figura A3.12.

1. Pulsar sobre: “M/Ok” > **Usuarios** > **Seleccionar usuario**
2. Escoger **Eliminar** > **Elegir una opción** > **Aceptar**

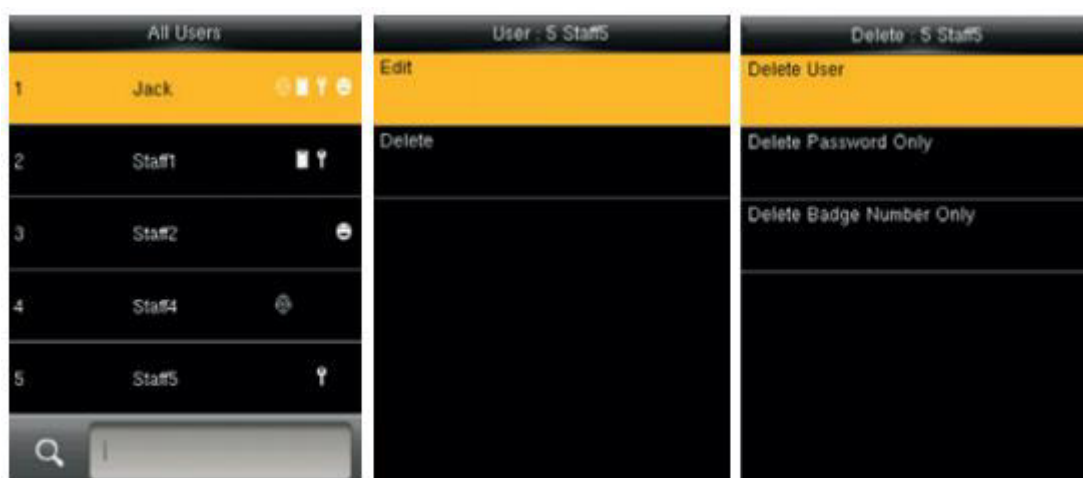


Figura A3.12 Eliminación de los parámetros

4.2. ZKTECO-MA300

El biométrico ZKTeco-MA300 permite ingresar usuarios tanto de forma manual como a través del *software*.

CONFIGURACIÓN MANUAL DE USUARIOS

- REGISTRO DE USUARIOS, HUELLAS DIGITALES Y TAGS

Este proceso complementa lo realizado con anterioridad, completada la configuración mediante *software* y manual, la vinculación entre datos y usuario es más sencilla.

1. En el biométrico se debe pasar la tarjeta de administrador **UNA VEZ** sobre el lector con esto se ingresa al **MODO DE REGISTRO DE USUARIOS**.
2. El biométrico solicita ingresar el **tag A REGISTRAR UNA SOLA VEZ** posterior se espera 5 (s) para que el registro sea un éxito.
3. Inmediatamente después, se solicita que ingrese el **DEDO** de su preferencia al **LECTOR**, repetir el proceso **TRES VECES**. Esperar que la bocina diga: **“Número del usuario”** y **“El registro ha sido exitoso”**

NOTA: Asegurarse de que el dedo se encuentre sobre la superficie del lector al momento del registro y de que no tenga ningún tipo de cicatriz que altere la huella dactilar. Esto para asegurar un registro exitoso como se puede observar en la Figura A3.13.



Figura A3.13 Registro exitoso

NOTA: Si no se tiene contestación a los 30 (s) de haber concluido el proceso, repetir el mismo hasta que la bocina del mensaje de registro sea exitoso.

- ELIMINACIÓN DE USUARIOS

Este proceso sirve para borrar a los residentes que la administración considere necesario, este procedimiento se muestra en la Figura A3.14.

1. Ingresar al **Modo de verificación**, pasar la tarjeta de administrador **UNA VEZ** sobre el lector.
2. Pasar la tarjeta de administrador **CINCO VECES**, esperar el ingreso al **ESTADO DE BORRADO**.
3. Colocar el **tag A BORRAR** sobre el lector y esperar **5 (s)** para su eliminación.
4. Esperar que la bocina diga: “Número del usuario” y “Borrado con éxito”.

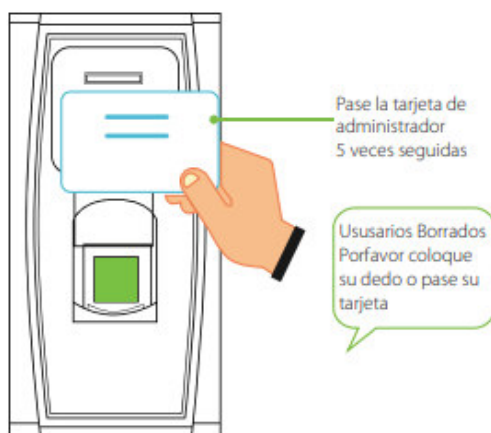


Figura A3.14 Eliminación exitosa

4.3. ENRUTADOR *RANGE BOOSTER N650 DIR-635*

El enrutador *Range Booster N650 DIR-635* pertenece a la marca D-LINK, cabe recalcar que, para cargar la información de los residentes del Conjunto hacia cada una de los biométricos, es necesario que los equipos se conecten al enrutador a través del cable de red.

CONFIGURACIONES BÁSICAS.

Todas las configuraciones detalladas a continuación son para la primera vez que se va a configurar del enrutador, este proceso se evidencia la Figura A3.15.

1. Ingresar a un navegador y colocar en la barra de búsqueda la dirección IP **192.168.0.1**.
2. En la pantalla emergente colocar el **usuario: ADMIN**, la **contraseña: DEJAR VACÍA** y pulsar sobre **LOGIN**.
3. Configurar la red de área local:
LAN Setup > Router IP Address > Default Subnet Mask > Guardar > Aceptar

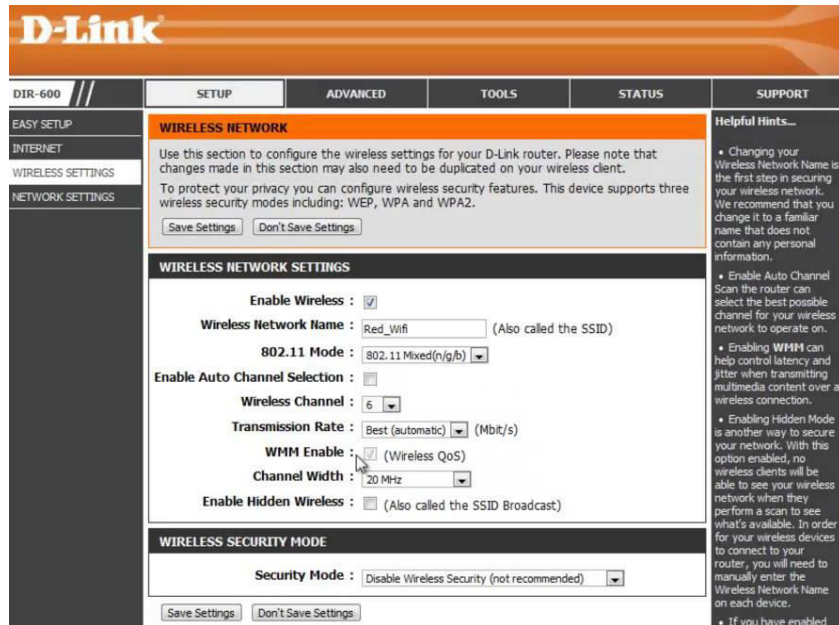


Figura A3.15 Configuración del enrutador

5. CONFIGURACIÓN DE USUARIOS EN EL SOFTWARE

La implementación de los tres biométricos conforman la red del Conjunto Residencial “Conde 4”, la cual se monitorea con el *software* del fabricante *ZKTeco*, este *software* es compatible con todos los equipos.

5.1. INGRESO AL SISTEMA

El administrador del *software* puede ingresar con el usuario y contraseña por defecto:

Usuario: admin, **Contraseña:** admin, tal cual se evidencia en la Figura A3.16.

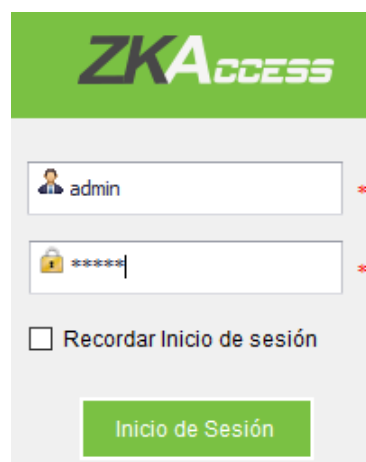


Figura A3.16 Ingreso del administrador al *software*

Una vez dentro de la pantalla principal, usted podrá escoger cualquier opción de las mostradas en la Figura A3.17.



Figura A3.17 Pantalla principal del *software*

5.2. MENÚ DEL SISTEMA

- DISPOSITIVO

Esta opción permite crear **Área, Dispositivo** y buscar **Dispositivos**.

- CONTROL DE ACCESO

Esta opción posibilita el crear **Horarios, Días Festivos, Niveles de acceso, Monitoreo en tiempo real, etc.**

- PERSONAL

Esta opción permite crear **Departamentos, Usuarios** y un **Registro de tarjetas**.

- REPORTES

En esta sección se puede imprimir los usuarios que ingresan o salen del Conjunto para que se cuente con un reporte del uso de *tag* o huellas de usuarios determinados.

- SISTEMA

BASE DE DATOS

Esta opción posibilita la oportunidad de ejercer mayor control sobre la **base de datos** registrada dentro del biométrico y del *software*; además, permite generar **respaldos, recuperar y corregir** la información ingresada. En la Figura A3.18 muestra la base de datos del *software*.

	<input type="checkbox"/>	ID de ...	Nombre	Apellido	Número...	No. de ...	Depart...	Género	Huellas v...	Huellas ...	Venas	Rostros (Pull)
1	<input type="checkbox"/>	1	Gariña	Guardia	7503153	1	Conj. H...	Masculi...	1	0	0	0
2	<input type="checkbox"/>	2	Alicia E...	2		1	Conj. H...	Masculi...	1	0	0	0
3	<input type="checkbox"/>	3	Lizbeth ...	2	4700948	1	Conj. H...	Masculi...	1	0	0	0
4	<input type="checkbox"/>	4	David E...	2	4701321	1	Conj. H...	Masculi...	1	0	0	0
5	<input type="checkbox"/>	8	Angel G...	3	125886...	1	Conj. H...	Masculi...	0	0	0	0
6	<input type="checkbox"/>	14	Flor Mol...	5	2159636	1	Conj. H...	Femeni...	0	0	0	0
7	<input type="checkbox"/>	17	Freddy ...	6	8018099	1	Conj. H...	Masculi...	1	0	0	0
8	<input type="checkbox"/>	18	Freddy ...	6	8058285	1	Conj. H...	Masculi...	0	0	0	0
9	<input type="checkbox"/>	20	Julio Es...	7	6687210	1	Conj. H...	Masculi...	1	0	0	0
10	<input type="checkbox"/>	21	Pamela...	7		1	Conj. H...	Femeni...	1	0	0	0
11	<input type="checkbox"/>	22	Odalis ...	7		1	Conj. H...	Femeni...	1	0	0	0
12	<input type="checkbox"/>	23	Lina Es...	7		1	Conj. H...	Femeni...	1	0	0	0
13	<input type="checkbox"/>	38	Mariane...	12	6693334	1	Conj. H...	Masculi...	0	0	0	0
14	<input type="checkbox"/>	47	Anthony...	15		1	Conj. H...	Masculi...	1	0	0	0
15	<input type="checkbox"/>	48	Sebasti...	15		1	Conj. H...	Masculi...	1	0	0	0
16	<input type="checkbox"/>	49	Lorena ...	15		1	Conj. H...	Masculi...	1	0	0	0
17	<input type="checkbox"/>	50	Paul Ba...	15		1	Conj. H...	Masculi...	1	0	0	0
18	<input type="checkbox"/>	51	Concep...	15		1	Conj. H...	Femeni...	1	0	0	0
19	<input type="checkbox"/>	53	Belen G...	16		1	Conj. H...	Masculi...	1	0	0	0
20	<input type="checkbox"/>	54	Javier G...	16		1	Conj. H...	Masculi...	1	0	0	0
21	<input type="checkbox"/>	55	Gabriel...	17	129618...	1	Conj. H...	Masculi...	0	0	0	0
22	<input type="checkbox"/>	60	Alexand...	19		1	Conj. H...	Femeni...	1	0	0	0

Figura A3.18 Base de datos del software

SISTEMA

Permite modificar los parámetros de: **privilegios, usuarios del sistema, cambios de contraseña y el cambio de idioma.** Los procesos especificados con anterioridad pueden ser realizado tras completar los campos obligatorios de cada pantalla mostrada en la Figura A3.19.

The image shows three screenshots of system configuration windows:

- Modificar Contraseña:** A window with three input fields: 'Antigua Contraseña', 'Nueva Contraseña', and 'Confirmar Contraseña'. Each field has a red asterisk indicating it is required. There are 'OK' and 'Cancelar' buttons at the bottom.
- Cambiar Idioma:** A window with a dropdown menu labeled 'Elija el idioma:' currently set to 'Spanish'. There are 'OK' and 'Cancelar' buttons at the bottom.
- Inicializar Sistema:** A window with a tree view under 'Todo' containing five sub-items: 'Personal', 'Reporte', 'Dispositivo', 'Control de Acceso', and 'Sistema'. Each item has an unchecked checkbox.

Figura A3.19 Configuraciones del sistema del software

NOTA: Para más información consulte el **“Manual del software ZKTeco Access 3.5”**.

5.3. PROCESO DE CONFIGURACIÓN

- CREACIÓN DE ÁREA

La creación del área sirve para la posterior asignación de la misma en la creación de los dispositivos, ya que este parámetro es de suma importancia para el administrador de la red a la hora de realizar el control de acceso. Este proceso se muestra en la Figura A3.20.

1. Ingresar a: **Dispositivo**
2. Pulsar sobre la opción **Área**
3. Seleccionar la etiqueta **Editar**
4. Escoger el área a ser editada y
5. Finalmente, llenar los **campos obligatorios > OK**

OJO: En el caso de requerir agregar un área, pulsar sobre el botón **Agregar** y repetir el proceso anterior.

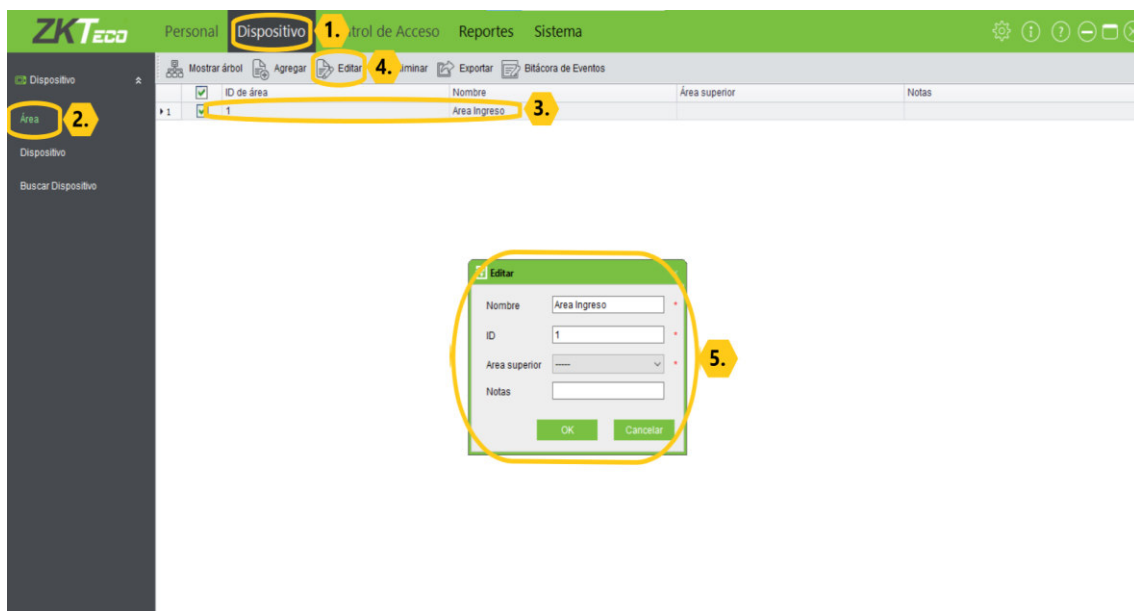


Figura A3.20 Configuraciones de la creación del área

- CREACIÓN DEL DISPOSITIVO

La creación del dispositivo dentro del *software* facilita el proceso de asignación de usuarios, registro de huellas y *tag*. Este proceso se evidencia en la Figura A3.21.

1. Ingresar a la pestaña **Dispositivo**.
2. Pulsar sobre la opción **Dispositivo**.
3. Seleccionar la etiqueta **Agregar**.
4. Acceder al **Modo Profesional**, ubicado en la parte inferior izquierda de la pantalla emergente.

5. Llenar los **campos obligatorios** evidenciados con asteriscos rojos:
Nombre del dispositivo > Tipo de panel > Área > Modo de comunicación > Dirección IP > Puerto.

Tanto la dirección IP como el puerto, deben ser únicos para cada dispositivo creado. Además, se debe activar la opción “Eliminar los datos del equipo al ingresar” para que no exista un conflicto entre la información del sistema y del dispositivo.

6. **Probar la conexión con el dispositivo**, en caso de que la conexión no sea exitosa se debe realizar nuevamente el proceso.
7. Pulsar sobre **OK** para finalizar.

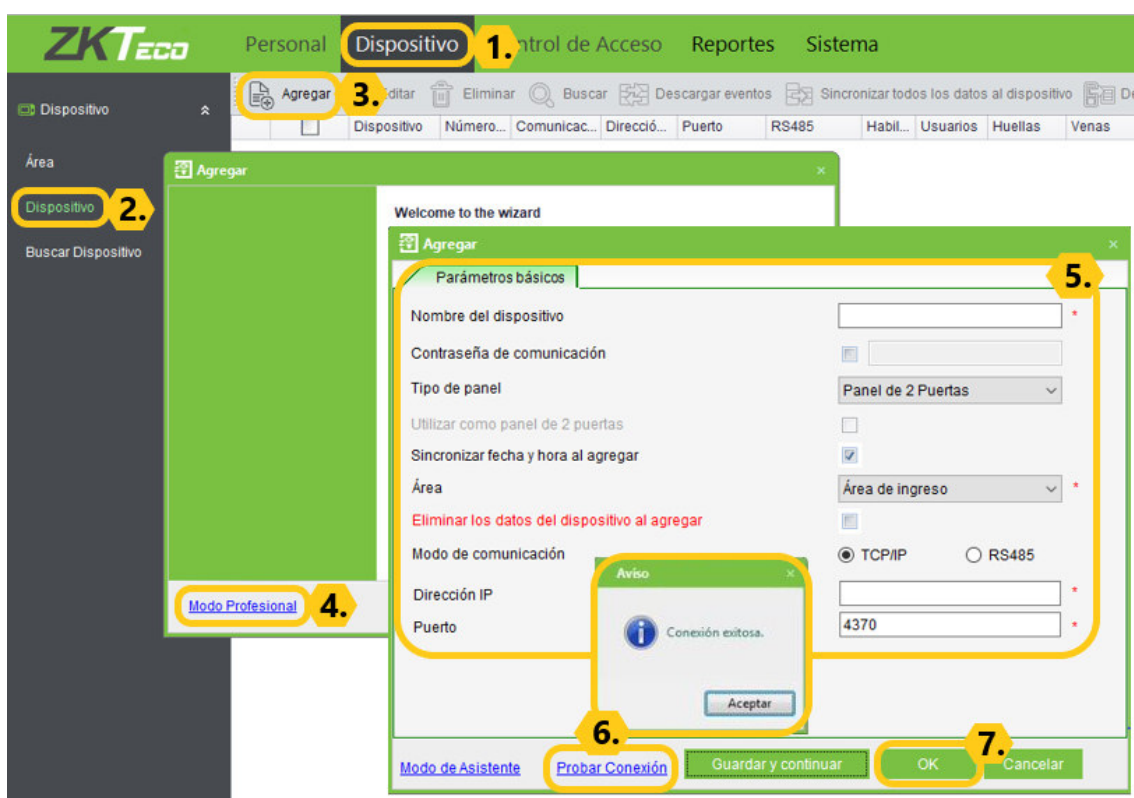


Figura A3.21 Configuraciones de la creación del dispositivo

- CREACIÓN DE NIVEL DE ACCESO

La creación de las listas para los niveles de acceso sirve para facilitar el proceso de ubicación de los usuarios según la zona a la cual van a tener acceso. Este proceso se evidencia en la Figura A3.22.

1. Ingreso a la pestaña **Control de acceso**.
2. Seleccionar la opción **Niveles de acceso**.

3. Para añadir el control de acceso al biométrico se debe pulsar sobre la etiqueta **Agregar**.
4. Llenar los **campos obligatorios: Nombre del acceso > Horario**.
5. Seleccionar el dispositivo para cargar los datos de los usuarios:
 - **PUERTAS:** En esta sección debe ubicarse las puertas que **no tendrán acceso al Conjunto**.
 - **PUERTAS SELECCIONADOS:** En esta sección debe ubicarse las puertas que **tendrán acceso al Conjunto**.
6. Cargar toda la base de datos y realizar las configuraciones pertinentes:
 - **USUARIOS:** En esta sección debe colocarse a los usuarios a quienes se le **denegará el acceso al Conjunto**.
 - **USURIOS SELECCIONADOS:** En esta sección debe colocarse a los usuarios a quienes se le **otorgará el acceso al Conjunto**.
7. Finalmente, pulsar **OK** y esperar que la información se sincronice entre los dispositivos.

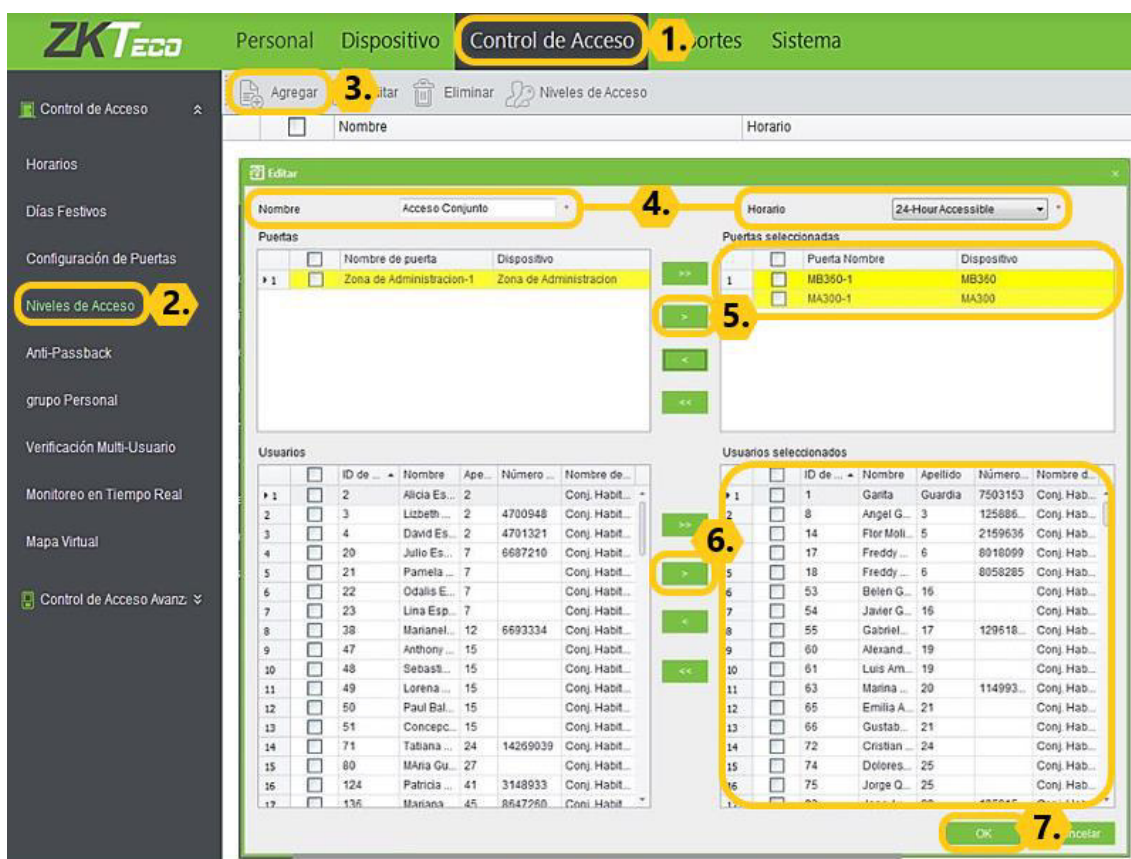


Figura A3.22 Configuración para la creación de los niveles de acceso

- CREACIÓN DE DEPARTAMENTO

El departamento sirve para especificar el grupo al cual pertenece dicho usuario, en este caso se usó el nombre “Residencia Conde4” porque este es el nombre del Conjunto. Este proceso se puede observar en la Figura A3.23.

1. Ingresar a la pestaña **Departamentos > Agregar**.
2. Llenar los datos solicitados > **OK**.

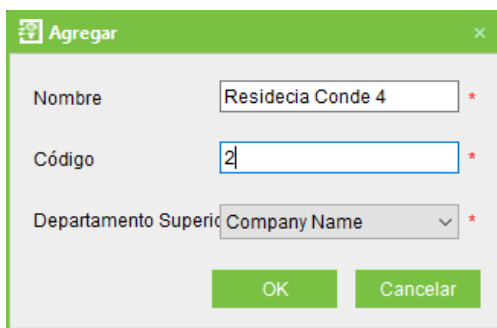


Figura A3.23 Creación del departamento

- CONFIGURACIÓN DE PUERTAS

La configuración de las puertas sirve para controlar el tiempo de apertura de las mismas; además, permite seleccionar el tiempo de reconocimiento de cada biométrico.

1. Ingresar a: **Control de acceso > Configuración de Puertas > Seleccionar dispositivo > Editar**.
2. Configurar todos los parámetros obligatorios evidenciados con asteriscos rojos, los cuales se muestran en la Figura A3.24.

NOTA: El intervalo de tiempo debe ser configurado en base a un análisis previo, donde se evalúe la tardanza del usuario al entrar o salir del Conjunto residencial.

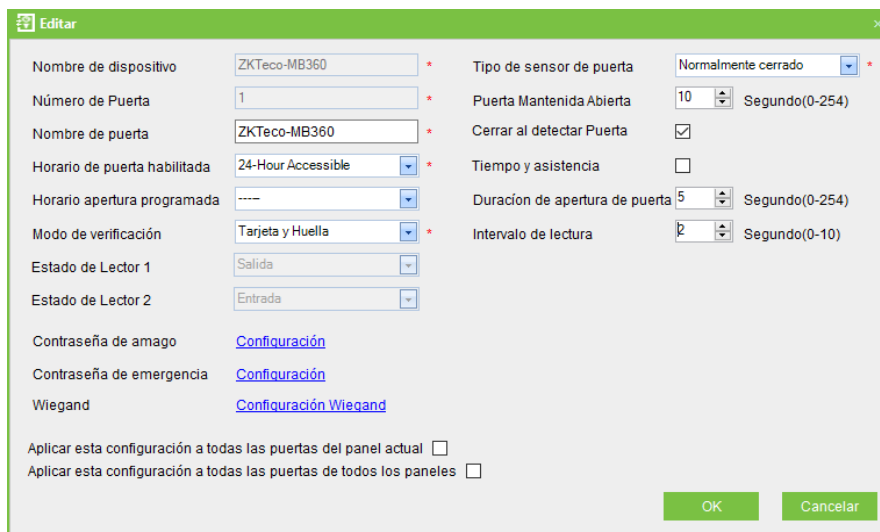


Figura A3.24 Configuración de los parámetros para las puertas

- CREACIÓN DE USUARIOS

Con la creación de usuarios se posibilita la oportunidad de configuración y administración de los mismos con el uso del *software*, para realizar este procedimiento se efectuó los puntos que se pueden observar en la Figura A3.25.

1. Ingresar a la pestaña **Personal**.
2. Seleccionar la opción de **Usuarios**.
3. Pulsar sobre la etiqueta **Agregar**.
4. Llenar los campos con asteriscos rojos de la pantalla **Información Personal**
Obligatorios: **ID del usuario y Departamento**.

Es importante enfatizar que para el campo “Apellido” se optó por colocar el número de casa del residente, el resto de campos en esta pantalla deben ser completados como mejor considere el administrador.

En la Figura A3.26 se evidencia el proceso realizado en la pestaña **Niveles de acceso**.

5. En esta pantalla, se va a **otorgar acceso** a los usuarios correspondientes, para esto en la parte de nivel de acceso se selecciona la lista y con la flecha individual se la pasa a niveles de acceso seleccionados.
6. Finalmente, se debe pulsar sobre **Guardar > OK**

NOTA: Si se desea que un usuario tenga activada la huella y el *tag* por un periodo de tiempo determinado, debe llenarse el **punto 7**

Figura A3.25 Creación de usuarios

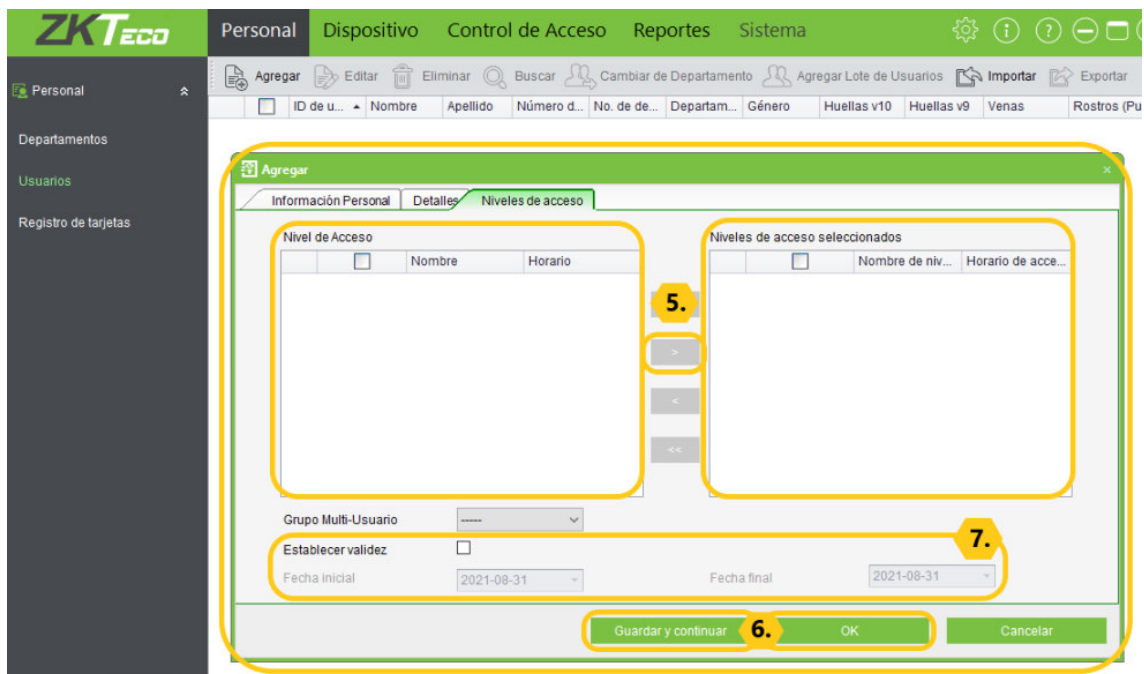


Figura A3.26 Configuración de los niveles de acceso para el usuario

6. MODOS DE VERIFICACIÓN

El usuario puede salir e ingresar al Conjunto, sea con el uso de la huella dactilar o con el uso de un *tag*, cualquier opción permite la verificación.

6.1. HUELLA DIGITAL

- Para este tipo de reconocimiento basta con ingresar el dedo de forma paralela a la superficie de lector y esperar **3 (s)** a que la bocina del dispositivo diga “**Acceso correcto**”, de esta manera el usuario podrá salir e ingresar. En la Figura A3.27 se evidencia la forma correcta del ingreso del dedo en el biométrico.
- En el caso de usar la huella dactilar, **es importante recordar el dedo con el cual se registró.**

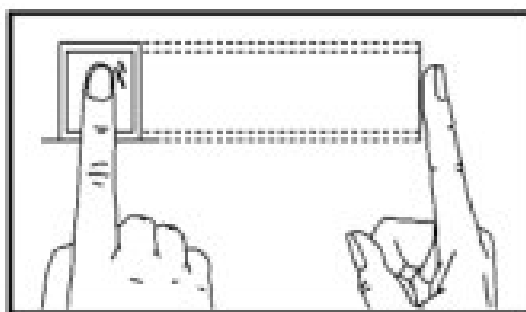


Figura A3.27 Forma correcta del ingreso del dedo en el biométrico

6.2. TAG

Para este tipo de reconocimiento basta con colocar el **tag**:

- De **forma diagonal** frente al **lector** en el caso del **biométrico ZKTeco-M360**.
- Frente al **lector de tag** en el caso del **biométrico ZKTeco-MA300**.

Una vez ejecutado cualquier proceso, se debe esperar **3 (s)** para que el reconocimiento se finalice y la bocina del dispositivo indique “**Acceso correcto**”.

7. PRECAUCIONES

- **NO** colocar ningún objeto sobre el lector del biométrico.
- **NO** limpiar el vidrio del lector con alcohol o cualquier sustancia líquida.
- **NO** pulsar de forma agresiva el teclado del biométrico.
- **NO** pisar ni jalar el cableado estructurado.
- **NO** golpear y forzar el biométrico.
- **Proteger** el equipo de factores climáticos como exceso de luz solar o lluvia, para evitar fallas en el reconocimiento dactilar y *tag*.
- **Evitar** lesiones en los dedos.
- **Realizar** inspecciones cada cierto periodo para prever daños en los equipos.
- **En caso de** mal funcionamiento del equipo comunique al guardia o a la administración.

NOTA: La garantía de los equipos solo cubre fallas internas con los dispositivos.