Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería Mecánica Eléctrica

DISEÑO DE SISTEMAS DE CONTROL BIOMÉTRICO PARA EL MONITOREO Y CONTROL DE NIÑOS CON SERVICIO DE BUS ESCOLAR EN EL ÁREA METROPOLITANA EN LA CIUDAD DE GUATEMALA

Luis Fernando Herrera Escobar
Asesorado por la Inga. Ingrid Salomé Rodríguez de Loukota

Guatemala, agosto de 2021

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

DISEÑO DE SISTEMAS DE CONTROL BIOMÉTRICO PARA EL MONITOREO Y CONTROL DE NIÑOS CON SERVICIO DE BUS ESCOLAR EN EL ÁREA METROPOLITANA EN LA CIUDAD DE GUATEMALA

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR:

LUIS FERNANDO HERRERA ESCOBAR
ASESORADO POR LA INGA. INGRID SALOMÉ RODRÍGUEZ DE LOUKOTA

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO ELECTRÓNICO

GUATEMALA, AGOSTO 2021

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANA	Inga. Aurelia Anabela Cordova Estrada
VOCAL I	Ing. José Francisco Gómez Rivera
VOCAL II	Ing. Mario Renato Escobedo Martínez
VOCAL III	Ing. José Milton de León Bran
VOCAL IV	Br. Christian Moisés de la Cruz Leal
VOCAL V	Br. Kevin Armando Cruz Lorente
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Pedro Antonio Aguilar Polanco
EXAMINADORA	Inga. Ingrid Salomé Rodríguez de Loukota
EXAMINADOR	Ing. Byron Odilio Arrivillaga Méndez
EXAMINADOR	Ing. Carlos Eduardo Guzmán Salazar
SECRETARIA	Inga. Lesbia Magalí Herrera López

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

DISEÑO DE SISTEMAS DE CONTROL BIOMÉTRICO PARA EL MONITOREO Y CONTROL DE NIÑOS CON SERVICIO DE BUS ESCOLAR EN EL ÁREA METROPOLITANA EN LA CIUDAD DE GUATEMALA

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería Mecánica Eléctrica, con fecha 14 de febrero de 2020.

Luis Fernando Herrera Escobar

Guatemala 7 de septiembre de 2020

Ingeniero
Julio César Solares Peñate
Coordinador del Área de Electrónica
Escuela de Ingeniería Mecánica Eléctrica
Facultad de Ingeniería, USAC.

Apreciable Ingeniero Solares,

Me permito dar aprobación al trabajo de graduación titulado ¨**Diseño de sistemas de control biométrico para el monitoreo y control de niños con servicio de bus escolar en el área metropolitana en la Ciudad de Guatemala**¨, del señor **Luis Fernando Herrera Escobar**, por considerar que cumple con los requisitos establecidos.

Por tanto, el autor de este trabajo de graduación y, yo, como su asesora, nos hacemos responsables por el contenido y conclusiones de este.

Sin otro particular, me es grato saludarle.

Atentamente,

Inga. Ingrid Rodríguez de Loukota
Colegiada 5,356
Asesora

Ingrid Rodríguez de Loukota
Ingeniera en Electrónica
colegiado 5356

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERIA

Guatemala, 14 de septiembre de 2020

Señor Director
Armando Alonso Rivera Carrillo
Escuela de Ingeniería Mecánica Eléctrica
Facultad de Ingeniería, USAC

Estimado Señor Director:

Por este medio me permito dar aprobación al Trabajo de Graduación titulado **DISEÑO DE SISTEMAS DE CONTROL BIOMÉTRICO PARA EL MONITOREO Y CONTROL DE NIÑOS CON SERVICIO DE BUS ESCOLAR EN EL ÁREA METROPOLITANA EN LA CIUDAD DE GUATEMALA,** desarrollado por el estudiante **Luis Fernando Herrera Escobar**, ya que considero que cumple con los requisitos establecidos.

Sin otro particular, aprovecho la oportunidad para saludarlo.

Atentamente,

ID Y ENSEÑAD A TODOS

Ing. Julio César Solares Peñate
Coordinador de Electrónica

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÍA

ESCUELA DE INGENIERIA MECÁNICA ELECTRICA
FACULTAD DE INGENIERÍA

REF. EIME 86. 2021.

El Director de la Escuela de Ingeniería Mecánica Eléctrica, después de conocer el dictamen del Asesor, con el Visto Bueno del Coordinador de Área, al trabajo de Graduación del estudiante; LUIS FERNANDO HERRERA ESCOBAR titulado; DISEÑO DE SISTEMAS DE CONTROL BIOMÉTRICO PARA EL MONITOREO Y CONTROL DE NIÑOS CON SERVICIO DE BUS ESCOLAR EN EL ÁREA METROPOLITANA EN LA CIUDAD DE GUATEMALA, procede a la autorización del mismo.

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DIRECCION ESCUELA DE INGENIERIA MECANICA ELECTRICA
FACULTAD DE INGENIERIA

Ing. Armando Alonso Rivera Carrillo

GUATEMALA, 29 DE ABRIL 2,021.

Decanato
Facultad de Ingeniería
24189101 - 24189102

DTG. 334-2021

La Decana de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería Mecánica Eléctrica, al Trabajo de Graduación titulado: **DISEÑO DE SISTEMAS DE CONTROL BIOMÉTRICO PARA EL MONITOREO Y CONTROL DE NIÑOS CON SERVICIO DE BUS ESCOLAR EN EL ÁREA METROPOLITANA EN LA CIUDAD DE GUATEMALA**, presentado por el estudiante universitario**: Luis Fernando Herrera Escobar,** y después de haber culminado las revisiones previas bajo la responsabilidad de las instancias correspondientes, autoriza la impresión del mismo.

IMPRÍMASE:

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANA
FACULTAD DE INGENIERÍA

Inga. Anabela Cordova Estrada
Decana

Guatemala, agosto de 2021

AACE/asga

ACTO QUE DEDICO A:

Dios	Por cada bendición y amor derramado en mi vida y por siempre iluminar y guiar mi camino.
Mis padres	Miriam Liliana Escobar García de Herrera y Edgar Fernando Herrera Alvizurez, por impulsarme para alcanzar mis metas brindándome su apoyo, por ser mi mayor inspiración y ejemplo de vida, humildad y amor, ya que sin ellos la vida no sería igual de bella.
Mis hermanas	Cintia Gabriela y Heidy Rocío Herrera por su comprensión, apoyo y amor incondicional.
Mis abuelos	María Teresa García Rosales (q. e. p. d.), quien fue y será mi mayor ejemplo amor y unión familiar y a mi abuelo Marco Antonio Escobar Toledo (q. e. p. d.), por su ejemplo de superación y siempre mostrar interés genuino por mí.
Mi familia	Tías, tíos, primos, primas y sobrinos por ser siempre influencia muy especial de amor y admiración en mi vida y por apoyarme en todo momento.
María Stephanie Cruz	Por brindarme su apoyo incondicional.

Mis amigos

Roberto Carlos Yaquian Ortega (q. e. p. d.); y a José Eduardo Soto Castellanos (q. e. p. d), amigos, compañeros y colegas con quienes compartimos y trabajamos por cumplir esta meta y aunque se nos adelantaron siempre los llevaré en mí corazón.

AGRADECIMIENTOS A:

Universidad de San Carlos de Guatemala	*Alma máter,* casa de estudios que me brindo los valores, las herramientas y los recursos necesarios para alcanzar esta meta profesional y por fomentar la educación superior permitiendo a los ciudadanos crear una mejor nación.
Facultad de Ingeniería	Por ser el lugar donde adquirí mis conocimientos profesionales.
Ingeniera Ingrid de Loukota	Por compartir sus conocimientos durante toda mi formación profesional y por el apoyo incondicional durante la asesoría de mi trabajo de graduación.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

GLOSARIO

AC Abreviatura de corriente alterna. Corriente que tiene un movimiento en un sentido durante un tiempo y después en sentido opuesto, repitiéndose el mismo proceso en forma constante.

Algoritmo Sucesión de pasos requeridos en la solución de un problema.

Amplificador Circuitos que se utilizan para aumentar el valor de la señal de entrada generalmente muy pequeña, y así obtener una señal a la salida con una forma mucho mayor a la señal de entrada.

Capacitancia Magnitud de energía almacenada para una tensión dada.

Foto detector Elemento que transforma la energía de la luz en una señal eléctrica.

Minucia Detalles pequeños donde concluyen las líneas en una huella, o la bifurcación de las líneas de una huella.

Píxel Unidad de medida que se utiliza para expresar la capacidad de resolución de una pantalla. Los pixeles son puntos de colores o en escala de grises.

Periférico	Dispositivo conectado a la unidad central de proceso. Un teclado, módem, ratón, por ejemplo, son periféricos.
Sistema biométrico	Sistema que opera sus instrucciones de reconocimiento bajo un rasgo físico personal que es comparada y verificado de forma automática.
USB	Siglas del puerto en inglés Universal Serial Bus, este es el intermediario de conexión de periféricos externos. También es un dispositivo o un conector externo que se utiliza como memoria externa.

RESUMEN

En la actualidad los centros educativos en general brindan el servicio de traslado por medio de buses escolares, este servicio es utilizado tanto para el ingreso de los alumnos desde su casa a la institución como viceversa. Sin embargo, los adolescentes con la finalidad de evitarlos mienten en sus hogares indicando que los dejaron o no salieron a tiempo teniendo en cuenta que los padres trabajan y es complicado que estos se movilicen, dejando a discreción de este el retorno a sus hogares, como se puede dar el caso de ser un descuido, se puede considerar que es a propósito.

> En los medios de comunicación social se observa un creciente número de denuncias de desapariciones de adolescente, aunado a la situación de inseguridad imperante en el país. De acuerdo con la información oficial, del 1 de enero al 21 de abril del año 2019, ha activado 1 mil 948 alertas Alba-Keneth, que corresponden a 2 mil 290 NNA reportados como desaparecidos. De la estadística, 1 mil 432 menores de edad fueron localizados, pero todavía hace falta encontrar a 858. Según la Unidad, existe una coordinadora de búsqueda encargada de la localización de los menores de edad.
>
> Las instituciones que integran la coordinadora son la Procuraduría General de la Nación (PGN) que es la responsable de la Unidad Operativa del Sistema de Alerta Alba-Keneth, el Ministerio Público (MP), la Policía Nacional Civil (PNC), el Ministerio de Relaciones Exteriores (Minex), la Secretaría contra la Violencia Sexual, Explotación y Trata de Personas (SVET) y la Secretaría de Comunicación Social de la Presidencia. La Coordinadora la preside la PGN.[1]

Implementar un sistema de control biométrico al ingresar al bus quedaría registrado la hora y lugar por parte del sistema, llevando un control lo que facilitaría en un menor tiempo reportar la ausencia del niño o adolescente; en casos de desaparición el tiempo es un elemento vital para la ubicación; este control también constituiría un apoyo para el establecimiento educativo por el

[1] Diario La Hora *.Alba-keneth ha reportado 2 mil 290 casos de niñez desaparecida.* https://lahora.gt/alba-keneth-ha-reportado-2-mil-290-casos-de-ninez-desaparecida/.

registro de asistencia del alumno; como a nivel administrativo con relación al pago del servicio.

Dicha propuesta se realizaría por medio de un router con conexión móvil, es decir que se conecte al sistema de telefonía móvil ya que se va acoplando a la cobertura móvil que hay en la calle dependiendo del proveedor, esto para que no pierda la señal y tampoco la información que se tendrá almacenada.

Con un servicio de enlace de datos este será responsable de la transferencia fiable de la información a través de un circuito de trasmisión de datos. Sin necesidad de que se tenga acceso o salida a internet ya que la por medio de enlaces de datos la información viaja de manera más segura.

OBJETIVOS

General

Desarrollar un sistema de control biométrico para el monitoreo y control de niños con servicio de bus escolar en el área metropolitana en la ciudad de Guatemala.

Específicos

1. Realizar un diagnóstico actual para el monitoreo de servicio de transporte escolar en el municipio del departamento de Guatemala.

2. Identificar el proceso necesario para el diseño de sistemas de control biométrico para el monitoreo y control de niños con servicio de bus escolar.

3. Determinar el sistema de control biométrico para el monitoreo y control de niños con servicio de bus escolar.

4. Identificar la funcionalidad de los sistemas de control biométrico para el monitoreo y control de niños con servicio de bus escolar.

5. Identificar los principales beneficios de los sistemas de control biométrico para el monitoreo y control de niños con servicio de bus escolar.

INTRODUCCIÓN

Ante la alta preocupación respecto a la seguridad de los alumnos en diferentes instituciones educativas públicas y privadas se observó que este tema no está entre los más analizados o comentados en cuanto a ciudadanos y controles. Surge la preocupación de restringir o reducir la probabilidad de que un alumno abandone o se retire de la institución escolar sin que lo recoja el personal autorizado para hacerlo y evitar que una persona sin la autorización correspondiente retire a un alumno de las instalaciones educativas; siempre teniendo excepciones de aquellos alumnos que necesiten un permiso extraordinario para retirarse en esa circunstancia. Y así mismo ayudar y controlar la preocupación de los padres de familia y personal educativo con respecto a este tema.

Sin embargo, la ciudad capital en la actualidad se encuentra saturada por el aspecto del tráfico, lo que produce que los escolares en algunos casos deban abordar desde horas que aún no ha amanecido por completo; regresando a sus hogares en horas de la tarde, por lo que un sistema de control biométrico para el monitoreo y control de niños con servicio de bus escolar es una alternativa viable y segura para los establecimientos educativos y para tranquilidad de los padres.

1. ANTECEDENTES GENERALES

1.1. Empresa de servicios de transporte escolar

Se le llama transporte escolar a todo transporte especializado para desplazamiento o traslado de alumnos y alumnas desde su domicilio hasta el centro educativo y del centro educativo a su domicilio.

El transporte escolar se ejecuta en vehículos autorizados y bien identificados, están destinados para toda la comunidad educativa.

En todas las instituciones y establecimientos educativos, la asistencia de transporte escolar se ofrece:

- Rutas específicas de transporte escolar, analizadas y contratadas directamente por las instituciones y establecimientos educativos.
- Adquisición y contratación de las plazas necesarias para el servicio y asistencia de transporte educativo.
- Las instituciones educativas públicas y privadas, el servicio de transporte, que podrá ser adquiridos por estas mismas o por las asociaciones de padres de familia que estén constituidas con todos sus requisitos.

1.2. Inicios de la compañía en Guatemala

Transportes Seguros, fue constituida el 6 de marzo de 2005, uno de los principales objetivos es aportar desarrollo sostenible y productivo a la sociedad, mediante plazas de empleo fijas, brindando oportunidades a hombres y mujeres,

y al mismo tiempo cumple con las leyes y requerimientos legales que se necesitan para operar en el país. La empresa posee infraestructura física y equipo necesario, para realizar ciclos operativos, personal con experiencia en la naturaleza del negocio.

La organización se dedica a la prestación de servicio de transporte, posee buses confortables con tecnología moderna de características ergonómicas para escolares, con el objetivo de resguardar la integridad física de los usuarios, así como los bienes de quienes lo abordan, proporciona servicios de transporte para excursiones de tipo exprés en el territorio guatemalteco, en jornadas nocturna, diurna y mixta, las actividades diarias que se realizan en el giro normal de operaciones son, con el objetivo principal de asegurar la presencia física de los tripulantes en los tiempos y lugares pactados, el principal servicio se proporciona a los colegios de la ciudad capital, también para excursiones.

1.3. Información general

Es una organización que brinda el servicio y asistencia de transporte escolar a los establecimientos educativos para trasladarlos de forma adecuada, eficiente y segura de sus hogares a los establecimientos y de los establecimientos a sus hogares.

En la compañía se cuenta con 3 autobuses con capacidad para 60 usuarios, estos son Chevrolet modelo 1998. Estos tres vehículos, están habilitados dos, ya que una unidad se utiliza como parte de un plan de contingencia ante cualquier evento, emergencia, que presente cualquiera de los dos autobuses habilitados.

Figura 1. **Buses de la empresa**

Fuente: Prensa Libre. *Buses escolares*. https://www.prensalibre.com/ciudades/guatemala-ciudades/revision-de-buses-escolares-no-se-cumple-en-todos-los-municipios-asegura-la-pdh/. Consulta 5 de marzo 2020.

Este servicio está a la orden para los padres de familia que necesiten el traslado de sus hijos de edad escolar, y que sean de interés las rutas de las zonas 9, 10, 13, 14, 15 de la ciudad capital.

En la agencia central se tiene una atención personalizada con cada consulta a realizar, en la central se cuenta con parqueo para las unidades de transporte que estén fuera de servicio.

Los competidores directos son todas las empresas grandes que ofrecen servicio de transporte escolar a diversas instituciones y establecimientos educativos. Y el servicio de bus escolar a varios establecimientos educativos y cuentan con rutas formadas y analizadas para la eficiencia del traslado de los alumnos.

Estos transportes escolares regularmente se identifican por ser de color amarillo, con una capacidad de trasladar un rango entre 44 a 92 alumnos.

Los microbuses cuentan con rutas predeterminadas de los domicilios a instituciones y establecimientos educativos, trasladan un aproximado de 10 a 15 alumnos.

La empresa tiene como meta, llegar a ser la empresa de mayor crecimiento posicionándose en la mente de los clientes, por su calidad de servicio, también utilizando tecnología en sus entregas, comprometiéndose con sus clientes a tener los estándares de calidad que requieren para ser el proveedor de transporte competitivo que su negocio requiera.

Transportes Seguros es una empresa de tipo mercantil con procesos industriales en el área de talleres y con procesos de logística en cuanto a los recorridos diarios para el transforme de los menores.

Por esa razón, y por la seguridad de su personal, particularmente los operarios y el personal de transporte por contratar, todos están capacitados en normas de calidad y procesos ISO 9000 y 14000 y aunque la empresa no está certificada, cumple con esos estándares normalmente.

La tecnología de Transportes Seguros consta básicamente del equipo de oficina, el equipo para mantenimiento y de limpieza, como se describe a continuación:

- 3 Pupitres.
- 2 Sillas ejecutivas.
- 2 Sillas secretariales.
- 4 Sillas de visitas.
- Butacas para sala de juntas.
- 1 Mesa de sala de juntas.

- 3 Ficheros para archivos.
- 3 Computadoras.
- 3 Software: programas y antivirus.
- 2 Impresoras.
- 1 Teléfono fijo.
- 5 Teléfonos celulares.
- 4 Juegos de papelería y escritorio.
- 8 Lockers.
- 8 Candados de seguridad para Lockers.
- 2 Oasis de agua.
- 1 Microondas.
- 1 Cafetera.
- 1 Mesa.
- 3 Autobuses.
- Kit de herramienta para reparaciones: Llaves, destornilladores, barreno, llave de tubo, lagarto, entre otros.

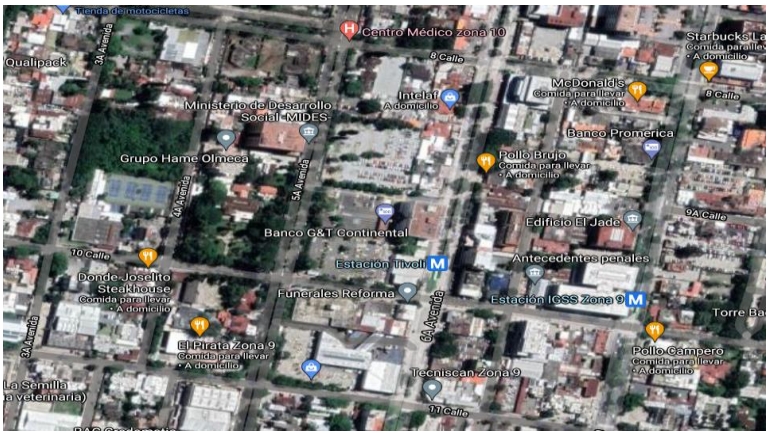
Figura 2. **Equipo de la empresa**

Fuente: elaboración propia, talleres Lico.

1.3.1. Ubicación

Las oficinas se encuentran en la zona 9, debido que es un lugar estratégico para la salida de los buses hacia los centros educativos a los cuales se les presta el servicio.

Figura 3. **Ubicación**



Fuente: Google maps. *Ubicación.* https://www.google.com/maps/@14.6052999,-90.5216064,706m/data=!3m1!1e3?hl=es Consulta: 5 de abril de 2020.

1.3.2. Misión

Proporcionar un servicio de transporte de usuarios que cubra con calidad y responsabilidad, mediante la seguridad de todos los usuarios, trasladándolos al destino con satisfacción y puntualidad.

1.3.3. Visión

Ser una empresa de transporte eficiente con un resultado integral, reconocidos como proveedores calificados, en transporte empresarial, turismo y

servicio escolar a través de la garantía en la prestación del servicio, comprometidos en beneficio de los clientes.

1.4. Tipo de organización

La organización consiste en identificar y clasificar las actividades requeridas, la agrupación de las labores necesarias para el acatamiento de los objetivos, asignación de cada grupo de laboral a un líder dotado de la autoridad y la estructura de la organización.

Transportes Seguros es una entidad de servicio que está integrada por una gerencia general, bajo su cargo están tres gerentes los cuales son: gerente administrativo, gerente de personal y gerente de talleres.

- La gerencia general, se encarga de validar los resultados de las demás áreas.

- El gerente administrativo dirige todas las operaciones financieras y administrativas, como el control de los recursos financieros, tiene a su cargo personal de atención al cliente.

- El gerente de personal, es el encargado de supervisar y administrar todo el personal que maneja las unidades de transportes, desde la contratación, pruebas de manejo y capacitaciones.

- El gerente de talleres, es el encargado de velar por el funcionamiento de las unidades de transportes como proporcionar una adecuada optimización de los recursos que se necesitan para el mantenimiento de los buses, tiene a cargo personal para brindar soporte necesario en

momentos de emergencia, coordina la logística para que las unidades de trasporte cumplan con los requisitos que las autoridades reguladoras de transportes requieran al momento de desplazarse por la ciudad o fuera de ella.

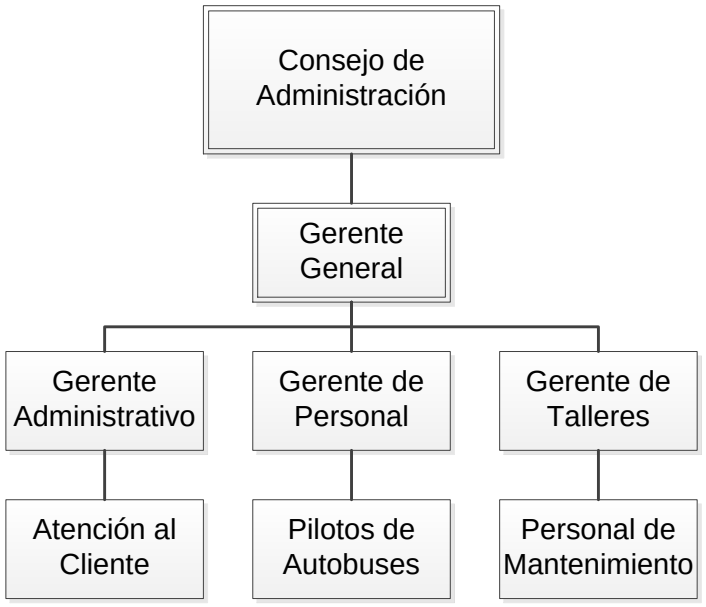
Figura 4. **Área de talleres**

Fuente: 1010 Experiancias.com. taller de restauración de buses. https://1010experiencias.com/experiencia/conoce-un-taller-de-restauracion-de-buses--taller-de-carpinteria-y-visita-un-proyecto-educativo?gallery=TRUE. Consulta: 5 de abril 2020

1.4.1. Organigrama

El organigrama es esencial para la empresa, hace comprender la estructura de la empresa fácilmente.

Figura 5. **Organigrama**



Fuente: elaboración propia, empleando Word.

La Empresa Transportes Seguros cuenta con accionistas, pilotos, mecánicos, clientes y proveedores:

- Accionistas son varios socios que aportan el mismo capital para las compras de las unidades.
- Empleados: son pilotos y mecánicos que revisan las unidades para que se mantengan en buen estado.
- Clientes: son las instituciones y establecimientos educativos y los padres de familia del alumnado estas mismas.
- Proveedores: abastecen las unidades de combustible y las ventas de repuestos para el mantenimiento de estas.

Figura 6. **Proveedores**

Fuente: Latam Energy. *Gasolineras Shell.* http://www.latam-energy.com/2017/09/06/mexico-shell-abre-su-primera-gasolinera-en-el-pais-azteca/. Consulta 6 de abril 2020

2. SITUACION ACTUAL

2.1. Análisis de la situación

La empresa de Transportes Seguros al ser constituida una empresa con fines de lucro ha logrado una evolución formidable en los últimos años. Gracias al excelente trabajo y el gran equipo que realizan una gestión con alto grado de eficiencia, saciando las necesidades como empres y al cliente.

La empresa no funciona al 100 % de eficiencia en su forma estructural y administrativa, debido a la falta de gestión estratégica. Lo que da como conclusión que la empresa no sea efectiva como se espera.

En la actualidad la empresa no cuenta con una orientación estratégica organizacionalmente en relación a las funciones y responsabilidades del personal contratado, quienes no cuentan con una capacitación que les dé una misión estratégica en cada una de sus actividades. No posee una visión clara y concisa que pueda figurar la empresa en el futuro, ni cuenta con estrategias que lleven a ejecutar los propósitos planteados. Falta de un buen movimiento para promocionar la flotilla de autobuses en el mercado. Para obtener los resultados deseados, que la compañía crezca y evolucione eficientemente para proporcionar bienestar tanto a propietarios y clientes.

La sede principal de la empresa cuenta con una infraestructura en mal estado, esto es un elemento que se contempla como obstáculo, no permite desarrollar adecuadamente las actividades correspondientes.

2.2. Oferta de las automotoras disponibles de la compañía

La organización siempre ha trabajado con el mejor equipo especialistas del volante, este está conformado por operadores especializados en distintas áreas: operadores, logísticas, conductores, mecánicos. Cada uno cuenta con la experiencia necesaria para brindar la mejor atención posible. El equipo se inclina para alcanzar los propósitos de calidad y excelencia en prestación del servicio ofrecido.

La compañía cuenta con pilotos profesionales de la mano una flotilla de vehículos modernos para que el desempeño sea eficiente:

- Maquinaria: carrocerías modernas, el mejor confort y diseño, alta calidad.
- Alumbrado: sistema de iluminación instalado en el autobús.
- Sistema de dirección: es la agrupación de elementos necesarios para alinear las ruedas directrices, a disposición del conductor.
- Neumáticos: denominados ruedas, fabricados de caucho, están en contacto con el suelo.
- Sistema de frenos: agrupación de mecanismos con finalidad de disminuir las revoluciones del automotor.
- Carrocerías: base o estructura del automóvil donde reposa los pasajeros.
- Sistema contra Incendios: medidas de seguridad que debe contener el autobús.
- Chasis: es la base fundamental del automotor, estructura donde reposan todos los mecanismos.

La empresa plasma su mercado objetivo en las instituciones y establecimientos educativos ubicados en zonas aledañas a la sede principal:

zonas 9, 10, 13, 14 y 15 de la ciudad capital de Guatemala. Cuenta con una flotilla de 60 vehículos competentes para el traslado de personal educativo.

Se desarrolla una descripción de la flotilla actual de la empresa:

Tabla I. **Flotilla de vehicular**

Microbuses	Furgonetas	Autobuses	Vacantes	Total
31	12	16	1	60

Fuente: elaboración propia, empleando Word.

2.3. Diagnóstico estratégico de la empresa

El análisis vincula la compañía en un entorno habitual y la competencia, analizando los 4 elementos básicos que contemplan el dictamen estratégico: debilidades, fortalezas, amenazas y oportunidades. Los elementos analizan el estado actual de la empresa actualmente, estableciendo así:

- "La empresa y su operación determinando los factores positivos, que se denominan Fortalezas, y los negativos llamados Debilidades, y
- El contexto, identificando los factores positivos y negativos, denominados respectivamente Oportunidades y Amenazas."[2]

La empresa Transportes Seguros, será transparente en cada diagnóstico estratégico y revelará de manera clara y detallada, los puntos fuertes y débiles. Claramente se mostrará los cuatro elementos esenciales: oportunidades y

[2] FAGA, Héctor Alberto. *Como profundizar en el análisis de sus costos para tomar mejores decisiones empresariales.* p. 87.

fortalezas, debilidades y amenazas. Y aprovechar de forma eficiente el pro y el contra de la empresa.

2.3.1. Antecedentes

El origen de la propuesta de crear una empresa de automotores para el servicio de transporte escolar es gracias al fundador. Los socios de la empresa son los amigos que con gran aprobación y aceptación apoyaron la propuesta. La finalidad de esta iniciativa era brindar un servicio de transporte especializado y cómodo, utilizando este objetivo principal se creó legalmente la empresa, que actualmente ha tenido una evolución eficiente. Cada aportación y esfuerzo en equipo han generado un servicio de alta calidad.

Se realizó la escritura pública para la creación y constitución de la empresa, en la ciudad de Guatemala el día 12 de julio de 2005. La empresa ha sufrido transformaciones importantes, que tienen un impacto desde su capital hasta su estructura, esto es un efecto positivo para la compañía. Existen sucesos que se describirán a continuación:

- Conformación de la compañía Transportes Seguros el 29 de agosto de 2005.
- El impacto del crecimiento de la empresa en el año 2006 crea la necesidad de aumentar el personal. Se contrata personal administrativo, contador y secretaria, para que realicen de forma eficiente las actividades que les competen dentro del establecimiento arrendado.
- Se crea el Consejo de Administración, el día número 6 del mes de septiembre del año 2007. En el año descrito se incremente considerablemente el capital de la empresa, el incremento fue de Q 52 500,00, sumando un total neto de Q 1 555 000,00, convirtiendo el

capital a una referencia universal, equivale a $ 201 822,21 Estadunidenses. Gracias a este crecimiento la compañía ha subido de estatus en el mercado local, cada beneficio, incremento y cada experiencia le suma un valor privilegiado a la institución.

- En el año 2017 en su aniversario se apertura la sede central de la compañía, se constituye las oficinas administrativas de la empresa, consta con un espacio grande para un salón de reuniones y eventos privados, ya sean de los mismos socios o que se haya puesto en alquiler. Y un lugar especial para estacionamiento de los autobuses. En este año se cumplen 12 años de funcionamiento de la empresa Transporte Seguros.

2.4. Capacidad financiera

Transportes Seguros se considera una empresa que posee una estructura muy solvente, con un alto nivel de liquidez que favorece en sostener un apalancamiento nulo.

No se tiene un departamento formado de contabilidad, este lo conforma solo una persona, esta se realiza de manera elemental, teniendo registros periódicos contables. También las responsabilidades tributarias, pero no se desarrolla el análisis correspondiente, no se aprecian los estados financieros.

A la empresa se le atribuye una debilidad media al no contar con un presupuesto que monitoree los, las ganancias y gastos para lograr utilidades.

2.5. Capacidad tecnológica

El departamento o área tecnológica de la empresa se puede catalogar como media, ya que cuenta con equipos tecnológicos básicos como teléfonos, para tener un medio de comunicación con el mismo personal y con la clientela. Una computadora, adaptada para las operaciones y actividades financieras:

- MemoryMagus: aporta un sistema automatizado para gestiones administrativas. Es una forma de crear archivos digitales para tipos de licitaciones en el portal de compras de carácter público, creando carpetas de distintos usuarios.
- MemoryCoty: este es un programa distintivo y para uso contable único y exclusivo para los protocolos y reportes contables.

Los equipos tecnológicos que constituyen la empresa son de gama media con procesadores dual core i5, discos solidos de 1 T, memory ram de 8gb, cada equipo cuenta con los softwares antes mencionados, para que de forma automática agilice, optimice los procesos y actividades administrativos.

En la empresa existe una desventaja, al ser una empresa de transporte escolar no cuenta con una flotilla de autobuses modernos que no poseen un sistema de rastreo satelital, este sistema está dentro del plan contingencia de la empresa, reduciendo la probabilidad de una pérdida total del autobús, y una forma de seguridad para los pasajeros. Los equipos tecnológicos también son catalogados como una debilidad baja.

2.6. Capacidad de Recursos Humanos

Transportes Seguros es una empresa que dispone de 65 personas que conforma el recurso humano, las cuales laboran en áreas y departamentos distintos:

- Administrativa-financiera: se conforma por un presidente, gerente, asesores, vocales, comisiones, secretaria, asistente de secretaria, contadores y jefes de servicios varios. Cada puesto es importante para el buen funcionamiento y estructura de la empresa.
- Servicios: conformada por los pilotos profesionales y los agentes de seguridad.

La gerencia general es la encargada de administrar todo lo relacionado con el personal desde los recursos humanos, y se responsabiliza de todos los procesos administrativos, laborales y sociales del personal de trabajo.

Se mantiene un proceso profesional y legítimo para la elección y postulación de los candidatos a laborar en la empresa, se trabaja con el proceso habitual, mediante referencias laborales y personales, estudios y experiencia, y por medio de evaluaciones prácticas e intelectuales. Los resultados son comparados y verificados con respecto al puesto a desempeñar. Este proceso está a cargo del gerente.

Se atribuye una debilidad alta para la evolución de los procesos organizacionales de la compañía, al no contar con un manual de operaciones básicas y uno de puestos y reclutamiento conformado por la selección y formación del personal.

El personal que labora para la compañía no cuenta con las capacitaciones correctas para cumplir y desempeñar de forma eficiente sus funciones correspondientes. Se considera un porcentaje medio a personal que cuentan con estudios de nivel superior.

Es atribuido como debilidad alta a la falta de personal en el departamento de recursos humanos, por ser administrada por el gerente general, no cuenta con la capacidad ni el tiempo de desarrollar capacitaciones para el personal.

2.7. Matriz FODA

Es una estrategia para evaluar la empresa por medio de un análisis por dos grupos, un grupo es el análisis de factores críticos denominados fortalezas y los aspectos positivos denominados oportunidades. El siguiente grupo es analizando los factores críticos llamados debilidades y aspectos negativos denominados amenazas. El uso de esta estrategia genera alternativas para la evolución y desarrollo de la empresa.

Para el análisis se requiere la utilización de dos tipos de matrices, la matriz EFE, matriz de evaluación de factor externo. Y la matriz EFI, matriz de evaluación de factor interno.

2.7.1. Matriz de evaluación de factor externo

Para el desarrollo de la matriz se consideró de la siguiente forma: débil = uno (1); media = dos (2); encima de la media = tres (3); excelente = cuatro (4), para tener un indicador de que tan eficaz es la estrategia con la cual la empresa está trabajando.

Tabla II. **Matriz EFE**

	Oportunidades	Peso	Calif.	Total, ponderado
1	Industria mal atendida	0,10	4	0,40
2	Necesidad de un traslado de calidad.	0,10	3	0,30
3	Costos competitivos	0,10	2	0,20
4	Proveedores de repuestos y mantenimiento de automotores	0,05	3	0,15
5	Mercados modernos	0,05	3	0,15
6	Riesgo país	0,05	2	0,10
7	Fuente de Consolidación	0,05	2	0,10
	Amenazas	**Peso**	**Calif.**	**Total, ponderado**
1	Reducción de presupuesto para proveedores de repuestos y mantenimiento de automotores	0,10	3	0,30
2	Contienda directa, mercado restringido	0,10	3	0,30
3	Variaciones en la legislación	0,05	3	0,15
4	Afluencia vehicular excesivo	0,05	3	0,15
5	Reglamentaciones perjudiciales	0,05	2	0,10
6	Falta de indagaciones científicas o tecnológicas	0,05	2	0,10
7	Contiendas corporaciones	0,05	2	0,10
8	Tasa de incremento oscilante	0,05	2	0,10
	Total	1,00		2,55

Fuente: elaboración propia, empleando Word.

Se comprende que el factor con mayor impacto en la empresa es el mercado o industria mal atendida, como lo indica la característica peso 0,10 con una puntuación de 4. El dato 2,55 que se encuentra en el total ponderado refleja que la empresa se encuentra por arriba del promedio, da una satisfacción que el empeño de perseguir estrategias que aprovechen las oportunidades externas y evitar amenazas.

2.7.2. Matriz de evaluación de factor interno

Se consideró lo siguiente: debilidad mayor = 1; debilidad menor = 2; fortaleza menor = 3; fortaleza mayor = 4

Tabla III. **Matriz EFI**

	Fortalezas	Peso	Calif.	Total, ponderado
1	Localización estratégica	0,10	3	0,30
2	Acceso a un financiamiento	0,10	3	0,30
3	Conocimiento de la industria	0,05	3	0,15
4	Servicio de alta calidad	0,05	2	0,10
5	Acatamiento de responsabilidades con instituciones públicas y privadas	0,05	2	0,10
6	Eficaz modelo administrativo y contable	0,05	2	0,10
7	Excelente ambiente laboral	0,05	2	0,10
	Amenazas	**Peso**	**Calif**	**Total, ponderado**
1	Políticas orientadas a las necesidades del cliente	0,10	4	0,40
2	Inspección y análisis financiero	0,10	3	0,30
3	Mantenimientos y rastreos de automotores	0,05	3	0,15
4	Coordinación de venta y post venta	0,05	3	0,15
5	Reclutamiento, capacitación del personal	0,05	3	0,15
6	Proyección mercantil, estrategias implementación de mercado	0,05	2	0,10
7	Representación y aspecto corporativo	0,05	2	0,10
8	Organigrama con deficiencia estructural	0,05	2	0,10
9	Desconocimiento del objetivo principal de la empresa	0,05	1	0,05
	Total	1,00		2,65

Fuente: elaboración propia, empleando Word.

Se nota que la fortaleza primordial para la empresa es políticas orientadas a las necesidades del cliente observando el indicador peso 0,10 con una puntuación 4. También se hace notar la debilidad mayor, es el desconocimiento principal del objetivo principal de la empresa con un peso 0,05 y puntuación de 1. El dato 2,65 que se encuentra reflejado en el total ponderado, revela que el nivel estratégico interna de la empresa cuenta una debilidad muy alta.

2.7.3. Hoja de trabajo

Es una técnica de análisis y encontrar los puntos claves de la estabilidad de la empresa, encontrando las fortalezas, oportunidades, debilidades y amenazas.

Tabla IV. **Matriz FODA**

Interno	**Externo**
Fortalezas	**Oportunidades**
• Localización estratégica. • Acceso a un financiamiento • Conocimiento de la industria • Servicio de alta calidad • Acatamiento de responsabilidades con instituciones públicas y privadas • Eficaz modelo administrativo y contable • Excelente ambiente laboral	• Industria mal atendida • Necesidad de un traslado de calidad. • Costos competitivos • Proveedores de repuestos y mantenimiento de automotores • Mercados modernos • Riesgo país • Fuente de Consolidación
Debilidades	**Amenazas**
• Políticas orientadas a las necesidades del cliente • Inspección y análisis financiero • Mantenimientos y rastreos de automotores • Coordinación de venta y post venta • Reclutamiento, capacitación del personal • Proyección mercantil, estrategias implementación de mercado • Representación y aspecto corporativo • Organigrama con deficiencia estructural • Desconocimiento del objetivo principal de la empresa	• Reducción de presupuesto para proveedores de repuestos y mantenimiento de automotores • Contienda directa, mercado restringido • Variaciones en la legislación • Afluencia vehicular excesivo • Reglamentaciones perjudiciales • Falta de indagaciones científicas o tecnológicas • Contiendas corporaciones • Tasa de incremento oscilante

Fuente: elaboración propia, empleando Word.

3. BIOMETRÍA

3.1. Qué es biometría

"El concepto biometría proviene de las palabras bio y metría que representa vida y respectivamente medida, se define biometría como el estudio de identificación de personas mediante el uso de sus características físicas o su comportamiento."[3]

Cada persona cuenta con características que los hacen distintos los unos de los otros, con lo que los hace diferentes. A través de la utilización de un equipo biométrico se pueden identificar y medir las características de los individuos.

Este tipo de equipo cuenta con características con las que se poder realizar mediciones, comparaciones, codificaciones, almacenamiento de datos y reconocimiento de las particularidades de un individuo con un nivel de confiabilidad muy certero. Según lo indica Marí Sagarra, este tipo de dispositivos constan de tres partes:

> por una parte, utiliza un mecanismo automático que detecta y obtiene una captura de una imagen digital o análoga de la muestra a analizar. Disponen de un departamento para manipular aspectos como la comprensión, almacenamiento o comparación de los datos adquiridos con los almacenados en una base de datos (que son considerados válidos), y también ofrecen una interfaz para las aplicaciones que los utilicen.[4]

Estos dispositivos no son riesgosos para la salud o la seguridad del ser humano, lo cuales no dejan marcas ni toman muestras, además, el contacto para

[3] IBARRA SIXTOS, Alejandro. *Diccionario de física*. p. 560.
[4] MARÍ SAGARRA, Ricard. *El código PBI.* p.145.

ser utilizados es mínimo. El diseño de los dispositivos fue creado para que su utilización sea fácil, son de uso rápido y sencillo.

En la actualidad, las aplicaciones para autenticación personal utilizan números personales de identificación o tarjetas personales, los que no cuentan con un nivel alto de seguridad, debido a que estos pueden ser utilizados por otras personas a diferencia de los datos que se almacenan de forma biométrica, debido a que estos son datos específicos únicos de cada individuo, los cuales son personales.

La forma de identificación por estos medios brinda un control más eficaz y exacto de los individuos, con el cual se puede identificar al usuario con un elevado grado de eficacia a la persona que hace uso de un dispositivo biométrico, esto difiere de otros métodos como los son las claves, la firma o el código de barras.

Este modelo de reconocimiento brinda un registro real en lo relacionado a la identificación de un individuo, reduciendo de esta forma la posibilidad que alguien que no tenga una autorización de ingresar a cierto lugar lo haga, y, de esta forma se eliminan los posibles fraudes por suplantación.

La implementación de avances biométricos y electrónicos ha permitido el desarrollo de tecnologías avanzadas que permiten una mejor identificación de forma biométrica.

Mucho de los avances en la biometría se han implementado en las distintas áreas de la industria, las cuales han resultado en una mejor forma de identificar al personal y en distintos casos se ha utilizado en distintos tipos de instituciones, como las instructivas, en las que ha logrado autenticar, identificar y mantener un mejor control de los individuos que se localizan dentro de este entorno. Esta

tecnología es el inicio de un conjunto de alternativas que ayudan a la verificación del personal y en la utilización de aplicaciones que necesitan de un grado alto de seguridad.

Distintas aplicaciones de este tipo son utilizadas para proporcionar la seguridad en relación con la confidencialidad y la privacidad de las transacciones financieras. Este tipo de tecnología tiene infinitas utilidades en distintos sectores de la sociedad, como en los comercios, centros educativos, instituciones gubernamentales, entre muchos otros sectores.

3.2. Tipos de tecnología biométrica

La tecnología biométrica se basa en las características físicas y el comportamiento de los individuos, debido a ello se pueden establecer dos tipos de tecnología biométrica, las cuales se mencionan a continuación:

3.2.1. Biometría estática

Este tipo de biometría es basada en la toma de medidas directamente de un individuo para luego ser utilizadas como parte de este sistema, entre estas se encuentran: “las huellas digitales, la geometría de la mano, el análisis del iris o de la retina y el reconocimiento facial, el ADN, entre otros.”[5]

[5] FARRIOLS I SOLÁ, *Antoni. La protección de datos de carácter personal en los centros de trabajo.* p. 26.

3.2.2. Biometría dinámica

Con esta se mide el comportamiento de quién lo utilizará, son mecanismos que se dirigen a reconocer o autentificar al individuo relacionado con su comportamiento, tomando en cuenta la forma de articular, los movimientos y como se relaciona con el sistema y la forma de reconocimiento, entre ellas se encuentran los siguientes:

- “Patrón de voz.
- Firma manuscrita o verificación de escritura.
- Dinámica del tecleo.
- Análisis gestual, entre otros.”[6]

3.3. Almacenamiento de un registro biométrico

Estos dispositivos almacenan los datos de los individuos, ya sean dinámicos o estáticos, convirtiendo los datos almacenados en patrones que serán utilizados como medios de identificación en el momento que sea requerido, este procedimiento se divide en:

3.3.1. Sumisión

Este es el procedimiento por medio del cual se obtienen los datos requeridos del individuo que los utilizará, estos se obtienen dependiendo del tipo de técnica biométrica que se utilice. Si es utilizado el método de reconocimiento facial, se considera cuando el individuo ve de forma directa a la cámara y si se

[6] PRESSMAN, Roger S. *Ingeniería del software: Un enfoque práctico*. p. 174.

utiliza la huella digital, es por medio de la colocación del dedo en el aparato receptor de la huella.

3.3.2. Registro

Este es el procedimiento por medio del que se obtiene el modelo o tipos para ser evaluados y guardados continuando con el procedimiento del sistema biométrico, el cual radica en el establecimiento de la relación entre los datos obtenidos del individuo y los necesarios de identificación. Lo que quiere decir que se relaciona el modelo que se obtuvo con un tipo de clave de identificación de propietario de la muestra. Entre los ejemplos se puede mencionar la verificación de la huella dactilar, el reconocimiento del iris o un código de identificación único de quien se le fue tomada la muestra inicial.

3.3.3. Dispositivo de captura

El programa o hardware utilizado para tomar los modelos biométricos. Entre los dispositivos que se utilizan para la captura de datos biométricos, se encuentran los siguientes:

- Reconocimiento de la huella digital. Periférico de escritorio, ratón, chip o lector integrado en el teclado. Puede ser óptico o capacitivo.
- Reconocimiento de la voz. Micrófono o teléfono.
- Reconocimiento facial. Cámara digital.
- Lectura del iris. Cámara de vídeo de infrarrojos integrada en la computadora y otros tipos de cámaras digitales aptas para realizar esta tarea.
- Lector de la firma. Bolígrafo perceptible al movimiento. pantalla perceptible al movimiento.
- Identificación de la manera de escribir en el teclado. Localizado en dispositivo electrónico.[7]

[7] SERRATOSA, Francesc. *Biometría.* p. 74.

3.4. Términos utilizados en tecnología biométrica

A continuación, se presentan algunos términos relacionados con la tecnología biométrica:

3.4.1. Muestra biométrica

Radica en la recopilación de características físicas o de la conducta establecida en la fase de sumisión que es utilizada para la generación de los modelos biométricos. El cuadro siguiente muestra los tipos de modelos relacionados con las tecnologías biométricas que existen.

Tabla V. **Muestras biométricas**

Tecnología biométrica	Clase de muestra
Identificación por huella dactilar	Modelo de la huella dactilar
Identificación por voz	Modelo de la voz en grabación digital
Identificación del rostro	Modelo digital del rostro
Identificación de la geometría de la mano	Modelo digital de la mano en 3D
Identificación de la firma	Modelo de la firma y los movimientos de esta gravados
Identificación de los datos biométriícos del teclado	Modelo de los carateres que utiliza el individuo relacionadas normalmente secuencias y tiempo

Fuente: elaboración propia, empleando Word.

3.4.2. Extracción de las características

Es el procedimiento en el cual se almacenan y codifican los caracteres individuales que serán el patrón biométrico, cuyo objetivo es crear un modelo de registro. La forma de extraer estas se realiza por medio de imágenes y de tipos que se procesan para tener los datos fiables y precisos.

Como ejemplo se puede mencionar la identificación por voz, con la que se puede filtrar ciertas frecuencias y rasgos característicos y con la identificación de la huella se pueden extraer los rasgos hasta los patrones más pequeños que no se alcanzan a reconocer a simple vista.

Además, si el modelo no es extraído de una forma adecuada para contar con las características fidedignas, el mismo sistema indicara al individuo que proporcione otra prueba. Los caracteres más recurrentes utilizados para este proceso son las que a continuación se describen:

- Reconocimiento de la huella digital. Localización y dirección del comienzo y fin de los arcos y bifurcaciones de la huella digital.
- Reconocimiento de la voz. Frecuencia, cadencia y duración del patrón de voz.
- Reconocimiento de la cara. Posición relativa y forma de la nariz, posición de las mejillas.
- Reconocimiento del iris. Forma del iris.
- Reconocimiento de la retina. Forma de los capilares de la retina.
- Reconocimiento de la mano. Alto y ancho de los dedos y juntas entre los dedos y la mano.
- Reconocimiento de la firma. Rapidez, fuerza, presión y apariencia de la firma.
- Reconocimiento de la escritura en el teclado. Secuencia del tecleo, duración entre caracteres.[8]

[8] MURIAS RIGUAL, Marta. *Estudio de adaptación de un sistema de reconocimiento biométrico en ATMs.* p. 41.

3.4.3. El patrón

Se refiere a un archivo relativamente diminuto en el cual se almacenan las características de los patrones obtenidos del individuo, con las cuales se dará el reconocimiento en el proceso biométrico de autenticación. Este es creado a través de un complicado procedimiento algorítmico que convierte las distintas características muestrales.

Este concepto es uno de los componentes primordiales que establecen la tecnología biométrica, pese a que no todos los procedimientos biométricos necesitan patrones para establecer los procesos comparativos, debido a que algún método de identificación por voz usa el modelo original para efectuar la comparación biométrica. Los patrones dependen del momento que fueron creados, ya que pueden ser para verificación o registro.

- Patrones de registro. Se crean en la primera interacción del usuario con el sistema biométrico, y se almacenan para ser utilizados en futuras comparaciones.
- Patrones de verificación. Se generan durante los siguientes intentos de verificación, al comparar la característica con la almacenada en el patrón.[9]

Pueden ser utilizadas varias muestras para la generación de los patrones de registro, por ejemplo, para el reconocimiento facial, se debe utilizar distintas imágenes del rostro para poder crear el patrón de registro. Mientras que para el patrón de verificación se realiza una muestra única. Este tipo de patrones puede ser comparado con el patrón de registro y así establecer el nivel de similitud.

Cualquier tipo de patrón puede ser utilizado solamente para un tipo de tecnología fabricado por una empresa, lo que indica que una empresa distinta a

[9] ROMERO CASTRO, Martha Irene; et al. *Introducción a la seguridad informática y el análisis de vulnerabilidades.* p. 54.

la que tomo las muestras originales no puede hacer uso de los patrones establecidos.

3.5. Proceso para la autenticación

Anteriormente se ha hecho referencia a lo que es el almacenamiento del registro biométrico, y aquí se describe lo referente al proceso de autenticación, lo que en resumen se refiera a la comparación de los registros que fueron guardados de los datos que fueron obtenidos para ser utilizados por el sistema biométrico.

Aunque el proceso de cada tecnología biométrica es diferente, debido a que en cada una los pasos son específicos para ellas, existen algunos que son comunes para los diferentes modelos de autenticación, como lo son:

- Adquisición o Captura. Lectura de las muestras del usuario a verificar expone.
- Extracción. Obtención de ciertas características de la muestra.
- Comparación. Se cogen las muestras las muestras actuales del usuario y se busca una relación con el registro almacenado en la base de datos.
- Decisión. Se analiza si el usuario es válido o no.[10]

3.6. Arquitectura de los sistemas biométricos

En un sistema biométrico, la arquitectura se refiere principalmente a sus componentes, lo que se puede indicar que son los patrones establecidos para el funcionamiento, como se hace referencia a continuación:

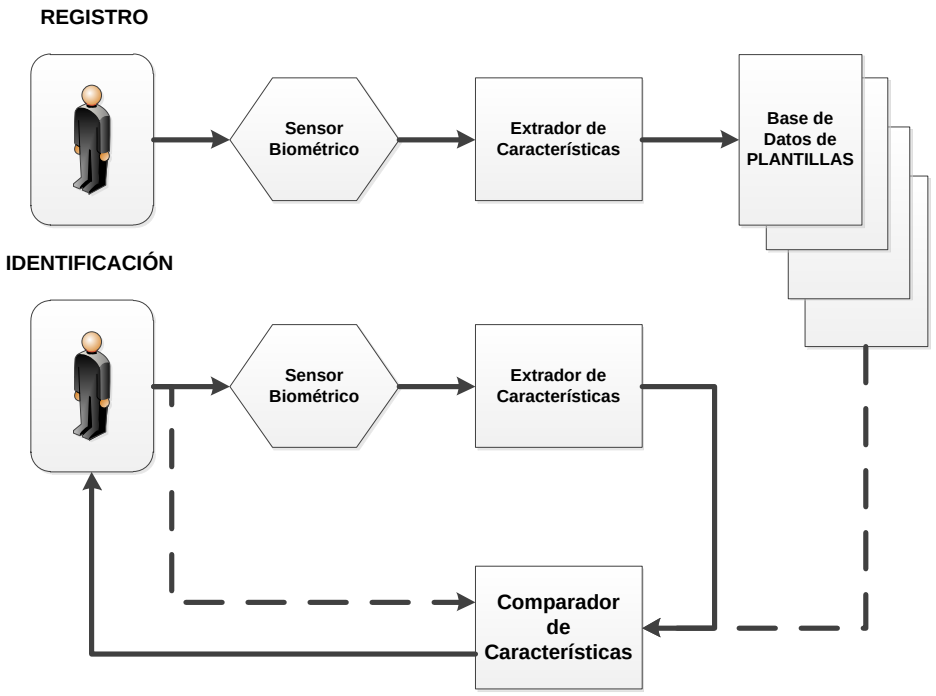
- Se obtiene un modelo por medio del manejo de sensores.

[10] ROMERO CASTRO, Martha Irene; et al. *Introducción a la seguridad informática y el análisis de vulnerabilidades.* p. 57.

- genera una representación al ingreso del sistema por medio de un algoritmo Se para extraer las características.
- Se decide basándose en el modelo de ingreso y el patrón que previamente fue ingresado al sistema.

A continuación, se ilustra la arquitectura del sistema biométrico.

Figura 7. **Arquitectura de un sistema biométrico**



Fuente: TAPIADOR MATEOS, Marino; SIGÜENZA PIZARRO, Juan Alberto. *Tecnologías biométricas aplicadas a la seguridad.* p. 122.

En este tipo de sistema consta de dos elementos, el registro y la autenticación.

El módulo de registro se relaciona con la identidad de los individuos que se encuentren registrados en el e sistema por medio de los datos biométricos previamente obtenidos. Registradas con representaciones de su medida biométrica. En el momento que el sistema recibe la señal biométrica, reconoce el nombre del usuario, por vía de las características personales del individuo, las cuales se guardan en la base de datos del sistema.

Luego, por medio del dispositivo se autentifica la identificación del individuo que pretende ingresar al sistema, este requiere ser identificado al presentar sus características ante el sistema por medio del sensor biométrico, el cual al extraer la característica registrada la compara con los datos almacenados para poder comprobar la identidad del individuo, por medio de este método se especifica si la identificación es la almacenada para poder dar acceso al usuario.

3.7. Biometría del tecleo

Este pertenece a la biometría dinámica, el cual se basa en elementos que no son rígidos, que se relacionan a los movimientos y forma de comportarse del individuo. El medio principal de un individuo con un ordenador es el teclado, también existen otros como el mouse, los dispositivos de audio y de video, pese a todos estos medios de relación con el computador la mayor interacción proviene del teclado, el cual es un componente del sistema operativo del equipo que predeterminado en los computadores. Los cual es una ventaja primordial para un sistema de seguridad en el ciberespacio.

De esta forma es como existe esta rama de la biometría, la que se dedica al reconocer los patrones relacionados con la forma de teclear del individuo, la que se enfoca en los métodos necesarios para la identificación de la regularidad de teclear de un individuo en un ordenador.

El método de teclear es un procedimiento complicado y que repercute en el aspecto físico, es una capacidad que se origina de la dinámica del cerebro, desde este se generan los estímulos que se necesitan y que realizan la transmisión en el sistema nervioso hasta los músculos, los cuales realizan los movimientos para realizar los tecleos en un computador, en dicha acción se plasma la información que el cerebro procesa en cierto momento.

Para esta tecnología no es necesario contar con un hardware extra para realizar el muestreo de los patrones, lo que lo hace perfecto para las aplicaciones relacionadas con los medios digitales.

3.7.1. El muestreo

En la biometría del tecleo, para realizar el procedimiento de extracción de las muestras para validación se utiliza una medición de tiempos sobre las distintas pulsaciones sobre la forma de teclear del individuo, aunque este cálculo es independiente a la velocidad del microprocesador del computador. Entre las distintas formas de sacar las muestras sobre el tecleo se encuentran:

- Con tiempo. El muestreo con tiempo utiliza un reloj para obtener la medición entre cada pulsación y analizar la distancia entre cada dedo. Normalmente, la mayor precisión que nos dará el lenguaje que estemos utilizando será como mucho de centésimas de segundo.
- Con ciclos máquina con chequeo constante. Estas son las frecuencias más influyentes de muestreo que se logran obtener en un computador, al hacer uso de estas frecuencias se pueden conseguir mediciones con altas precisiones entre dos pulsaciones de teclas en una situación común de tecleo. Con el persistente monitoreo agregan ciclos mientras en ese tiempo el buffer de tecleo esté vacío.
- Con ciclos máquina con tiros de evento. Típicamente esta técnica usa programación multithread para con una pulsación de tecla arrancar un thread contador que acumula ciclos máquina hasta que, de forma asíncrona, y sin chequear constantemente el buffer de teclado, se para cuándo lo corta otro por haberse producido un evento de pulsación de tecla.[11]

[11] CARRETERO, Jesús; GARCÍA-CARBALLEIRA, Félix; PÉREZ Fernando. *Prácticas de sistemas operativos.* p. 164.

3.8. Verificación de escritura

La firma no es una característica biométrica, se encuentra dentro de la biométrica dinámica. El fin de esta no es realizar una interpretación de lo que el individuo escribe, busca autenticar las características de esta basado en los rasgos obtenidos previamente.

Además de la forma en que se firmar, en estos modelos son utilizados las características dinámicas como: “el ángulo, el tiempo empleado el desarrollo de la firma, las separaciones del bolígrafo del papel.”[12]

3.8.1. Muestra

Para que pueda ser utilizado un sistema de autenticación respaldado en las firmas se le requiere a quien lo utilizará, primero, cierta cantidad de firmas, de las cuales el software toma y guarda algunas de estas características, a lo cual se le llama etapa de aprendizaje, en la cual el obstáculo más recurrente se refiere a que las personas no firman exactamente igual cada vez que lo realizan.

Cuando el sistema ya ha reconocido las firmas de los individuos y estos quieren acceder, se les pide que realicen esta, con cierta cantidad de intentos para poder acceder. Esta firma introducida a través de un lápiz que cuenta con un receptor óptico o por dispositivos que cuenta con un sensor lector sensible, en ocasión se utilizan los dos, luego el sistema compara con las rúbricas almacenadas en el artefacto inteligente y luego de ser verificadas, establecida como autentica, se puede ingresar.

[12] MARTÍN RAMOS, Rafael. *Documentoscopía: Método para el peritaje científico de documentos.* p. 367.

3.9. Corroboración de plantillas oculares

Los modelos fundamentados en los patrones del ojo, visuales, se clasifican en dos técnicas diferentes: el análisis de patrones de retina y el análisis de patrones del iris.

Este tipo de tecnología representa una desventaja para los usuarios, debido a que consideran incomodo colocar sus ojos ante un binocular o un monóculo, lo cual se hace necesario para este tipo de receptor, además muchos consideran que esta tecnología revela alguna enfermedad médica o el consumo de drogas y alcohol, lo cual pretende este tipo de usuarios mantener en secreto.

Este tipo de tecnología no está en las posibilidades de cualquier empresa o persona particular, lo que resulta que no es de fácil adquisición, esto es una desventaja y el procedimiento de recolección de los datos oculares no es tan rápido como en otros sistemas, sobre todos cuando existen grandes poblaciones dentro de las empresas en las que desea implementar este sistema, por lo cual esto limita su utilización, principalmente a órganos, generalmente de los gobiernos, los que requieren una grado alto de seguridad.

3.9.1. Iris

El reconocimiento del iris, como tecnología, es basada en el análisis de la pupila, específicamente en la parte más colorida del ojo, este análisis es menos asequible a los sistemas biométricos del ojo, ya que este no utiliza los elementos convencionales como una cámara digital, además que no es necesario el contacto entre el lector y el individuo.

Entre la lectura del iris y la de la huella dactilar existen similitudes como su forma en la cual no se transforma, no cambia de color ni de apariencia, el iris no puede ser alterado de ninguna forma.

El objeto del reconocimiento de este es la extracción de las muestras a través de tecnología con un grado alto de seguridad y confiabilidad para la verificación de un individuo, utilizando un ejemplar matemático aleatorio el cual identifica el patrón del ojo a determinada distancia.

El iris como órgano interno del cuerpo humano se encuentra protegido con una membrana que lo hace inmune a las alteraciones del medio ambiente, por lo cual este es una clave propia de cada individuo la cual no debe ser recordada, siempre mantendrá sus características.

Este solo se ve afectados ante las alteraciones que provoca la luz. Estas deformaciones relacionadas con la dilatación y contracción se corrigen de forma rápida y permite el dispositivo de reconocimiento detectar los bordes del iris y con ello reconocer este de forma confiable.

3.9.2. Retina

La biometría de la retina se apoya en el análisis de los vasos del ojo que se encuentran en la parte de atrás del ojo. Esta tecnología comprende: “el usar una fuente de luz de baja intensidad a través de un dispositivo óptico para examinar los modelos únicos de la retina.”[13]

Como en el sistema de reconocimiento del iris, en este sistema se utiliza un binocular ajustando la distancia del ojo y la cabeza para luego oprimir un botón

[13] THIEMAN, William J.; PALLADINO, Michael A. *Introducción a la biotecnología.* p. 279.

para que el sistema reciba la orden de realizar el análisis. Posterior a la pulsación el dispositivo realiza un escaneo de la retina por medio de una luz infrarroja de intensidad baja en forma de espiral, detectando los patrones establecidos para el reconocimiento, al aceptar el sistema la verificación de la retina procede a dar acceso al individuo.

3.10. Geometría de la mano

La tecnología de verificación de la forma de la mano radica en analizar las medidas y los rasgos característicos de la mano. Este sistema es útil en donde existen muchos usuarios o en donde las personas ingresan a este con frecuencia.

Este método consiste en un tipo de lector que cuenta con unos sensores tipo alfiler, en el cual la persona coloca la mano sobre el lector y este mide el grueso y largo de los dedos, además de la distancia entre estos, con esto crea algoritmo que es único y se almacena en una banda similar a las de tarjetas de crédito. Se debe colocar la mano directamente sobre los lectores, como se muestra a continuación. Este método es de fácil uso, aunque en ocasiones presenta lectura errónea si la mano no es colocada en la forma establecida.

Figura 8. **Lector biométrico para geometría de la mano**

Fuente: GÓMEZ VIEITES, Álvaro. *Seguridad en equipos informáticos.* p. 128.

Es almacenada la captura del contorno de la mano de forma tridimensional, el lector corrobora la mano colocada en el dispositivo y busca una relación con una muestra que se encuentra almacenada en la base del sistema, ignorando los elementos ajenos a la palma de esta, luego emite una señal que indica que el usuario si es quien solicita la autorización.

3.11. Reconocimiento de voz

La tecnología de reconocimiento de voz tiende a confundirse con las aplicaciones que reconocen las palabras o las que reciben comandos de voz, los que existen integrados dentro de los softwares de las computadoras. Estos programas no pertenecen al sistema biométrico, ya que no representan ningún grado de seguridad solo reconoce las palabras que emite la persona que lo utiliza independientemente de quien sea el usuario original.

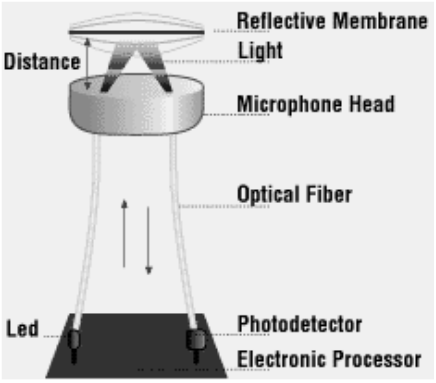
En los sistemas de seguridad por medio de reconocer de voz el usuario, se identifican los patrones característicos de quien será el que lo utilice. Para realizar el reconocimiento a través de este tipo debe realizar una grabación digital y almacenarla en la nube de datos del programa, para que en el instante que el receptor reciba la voz de la persona y la verifique se le dé acceso.

3.11.1. Sensores de verificación de voz

En estos tipos se encuentran “los actuadores ópticos unidireccionales, por lo que actúan del siguiente modo: un diodo emisor de luz se encuentra sobre una membrana reflectora, por medio de fibra óptica.”[14] Cuando se produce el sonido y las ondas se reflejan en la membrana, se produce una vibración, realizando la transformación como se indica en la figura 9.

[14] PRABHAKAR, Salil; ARUN A. Ross. *Biometric technology for human identification*. p. 70.

Figura 9. **Micrófono óptico**



Fuente: PRABHAKAR, Salil; ARUN, Ross. *Biometric technology for human identification*. p. 71.

Es registrada la luz por medio del reflejo recibido por un fotodetector que aunado a la electrónica se procesan las ondas para obtener un modelo confiable del sonido a identificar.

3.12. Utilización de la tecnología biométrica

La investigación biométrica se originó por la necesidad del ejército de aumentar los controles de defensa, utilizando escáneres infrarrojos diseñados para detectar intrusos en los alrededores del perímetro de ciertas zonas militares.

En la actualidad ha sido desarrolladas aplicaciones en el sector privado para controlar los accesos a los trabajadores o colaboradores a los ordenadores personales, a la red y a los teléfonos móviles, entre otros. Algunas de estas aplicaciones utilizadas para realizar los controles biométricos son:

- Control de accesos físicos.
- Comercio electrónico.
- Organizaciones de salud público y privado.
- Prototipos bancarios físicos y electrónicos.
- Monitoreo y control de personal laboral.

- Acceso a redes de telecomunicación.
- Modelos electorales.
- Acceso a información personal.
- Autorización a la utilización de datos personales.
- Aeropuertos.
- Industria en general.[15]

La forma de acceder a las computadoras personales es de las aplicaciones más utilizadas para el reconocimiento biométrico. Las empresas que ofrecen este tipo de sistemas tienen muchas opciones desarrolladas para proteger los ordenadores, lo más factible es cargar un programa de reconocimiento del lector, conectar este y ya se puede acceder a este sistema, estos son muy parecidos al mouse que se utilizan e incluso vienen integrados al teclado.

3.13. Huella digital

El tipo de sistema por verificación de huella dactilar es parte de la biometría estática y se fundamenta en la verificación de la huella dactilar de las personas, la funcionalidad del reconocimiento dactilar se concentra en:

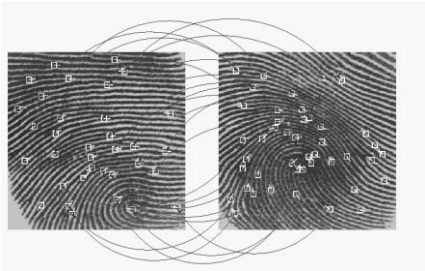
> Capturar una muestra (imagen) de la huella dactilar y a través de algoritmos complejos se reduce la muestra (imagen) a una representación matemática llamada comúnmente plantilla. Ésta se almacena en una base de datos asociada a un número o clave de identificación personal.[16]

La huella digital es la presentación de la piel de los dedos de la mano. Cuenta con una serie de líneas en las yemas de los dedos las que se enlazan o termina de forma repentina. “Los puntos donde las líneas terminan o se bifurcan se conocen técnicamente como minucias.”[17]

[15] AGUILERA, Purificación. *Seguridad informática*. p. 136.
[16] TAPIADOR MATEOS, Marino; SIGÜENZA PIZARRO, Juan Alberto. *Tecnologías biométricas aplicadas a la seguridad.* p. 184.
[17] FERRO VEIGA, José Manuel. *Técnicas de investigación en investigación privada.* p 283.

Si cuando las huellas dactilares no coinciden con la persona, se inicia un proceso que inicia con la clasificación de esta y culmina con la comparación de las minucias entre ambas huellas. En la figura que se muestra a continuación se ejemplifica el procedimiento comparativo en los modelos de las huellas digitales.

Figura 10. **Comparación entre plantillas**



Fuente: SAGARRA, Ricard Marí. *El código PBIP.* p. 154.

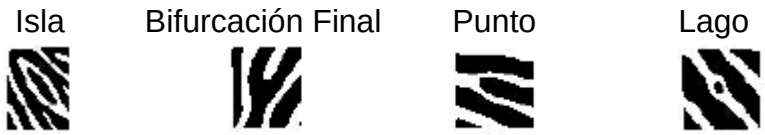
La huella se establece por medio de dos tipos de patrones, los cuales son: “el patrón de crestas y surcos, así como el de detalles.”[18]

3.13.1. Basadas en detalles

Para el desarrollo de esta técnica se realiza un croquis sobre los detalles de la huella dactilar, estos permiten la ubicación segura de una persona. Aunque pueden existir algunas complicaciones cuando es utilizada esta técnica, es dificultoso establecer los detalles de forma precisa cuando la muestra de la huella no es tomada con una calidad alta. En esta no se toma le modelo de los surcos y las crestas. En la figura 11 se muestran algunos de los detalles encontrados en la huella dactilar.

[18] FERRO VEIGA, José Manuel. *Técnicas de investigación en investigación privada.* p. 271.

Figura 11. **Detalles de la huella dactilar**



Fuente: SERNA ARAUJO, Lourdes; MARTÍNEZ UNANUE, Raquel; RODRÍGUEZ ARTACHO, Miguel. *Programación y estructuras de datos avanzadas.* p. 48.

Cada usuario dispone una composición única de peculiaridades, como se presenta en la figura 11, el cual se puede describir por un modelo probabilístico:

"P(C)=P(N).P(M).P(A)

Donde:

P(C) = f (Ley de Poisson)
P(M)= f (frecuencia de aparición del detalle)
P(A) = f (número de permutaciones posibles de detalles)."[19]

3.13.2. Fundamentadas en correlación

Este modelo requiere la localización exacta de una marca de registro, punto que se ve damnificado por el movimiento de la muestra. Al obtenerse la muestra de la huella, se necesita clasificarla. Proceso el cual radica en colocar la huella entre los demás tipos existentes, los que cuentan con un mecanismo ordenado; esto se realiza con el objeto de minimizar el lapso de búsqueda.

[19] VILLEGAS, Hyxia; BOSNAJK Antonio. *Bioingeniería en Venezuela: Tendencias, propuestas y avances. Venezuela*. p. 143.

Los algoritmos que se encuentran ingresados en el programa hacen que pueda ser clasificada las huellas en cinco clases, que son:

- Aro de crestas.
- Lazo derecho e izquierdo.
- Curva o arco.
- Arco de carpa.

> La función estos algoritmos es dividir la cantidad de crestas en diferentes direcciones, específicamente en cuatro (0°, 45°, 90° y 135°) a través de un filtrado de la sección central de la muestra.[20]

Este procedimiento de identificación necesita utilizar técnicas firmes que no sean damnificadas por cierto sonido que interfiera en la muestra, asimismo se ve incrementada la exactitud de este instante.

3.13.3. Tipos de sensores para huella dactilares

Entre estos sensores, existen varios tipos, a continuación, se exponen y se detallan dos modelos de actuadores:

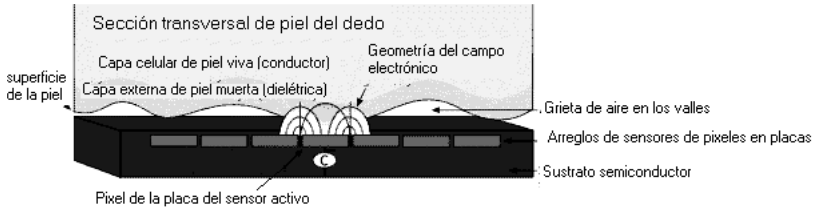
3.13.3.1. Sensor de matriz capacitivo

Sobre el plano de un circuito integrado hecho de silicona se ubican las placas de los sensores capacitivos como se ilustra en la figura que se muestra a continuación.

> La capacitancia en cada píxel del actuador se dimensiona individualmente, colocando una carga determinada sobre el mismo píxel. El voltaje estático producido por esa carga es equitativo a la capacitancia del píxel y de aledaños. Por la forma del dedo, las líneas de flujo producidas desde el actuador (sensor) energizado se excita en el fragmento de piel instantáneamente adyacente a este actuador, concluyendo en actuadores inactivos o en la base.[21]

[20] SIMÓN ZORITA, Danilo. *Reconocimiento automático mediante patrones biométricos de huella dactilar*. p. 106.
[21] ASIS Internacional. *Protección de activos: Seguridad física*. p. 307.

Figura 12. **Actuador de matriz capacitivo**



Fuente: TAPIADOR MATEOS, Marino; SIGÜENZA PIZARRO, Juan Alberto. *Tecnologías biométricas aplicadas a la seguridad.* p.192.

El diseño de este sensor tiene como ventaja que es muy simple y entre las desventajas se encuentra que entre la geometría esférica proveniente del campo eléctrico que es generado por el sensor, se tiene una reacción de solapamiento sobre los píxeles vecinos, lo cual causa que el sector escaneado aumente su tamaño, lo que consecuentemente produce una serie de datos cruzados entre todos los sensores, minimizando de forma considerable la resolución de la imagen.

3.13.3.2. Sensor de matriz antena

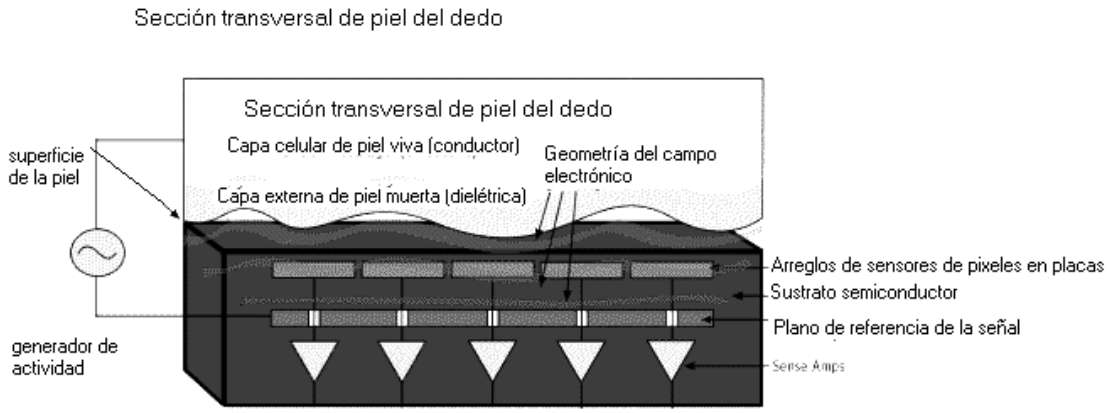
> Un pequeño campo de Radio Frecuencia (RF) es ubicado dentro de dos películas conductoras, una oculta en el interior de un chip de silicón denominado plano de referencia del indicio de estimulación, y la otra localizada por debajo de la piel del dedo.[22]

Esto se ejemplifica en la figura 13. El campo que se forma entre las capas es reproducido de la manera de la capa conductual de la piel en el campo de la corriente alterna, pequeños sensores implantados debajo del plano del semiconductor y por encima de la capa conductora, toman la medida del contorno de este.

[22] TAPIADOR MATEOS, Marino; SIGÜENZA PIZARRO, Juan Alberto. *Tecnologías biométricas aplicadas a la seguridad.* p. 195.

Los amplificadores que se conectan de forma directa a cada placa de este sensor transforman esta potencia generada a voltajes, presentando así el modelo de la huella. Dichas señales se acondicionan en la siguiente fase para ser multiplexadas en el programa.

Figura 13. **Actuador de matriz de antena**



Fuente: TAPIADOR MATEOS, Marino; SIGÜENZA PIZARRO, Juan Alberto. *Tecnologías biométricas aplicadas a la seguridad.* p. 19

4. DESARROLLO DISEÑO DE SISTEMAS DE CONTROL BIOMÉTRICO PARA EL MONITOREO Y CONTROL DE NIÑOS CON SERVICIO DE BUS ESCOLAR EN EL ÁREA METROPOLITANA EN LA CIUDAD DE GUATEMALA

4.1. Descripción del programa

La huella digital de una persona es un modelo muy útil en el sistema de reconocimiento y verificación de usuarios de forma efectiva y segura, debido a que los rasgos de las yemas de los dedos son distintas unas de otras y con patrones que no se repiten en ningún individuo.

La evolución de esta aplicación ha tenido como objetivo controlar el acceso a las personas, siendo estos las monitoras de los buses, profesores y principalmente de alumnos, realizando la identificación utilizando la huella digital. Cada persona se asocia a un código el cual es la identificación la que se le designa código de identificación personal.

Cuando la persona necesita ser autenticada por el sistema, ingresa dicho código, el cual está almacenado en la base del sistema, este es ingresado a través de la colocación de la yema del dedo en el dispositivo biométrico, este extrae la muestra de la yema del dedo y toma además las minucias, las cuales compara con el modelo guardado en la base de datos del sistema, registro que identifica el código de personal de cada individuo. Cuando el modelo no concierne al usuario, este deniega el acceso, almacenando este como un código erróneo para contar con un historial de quienes han ingresado con una identificación que no se encontraba almacenada en la base de datos.

Si los datos almacenados concuerdan con la huella colocada en el sensor, el sistema procede a la autorización de la entrada del individuo, almacenado en la base de datos la fecha y la hora en la que se ha accedido al sistema, con lo cual se generan reportes para tener un monitoreo sobre los movimientos de quienes ingresan al sistema.

El procedimiento relacionado con el almacenaje del modelo de las huellas digitales de las personas se efectúa utilizando un algoritmo creado por la empresa que fabrica el sensor, requiriendo extraer cuatro muestras de esta y posteriormente el sistema aplica procesos matemáticos y estadísticos con los que es generado un modelo que es asociado a código de identificación de cada persona.

Al ser un modelo para ser utilizado en instituciones educativas y en servicios de bus escolar, con énfasis dentro de los buses escolares luego que ingrese el usuario al transporte escolar y coloque su huella digital dejando un registro en la base de datos, existirá un súper usuario o usuario encargado que pondrá una confirmación a través de su huella digital que el usuario en este caso el alumno si se ingresó al transporte escolar esto para evitar algún inconveniente con algún usuario. Es decir, luego de que el alumno registre su huella el sistema le pedirá ingresar una huella más para completar el proceso y esta huella será la del súper usuario que es la que dará la confirmación de que el usuario ingreso o egreso correctamente.

4.2. Requerimientos de hardware y software

- Lector: el lector utilizado para la captura de la huella digital es Suprema BioMini Plus 2 de Digital Persona, véase figura 14. El sensor y lector de huella digital BioMini Plus 2 ha sido creado para proporcionar con un alto grado de seguridad biométrica, posee la certificación del FBI-PIV & STQC.

Figura 14. **Lector biométrico Suprema BioMini Plus 2**

Fuente: Kimaldi. *Lector.* https://www.kimaldi.com/. Consulta: 12 de mayo de 2020

Además del lector se utilizará lo siguiente:

- Procesador CORE i5-9400F
- 9 GB RAM
- Puerto USB
- Sistema operativo:
- Windows 10

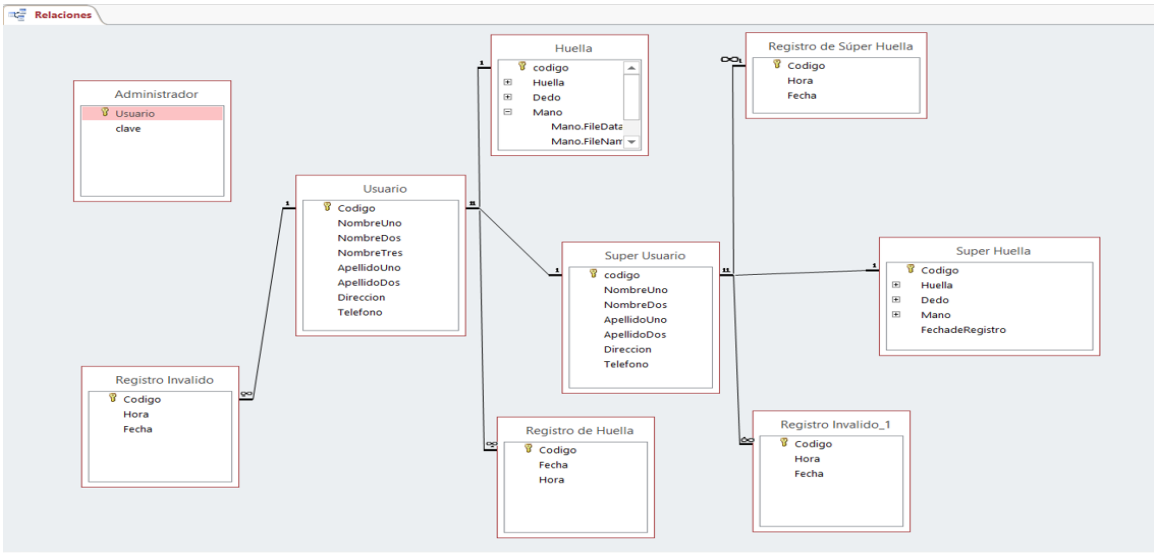
4.3. Análisis y diseño de la aplicación

El diseño de la aplicación se realizó por varias etapas.

4.3.1. Modelo entidad-relación

En la figura 15, se ilustra la manera la cual se relacionan en el programa la identidad de las personas, usuarios, a través del administrador de datos, en los cuales se presentan la información, datos, a ingresar como el código, hora y fecha de ingreso, registro de la huella y el nombre del usuario.

Figura 15. **Modelo entidad relación de la aplicación**



Fuente: elaboración propia, empleando Access.

4.3.2. Descripción de las tablas utilizadas

- Usuario. Es utilizado para el almacenamiento de los datos de cada persona que utilizará el sistema.

Tabla VI. **Datos del usuario**

Campo	Caracterización
Código	Código único de identidad de cada individuo, usuario
01Nombre	Registra el primer nombre del individuo
02Nombre	Registra el segundo nombre del usuario
03Nombre	Si posee, registra el tercer nombre del usuario
01Apellido	Registra el primer apellido del usuario
02Apellido	Registra el segundo apellido del usuario
Teléfono	Registra el teléfono del usuario
Dirección	Registra la dirección del usuario

Fuente: elaboración propia, empleando Word.

.

Huella dactilar, es registrada, almacenada y afiliada con el código de identidad del usuario.

Tabla VII. **Registro y almacenamiento de huella**

Campo	Caracterización
Código	Codificación de la identificación personal del usuario
Huella	Se toman cuatro muestras y se almacena el patrón de la huella de la persona
Dedo	Se guarda el código del dedo seleccionado para utilizar con el sensor

Continuación de tabla VII.

Mano	Se almacena el código de la mano a utilizar
DateRegistro	Se guarda en el sistema la fecha de almacenamiento de la huella

Fuente: elaboración propia, empleando Word.

- Registro Huella. Con este se establece un historial que acece a las personas que ingresarán al sistema.

Tabla VIII. **Registro de huella**

Campo	Caracterización
Fecha	Es almacenada la fecha de registro de las personas
Hora	Se almacena en el sistema la hora del registro de cada persona
Código	Codificación de la identificación personal de cada persona

Fuente: elaboración propia, empleando Word.

- Registro Invalido. Este establece un registro del historial de las personas que intentaron ingresar al sistema y no contaban con un registro válido.

Tabla IX. **Registro invalido**

Campo	Caracterización
Hora	Se guarda en el sistema la hora del intento de acceso
Fecha	Se guarda la fecha de del intento de acceso
Código	Codificación de la identificación personal de cada persona

Fuente: elaboración propia, empleando Word.

- Administrador. Este es quién guarda en el sistema los registros de cada persona, la clave de registro de huella y emite reportes.

Tabla X. **Administrador**

Campo	Caracterización
Login	Persona con autorización para acceder con datos registrados
Password	Clave del administrador almacenada en el sistema

Fuente: elaboración propia, empleando Word.

- Súper usuario. Este es el usuario que confirma la validación de un usuario.

Tabla XI. **Súper usuario**

Campo	Caracterización
Código	Codificación de la identificación personal del súper usuario
Huella	Se toman cuatro muestras y se almacena el patrón de la huella de la persona
Dedo	Se guarda el código del dedo seleccionado para utilizar con el sensor
Mano	Se almacena el código de la mano a utilizar
DateRegistro	Se guarda en el sistema la fecha de almacenamiento de la huella

Fuente: elaboración propia, empleando Word.

4.3.3. Codificación de las manos y los dedos

Para poder implementar el sistema se deben de establecer algunos códigos especiales para poder ingresar las huellas de los usuarios. Tanto la mano como

el dedo de la huella digital la cual fue asociada al sistema es almacenada en base de datos del sistema, codificado de la siguiente manera:

Tabla XII. **Códigos para las manos**

Caracterización	Código
Izquierda	1
Derecha	0

Fuente: elaboración propia, empleando Word.

Tabla XIII. **Códigos para los dedos**

Descripción	Código
Meñique	4
Anular	3
Medio	2
Índice	1
Pulgar	0

Fuente: elaboración propia, empleando Word.

4.3.4. Descripción de los algoritmos y diagramas de flujo

Los algoritmos que se utilizan en este sistema se describen a continuación.

4.3.4.1. Registro de usuarios

Este es la llave para ingresar al sistema, por medio de un algoritmo que establece el código de cada persona, cuando la codificación es inexistente, el

sistema indicará el error para luego almacenar esta información para llevar el registro de usuarios erróneos, ver la figura 16.

Procedimiento Registro_de_Usuario

Código ← Ingresar_Código

Busqueda_código (Código)

Si existe código:

Adquirir (1Nombre, 2Nombre, 3Nombre, 1Apellido, 2Apellido, teléfono, dirección)

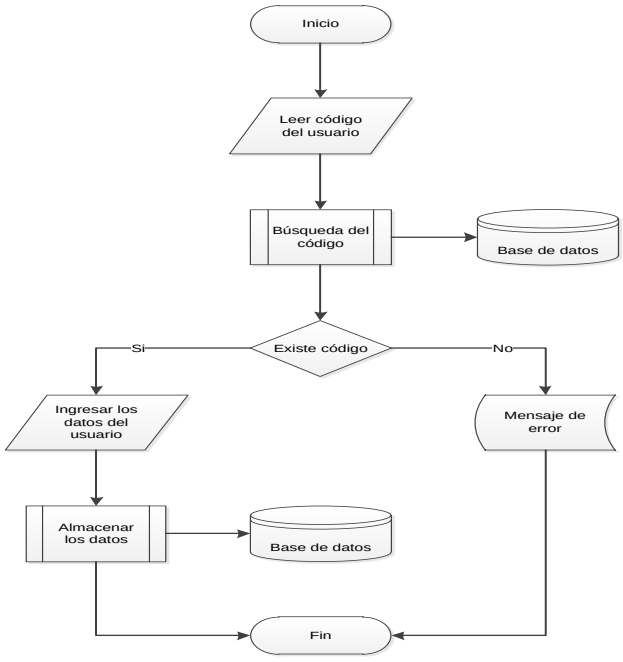
Abrir_Tabla (Usuario)

Almacenar_Datos

Si no existe código: Mostrar_Mensaje_Error

Fin Procedimiento Registro_Usuario

Figura 16. **Diagrama de flujo de registro de usuarios**



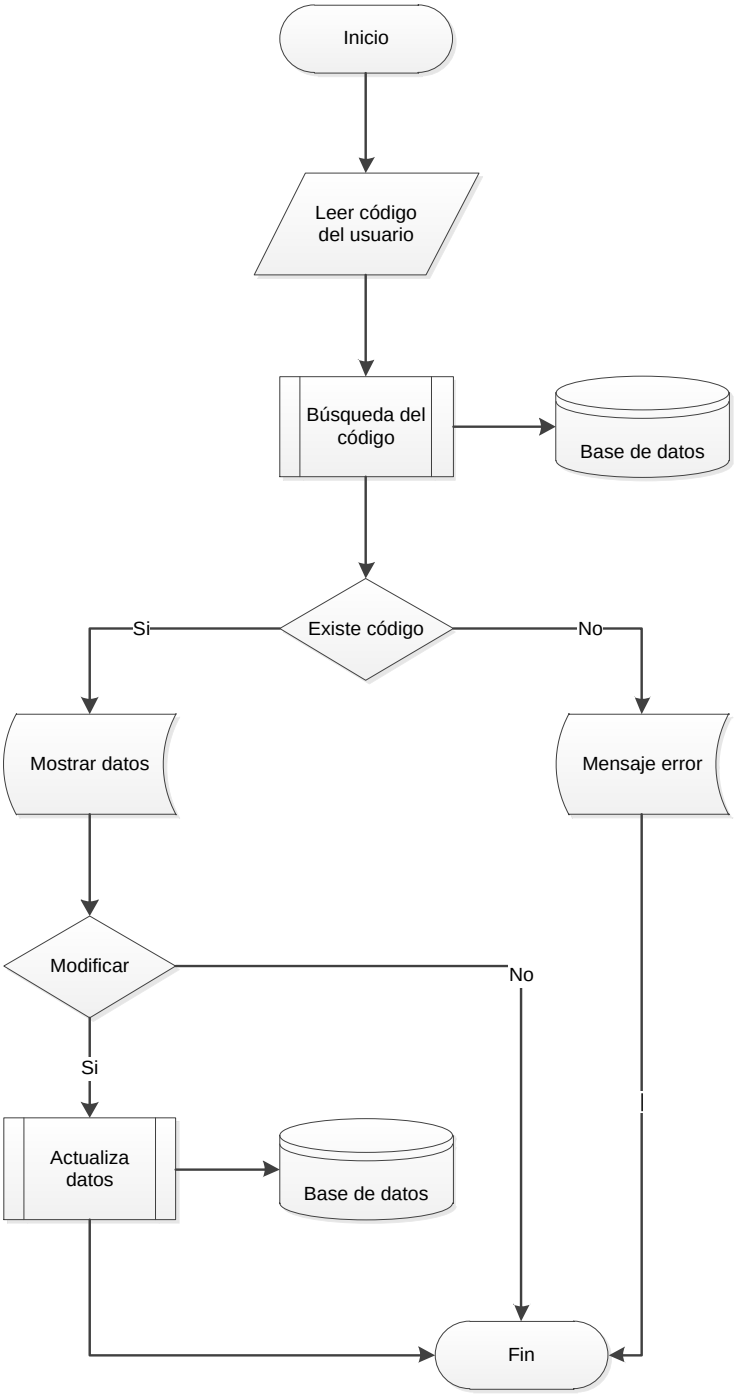
Fuente: elaboración propia, empleando Lucidchart.

4.3.4.2. Cambio de datos de usuarios

Para poder realizar modificaciones es necesario que el sistema establezca un algoritmo utilizando el código de la persona, ver figura 17.

```
Procedimiento Modifica _ Usuario
    Código ← Ingresar_Código
    Abrir_Tabla (Usuario)
        Busqueda_código (Código)
    Si existe código:
    Adquirir (1Nombre, 2Nombre, 3Nombre, 1Apellido, 2Apellido, Teléfono,
    Dirección)
    Actualizar_Datos
    Si no existe código:
        Mostrar_Mensaje_Error
Fin Procedimiento Modificar_Usuario
```

Figura 17. **Diagrama de flujo de cambio de usuarios**



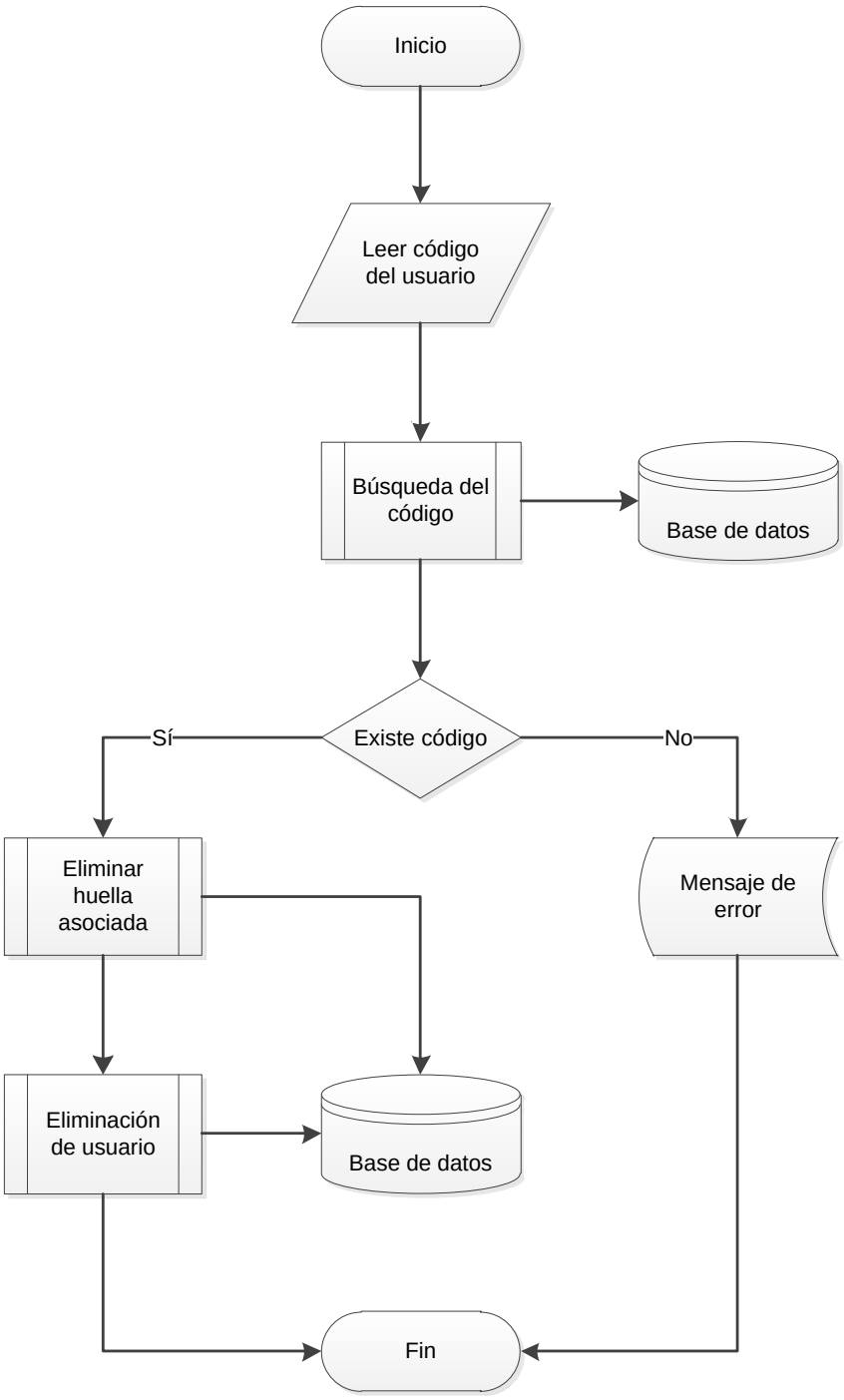
Fuente: elaboración propia, empleando Lucidchart.

4.3.4.3. Eliminación de usuarios

Para poder eliminar a una persona del sistema se debe utilizar la clave personal para acceder al sistema, de esta forma se eliminará el registro de la huella almacenada, ver figura 18.

```
Procedimiento Eliminar _ Usuario
    Código ← Ingresar_Código
    Abrir_Tablas (Usuario, Huella)
        Busqueda_código (Código)
    Si existe código:
    Buscar_huella (código)
    Si existe_huella
        Eliminar_huella
    Eliminar_Usuario
    Si no existe código:
        Mostrar_Mensaje_Error
Fin Procedimiento Eliminar_Usuario
```

Figura 18. **Diagrama de flujo de eliminación de usuarios**



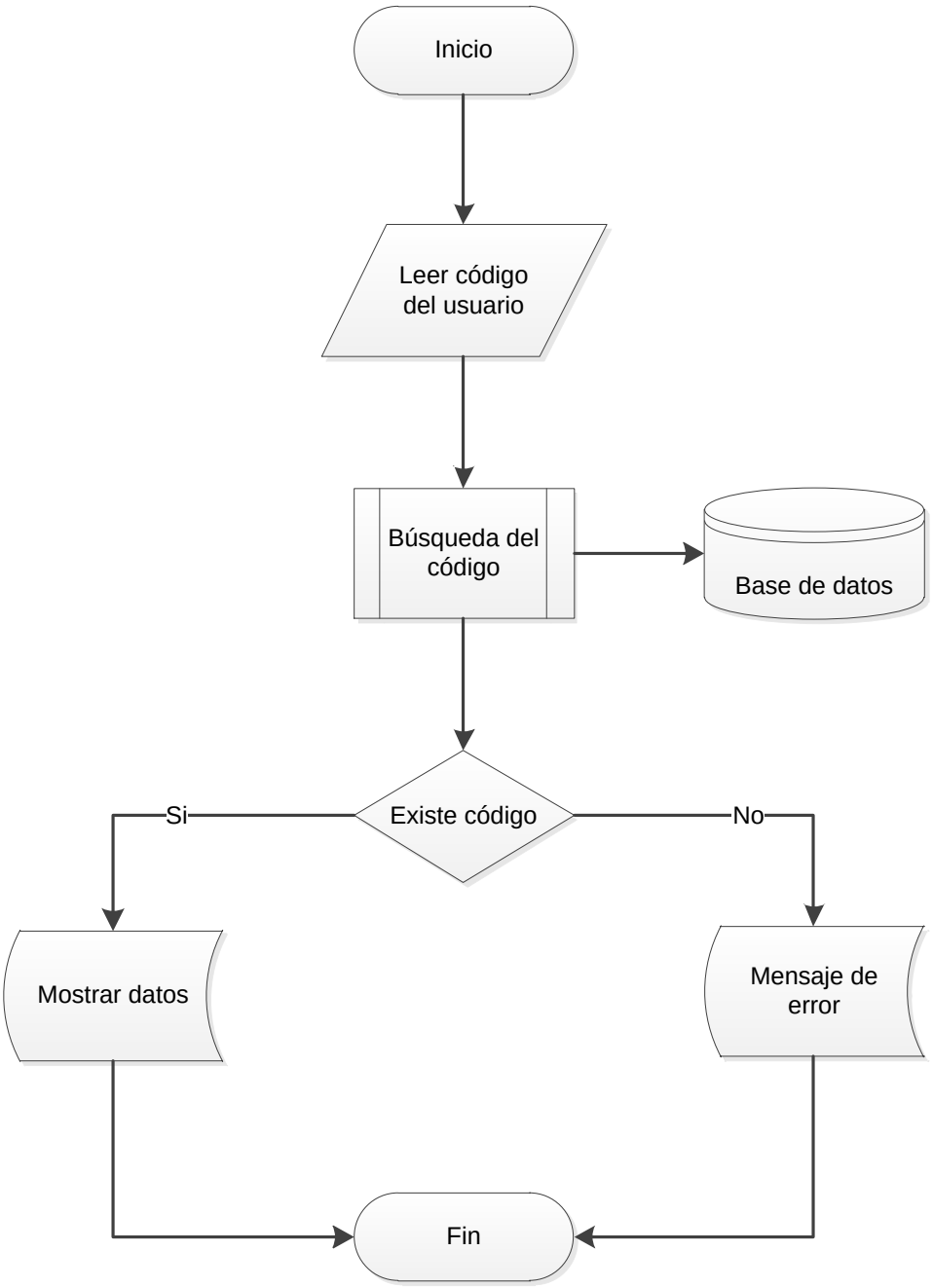
Fuente: elaboración propia, empleando Lucidchart.

4.3.4.4. Consulta de usuarios

Con esta función se puede acceder a la base de datos del sistema para obtener la información del usuario de interés, esta búsqueda se puede realizar entre todos los usuarios registrados en el sistema, por código, nombre o por apellido, cualquiera de estas brinda los datos que se deseen son el usuario, ver figura 19.

```
Procedimiento Consulta_ Usuarios
    Principio ← Registre_Principio_de_búqueda
        Exploración_de_datos (Principios)
    Si existe relación:
    Presentar_Información (Datos)
    Si no existe relación:
        Presentar_Mensaje_Error
Fin Proceso Búsqueda_Usuarios
```

Figura 19. **Diagrama de flujo de consulta de usuarios**



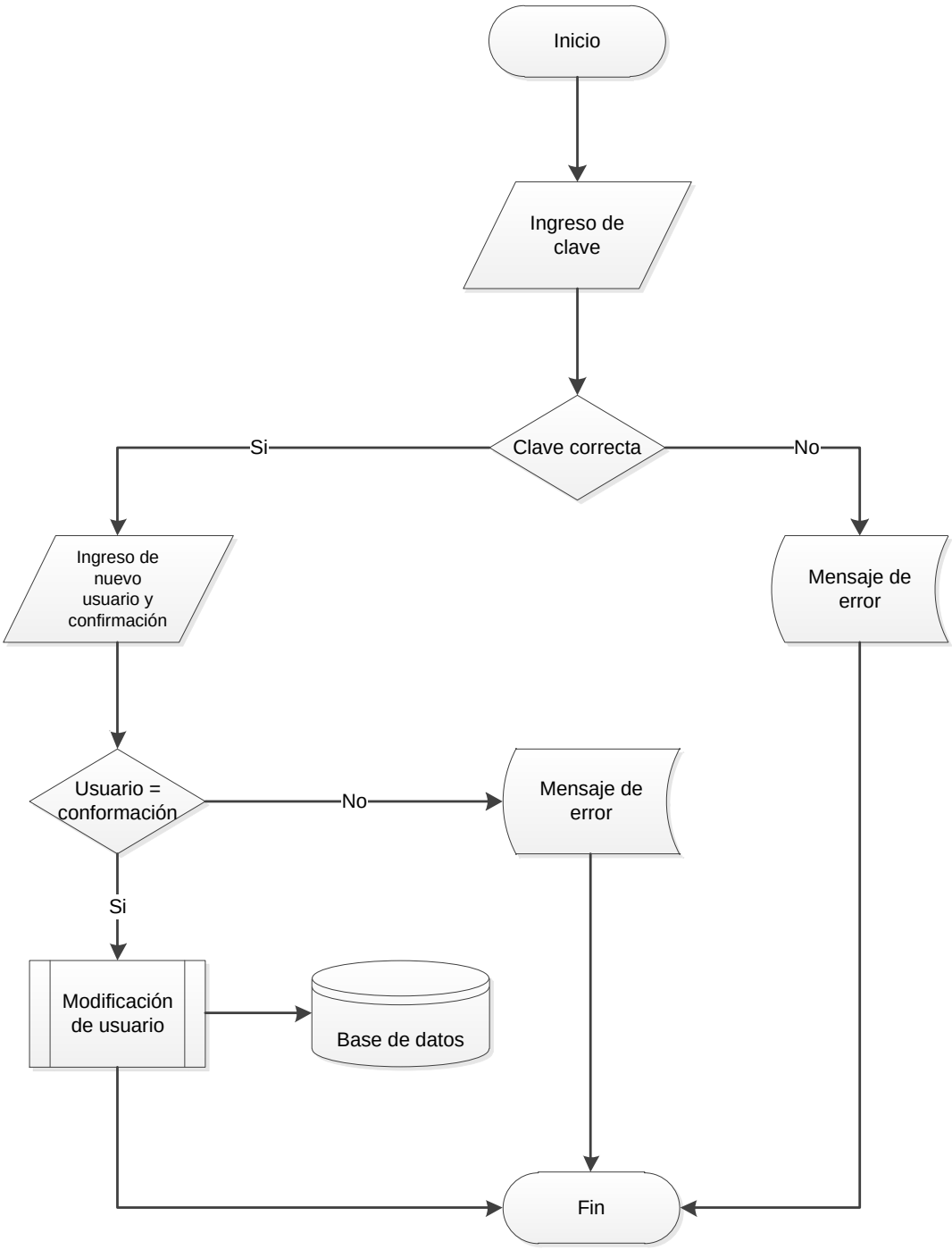
Fuente: elaboración propia, empleando Lucidchart.

4.3.4.5. Cambio de usuario administrador, súper usuarios y alumnos

Por medio de este algoritmo se puede realizar cambios en el nombre de los usuarios ingresados en el sistema accediendo al mantenimiento de las huellas dactilares, ver figura 20.

```
Proceso Modificación_ Usuario_Administrador
    Registrar_Usuario
    Registre_Clave
        Si Contraseña_correcta
        Adquirir (Usuario_Actual, Usuario_Nuevo, Rectificación)
    Si Usuario_Actual es diferente a Usuario_Nuevo:
        Y Usuario_Nuevo concuerda a Rectificación
            Desplegar_Tabla (Administrador)
            Actualizar_Usuario_Administrador
        Si no es diferente:
            Presentar_Mensaje_Error
        Si no es Contraseña_válida:
            Presentar_Mensaje_Error
Fin Proceso Modificación_Usuario_Administrador
```

Figura 20. **Diagrama de flujo de cambio de usuario administrador**



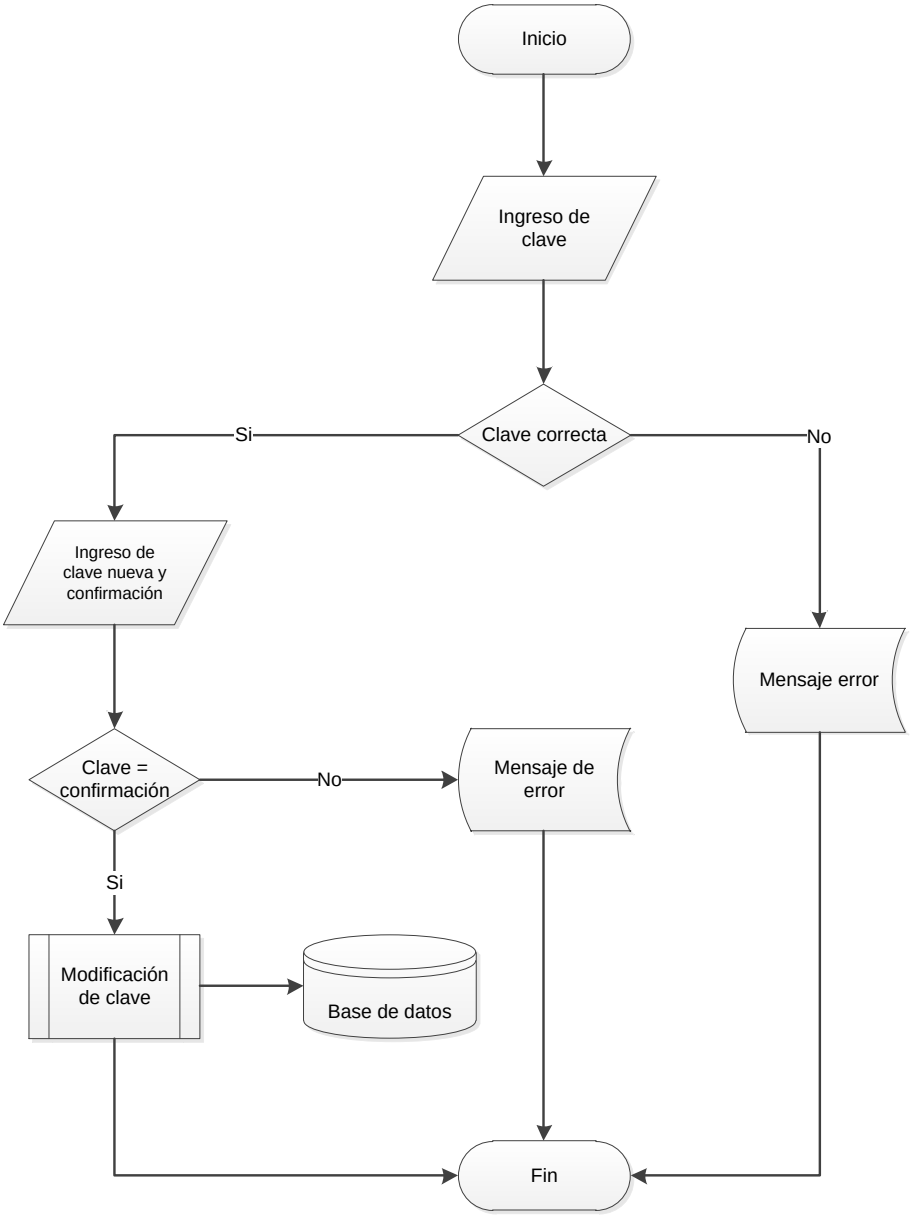
Fuente: elaboración propia, empleando Lucidchart.

4.3.4.6. Modificación de contraseña del administrador

Para poder realizar el cambio de la clave de los usuarios se utiliza este algoritmo, accediendo al mantenimiento de huellas dactilares, ver figura 21.

```
Proceso Modificación_ Contraseña_Administrador
    Registrar_Usuario
    Registrar_Contraseña
        Si Contraseña_válida:
        Adquirir (Contraseña_Actual, Contraseña_Nueva, Rectificación)
        Si Contraseña_Actual es diferente a Contraseña_Nueva
        Y Contraseña_Nueva es igual a Rectificación:
            Desplegar_Tabla (Administrador)
            Actualizar_Contraseña_Administrador
        Si no es diferente:
            Presentar_Mensaje_Error
        Si no es Contraseña_correcta:
            Presentar_Mensaje_Error
Fin Proceso Modificación_Contraseña_Administrador
```

Figura 21. **Diagrama de flujo de modificación de contraseña del administrador**



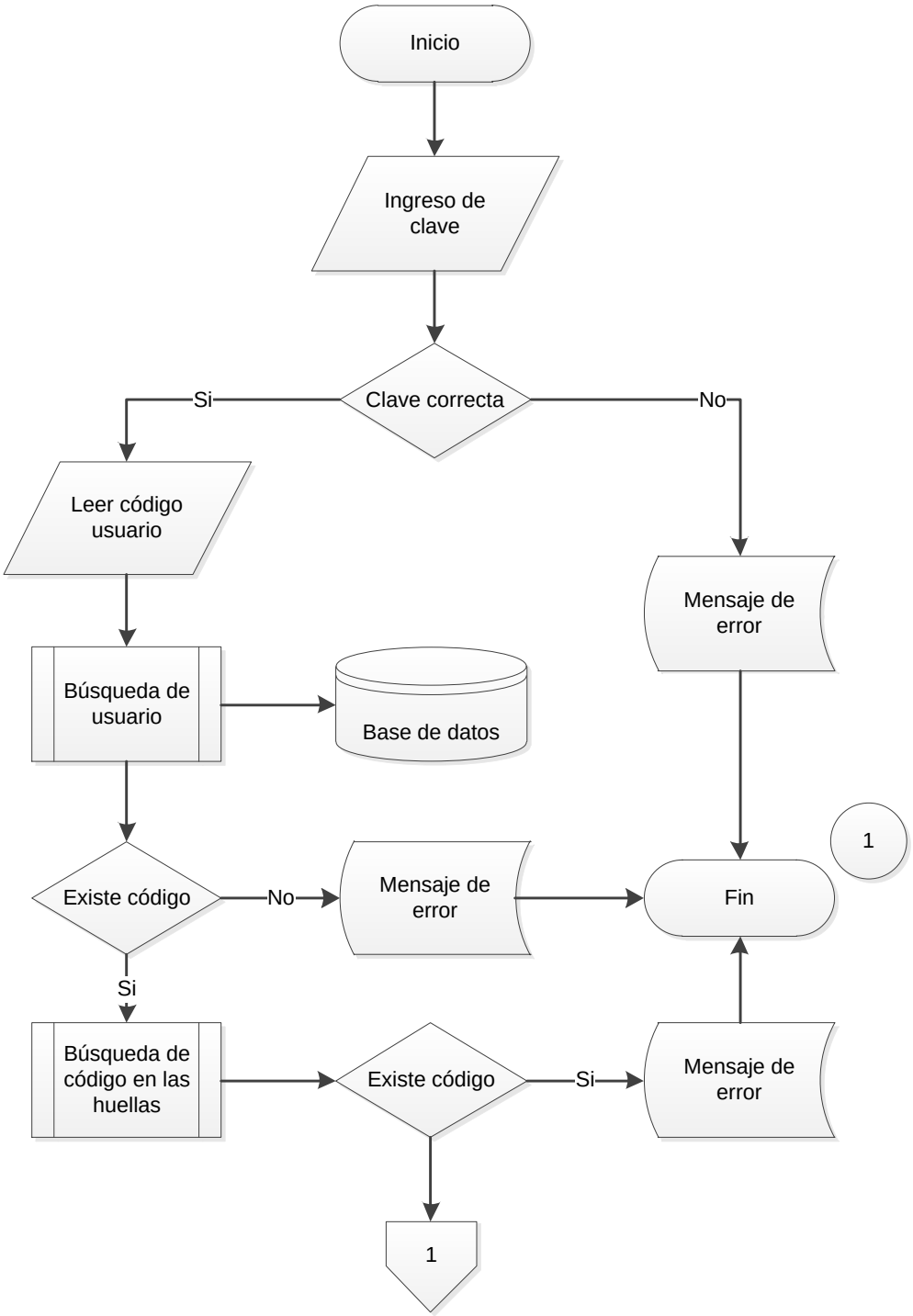
Fuente: elaboración propia, empleando Lucidchart.

4.3.4.7. Registro de huella

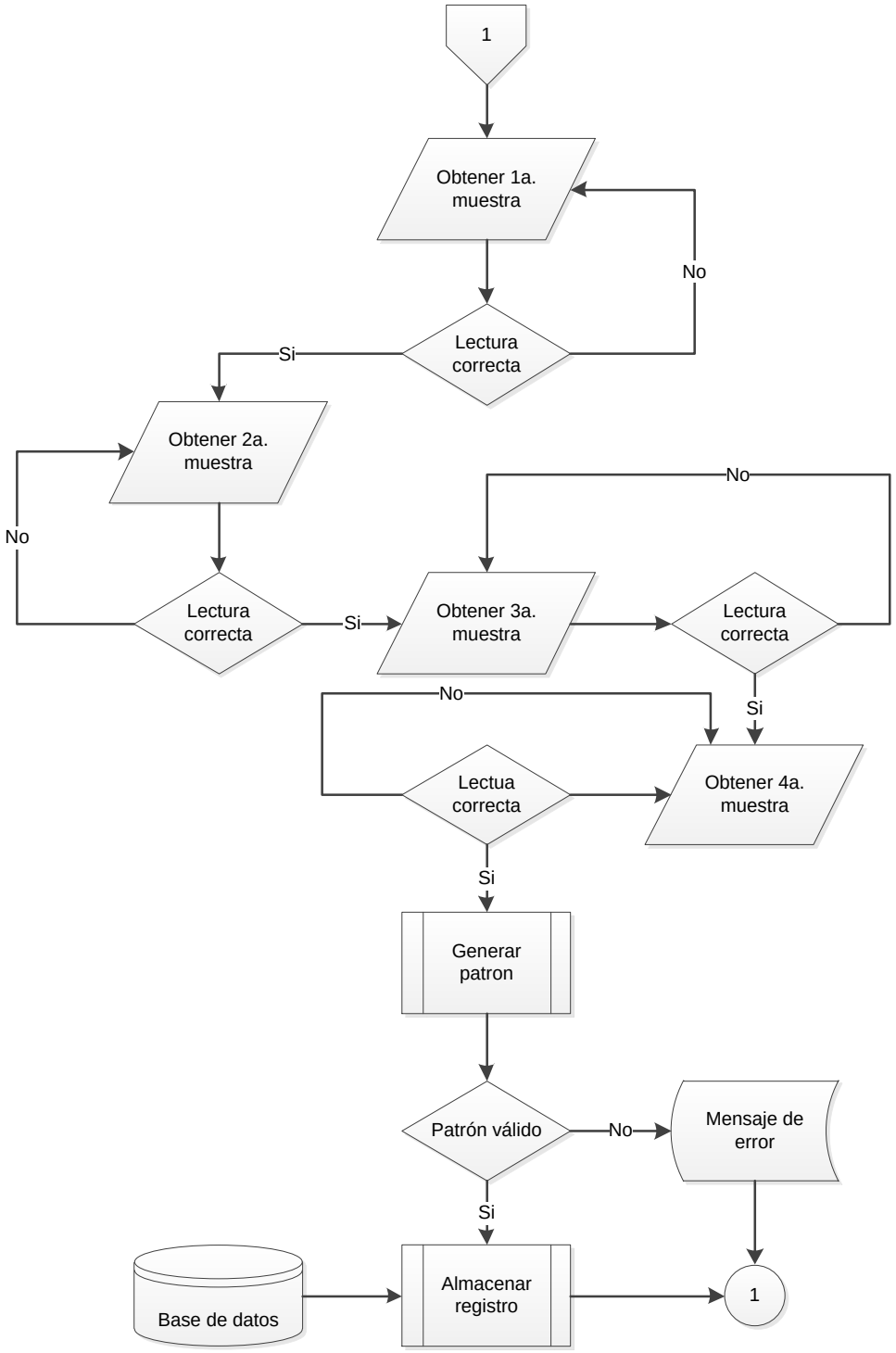
Para poder registrar las huellas de las personas que se requiere ingresar al sistema se utiliza este algoritmo, ver figura 22.

```
Proceso Registrar _ Huella
    Código ←Registrar_Código
    Desplegar_Tabla (Usuario,Huella)
        Consulta_código (Código)
    Si existe código:
        Búsqueda_Huella (Código)
        Si Existe_relación_huella:
            Presentar_Mensaje_Error
    Si no Existe_Relación_huella:
            Adquirir_muestras_de_huella
        Crear_patrón
        Guardar_Huella
    Si no existe código:
        Presentar_Mensaje_Error
Fin Proceso Registrar_Huella
```

Figura 22. **Diagrama de flujo de registro de huella**



Continuación figura 22



Fuente: elaboración propia, empleando Lucidchart.

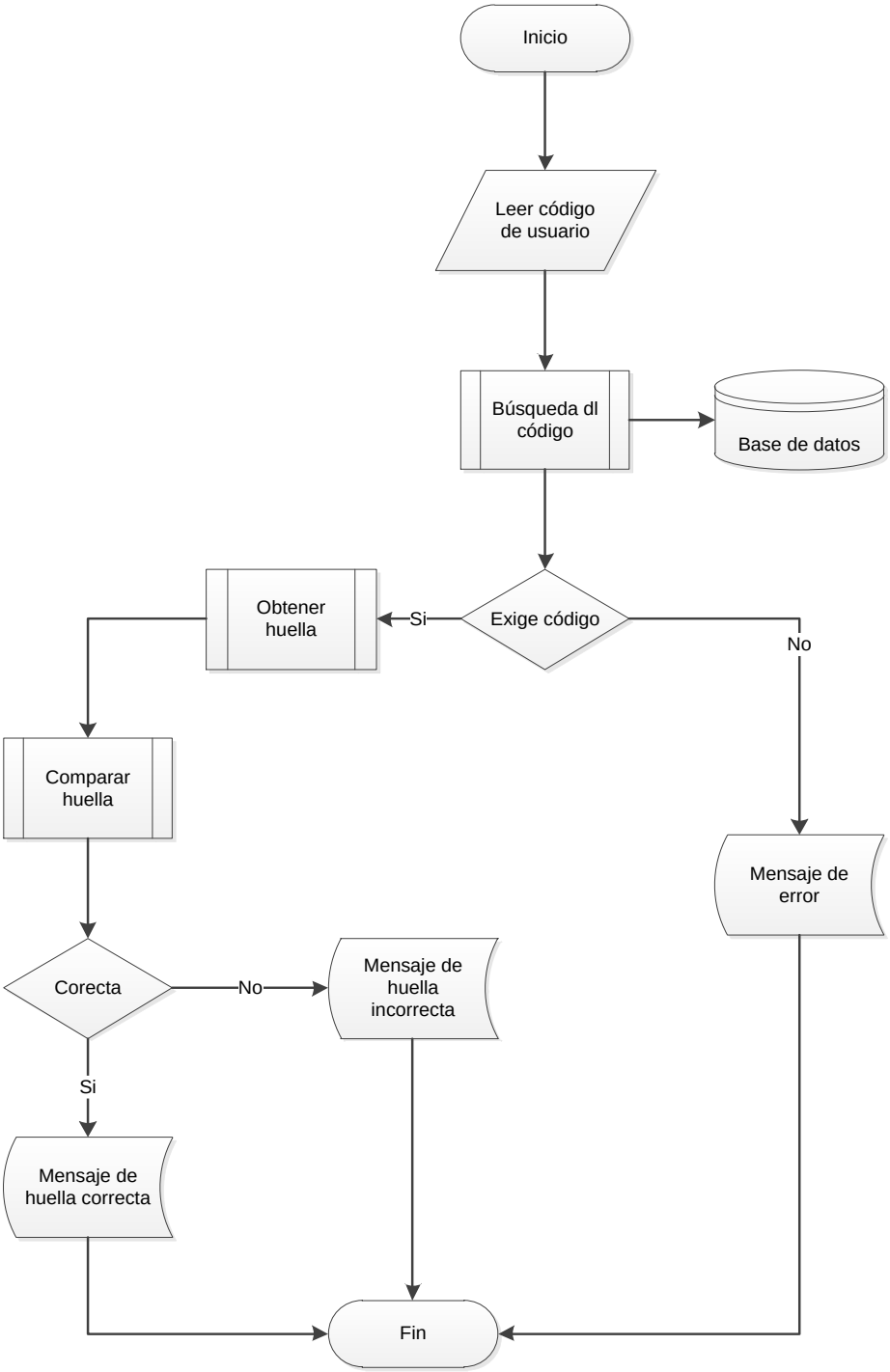
.

4.3.4.8. Comparación de huella

Para poder realizar la comparación de una huella dactilar se utiliza este algoritmo, así se puede realizar una verificación se el almacenamiento de esta es el correcto, ver figura 23.

```
Proceso Comparar _ Huella
    Código ← Registrar_Código
    Desplegar_Tabla (Huella)
        Consulta_Huella (Código)
    Si existe código:
        Adquirir_Patrón
        Comparar_Huella
        Presentar_Resultado
    Si no existe código:
        Presentar_Mensaje_Error
Fin Proceso Comparar_Huella
```

Figura 23. **Diagrama de flujo de comparación de huella**



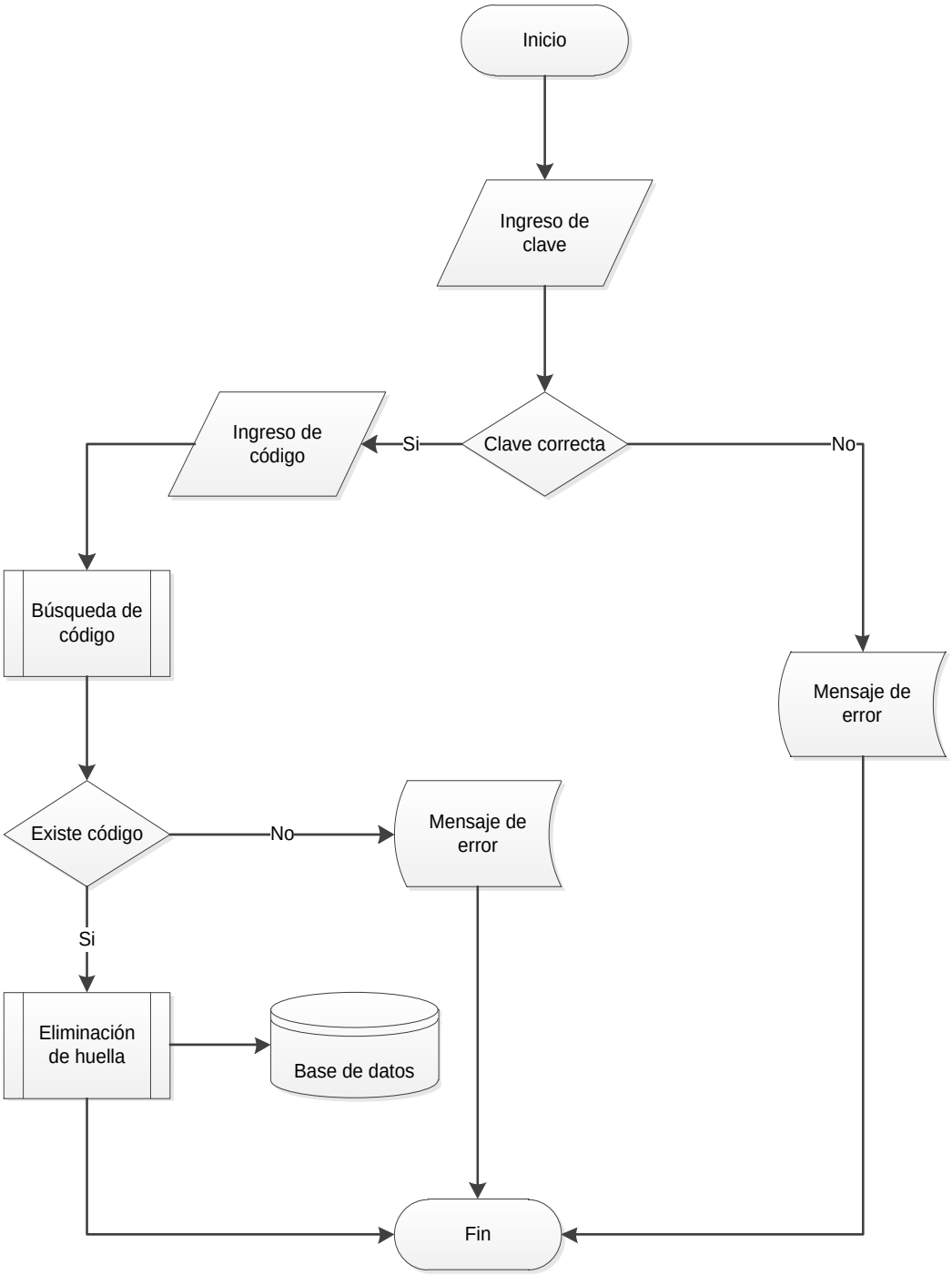
Fuente: elaboración propia, empleando Lucidchart.

4.3.4.9. Eliminación de huella

Por medio de este algoritmo se logra eliminar a los usuarios no deseados dentro de la base de datos por cualquier razón, ver figura 24.

```
Proceso Eliminar _ Huella
    Código ← Registrar_Código
    Desplegar_Tabla (Huella)
        Consulta_Huella (Código)
    Si existe código:
        Eliminar_Huella (Código)
    Si no existe código:
        Presentar_Mensaje_Error
Fin Proceso Eliminar_Huella
```

Figura 24. **Diagrama de flujo de eliminación de huella**



Fuente: elaboración propia, empleando Lucidchart.

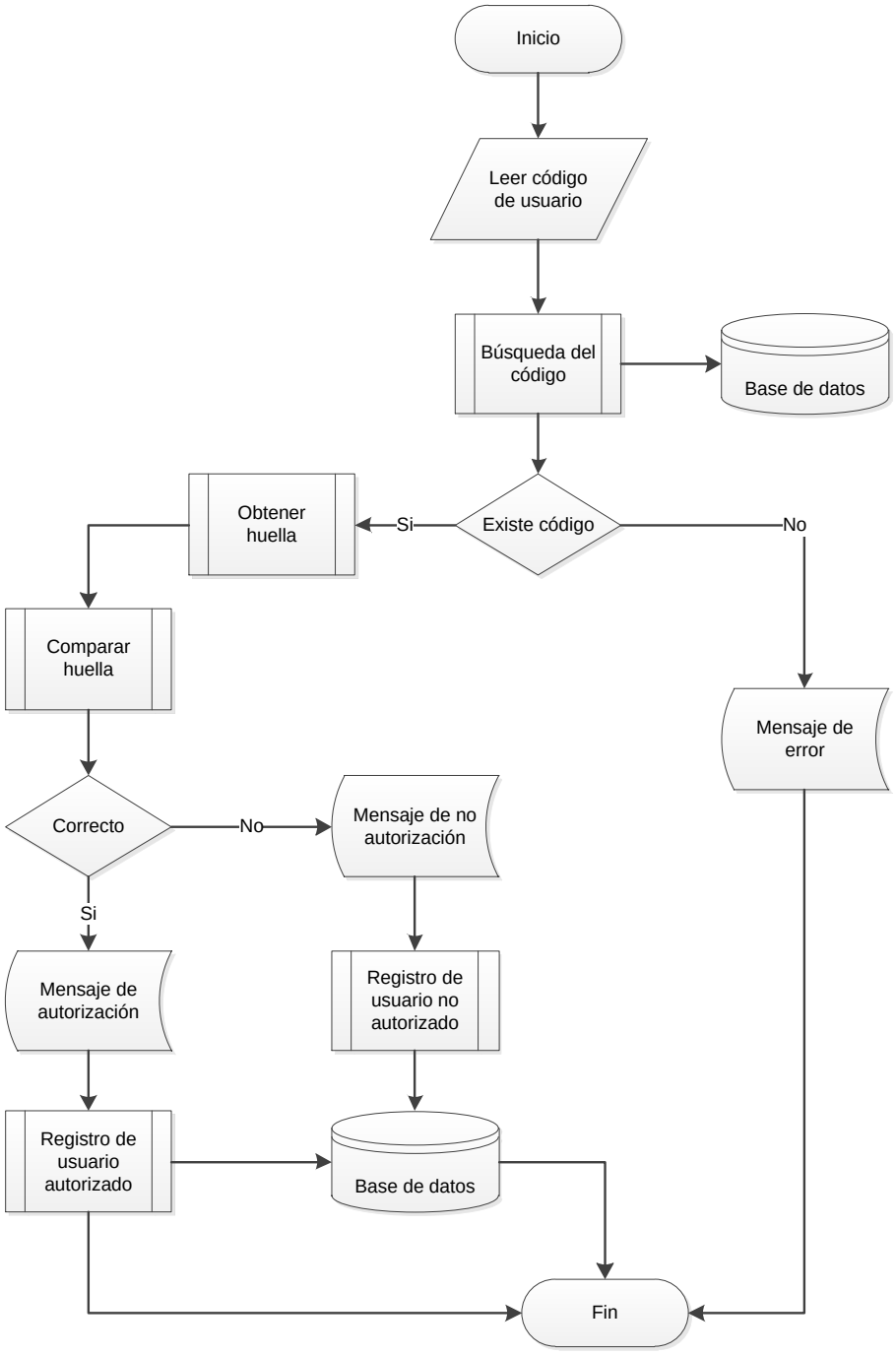
.

4.3.4.10. Registro de ingreso de los usuarios

Con el algoritmo que se presenta a continuación se logra constituir un monitoreo acerca del acceso de quienes ingresan al sistema. La persona debe ingresar el código personal y el paso siguiente es colocar la huella digitan el sensor, la que se compara en la base de datos del sistema, si esta autenticada, guarda el registro dentro del sistema, de lo contrario es almacenada en el historial de los ingresos denegados, ver figura 25.

```
Proceso Registro_ de_Acceso
   Código ← Registrar_Código
      Consulta_Huella (Código)
   Si existe código:
      Adquirir_Plantilla
      Verificar_Huella
      Si huella_correcta
         Desplegar_Tabla (RegistroHuella)
         Registar_Datos_Ingreso
      Si no es huella_correcta:
      Desplegar_Tabla (RegistroInvalido)
      Registrar_Datos_Acceso
   Si no existe código: Presentar_Mensaje_Error
Fin Proceso Registro_de_Acceso
```

Figura 25. **Diagrama de flujo de registro de acceso de usuarios**



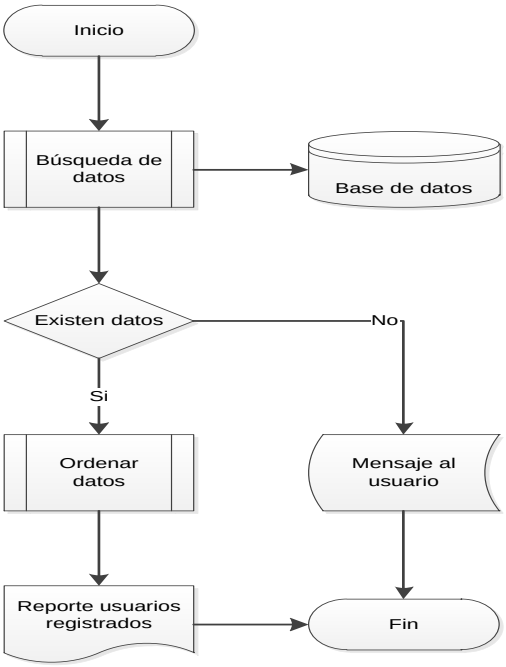
Fuente: elaboración propia, empleando Lucidchart.

4.3.4.11. Informes de usuarios registrados

Para generar los informes de las personas registradas dentro del sistema es utilizado el algoritmo siguiente, ver figura 26.

Proceso Informe_ de_Usuarios
  Desplegar_Tabla (Usuario)
    Adquirir_Datos
  Si existen datos:
    Crear_informe
  Si no existen datos:
    Presentar_Mensaje
Fin Proceso Informe_Usuarios

Figura 26. **Diagrama de flujo de informe de usuarios**



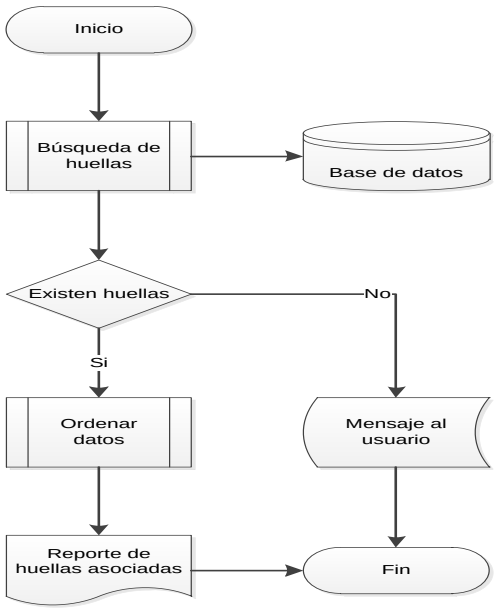
Fuente: elaboración propia, empleando Lucidchart.

4.3.4.12. Informe de huellas asociadas

La finalidad del algoritmo que se presenta a continuación es realizar un informe acerca de las huellas dactilares de los usuarios registrados y almacenados en la base del sistema, ver figura 27.

Proceso Informe_ de_Huellas
    Desplegar_Tabla (Usuario)
        Adquirir_Datos
    Si existen datos:
        Crear_Informe
    Si no existen datos:
        Presentar_Mensaje
Fin Proceso Informe_de_Huellas

Figura 27. **Diagrama de flujo de informe de huellas asociadas**



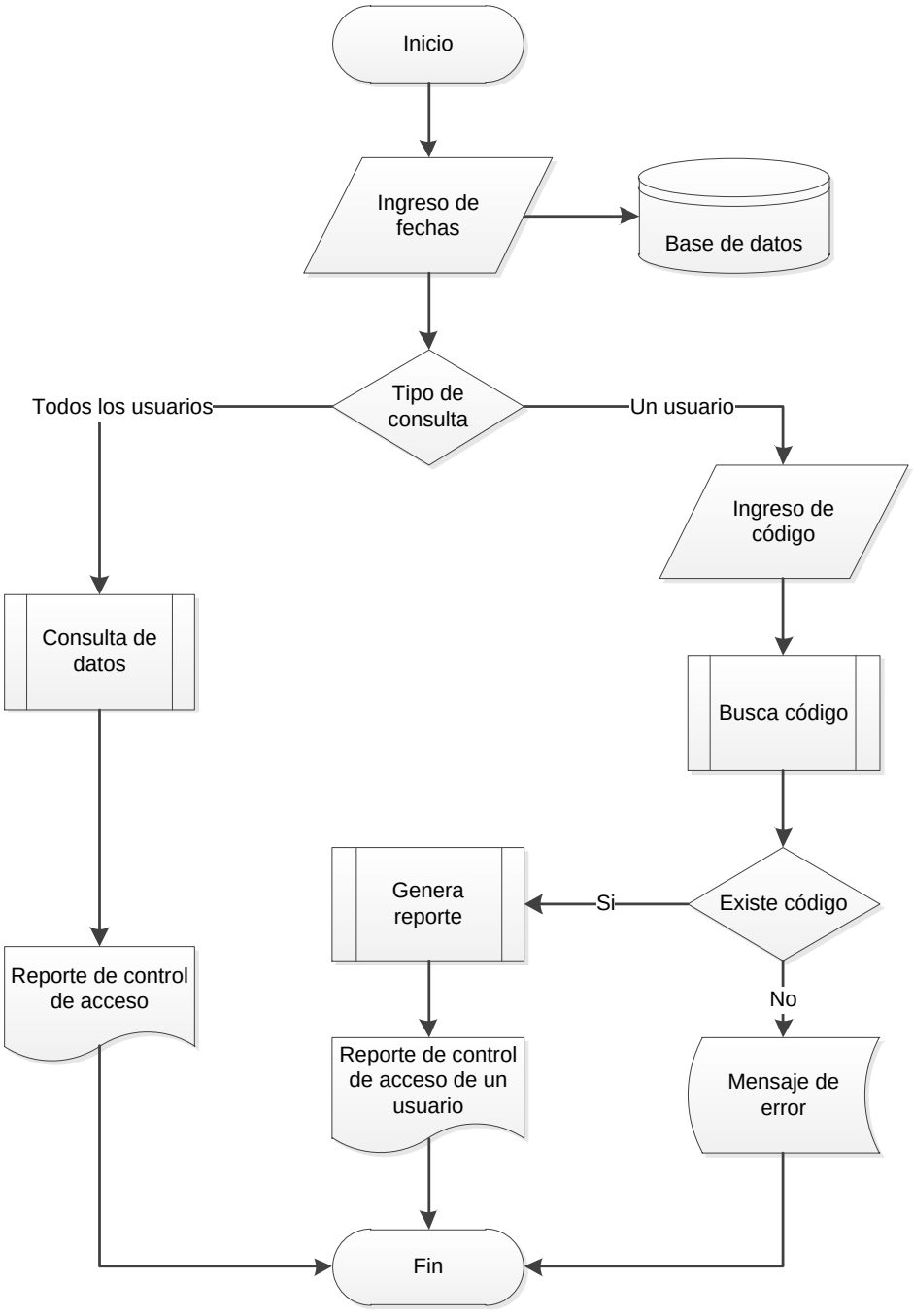
Fuente: elaboración propia, empleando Lucidchart.

4.3.4.13. Informe de control de acceso de los usuarios

Para realizar un reporte de sobre el control de ingresos al sistema de las personas registradas se utiliza el algoritmo siguiente, con el que se puede realizar en reporte general o particular, ver figura 28.

```
Proceso Informe_ de_Monitoreo_de_Ingreso
    Desplegar_Tabla (Usuario, RegistroHuella)
        Adquirir_Datos_Según_Principios
    Si existen datos:
        Crear_informe
    Si no existen datos:
        Presentar_Mensaje
Fin Proceso Informe_Monitoreo_de_Ingreso
```

Figura 28. **Diagrama de flujo de informe de control de acceso**



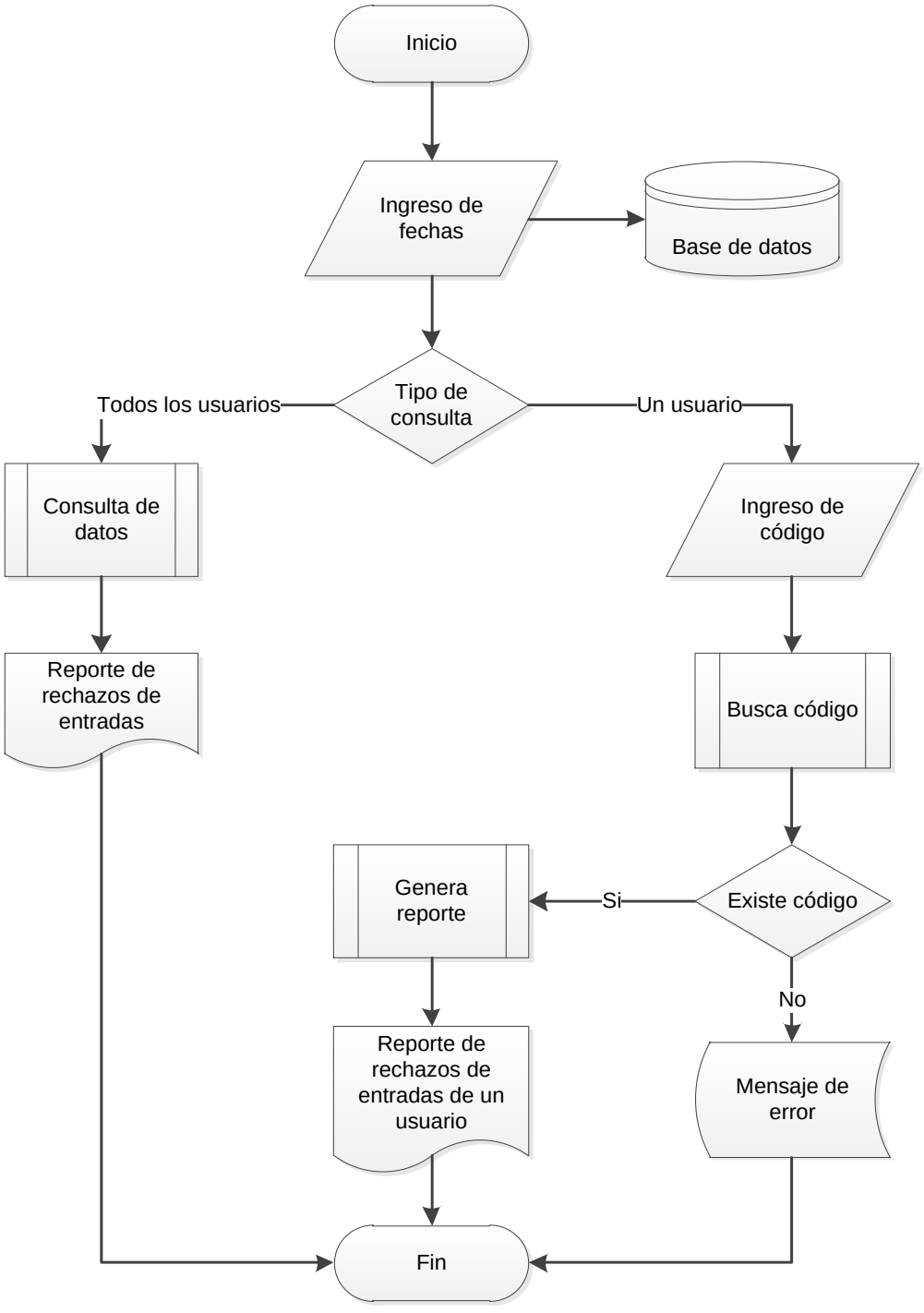
Fuente: elaboración propia, empleando Lucidchart.

4.3.4.14. Informe de usuarios rechazados

Al contrario del algoritmo anterior, este se utilizar para realizar reporte de quienes no están registrados y almacenados en el sistema, los cuales son rechazados al momento de ingresar al sistema y se realizar un reporte individual o colectivo de quienes intentaron acceder sin contar con un registro en la base del sistema, ver figura 29.

```
Proceso Informe_ de_Monitoreo_de_acceso
    Desplegar_Tabla (Usuario, RegistroHuella)
        Adquirir_Datos_Según_principio
    Si existen datos:
        Crear_Informe
    Si no existen datos:
        Presentar_Mensaje
Fin Proceso Informe_Monitoreo_de_acceso
```

Figura 29. **Diagrama de flujo de informe de usuarios rechazados**



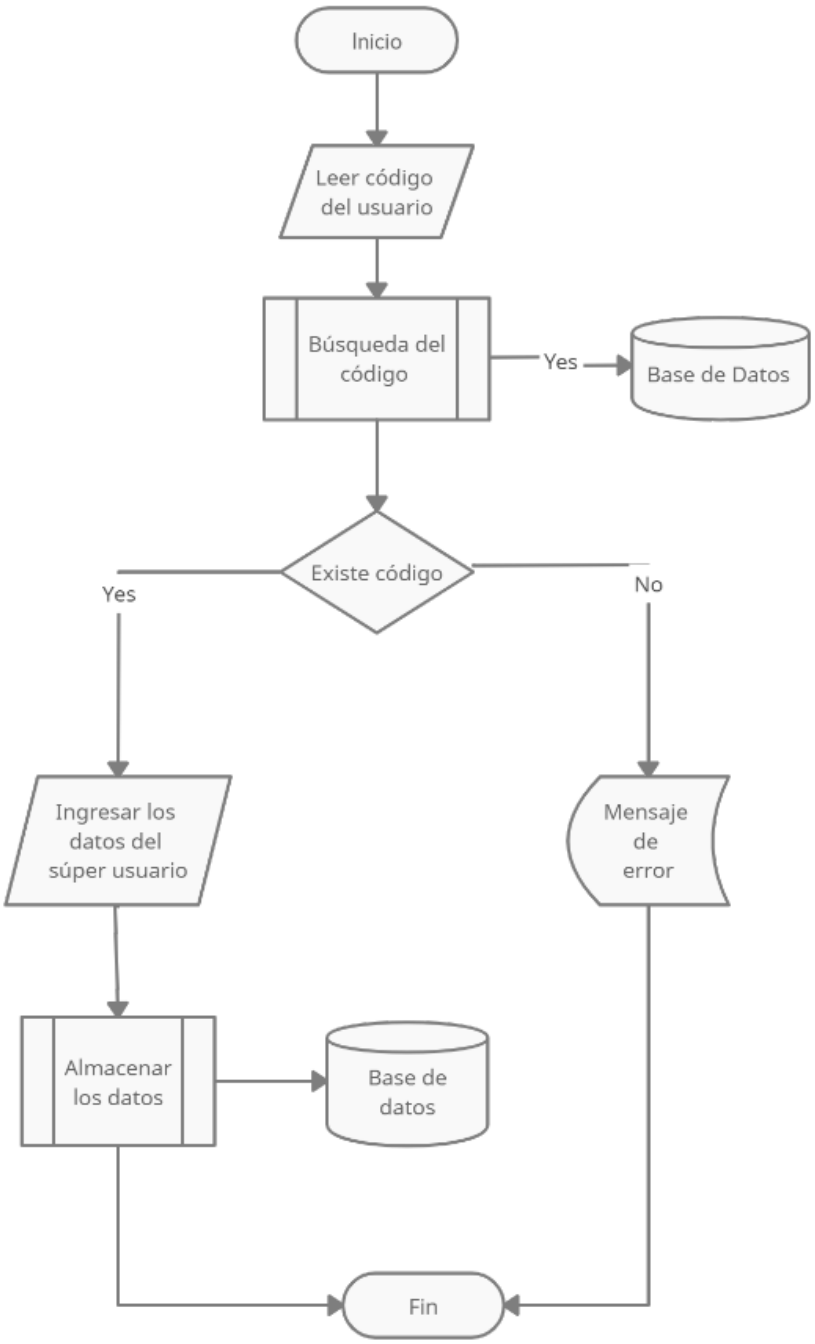
Fuente: elaboración propia, empleando Lucidchart.

4.3.4.15. Súper usuario

Este algoritmo se utilizará para poder darle un súper usuario a cada usuario, quien realizará una búsqueda para ingresar el código del usuario y si este existe se otorgará un súper usuario, ver figura 30.

Procedimiento Registro_de_Súper_Usuario
Código ← Ingresar_Código_usuario
Búsqueda_código (Código)
Si existe código:
Adquirir (1Nombre, 2Nombre, 3Nombre, 1Apellido, 2Apellido, teléfono, dirección)
Abrir_Tabla (Usuario)
Almacenar_Datos
Si no existe código: Mostrar_Mensaje_Error
Fin Procedimiento Registro_Súper_Usuario

Figura 30. **Diagrama de flujo de registro de súpero usuario**



Fuente: elaboración propia, empleando Lucidchart.

4.3.5. Desarrollo de la aplicación

La aplicación fue desarrollada por medio del lenguaje visual basic y la base de datos en Access fue la utilizada. Para establecer la comunicación entre el sensor para la huella dactilar con el administrador, fueron utilizados algoritmos que se encuentran incluidos en el paquete para desarrollar el software por el fabricante del sensor, Suprema BioMini Plus 2.

En estos algoritmos para reconocer la huella dactilar son utilizados términos que se denominan tasas de error:

- Tasa de falsa aceptación (FAR, por sus siglas en inglés, False Acceptance Rate). Se define como la probabilidad de que un individuo no autorizado sea aceptado por el sistema.
- Tasa de falso rechazo (FRR, por sus siglas en inglés, False Rejection Rate). Definida como la probabilidad de que un individuo autorizado es rechazado por el sistema.[23]

La falsa tasa de aceptación y la de falso rechazo son mecanismos del programa que alcanzan el grado de seguridad que se busca. Prácticamente, la derivación del procedimiento de identificar o verificar es un número real establecido entre el intervalo [0, 1], el cual indica que la correlación entre el modelo biométrico proporcionado por la persona y la registrada en el sistema.

En la actualidad, los algoritmos de Suprema BioMini Plus 2 que se utilizan para esta suministran una tasa de aceptación falsa del 0,01 % y una de falso rechazo del 1,4 %.

La comprobación de la huella dactilar en la aplicación consta de los siguientes procesos.

[23] VILLALÓN HUERTA, Antonio. *Seguridad en Unix y redes. Versión 2.1'*. p 205.

- Obtención de la muestra, huella en imagen

Para iniciar la identificación de la muestra se debe capturar una imagen de esta, usada como modelo. Cuando la persona coloca el dedo en el lector, se captura la muestra, se encripta y se comprime y se envía al receptor del sistema, la computadora.

- Descompresión del modelo

Al recibir el sensor la muestra, es desencriptada y descomprimida en el modelo, extrayendo las características y creando una plantilla.

- Creación de la plantilla

Luego de culminar con el proceso de verificación o registro se establece la plantilla adecuada, esta es una representación matemática de los propios caracteres de la huella dactilar, a este se le asigna el pre-registro o la verificación de esta.

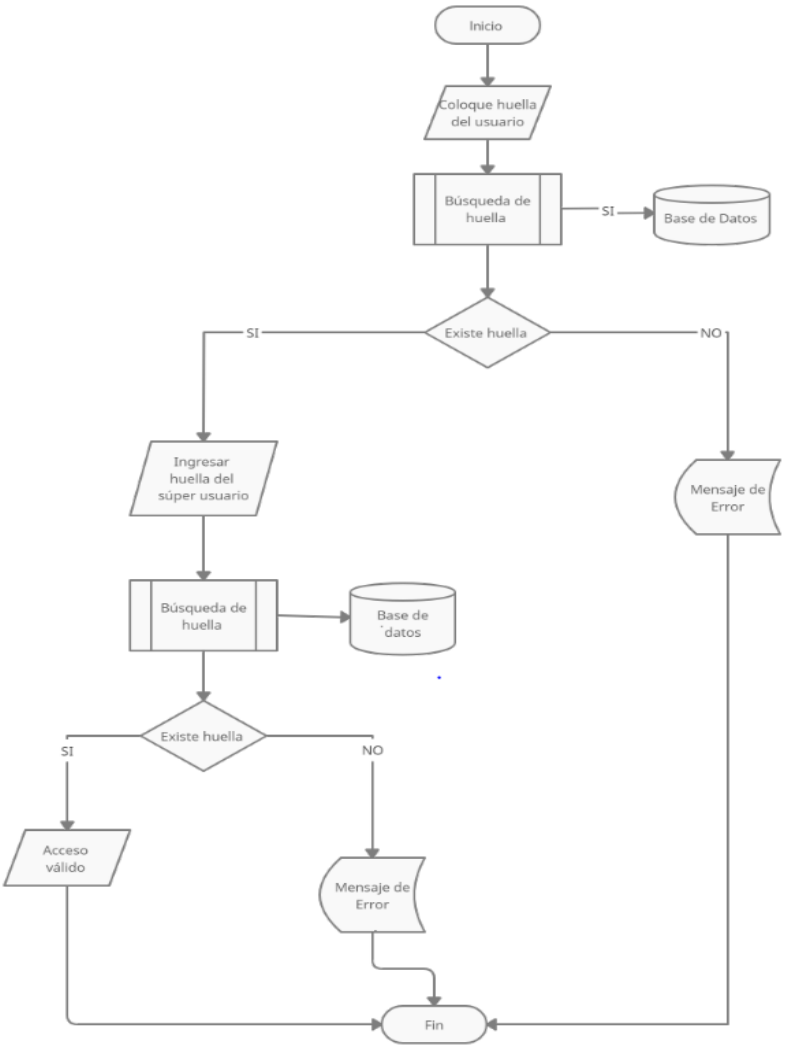
- Ejecución operativa de la verificación o registro

Para realizar el registro de una huella dactilar, se hace necesarios la toma de cuatro muestras, las que luego son empleadas para la generación de la plantilla, al contar con la plantilla definitiva, esta se carga en la base de datos para utilizarla cuando se requiera. Para poder ser verificada la identificación del patrón se compara con la registrada en la base de datos.

4.3.5.1. Diagrama de flujo de la aplicación

A continuación, se muestra el proceso de la aplicación para el ingreso o egreso de un usuario, ver figura 31.

Figura 31. **Diagrama de flujo de la aplicación**

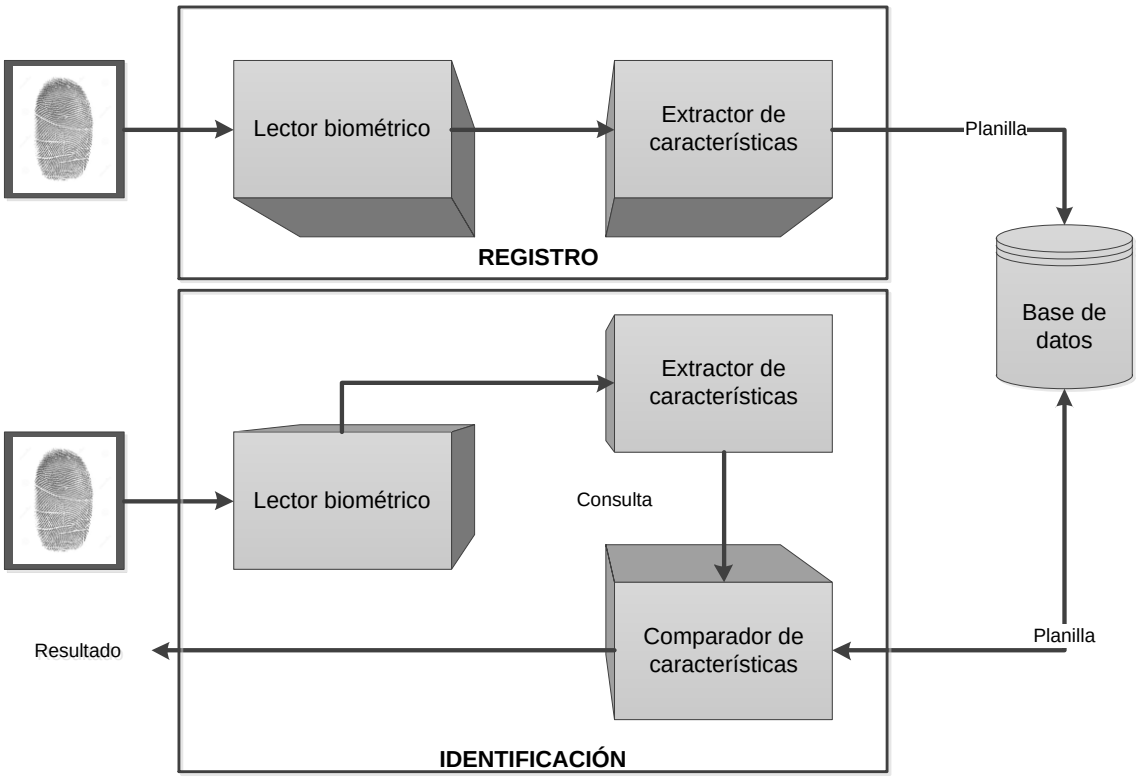


Fuente: elaboración propia, empleando Lucidchart.

4.3.5.2. Arquitectura del reconocimiento de la huella digital

A continuación, se ilustra el diseño del proceso para reconocer una huella dactilar.

Figura 32. **Arquitectura de un sistema de verificación y reconocimiento de huella dactilar**



Fuente: elaboración propia, empleando Lucidchart.

Al registrarse una persona, este ofrece al programa las muestras requeridas con la que se extraen las características de este y se realiza la plantilla que se almacena en la base de datos.

Por su parte, el procedimiento se inicia cuando el sensor biométrico recibe la característica de la huella para poder realizar la identificación y lo transforma en un formato digital, esto con la finalidad de producir una representación más pequeña en el mismo formato digital, esta representación realiza la consulta en el sistema y envía una señal para comparar las características con la almacenada en la base de dado y de esta forma establece si es la identidad establecida.

4.3.5.3. Descripción de los algoritmos para el dispositivo biométrico

Los algoritmos que se muestran a continuación se adaptaron para ser utilizados por el sistema, transformando el código original que se encontraba incluido en el programa para poder poner en marcha el sistema.

- Registro de la huella dactilar

Inicialmente es primordial crear un modelo FPTemplate y un FPRegisterTemplate, del objeto, los cuales serán utilizados para efectuar el registro de la huella dactilar.

Dim WithEvents op As FPRegisterTemplate
Dim cursample As Iteger
Dim regtemplate As FPTemplate

Seguido al registro de la huella dactilar, se hace necesario tomar cuatro modelos para la generación de una plantilla. Este es realizado gracias a un algoritmo el cual contiene la función op.run con la que se realiza una llamada al método que es el objeto FPRegisterTemplate, por medio del cual se realiza el proceso de registro.

```
Sub AdquiereHuella ()
    Dim i As Integer
    cursample = 0
    For i = 0 To 3
        picSample(i).Picture = Nothing
        dot(i).Visible = False
    Next i
    dot(cursample).Visible = True
    Dim WithEvents op As FPRegisterTemplate
    Dim cursample As Integer
    Dim regtemplate As FPTemplate
    85
    op.Run
    LblMensajes.Caption = "Mensajes:"
    Mensajes.Caption = "Coloque el dedo en el sensor"
    lblQuality.Caption = ""
    lblTemplateID.Caption = ""
    lblEvents.Caption = ""
End Sub
```

Luego del registro se procede a la verificación de la calidad del modelo dactilar, por medio de una codificación se hace esta verificación, si el modelo fue tomado de forma correcta, si no está clara, si no se tomó la región central.

```
Private Sub op_SampleQuality(ByVal Quality As
DpSdkEngLib.AISampleQuality)
    Dim Error As Integer
        Select Case Quality
```

Continuación de código de verificación

```
Case AISampleQuality.Sq_Good
    lblQuality.Caption = "OK"
    cursample = cursample + 1
    dot(cursample - 1).Visible = False
    If cursample <> 4 Then
        dot(cursample).Visible = True
        End If
Case AISampleQuality.Sq_LowContrast
    lblQuality.Caption = "Muestra incorrecta"
    Error = 1
Case AISampleQuality.Sq_NoCentralRegion
    lblQuality.Caption = "Muestra incompleta" Error = 1
Case AISampleQuality.Sq_None
    lblQuality.Caption = "Muestra incorrecta"
    Error = 1
Case AISampleQuality.Sq_NotEnoughFtr
    lblQuality.Caption = "Muestra incorrecta"
    Error = 1
Case AISampleQuality.Sq_TooDark
    lblQuality.Caption = "Muestra incorrecta"
    Error = 1
Case AISampleQuality.Sq_TooLight
    lblQuality.Caption = "Muestra incorrecta"
    Error = 1
Case AISampleQuality.Sq_TooNoisy
    lblQuality.Caption = "Muestra incorrecta"
    Error = 1
```

Continuación de código de verificación

```
    End Select
    If Error = 0 Then
        lblEvents.Caption = "Muestra correcta"
        LblMensajes.Caption = "Mensajes:"
        Mensajes = "Coloque el dedo en el sensor"
    Else
        lblEvents.Caption = "Coloque nuevamente el dedo"
        Mensajes = "Coloque nuevamente el dedo"
    End If
End Sub
```

Si fuera el caso que ha ocurrido alguno de los errores mencionados con anterioridad, se debe solicitar al usuario que realice una nueva toma hasta que se obtengan un modelo adecuado. El siguiente paso es realizar la prueba de la imagen que fue adquirida en el lector. Cuando el modelo es solicitado por el lector, se activa la imagen proporcionada y almacenada en la base del sistema se emplea el algoritmo que se presenta a continuación.

```
Private Sub op_SampleReady(ByVal pSample As Object)
    pSample.PictureOrientation = Or_Portrait
    pSample.PictureWidth = picSample(cursample).Width /
Screen.TwipsPerPixelX
    pSample.PictureHeight = picSample(cursample).Height /
Screen.TwipsPerPixelY
    picSample(cursample).Picture = pSample.Picture
    lblEvents.Caption = "Listo"
End Sub
```

Para culminar el procedimiento debe de almacenarse el modelo asignado, si este genera un registro que sea válido, se traslada el modelo en la plantilla establecida y se almacena en la base de datos.

```
Dim blob() As Byte
regtemplate.Export bvariant
blob = bvariant
```

- Procedimiento de comprobación de la huella dactilar

La verificación es primordial, definiendo el modelo que realizará esta acción.

```
Dim WithEvents op As FPVerifyTemplate
Dim regtemplate As FPTemplate
```

Luego de realizar la comprobación es necesario extraer de la base de datos el modelo previamente generado de la persona que identificara el sistema, la que se debe asociar con la identidad del usuario por medio del código de identificación. Es creada una nueva solicitud FPTemplate la cual importa los valores que fueron obtenidos de la base de datos, a continuación, se muestra el código empleado:

```
Set regtemplate = New FPTemplate
res = regtemplate.Import(blob)
```

Posterior a la se debe activar el procedimiento para reconocer la huella del individuo por medio de la toma dactilar en el sensor y es comparada con la que se encuentra como modelo en la base de datos.

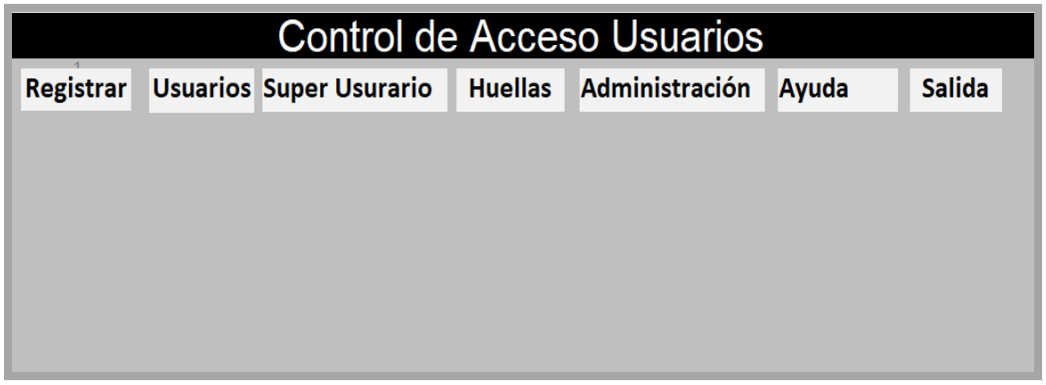
```
op.Run regtemplate
```

Por último, son activadas las acciones que se señalaron para realizar el registro de la huella, los que establecen la calidad del modelo obtenido y se debe realizar la comparación de las muestras, estableciendo de esta forma si es aceptado o denegado el registro.

4.4. Funcionamiento del sistema

En el menú principal del sistema existen las alternativas de registro, los usuarios, las huellas y la administración, como se observa en la figura 33.

Figura 33. **Menú principal**



Fuente: elaboración propia, empleando Access.

En los apartados que se presentan a continuación, son descritas las opciones del menú principal.

4.4.1. Registrar

Un individuo con un modelo almacenado con antelación lo utiliza en el sistema para realizar el ingreso del registro de entrada. Este introduce el código personal el cual es autorizado, colocando la yema del dedo en el actuador

biométrico, lo cual genera un modelo que es comparado con el que se encuentra almacenado en la base de datos y que se asocia al código personal.

Si al realizar esta acción los patrones coinciden, se procede a registrar fecha y hora de ingreso al programa dando el visto bueno al individuo. Si los patrones o modelos son inválido, se procede a generar un registro y se almacena con la hora y el día que se realizado el intento de acceso, esto se ilustra en la figura 34.

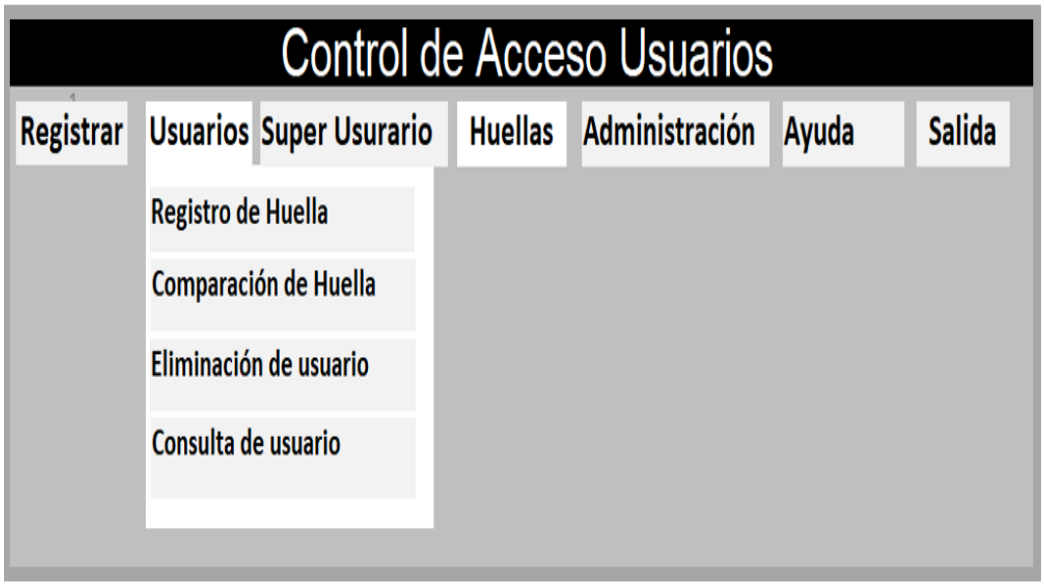
Figura 34. **Registrar**

Fuente: TAPIADOR MATEOS, Marino; SIGÜENZA PIZARRO, Juan Alberto. *Tecnologías biométricas aplicadas a la seguridad.* p. 217.

4.4.2. El menú usuarios

A continuación, se ilustra este menú.

Figura 35. **Menú usuarios**



Fuente: elaboración propia, empleando Access.

El menú de usuarios cuenta con las siguientes opciones:

4.4.2.1. Registro de usuarios

Esta función le solicita al individuo que introduzca el código personal, el cual es validado si se tiene relación con un registro en la base de datos, si no existe se marcará como error. Al momento de no existir, el programa le pide al individuo que introduzca la información como el nombre y apellidos, la dirección y el número telefónico y son ingresados en la base de datos, ver figura 36.

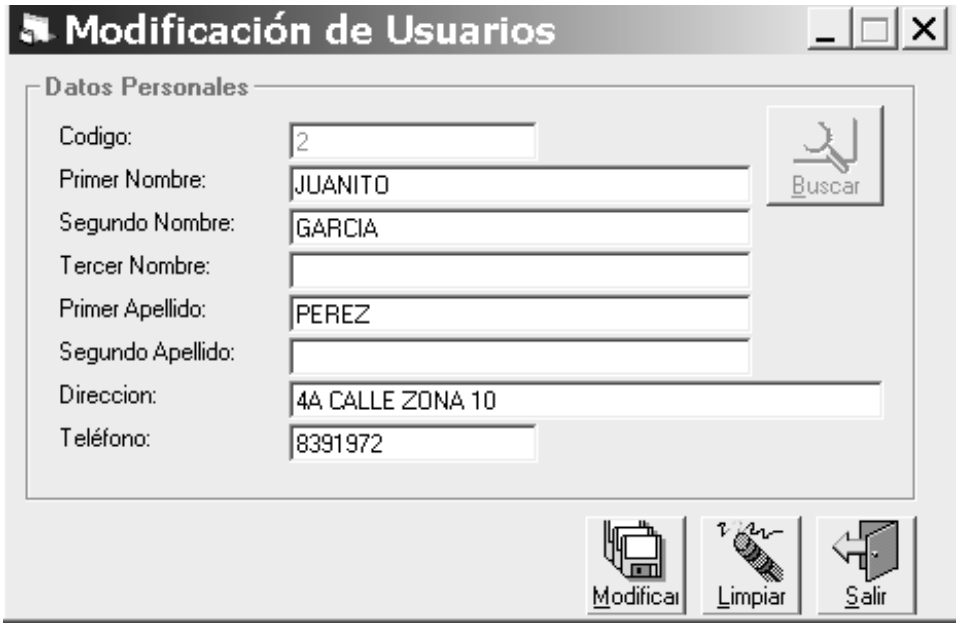
Figura 36. **Ingreso de datos**

Fuente: TAPIADOR MATEOS, Marino; SIGÜENZA PIZARRO, Juan Alberto. *Tecnologías biométricas aplicadas a la seguridad.* p. 220.

4.4.2.2. Modificación de usuarios

Para realizar modificaciones en el registro de los individuos, el sistema solicita que sea ingresado el código personal, cuando es aceptado por la base de datos, si estos datos existen dentro del programa se procede a habilitar el sistema para realizar las modificaciones, al realizar las modificaciones estas son actualizadas, ver figura 37.

Figura 37. **Modificación de usuarios**

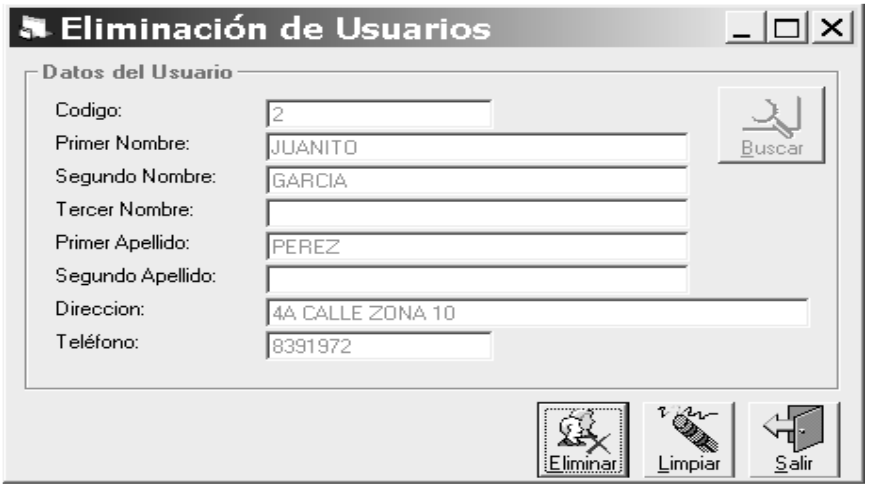


Fuente: TAPIADOR MATEOS, Marino; SIGÜENZA PIZARRO, Juan Alberto. *Tecnologías biométricas aplicadas a la seguridad.* p. 220.

4.4.2.3. Eliminación de usuarios

Esta función que se encuentra en el menú del usuario permite eliminar a estos cuando ya no sea necesario tenerlos en el sistema, para realizar esta acción se le pide al individuo que introduzca el código personal y al igual que las otras opciones debe de ser validado por el sistema para acceder y al elegir la opción de eliminación y confirmar la acción, el programa de forma automática elimina todos los datos almacenados del usuario que se pretende eliminar, ver figura 38.

Figura 38. **Eliminación de usuarios**

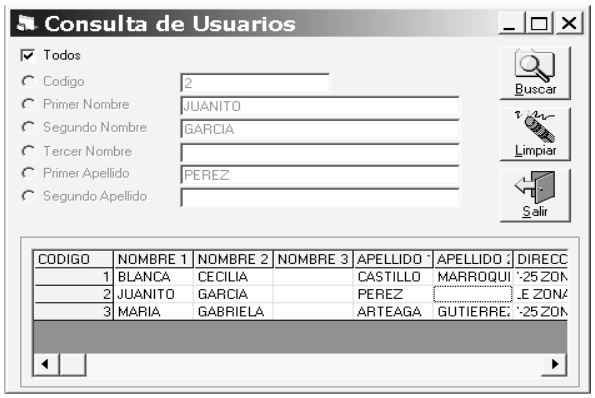


Fuente: TAPIADOR MATEOS, Marino; SIGÜENZA PIZARRO, Juan Alberto. *Tecnologías biométricas aplicadas a la seguridad.* p. 222.

4.4.2.4. Consulta de usuarios

Esta opción se utiliza para mostrar los datos uno de los usuarios y si cuenta con una huella asociada, se realiza por medio del código o por el nombre y apellidos, ver figura 39.

Figura 39. **Consulta de usuarios**

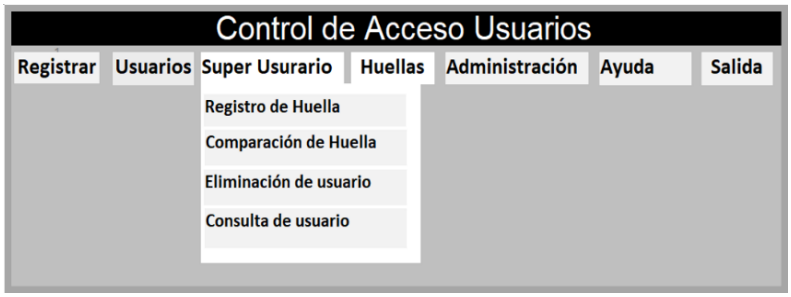


Fuente: TAPIADOR MATEOS, Marino; SIGÜENZA PIZARRO, Juan Alberto. *Tecnologías biométricas aplicadas a la seguridad.* p. 222.

4.4.3. El menú súper usuario

Esta opción es para crear un súper usuario que será el encargado de dar la confirmación si el usuario ingreso o egreso correctamente y si en verdad entro al establecimiento o al bus escolar. Los súper usuarios serían los encargados como el piloto, padres de familia, recalus. El proceso para el registro de un súper usuario es el mismo que el de la sección 4.4.2., ver figura 40.

Figura 40. **Menú súper usuario**

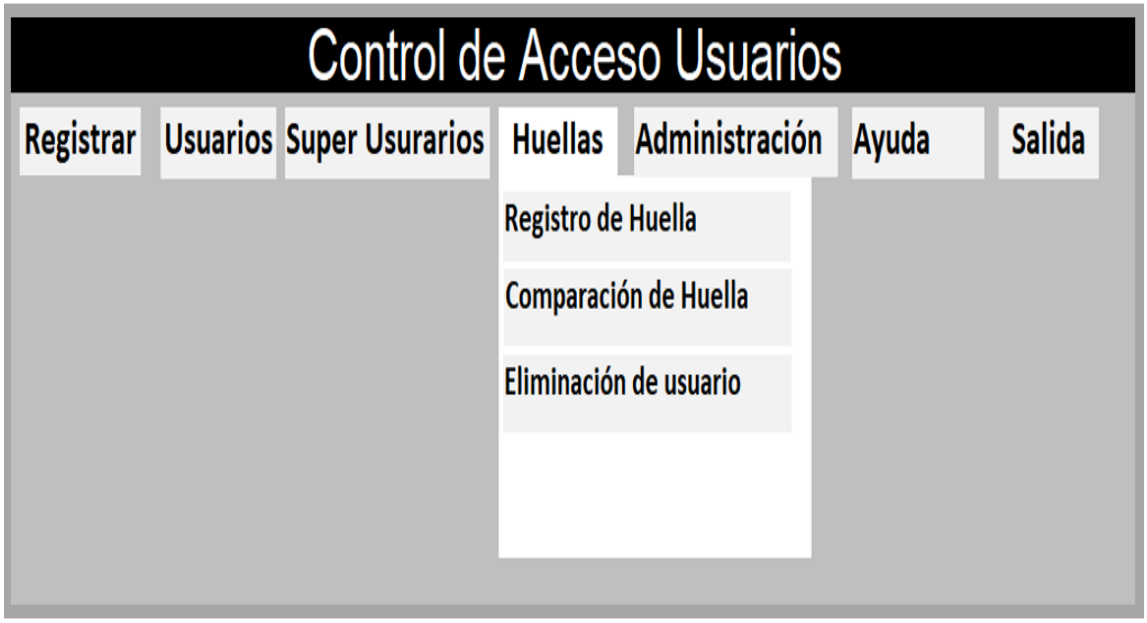


Fuente: elaboración propia, empleando Access.

4.4.4. El menú huellas

Para acceder a esta función al igual que las otras, el sistema solicita ingresar el código de identificación y una vez verificado se puede ingresar a opciones como registro, comparación o eliminación, ver figura 41.

Figura 41. **Menú huellas**



Fuente: elaboración propia, empleando Access.

4.4.4.1. Registro de huella

Para realizar el registro de la huella se debe validar la información del individuo por medio de la colocación de la yema del dedo en cuatro veces para que el modelo sea validado y asociado con la base de datos. ver figura 42.

Figura 42. **Registro de huella**

Fuente: TAPIADOR MATEOS, Marino; SIGÜENZA PIZARRO, Juan Alberto. *Tecnologías biométricas aplicadas a la seguridad.* p. 225.

4.4.4.2. Comparación de huella

Esta función es empleada para comprobar si el registro de la huella dactilar se realizó de forma correcta, ver figura 43. Al igual que todas las funciones es necesario acceder por medio del ingreso del código personal para que se pueda validar que este existe para luego ser comparado en la base de datos.

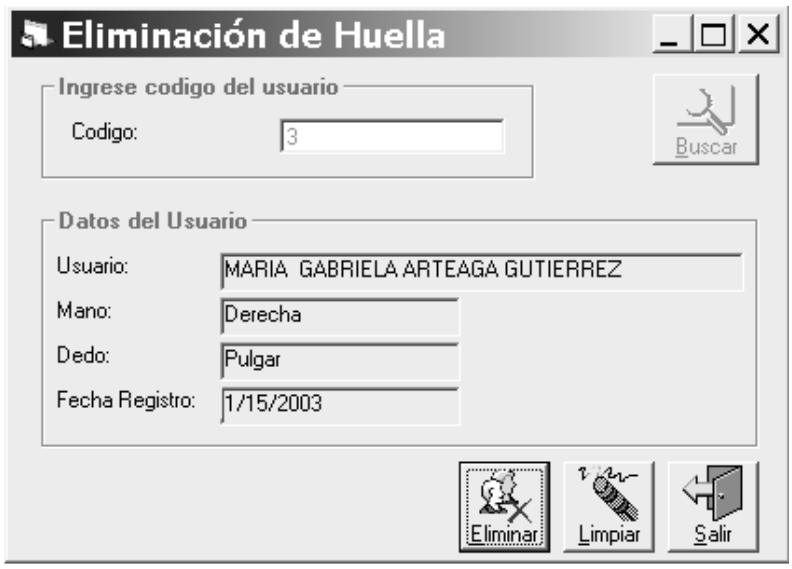
Figura 43. **Verificación de huella**

Fuente: TAPIADOR MATEOS, Marino; SIGÜENZA PIZARRO, Juan Alberto. *Tecnologías biométricas aplicadas a la seguridad.* p. 225.

4.4.4.3. Eliminación de huella

Para eliminar un registro de una huella del sistema, deben de realizarse los mismos pasos que en las opciones anteriores para poder ser autorizado y luego de ello se puede realizar la eliminación, ver figura 45.

Figura 44. **Eliminación de huella**

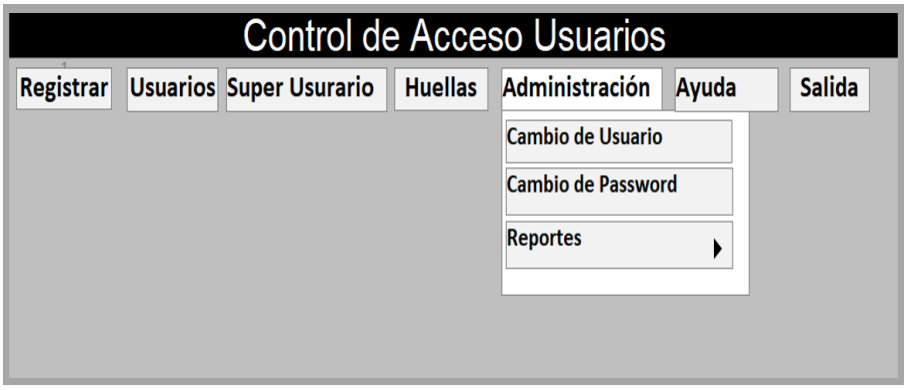


Fuente: TAPIADOR MATEOS, Marino; SIGÜENZA PIZARRO, Juan Alberto. *Tecnologías biométricas aplicadas a la seguridad.* p. 225.

4.4.5. El menú administración

Se realizan informes de los usuarios almacenados en la base de datos y de los que han intentado ingresar y han sido guardados como erróneos, para ingresar a este se requiere que sean validados por medio de la identificación del administrador.

Figura 45. **Menú administración**

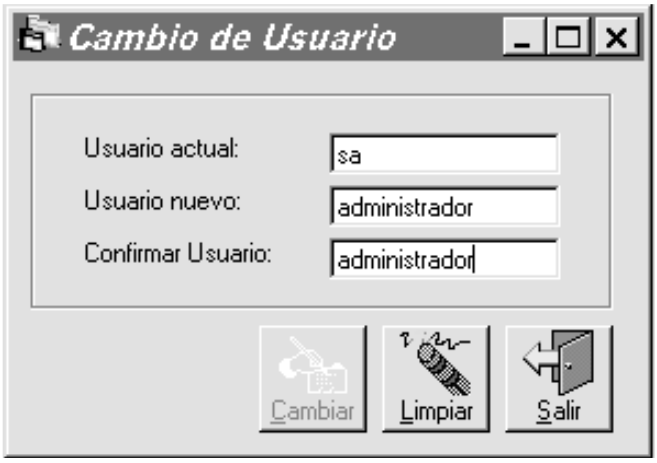


Fuente: elaboración propia, empleando Access.

4.4.5.1. Cambio de usuario

Esta función es utilizada por medio del ingreso del nombre del individuo actual y realizando el cambio de nombre para por último confirmar la acción, ver figura 46.

Figura 46. **Cambio de usuario**



Fuente: TAPIADOR MATEOS, Marino; SIGÜENZA PIZARRO, Juan Alberto. *Tecnologías biométricas aplicadas a la seguridad.* p. 229.

4.4.5.2. Cambio de clave

Esta función se utiliza del mismo modo que el cambio de administrador, se deben seguir los mismos pasos y al concluir con el cambio de clave se debe confirmar para que el sistema actualice el cambio, ver figura 47.

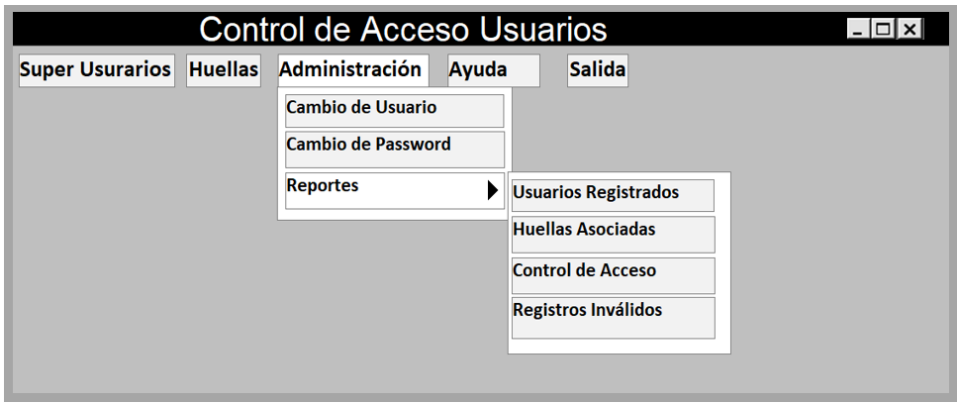
Figura 47. **Cambio de clave**

Fuente: TAPIADOR MATEOS, Marino; SIGÜENZA PIZARRO, Juan Alberto. *Tecnologías biométricas aplicadas a la seguridad.* p. 229.

4.4.5.3. Menú Reportes

Este menú se utiliza para controlar los ingresos y egresos del bus de los usuarios y sus datos, creando reportes que se pueden imprimir o simplemente ser almacenados en el computador en el programa Excel, ver figura 48.

Figura 48. **Menú de reportes**



Fuente: elaboración propia, empleando Access.

4.4.5.3.1. Usuarios registrados

Este se emplea para realizar informes de los usuarios localizados en la base de datos del sistema, ver figura 49.

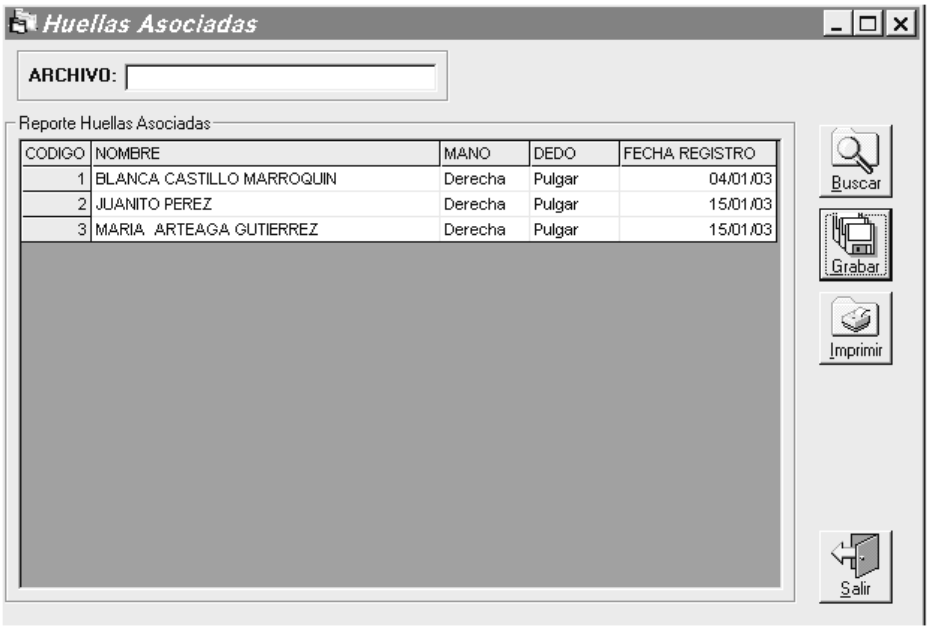
Figura 49. **Usuarios registrados**

Fuente: TAPIADOR MATEOS, Marino; SIGÜENZA PIZARRO, Juan Alberto. *Tecnologías biométricas aplicadas a la seguridad.* p. 231.

4.4.5.3.2. Huellas asociadas

Para realizar este reporte es necesario que la huella se encuentra registrada en la base de datos por la fecha que se ingresó la primera vez, ver figura 50.

Figura 50. **Huellas asociadas**

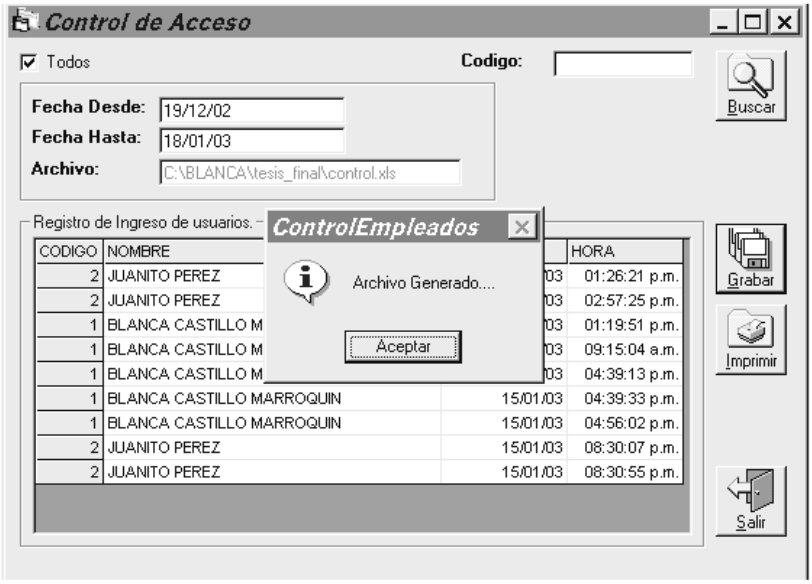


Fuente: TAPIADOR MATEOS, Marino; SIGÜENZA PIZARRO, Juan Alberto. *Tecnologías biométricas aplicadas a la seguridad.* p. 231.

4.4.5.3.3. Control de acceso

Con esta función se puede acceder al registro por fechas de todos lo0s individuos que han ingresado al sistema, además, en este se puede visualizar el código personal, el nombre, la fecha y la hora, ver figura 51.

Figura 51. **Control de acceso**

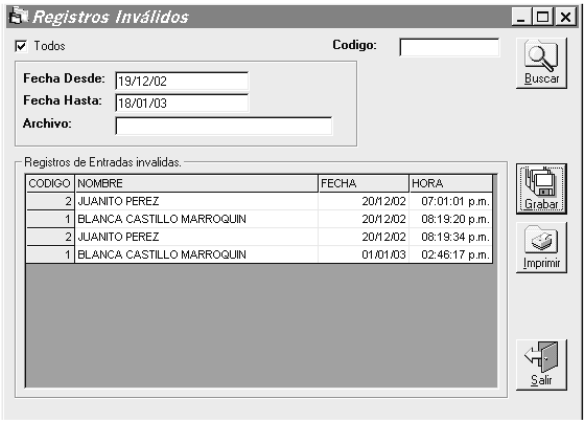


Fuente: TAPIADOR MATEOS, Marino; SIGÜENZA PIZARRO, Juan Alberto. *Tecnologías biométricas aplicadas a la seguridad.* p. 231.

4.4.5.3.4. Registros inválidos

Este registro muestra todas las fechas y la hora en que ha intentado ingresar algún usuario que no cuenta con una huella almacenada en base de datos, ver figura 49. Posterior a general un reporte, se puede almacenar este registro en hojas Excel, como se ejemplifica en la figura 52.

Figura 52. **Registros inválidos**



Fuente: TAPIADOR MATEOS, Marino; SIGÜENZA PIZARRO, Juan Alberto. *Tecnologías biométricas aplicadas a la seguridad.* p. 232.

Figura 53. **Reportes de control de acceso**

Microsoft Excel - control

Archivo Edición Ver Insertar Formato Herramientas Datos Ventana ?

B8 = 2

	A	B	C	D	E	F
1						
2			CONTROL DE ACCESO A USUARIOS			
3						
4		REPORTE:	Control de Acceso			
5		FECHA:	18/01/03 10:03:04 a.m.			
6						
7		CODIGO	NOMBRE	FECHA	HORA	
8		2	JUANITO PEREZ	01/01/03	01:26:21 p.m.	
9		2	JUANITO PEREZ	01/01/03	02:57:25 p.m.	
10		1	BLANCA CASTILLO MARROQUIN	02/01/03	01:19:51 p.m.	
11		1	BLANCA CASTILLO MARROQUIN	11/01/03	09:15:04 a.m.	
12		1	BLANCA CASTILLO MARROQUIN	15/01/03	04:39:13 p.m.	
13		1	BLANCA CASTILLO MARROQUIN	15/01/03	04:39:33 p.m.	
14		1	BLANCA CASTILLO MARROQUIN	15/01/03	04:56:02 p.m.	
15		2	JUANITO PEREZ	15/01/03	08:30:07 p.m.	
16		2	JUANITO PEREZ	15/01/03	08:30:55 p.m.	
17						
18						

Fuente: TAPIADOR MATEOS, Marino; SIGÜENZA PIZARRO, Juan Alberto. *Tecnologías biométricas aplicadas a la seguridad.* p. 234.

4.5. Costo total

El prototipo del proyecto se estima en:

Tabla XIV. **Costos directos**

COSTOS DIRECTOS		
No.	Descripción	Total en Q
1	Raspberry Pi 4	750
1	Pantalla LCD Raspberry Pi 4	500
1	Router Wi-fi 4G móvil	360
1	Inversor de corriente autmotriz	250
1	Lector de huella Suprema BioMini 2	480
Total de costos directos		2 340

Fuente: elaboración propia, empleando Word.

Tabla XV. **Costos indirectos**

COSTOS INDIRECTOS		
No	Descripción	Total en Q
1	Licencias de Programa	2 000
1	Espacio en la nube AWS	136
1	Imprevistos	1 000
Total de costos directos		3 136

Fuente: elaboración propia, empleando Word.

Tabla XVI. **Costo total**

COSTO TOTAL	Q 5 476

Fuente: elaboración propia, empleando Word.

5. SEGUIMIENTO O MEJORA

5.1. Resultados obtenidos

Ante la preocupación de instituciones, establecimientos escolares y padres de familia por el bienestar y seguridad de la comunidad estudiantil y al ver que no está dentro de los temas más relevantes entre ciudadanos e instituciones que deberían de velar por la seguridad de las personas. Se realizó este diseño con la finalidad de reducir la probabilidad que un alumno sea recogido de los establecimientos educativos sin tener la autorización correspondiente para llevar a cabo esta acción. Así mismo hacer decrecer la probabilidad que un alumno abandone los establecimientos educativos sin la supervisión adecuada, exceptuando a los casos extraordinarios que necesiten abandonar el establecimiento educativo. La gran mayoría de servicios enfocados en la localización del autobús, y no se concentran en el monitoreo de ingreso y egreso de la comunidad estudiantil en el autobús.

Hay sistemas diseñados para la seguridad, sistemas con metodología de monitoreo de todo el personal dentro del establecimiento educativo como en el automotor del sistema educativo, autobús, a través de dispositivos como cámaras de vigilancia más dispositivos que registran el acceso del personal como del alumnado. Estos sistemas de seguridad de control de acceso se han propagado con un grado de importancia alto ya que proporcionan un gran componente en los proyectos de seguridad.

Cabe agregar por cuestiones de criterio y por aceptación en el mercado no se puede definir como un sistema más eficiente que otro, siempre los sistemas

se pueden enfocar en diversos temas, en el caso del monitoreo y control de la comunidad educativa en este caso en los alumnos surge un conflicto ya que en la comunidad educativa de corta edad sigue latente, no portaran ningún tipo de dispositivo removible si se logra evitar, no se puede usar uno no removible, ya que provoca mucha discrepancia y conflicto dentro de la sociedad, por derechos humanos y consideraciones éticas. Denegando así el uso de microfichas. Existe una variedad de procedimiento de seguridad para el monitoreo y control, de los cuales sobresale el tener un control a través de una ficha colocada en la mochila del niño con toda la información correspondiente, siendo esta la más antigua.

El sistema tradicional de seguridad se basa en que los encargados ejecuten estos sistemas, sin embargo, se reduce la eficiencia por las tareas adicionales que los encargados deberán realizar. Al intentar retirar a un alumno del establecimiento educativo y el alumno no conociera a este individuo, este tendría que avisar a las autoridades correspondientes. Debido a la deficiencia de estos sistemas es que surge la necesidad de implementar los sistemas de seguridad avanzada como lo son los de seguridad biométrica.

Surge una complicación, es el tema de estacionamiento temporal, debido a la espera que tendrán que hacer ya que no se pueden retirar hasta que no se encuentre todos los alumnos que se trasladan en este vehículo.

El planteamiento y diseño del sistema genero elementos con alto grado de interés, uno de ellos es compartir el prototipo desarrollado con otros.

El sistema se diseñó para ser utilizado con cualquier clase de dispositivos de identificación de usuarios, es debido a que el funcionamiento del mismo se basa en los mecanismos de verificación y autenticación.

Se detallaron los requisitos que instruyeron al prototipo del sistema y del impacto del sistema y las funciones mencionadas. Posteriormente, se describen los elementos esenciales del prototipo de datos. Se adjuntan una descripción de las actividades y operaciones del proceso que condujo al modelo del sistema seleccionado. Se describe la función principal del sistema, el monitoreo y control del ingreso y egreso del alumno en el bus.

5.1.1. Interpretación

Existirá un súper usuario para control y monitoreo del sistema, a estos se les otorgará un único código para el acceso. Se utilizará elementos básicos hasta dispositivos biométricos. Es un sistema con la intención de ser más eficiente con el tiempo y abierto a la utilización de dispositivos con mejoras tecnológicas para tema de la seguridad, siempre poniendo como primera necesidad la seguridad de la comunicada educativa, y de esta comunidad al alumnado. Para mayor tranquilidad de los padres de familia y de los establecimientos de educación que velan por la educación y seguridad de los niños

Existirá un usuario con los permisos debidamente otorgados que podrán retirar a los alumnos de los establecimientos educativos, y para los buses se tendrá el sistema para que el alumno quede registrado la hora, fecha donde es dejado por el automóvil escolar, autobús. A los usuarios que tendrán los permisos para retirar a los alumnos se les denominara recalu. Sin embargo, agregaran restricciones en un factor muy importante el tiempo en que se podrá retirar a un alumno del establecimiento o del bus escolar o tener un rango de traslado de los alumnos en el transporte escolar del establecimiento hasta su punto de llegada.

Existirán casos que los recalus no podrán recoger al alumno del establecimiento y del bus escolar así que podrán delegar a otros usuarios esa

función y estos nuevos recalus son temporales con todos los permisos adecuados y registrados en el sistema, esos nuevos recalus no podrán ejecutar su función luego del tiempo que los delegados autorizaron y el sistema tendrá un rechazo de acceso si intentan acceder al retiro del alumnado. Se denominará portero a la persona o dispositivo que verificará el ingreso y egreso del alumnado ya sea en el establecimiento escolar o en el transporte escolar.

El sistema deberá proveer al portero en este caso a nuestro sistema de control biométrico, los datos necesarios para identificar al alumno que ingrese y egrese del transporte escolar, tanto como el establecimiento educativo.

El sistema está diseñado para que utilice los datos de un año escolar. Se le dará una bandera de inicio que será el mes uno, por lo que no se le incluye el año a cualquier registro. Todo estará ordenado según el año escolar. Siempre existirá una metodología para cada inicio escolar, se registrarán alumnos, personal educativo, recalu, delegadores.

Un factor muy importante, el cual es un componente útil, es el concepto de bloque de alumnos que egresarán de una manera simultánea del establecimiento educativo, todo el alumnado que utilizará el transporte escolar.

Este factor genera nuevas dificultades, una de ellas es el problema de tránsito durante el abordar de los alumnos en el establecimiento, donde el transporte escolar no llegará a la puerta, hasta que el bloque de alumnos que se transportará en ese autobús, estén listos para abordar.

5.1.2. Aplicación

Se definieron y describieron las funciones primordiales a partir de ciertos criterios y requisitos que la aplicación necesita para el control y monitoreo de los alumnos tanto en el autobús escolar como dentro del establecimiento educativo. El diseño comenzó como una metodología estructurada, se presentan requisitos, que se convierten en funciones que el modelo soporta. Las cuales se presentan en un listado, el orden del listado no tiene significado.

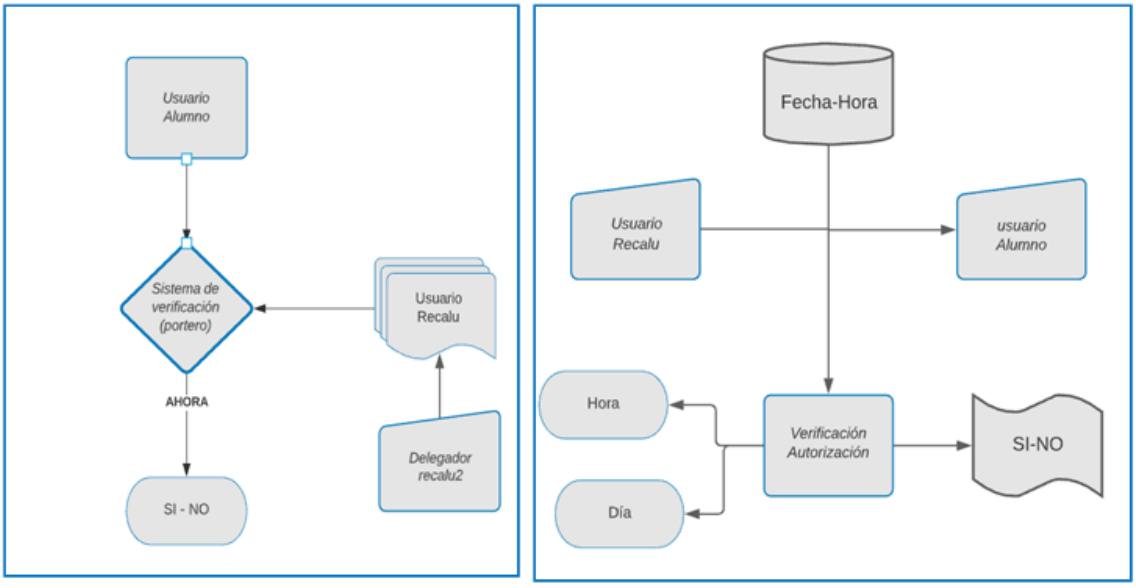
- Actualización de todo tipo de usuarios que requerirán el sistema, especialmente a los alumnos y a los que serán recalu de los alumnos.
- Registro de recalu y delegadores. Procedimiento para la creación de nuevos recalu y delegadores temporales con ciertas restricciones.
- Proceso para autorizar a recalus en el transporte escolar.
- Actualización del tipo de usuarios de empleas específicamente a los del transporte escolar.
- Actualización del tipo de usuarios alumnado que se trasladaran en el transporte escolar.
- Proceso que ejecutara cuando un usuario del alumnado pretenda retirarse del establecimiento.
- Proceso que se ejecutara cuando un usuario del alumnado cuando requiera retirarse del autobús en un lugar incorrecto o con un individuo no registrado.

La función se describe como verdadero/si-falso/no utilizando como clave la palabra alum para los alumnos y para el usuario encargado de retirar con al alumno con toda la autorización adecuada se utilizará reca:

F (alum, reca, fecha, hora) = verdadero/falso

La función será tomada como verdadera/si cuando el usuario denominado recalu sea el correcto, el usuario debe de estar autorizado y registrado los requisitos del permiso, la figura 51 describe este proceso esquemáticamente.

Figura 54. **Esquema del sistema**



Fuente: elaboración propia, empleando Lucidchart.

Se debe tomar la probabilidad que un usuario alumno tenga un permiso extraordinario de retirarse del establecimiento por su propia cuenta, se crea un usuario llamado solo, para que pueda recoger a cualquier usuario alumno siempre respetando todos los lineamientos.

5.2. Ventajas y beneficios

La necesidad de diseñar el sistema con la función principal de monitorear el ingreso y egreso del alumnado tanto al establecimiento educativo como en el transporte escolar, autobús. Se mencionan las complicaciones y dificultades que presentó el diseño descrito con anterioridad: registros y actualizaciones de los usuarios recalus y los usuarios delegadores o bien recalus2. La mayoría de estos usuarios son padres de familia, más cuando toman el papel de recalu2 o delegadores puesto que muchas veces solo utilizaran el sistema por ocasiones y/o delegan a terceros por situaciones impredecibles. Teniendo en cuento en todo momento la necesidad y prioridad de ofrecer el sistema más eficiente y sencillo para registro de permisos y dar las autorizaciones necesarias.

A cada persona se le otorgarán permisos para cada usuario alumno y serán almacenados. En el sistema se les llamara a los usuarios que asignan permisos como delegadores de permisos.

Al momento de interpretar y determinar si un usuario alumno G puede salir, con un usuario recalu C, el sistema procesa y verifica los permisos asignados al usuario C. Si el modelo del sistema permite el registro de información contradictoria, se hará notar efecto que toma por este tipo de información. Intencionalmente a la diversidad de registros se le asigno prioridad. Se hizo uso del principio: prohibiciones tienen prioridad sobre los permisos.

Al obtener un resultado deficiente y equivocado, se vio a la necesidad de complementar un principio cronológico. El dato más actual tenía proveniencia de la información antigua. Al complementar estos diseños generaron nuevas dificultades donde el diseño resalto el modelo que no se adoptaría.

Estas prácticas llevan a una conclusión, se debe almacenar los datos de forma contraria para esquivara contradicciones. No se guardará los horarios permitidos o denegados. Se ingresará y almacenará para cada día si existía permiso o no para cada recalu de cada usuario alumno. Se experimentó con dos tipos de modelos.

Un modelo, al notar la ausencia en un día, tomaba como permiso denegado. La respuesta del otro modelo, hizo que se desechara, no sumaba funcionalidad a la aplicación.

5.3. Propuestas de mejora basada en tendencias en el servicio de transporte de bus escolar

Lo anterior oriento al diseño implementado en sistema. Con las autorizaciones de los usuarios alumnos para el egreso del establecimiento educativo.

Se almaceno un indicador, de permiso existe/no existe y se desechó el modo registro para cada día. El indicador toma valor de 0-1, para cada día del mes, declarando 31 días por cada mes. Se sustituyó los caracteres por bits. Una cada de bits se toma de 32 bits y se almacena como 4 bytes.

Cada recalu adopto 12 campos uno para cada mes del año y cada campo se compone de 4 bytes. Los meses se tomarán por ciclo escolar, dejando nulo la numeración por calendario. Este diseño tuvo una reducción elevada de almacenamiento en el disco. Se hace mención de esta circunstancia, aunque no es clasificada como importante en diversidades instancias. Debido a las enormes capacidades de almacenamiento de los dispositivos, pero por fines de sistemas eficientes y muy bien diseñados aprovechar bien los recursos. Otra reducción

que se obtuvo con este diseño es en los procesos, aunque relativamente no causo tanto impacto, por lo grande que es proporcionalmente el diseño.

Tradicionalmente, disminuir un proceso no se percibirá si primeramente se contaba con el mismo retardo. No se notará el impacto especialmente en procesos que no se ejecutan simultáneamente en forma masiva. Aunque no sea notorio para los demás, pero para el desarrollador si causa impacto puesto que tienen la certeza que su trabajo se ha realizado con alto grado de eficiencia. Cabe mencionar que el sistema fue diseñado con la mayor eficiencia posible para uso simultáneo, es decir el establecimiento y transporte escolar lo pueden usar en distintas puertas o transportes. A estas estaciones o puertas llegaran usuarios alumnos simultáneamente esto significa que se crea un intervalo muy corto por cada ingreso y egreso.

El proceso para determinar si un usuario recalu posee permiso en un día de un mes, se verifica que bit corresponde a ese día. La secuencia de los bits es de izquierda a derecha, entonces el día uno tomara un bit 0, para verificar si un día concierne a un bit 1, se intersecta el valor que incluye los permisos de cada día con el valor de 2dia/1. Si la bandera del bit esta levantada es decir, si está encendida, se obtendrá el mismo resultado 2dia/1. De lo contrario, el bit tomara el valor de 0. Se registraron y almacenaron las potencias de base 2 en un arreglo A_pobase_de_dos [0 to 30]. Este arreglo servirá para no estar calculando la potencia en cada uso correspondiente. Tendrán un valor de 4 bytes, se guarda la potencia de base 2 concerniente al índice del arreglo. De esta forma se llama a ejecutar esta operación: Egreso aprobado = (N ∩ A_pobase_de_dos (día – 1) > 0).

Para los usuarios recalu2 o usuarios de los delegadores, se complementó el mismo modelo de los 12 campos que sus dígitos simbolizan cada día del mes.

CONCLUSIONES

1. La utilización del dispositivo de reconocimiento de huellas Suprema BioMini Plus 2, es un dispositivo fiable, duradero y resistente, y que además tiene una integración con los navegadores web.

2. Luego de aplicar la metodología de desarrollo Scrum, se resalta la eficacia de la metodología al lograr que el proyecto se centre en el desarrollo con pequeños entregables hechos de forma iterativa, permitiendo que el sistema vaya mejorando continuamente para el bienestar de los usuarios.

3. Los resultados logrados demuestran que, ante una necesidad como la toma de asistencia estudiantil, una aplicación web puede desarrollarse e implementarse de manera eficiente y capaz de cubrir la necesidad de la mejor manera posible.

4. En el resultado exitoso de estos sistemas de registro de asistencia, sobresale el sistema que se implementa en la web y con varias ventajas sobre otros que son para escritorio.

RECOMENDACIONES

1. Al usar el sistema que en caso la huella no sea detectada, tratar de colocar el dedo de forma suave pero firme e intentar una vez más.

2. Si con eso aún la huella no es reconocida, verificar que la pantalla del dispositivo esté de color azul y que parpadee unas luces rojas al colocar el dedo.

3. El sistema tiene un mecanismo de seguridad integrado que impide que personas ajenas a la institución manipulen el sistema, pero siempre tener la precaución de no dejar el dispositivo suelto sin ninguna protección, de no usar los módulos de registro y control de asistencia fuera de la institución educativa y no utilizar el sistema durante los mantenimientos programados.

4. No hay restricción del sistema operativo, pero se recomienda el uso de un sistema operativo Windows a partir de la versión 7 con una versión de Java 8.

BIBLIOGRAFÍA

1. ARAUJO SERNA, Lourdes; MARTÍNEZ UNANUE, Raquel; RODRÍGUEZ ARTACHO, Miguel. *Programación y estructuras de datos avanzadas.* Madrid, España: Editorial Universitaria Ramón Areces, 2011. 48 p.

2. ASIS Internacional. *Protección de activos: Seguridad física.* Estados Unidos de América: ASIS, 2014. 307 p.

3. CARRETERO, Jesús, GARCÍA-CARBALLEIRA, Félix; PÉREZ, Fernando. *Prácticas de sistemas operativos.* 2a ed. Estados Unidos de América: CreateSpace Independent Publishing, 2017. 164 p.

4. FAGA, Héctor Alberto. *Como profundizar en el análisis de sus costos para tomar mejores decisiones empresariales.* 2a ed*.* Buenos Aires, Argentina: Granica, 2006. 87 p.

5. FARRIOLS I SOLÁ, Antoni. *La protección de datos de carácter personal en los centros de trabajo.* España: Fundación Largo Caballero, 2006. 26 p

6. FERRO VEIGA, José Manuel. *Técnicas de investigación en investigación privada.* España: 2020. 1439 p.

7. GÓMEZ VIEITES, Álvaro. *Seguridad en equipos informáticos.* Madrid, España: Grupo Editorial RA-MA, 2014. 128 p.

8. IBARRA SIXTO, Alejandro. *Diccionario de física.* España: EComplutense S.A., 2007. 560 p.

9. MARÍ SAGARRA, Ricard. *El código PBI. España:* Universitat Politécnica de Catalunya, 2010. 145 p.

10. MARTÍN RAMOS, Rafael. *Documentoscopía: Método para el peritaje científico de documentos*. Argentina: La Ley, 2010. 367 p.

11. MURIAS RIGUAL, Marta. *Estudio de adaptación de un sistema de reconocimiento biométrico en ATMs.* España: Universitat Politécnica de Catalunya, 2016. 41 p.

12. PRABHAKAR, Salil; ARUN, A. Ross. *Biometric technology for human identification.* Estados Unidos de América: SPIE, 2007. 71 p.

13. PRESSMAN, Roger S. *Ingeniería del software: Un enfoque práctico.* México: McGraw Hill, 2013. 174 p.

14. ROMERO CASTRO, Martha Irene y otros. *Introducción a la seguridad informática y el análisis de vulnerabilidades.* España: 3Ciencias, 2018. 54 p.

15. SERRATOSA, Francesc*. Biometría. España:* Universitat Aberta de Catalunya, 2012. 74 p.

16. SIMÓN ZORITA, Danilo. *Reconocimiento automático mediante patrones biométricos de huella dactilar.* España: 2003. 106 p.

17. TAPIADOR MATEOS, Marino; SIGÜENZA PIZARRO, Juan Alberto. *Tecnologías biométricas aplicadas a la seguridad*. Madrid, España: Grupo Editorial RA-MA S.A., 2005. 456 p.

18. THIEMAN, William J.; PALLADINO, Michael A. *Introducción a la biotecnología.* 2a ed. España: Pearson, 2010. 279 p.

19. VILLALÓN HUERTA, Antonio. *Seguridad en Unix y redes. Versión 2.1.* España: Edicions Culturals Valenciannes, S.A., 2020. 205 p.

20. VILLEGAS, Hyxia; BOSNAJK, Antonio. *Bioingeniería en Venezuela: Tendencias, propuestas y avances.* Venezuela: Asociación Venezolana de Investigación y Desarrollo en Bioingeniería, BIOVEN, 2008. 143 p.