ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

Diseño e implementación de un sistema de control de asistencia de personal, mediante el uso de tecnología biométrica de huella dactilar

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y REDES DE INFORMACIÓN

LUIS MIGUEL CHUQUI CHICAIZA
luchuqui@gmail.com

DIRECTOR: ING. JOSÉ ADRIÁN ZAMBRANO MIRANDA
jose.zambrano@epn.edu.ec

Quito, Julio 2014

DECLARACIÓN

Yo, Luis Miguel Chuqui Chicaiza, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

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

Luis Miguel Chuqui Chicaiza

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Luis Miguel Chuqui Chicaiza, bajo mi supervisión.

Ing. Adrián Zambrano.
DIRECTOR DE PROYECTO

DEDICATORIA

Este trabajo es dedicado para mis padres, Magdalena del consuelo Chicaiza y Washington Leonardo Chuqui. Quienes me apoyaron con sus concejos, en este camino arduo, lleno de complicaciones e inconvenientes, a través de su motivación diaria para culminar la carrera; por transmitirme sus valores para ser una persona de bien, pero más que nada por su amor y apoyo incondicional.
La finalización de este proyecto es dedicado a ustedes.

Luis Miguel Chuqui Chicaiza.

El dinero hace personas ricas.

El Conocimiento hace personas sabias.

Pero la humildad hace grandes personas

Anónimo

AGRADECIMIENTOS

Agradezco a mis abuelitas, María Rosalía Toapanta y María Hortencia Maila, quienes con sus cuidados y respaldo, me ayudaron y apoyaron en la etapa universitaria.

A mis hermanos Washington Leonardo Chuqui y Richar Geovanny Chuqui, quienes fueron un apoyo y ejemplo, para culminar la carrera.

A mis amigos de la universidad, con quienes realice proyectos semestrales, estudiamos para las pruebas y exámenes finales, festejamos la aprobación de las materias y la amargura de pérdida de materia, muchas gracias por ser mis amigos.

A mi tutor de proyecto de titulación, Ing. Adrián Zambrano, por confiar en mí y tenerme paciencia en el desarrollo de este proyecto.

Agradezco a mis compañeros de COONECTA, por confiar en mis conocimientos y ayudarme con mi desarrollo profesional y personal.

Luis Miguel Chuqui Chicaiza

CONTENIDO

CONTENIDO FIGURAS

CONTENIDO TABLAS

CONTENIDO ECUACIONES

RESUMEN

El presente proyecto de titulación describe el desarrollo del sistema de registro de horas de empleados, utilizando la tecnología biométrica de huella dactilar, la cual cuenta con la documentación escrita en cinco capítulos, más diez anexos, que contiene información, para realizar el desarrollo de la aplicación biométrica; así como las pruebas realizadas para el proceso de registro mediante la autenticación del empleado.

El primer capítulo describe las características necesarias, que posee un sistema biométrico para realizar la identificación de la persona como es: unicidad, universalidad, permanencia y cuantificación. Estas características poseen los sistemas biométricos de huella dactilar, iris, retina, geometría de la mano, reconocimiento facial, termo gramas faciales y análisis de ADN. Además se describe el proceso de autenticación de cada uno de estos sistemas, y se realiza una comparación de estos procesos de autenticación y el hardware que necesita cada sistema. Finalmente, se describe el modelo de arquitectura distribuido de n capas, describiendo el funcionamiento, ventajas y desventajas de esta arquitectura.

EL segundo capítulo describe los requerimientos del sistema, para realizar la administración, mediante el análisis de requerimientos como: manejo de horario laborable, ingreso y actualización de datos del empleado, implementación de políticas de seguridad para proteger la información tales como manejo de perfiles de acceso, creación de usuarios para el sistema y manejo de archivos de configuración para los servicios. Además se realiza la comparación y selección del dispositivo biométrico de huella dactilar que interactuará con la aplicación y permitirá realizar la captura de la huella dactilar para ser procesada.

En el capítulo tres se realiza el diseño de la aplicación biométrica mediante los requerimientos establecidos en el capítulo dos, utilizando los métodos de modelado de software para realizar el desarrollo de la aplicación como: el modelo de clases de uso, modelo de clases, modelo de secuencia y modelo de flujo.

Considerando los distintos modelos de software, se procede a realizar la implementación de la aplicación del sistema, con ayuda del lenguaje de programación C#, y finalmente se utiliza para almacenar la información del sistema la base datos SQL Server 2008.

En el capítulo cuatro se presenta la información necesaria para realizar la instalación de las aplicaciones del sistema biométrico, los cuales son: cliente biométrico, servidor biométrico y administrador biométrico, en las computadoras destinadas para el funcionamiento del mismo. Además se utiliza el log de registros del servicio de autenticación y los registros almacenados en la base de datos, para determinar el porcentaje de aciertos del sistema biométrico y su uso del sistema biométrico por parte de los empleados.

En el capítulo cinco se presentan las conclusiones y recomendaciones obtenidas durante el proceso de desarrollo de la aplicación, tomando en cuenta las observaciones encontradas durante el proceso, como son elección del hardware, elección del tipo de datos seleccionados en el sistema y proceso de validación.

PRESENTACIÓN

La biometría es una tecnología que se dedica al estudio de las características únicas del individuo para la identificación como: huella dactilar, silueta de la mano, patrones de la retina, iris, voz o la firma.

La identificación del individuo por huella dactilar es una técnica, que es utilizada en la mayoría de las empresas grandes o pequeñas, debido a su bajo costo en comparación con las otras tecnologías biométricas, ya que permiten realizar la identificación del individuo con un margen de error mínimo.

El sistema a continuación desarrollado abarca la mayoría de requerimientos que necesita un sistema de control de horas de empleado tales como: creación y modificación de empleados, creación y modificación de horarios laborables, creación y modificación de dispositivos biométricos, registro de permisos de empleado, creación y modificación de usuarios y presentación de datos almacenados en el sistema mediante reportes.

CAPÍTULO 1
SISTEMAS BIOMÉTRICOS

En el presente capítulo se estudia los principales elementos que conforman un sistema biométrico, analizando sus elementos como: hardware y algoritmos utilizados para realizar la autenticación de los individuos con la finalidad de comprender el funcionamiento de estos sistemas.

Además, se explica el modelo de software arquitectónico de n capas que es utilizado en el desarrollo de aplicaciones distribuidas, el cual consiste en separar las funciones por cada capa o nivel como: la capa presentación, lógica de negocios y la capa de acceso a datos.

1.1 BIOMETRÍA

El término biometría proviene de las palabras: *bios* (vida) y *metron* (medida). “La biometría es la ciencia que estudia las características únicas que posee una persona” [1] tales como: rostro facial, mano, huella dactilar, voz, silueta e iris, mediante el uso de métodos estadísticos y algoritmos para conseguir la detección del individuo. Dichos métodos “presentan un pequeño margen de error en la realización de la identificación de la persona.”[1]

Los sistemas biométricos aquellos que pueden ser automatizados y dependen de los rasgos o características únicas que tiene una persona, para realizar su autenticación. Los métodos biométricos poseen la necesidad obligatoria de que la persona se encuentre físicamente en el lugar de la identificación, siendo o no obligatoria su colaboración[1].

La tecnología biométrica considera que existen elementos únicos e irrepetibles que los individuos poseen de tal forma que, dichos elementos se constituyen en la única alternativa técnicamente factible para identificar a una persona con un ligero margen de error sin necesidad de recurrir a firmas, contraseñas, clave, códigos;

[1] Colaboración se refiere a que el usuario interactúe con el hardware biométrico, mediante una correcta posición del elemento que biométrico para realizar la adquisición de su característica.

que sean sencillos de ser transferidos, sustraídos, descifrados o falsificados con fines fraudulentos.

Para realizar el almacenamiento y la autenticación en un sistema biométrico puede utilizar el siguiente algoritmo, el cual se describe a continuación.

a. Para realizar el almacenamiento de las características biométricas de una persona se utiliza un repositorio y sigue el siguiente procedimiento, el cual esta mostrado en la Figura 1.1.
    1. Obtener el dato biométrico elegido (dedo, mano, ojo, voz, etc.), con la ayuda de un dispositivo de adquisición.
    2. Procesar los datos biométricos utilizando un proceso de extracción y asignación de datos biométricos.
    3. Almacenar el registro procesado en un repositorio local, central o en un *token* portátil, como una tarjeta inteligente.
b. Para realizar la verificación de identidad de un individuo se utiliza el siguiente proceso mostrado en la Figura 1.2.
    1. Obtener el elemento biométrico elegido (dedo, mano, ojo, voz, etc.).
    2. Procesar los datos biométricos y extraer el registro biométrico.
    3. Verificar la coincidencia del registro biométrico escaneado con los registros biométricos almacenados, mediante la utilización de métodos estadísticos.
    4. Asignar una puntuación de coincidencia mediante la comparación de plantillas almacenadas y la plantilla adquirida con el dispositivo biométrico, con la finalidad de efectuar la toma de decisión e indicar si el usuario es quien dice ser.

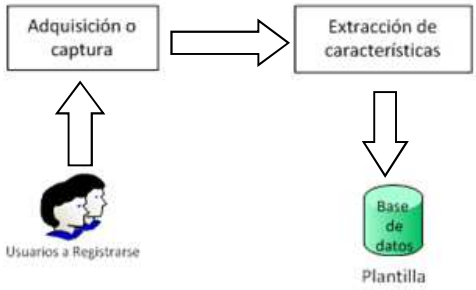

Figura 1.1. Almacenamiento de registro biométrico [1]

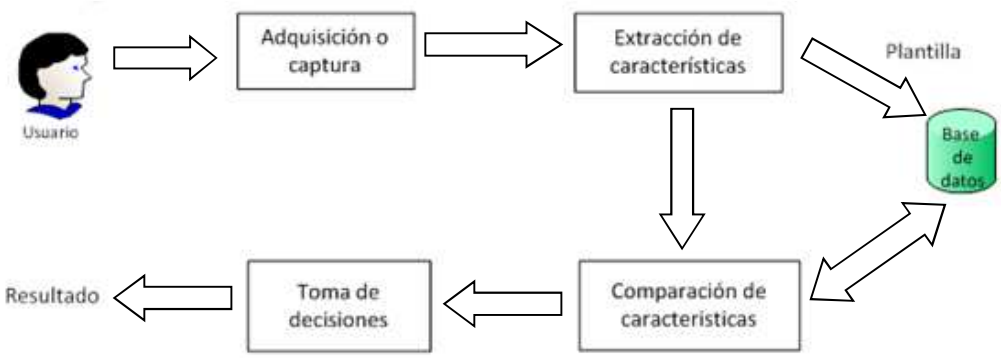

Figura 1.2. Identificación y autenticación de usuario [1]

El software y hardware utilizado en estos sistemas para realizar la adquisición y autenticación; debe poseer funciones específicas tales como: reconocimiento de formas, inteligencia artificial, complejos algoritmos matemáticos para realizar la toma de decisiones de autenticación. Estas funciones desempeñan el papel más importante en los sistemas de identificación biométrica.

1.2 REQUERIMIENTOS DE UN SISTEMA BIOMÉTRICO

Para conseguir un sistema biométrico cien por ciento confiable, se considera las características únicas que posee un individuo tales como: huella dactilar, iris, voz o firma; el cual debe cubrir los siguientes requisitos:

- *Universalidad*: Cualquier individuo posee esa característica.
- *Unicidad:* La probabilidad de que dos individuos posean una misma característica es muy baja.
- *Permanencia:* La característica no puede cambiar en un tiempo a corto plazo.
- Cuantificación: La característica puede ser medida en forma cuantitativa.

Estos requisitos son muy básicos al momento de realizar el estudio y selección de un sistema biométrico.

1.3 MÉTODOS DE IDENTIFICACIÓN BIOMÉTRICA

Los métodos para la autenticación biométrica del individuo pueden separarse en dos grupos tales como:

- *Físicos o Fisiológico.* Estudia las características biométricas que físicamente se encuentran en el individuo como son: huella dactilar, iris, rostro, retina, etc.
- *Comportamiento.* Comprende las características biométricas que dependen del comportamiento del individuo como son: firma, voz, forma, etc.

Cada una de estas características por su naturaleza posee ventajas y desventajas, por lo que la elección de la característica biométrica a emplearse en un sistema dependerá de los requerimientos, niveles de seguridad deseados y costo de implementación del mismo.

1.3.1 MÉTODOS FÍSICOS

En esta sección se describen los métodos más utilizados para realizar la autenticación del individuo:

- ✓ Identificación de huellas dactilares.
- ✓ Reconocimiento del iris.
- ✓ Reconocimiento de la retina.
- ✓ Identificación de la geometría de la mano.
- ✓ Reconocimiento facial.
- ✓ Reconocimiento mediante el uso de termo gramas faciales.
- ✓ Análisis de ácido desoxirribonucleico o ADN.

1.3.1.1 Identificación de huellas dactilares

“En la actualidad el reconocimiento de huellas dactilares es el más usado en todo el mundo” [1], debido a que las huellas dactilares han sido estudiadas y consideradas como una característica única del cuerpo humano. Por mucho tiempo el reconocimiento de huellas dactilares se ha destacado como una de las tecnologías biométricas más robusta; y de bajo costo en comparación con las otras tecnologías biométricas, ya que los sus elementos electrónicos pueden fabricarse en grandes cantidades, “utilizando circuitos integrados y dispositivos electrónicos.” [2]

1.3.1.1.1 Elementos de una huella dactilar

Para comprender cómo funcionan los sistemas biométricos basados en huellas dactilares se deben conocer los elementos que forman parte de la huella dactilar los cuales están representados en la Figura 1.3 y están descritos a continuación.

- *CRESTA:* Son aquellos relieves que forman líneas o segmentos en el dedo.
- *BIFURCACIÓN:* Es una separación de una cresta en dos, esto puede ser considerado como ensanchamiento de una cresta.
- *DIVERGENTE:* Son crestas que corren paralelas e inesperadamente se separan.
- *VALLES:* Es el espacio existente entre crestas.

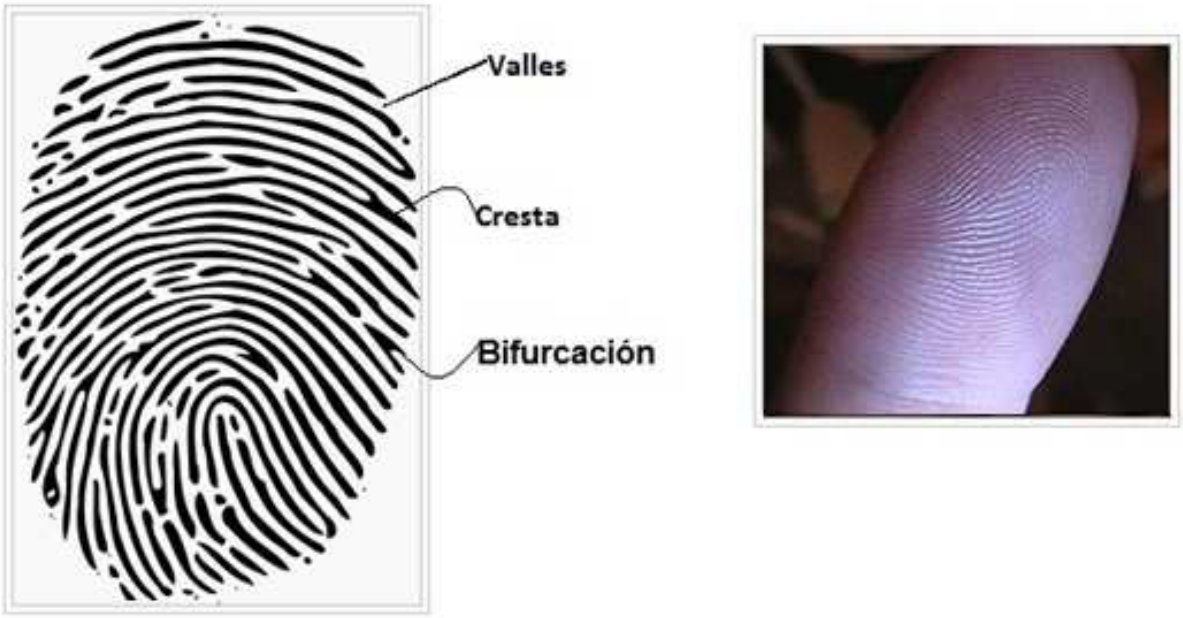

Figura 1.3. Huella dactilar [2]

Figura 1.4. Elementos de una huella dactilar [1]

1.3.1.1.2 Clasificación de la huella dactilar

La clasificación de la huella dactilar es una técnica, que consiste en asignar a una huella un tipo de figura. "Esta clasificación se puede realizar con un emparejamiento de crestas y valles" [3], por lo que primero se clasifica tomando en cuenta la figura que posee un dedo. Esta clasificación puede ser la siguiente.

- *Espiral o Whorl.*
- *Lazo derecho.*
- *Lazo izquierdo.*
- *Arco.*

El patrón de una huella que puede tener un dedo se representa en la Figura 1.5, la cual representa la forma de huellas más comunes. Lo primero es realizar la clasificación de la huella dactilar del individuo, luego se determina las minucias[2] y finalmente se puede realizar la identificación, mediante la utilización de algoritmos de comparación.

Figura 1.5. Tipos de patrones de huellas dactilares [2]

[2] Minucia.- Son puntos específicos que se toman de la huella dactilar para realizar la comparación. Estos puntos que se toman dependen del algoritmo usado para realizar la autenticación.

1.3.1.1.3 Técnicas de reconocimiento dactilar

Algunas técnicas de reconocimiento dactilar utilizan la comparación de las imágenes almacenada con la adquirida mediante la utilización de métodos de correlación, la imagen adquirida “es generalmente capturada en escala de grises”[3], la operación de correlación es precisa sólo si las imágenes tienen la misma orientación y posición en el plano; por consiguiente el hardware de adquisición de imágenes debe poseer una calidad aceptable.

Las técnicas empleadas para realizar la extracción de patrones se describen a continuación:

- Técnicas basadas en patrones de minucias extraídas de la estructura de las crestas.
- Técnicas basadas en las características de la estructura de crestas y valles.
- Técnicas basadas en la textura de la imagen.

a. Técnicas basadas en patrones de minucias

Esta técnica que identifica la posición de las minucias que posee en una huella dactilar, una minucia es una bifurcación que posee una huella dactilar la cual está representado en la Figura 1.6. Para realizar el análisis de detección de minucias se procede a realizar lo siguiente.

1. Captura la imagen de la huella dactilar.
2. Realizar el proceso de normalización para obtener el mismo tamaño de la imagen para guardar o comparar.
3. Determinar la minucia mediante un método interactivo el cual asigna un valor cuando ocurre una bifurcación y almacena esta posición en un vector.
4. No se considera como bifurcación el inicio de una cresta en los bordes de la imagen.

Para realizar la autenticación del individuo se procede a realizar la comparación con las minucias las adquiridas y almacenadas, mediante la utilización de un algoritmo estadístico mediante el cálculo de distancia que existe entre estas.

Figura 1.6. Minucias en una huella dactilar [3]

b. Técnicas basadas en el alineamiento de patrones

Esta técnica realiza el proceso de alineación de las huellas adquiridas y almacenadas antes de ser comparadas, "esta alineación consigue reducir el número de comparaciones necesarias para establecer el grado de similitud entre las huellas, reduciéndose significativamente el tiempo de respuesta" [3]. Un procedimiento muy frecuente es agrupar las huellas con respecto a sus puntos singulares. Se establece un sistema de referencia local para realizar la identificación de las minucias y luego la autenticación.

c. Técnicas basadas en la textura de la imagen

Esta técnica emplea diferentes métodos estadísticos o transformadas mediante la comparación de un conjunto de características como son rugosidad, homogeneidad, contraste, escala, borde y resolución con la finalidad de extraer las texturas[3] presentes en una imagen y capturar las características de la misma, de manera que pueda ser identificada de manera indiscutible.

[3] Textura es un patrón visual complejo compuesto de entidades o sub patrones, que tienen similares características de brillo, color, forma y tamaño.

1.3.1.1.4 Problemas al realizar la adquisición de la imagen

Para capturar la huella dactilar de los individuos es necesario realizar la presentación de la huella mediante la colocación o deslizamiento del dedo en un dispositivo de adquisición, para este proceso el individuo tiene que aplicar una cierta cantidad de presión para asegurar que la huella se adhiera completamente a la superficie de captura. Bajo esta presión, la piel del dedo se deforma y la imagen de la huella adquirida se distorsiona, debido a la imposibilidad de controlar la cantidad y la dirección de esta presión, ocurre una captura diferente en cada adquisición, por lo que el procesamiento es más complicado.

A continuación se describen los problemas que pueden ocurrir al momento de realizar la lectura de imagen por medio de un dispositivo.

- *Contacto no uniforme:* Ocurre por el desgaste de las crestas y valles debido a la sequedad de la piel, envejecimiento, enfermedades de la piel, el sudor, la suciedad y la humedad en el aire, todo esto puede influir en el resultado final para realizar la autenticación.

- *Contacto débil:* Se produce cuando el individuo no coloca suficiente fuerza en el dedo sobre el dispositivo de adquisición, esto puede causar deformaciones en la huella dactilar debida ya que puede agregar patrones que no corresponden al individuo.

- *Contacto irreproducible:* La estructura de la imagen es modificada continuamente por el trabajo manual, accidentes o lesiones en el dedo. Estos cambios a veces son permanentes o semipermanentes y puede introducir características adicionales de huellas falsas.

- *Huella latente:* Es aquella que es dejada en la superficie del escáner cada vez que un usuario coloca el dedo en el dispositivo de adquisición, debido a los aceites, humedad y sudor presente en la superficie de la piel del dedo. Esto representa una falta de seguridad para todo el sistema, ya que el dispositivo conserva huellas de una persona, que puede ser utilizado para otorgar un acceso a un impostor. Además, cuando un nuevo usuario coloca su dedo,

puede suceder que el dispositivo capture la huella dactilar y la nueva parte de la latente anterior, generando un modelo equivocado para el usuario actual e impide su autenticación.

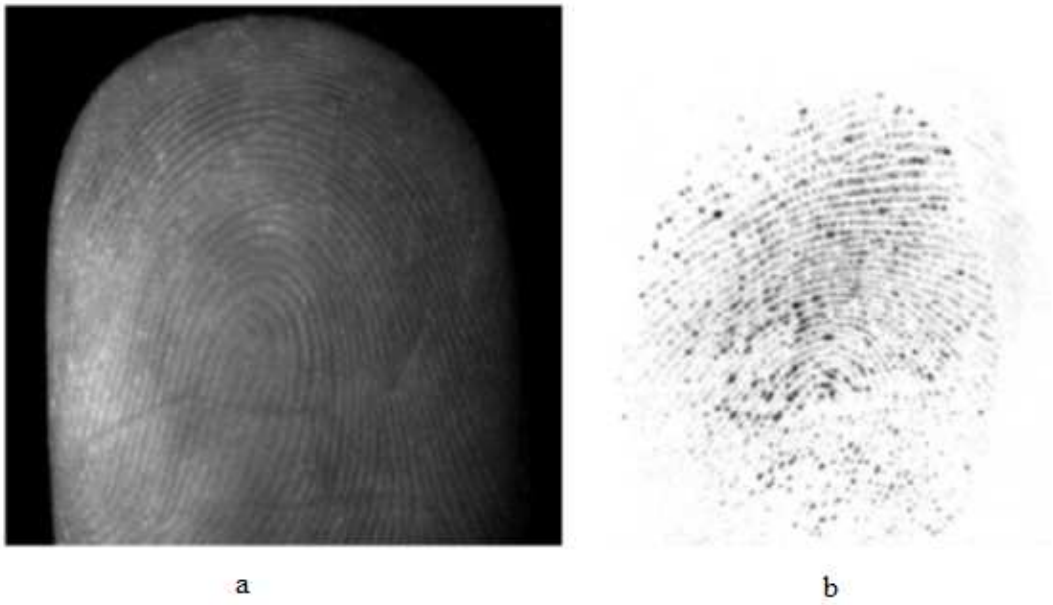

Figura 1.7. a) Huella dactilar adquirida con un dispositivo óptico sin problemas. b) dispositivo óptico basada en el contacto con huella latente [2]

1.3.1.2 Reconocimiento del iris

El reconocimiento del individuo a través del iris fue utilizado a principios de la década de los 90, ya que disminuye el error en la identificación del individuo “ya que el iris permanece invariante en el transcurso del tiempo.” [4]

El ojo humano es un órgano foto receptor, cuya función consiste en recibir las señales luminosas de los objetos de mundo exterior para transformar estas en impulsos eléctricos que son conducidos al centro nervioso del cerebro. “El sistema óptico está formado básicamente de tres capas: la capa externa, la capa media y la capa interna.”[4]

La función principal de la capa externa es proporcionar una protección al iris frente a los elementos externos.

La capa media, también denominada tracto uveal o simplemente úvea, está formada por el iris, el cuerpo ciliar y las coroides. El iris se encuentra situado entre la córnea y presenta una abertura en su parte central denominada pupila; el tamaño de la pupila depende de un músculo que rodea sus bordes; este aumentando o disminuyendo cuando se contrae o se relaja, controlando la cantidad de luz que entra en el ojo. El cuerpo ciliar es adyacente y continuo al iris, y se puede visualizar como un anillo.

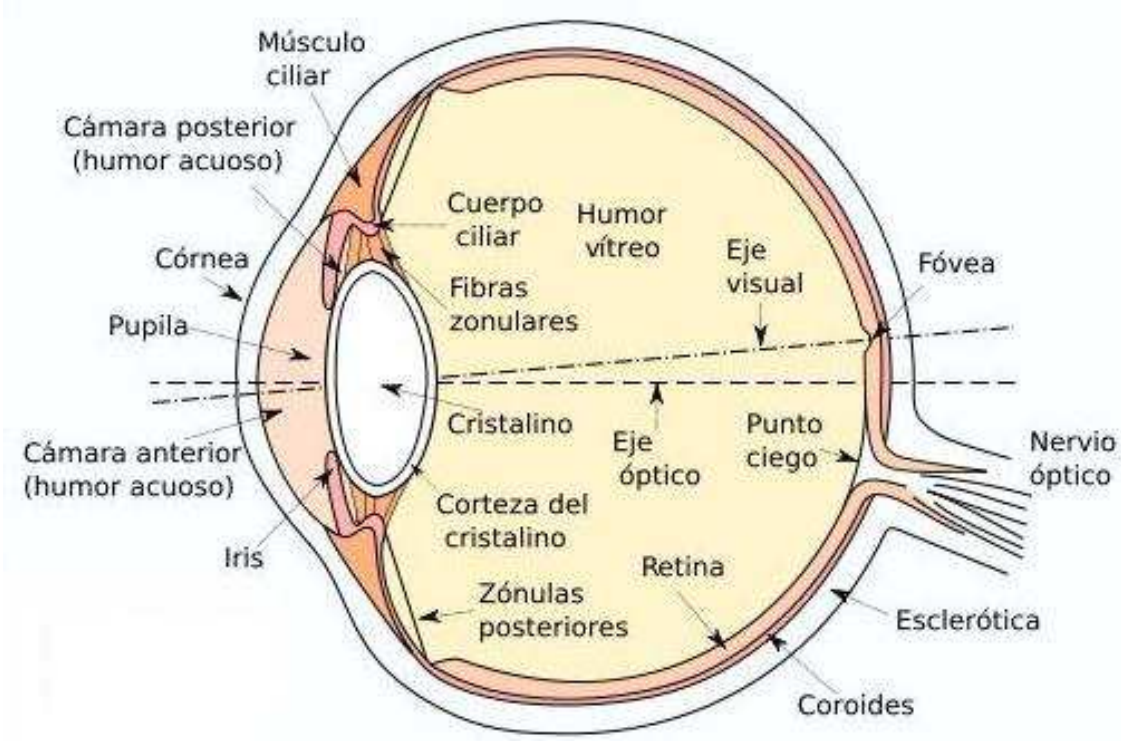

Figura 1.8. Elementos del ojo humano [4]

La capa interna del ojo se denomina retina; esta capa tiene la función de transformar la luz en un impulso nervioso que es enviado al cerebro. En la superficie de la retina se pueden observar diversas estructuras.

1.3.1.2.1 *Proceso de autenticación*

“El físico John G. Daugman (Laboratorio Informático de la Universidad de Cambridge) fue el pionero en este campo” [5], desarrolló algoritmos de reconocimiento del iris, mediante la especificación de procesos necesarios para la

adquisición y tratamiento de la imagen. “Los algoritmos de Daugman son la base de la mayoría de los sistemas de reconocimiento del iris que se introdujeron en el mercado hasta 2006.”[5]

1 Para realizar la adquisición de la imagen, se puede utilizar los siguientes sistemas: Sistema de Daugman y Sistema de Wildes ETAL, los cuales se describen en la Tabla 1.1.

ESPECIFICACIÓN	SISTEMA DE DAUGMAN	SISTEMA DE WILDES ETAL
Resolución y enfoque	“Entre los 100 y 200 pixeles en el diámetro del iris, a 15~45 cm, con un objetivo de 330 mm”[5]	“256 pixeles de diámetro del iris, a 20 cm y con un objetivo de 80 mm” [5]
Iluminación	Relativamente bajos, se realiza mediante LED, cámara de video estándar. Evita reflexión en gafas, pero no el efecto ojos rojos.	Iluminación difuminada, filtro polinizador y cámara de alta sensibilidad. Los filtros polinizadores circulares evitan la reflexión especular[4]
Centrado de la imagen	Proporcionan la toma de secuencias de imágenes (No se toma la imagen fija). Además si el usuario mira fijamente al dispositivo se tendrá una calidad y centrado de la imagen.	
Posicionamiento del Iris	Presenta una pantalla de cristal líquido con una secuencia de video correspondiente a la zona, de tal forma que el usuario pueda ajustar la posición del ojo. Luego se extrae una imagen tomando en cuenta el criterio de máximo centrado.	Presenta una retícula de ajuste basada en la superposición de dos cuadrados. Cuando el iris está en la posición adecuada, los cuadros coinciden y el usuario mismo selecciona la imagen.

Tabla 1.1. Especificaciones de los sistemas de adquisición de imágenes

2 Después de haber sido capturada la imagen del individuo mediante el dispositivo, se procede a realizar las siguientes operaciones.

3 *Localización del iris dentro de la imagen mediante el método Dougman.-* para determinar la posición del iris entre la parte exterior y la parte interior del ojo

[4] Reflexión especular. si la superficie de un material es microscópicamente lisa y plana, como en el caso del vidrio, los haces de luz incidentes y reflejados crean el mismo ángulo con una normal a la superficie de reflexión produciendo una reflexión especular.

humano, se busca sobre todo el dominio de la imagen el borde pupilar y el borde del iris, a través del método iterativo denominado *"De grueso a delgado",* como se muestra en la Figura 1.10. Luego, de una manera similar, es utilizada para detectar los bordes curvilíneos de los parpados.

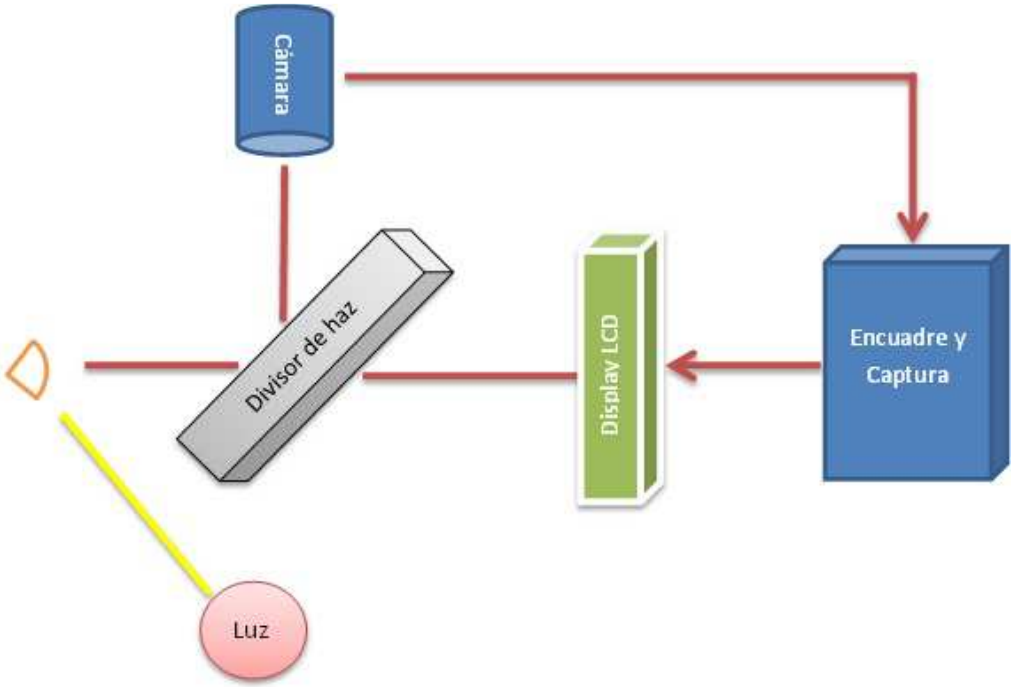

Figura 1.9. Sistema de Dougman [4]

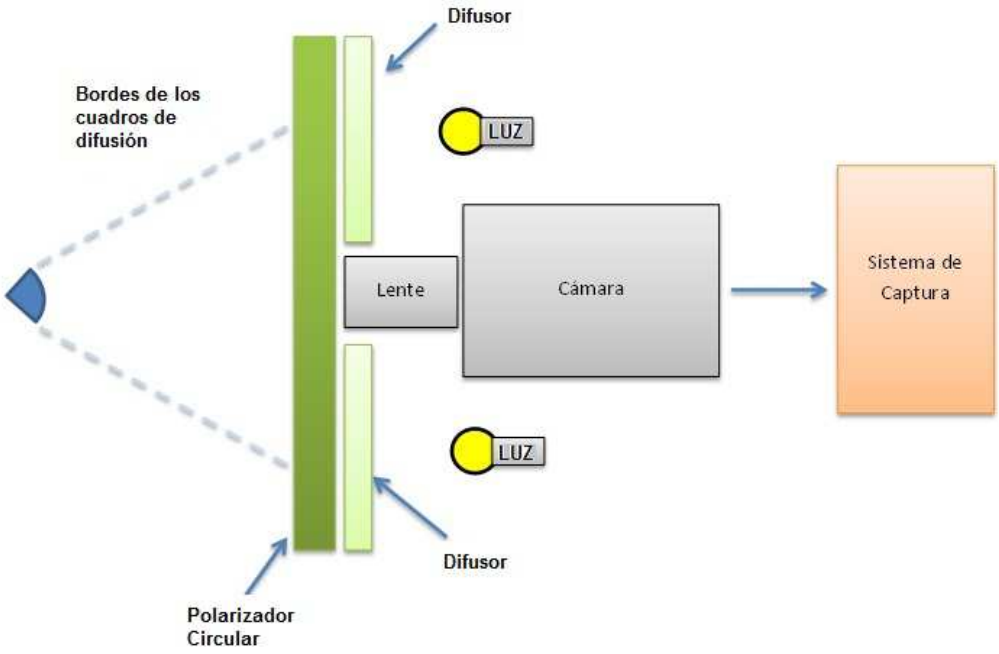

Figura 1.10. Sistema de Wildes ET AL [5]

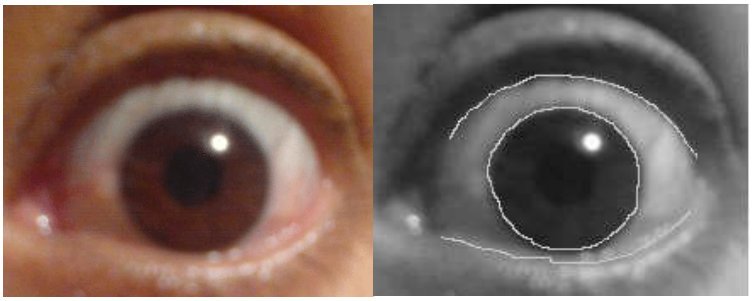

Figura 1.11. Localización el iris [5]

4 Normalización. La fase de normalización transforma la región anular del iris en una región rectangular de dimensiones constantes como se visualiza en la siguiente Figura 1.11. Para realizar esta normalización, se utiliza el algoritmo denominado "Homogéneo *rubber - sheet".* Este modelo asigna a cada punto en el iris un par de coordenadas cartesianas, que son definidos como combinaciones lineales del conjunto de puntos del borde de la pupila y el conjunto de puntos límite de limbos a lo largo del perímetro exterior del iris.

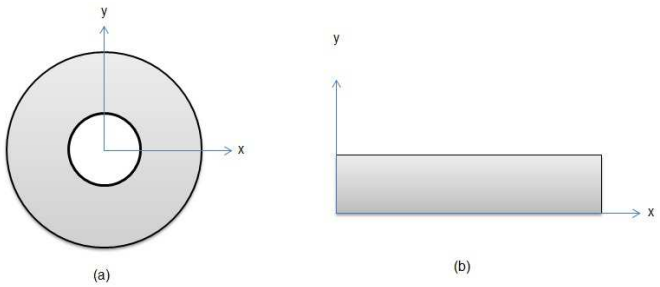

Figura 1.12. Normalización (a) Imagen Original, (b) Imagen Normalizada [6]

Además de generar la imagen normalizada del iris, en esta etapa se genera otra imagen denominada plantilla de ruido. La plantilla de ruido tiene las mismas dimensiones que el iris normalizado donde el patrón de iris es obstruido por los párpados, esta se utiliza como mascara en la etapa de comparación para evitar comparar regiones donde el iris es obstruido por los párpados.

5 *Codificación.*- El iris es de-modulado para extraer su información, usando la cuadratura 2D-Gabor-wavelets[5]. Esto conduce a una fase de digitalización del

[5] Los Filtros Gabor son utilizados para el análisis de imágenes debido a su relevancia biológica y propiedades computacionales, ya que sus núcleos son similares a las células corticales simples de los mamíferos. Además,

patrón del iris que permite un ajuste simultáneo de la resolución en espacio y frecuencia, “mediante este proceso de filtrado se permite expresar la información contenida en una imagen completa mediante una representación compacta de 256 bytes de información.” [7]

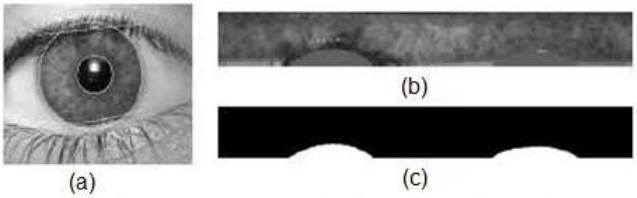

Figura 1.13. Normalización. (a) Imagen segmentada, (b) Iris normalizado, (c) Plantilla de ruido [6]

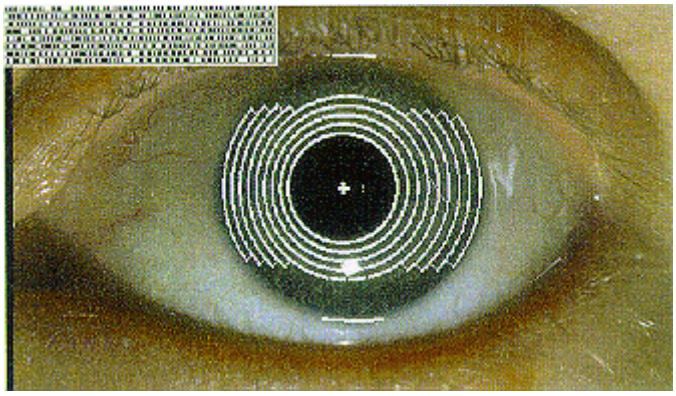

Figura 1.14. Codificación del iris [7]

6 *Reconocimiento.-* Para realizar este proceso se discrimina los coeficientes entre positivos y negativos, asignando un "1" a los positivos (o nulos) y un "0" a los negativos. Con la secuencia de bits obtenida, se aplica una distancia de Hamming para obtener la distancia entre el patrón previamente almacenado, y la muestra a verificar; se utiliza la expresión booleana XOR, el cual detecta falta de concordancia entre los correspondientes pares de bits, y asegura que los bits comparados no sean mal interpretados, y obtienen la medida de disimilitud entre los irises, por lo que el resultado de la operación indicará para valores pequeños, mayor coincidencia.

---

se pueden seleccionar orientaciones y frecuencias específicas que se pueden localizar fácilmente en los dominios del espacio y la frecuencia.
Los filtros Gabor de 2D son filtros pasa banda selectivos a la orientación y la frecuencia haciéndolos confiables para la extracción de características en imágenes.

1.3.1.3 La retina

Esta técnica biométrica se basa en la comparación de los vasos sanguíneos contenidos en la retina, el patrón de distribución de los vasos sanguíneos que proceden del nervio óptico, es una fuente de información biométrica altamente distintiva, ya que no existen dos patrones iguales, incluso en hermanos gemelos idénticos. Es estable a lo largo de la vida de una persona, pero puede verse afectada por glaucomas[6], diabetes o enfermedades degenerativas.

1.3.1.3.1 Elementos de la retina

La retina es una capa delgada y parcialmente transparente, está en contacto con la cara interna de la coroide y con el humor vítreo. En su superficie se pueden observar diversas estructuras las cuales se describen a continuación:

- *Papila, o disco óptico:* La papila es el punto donde el nervio óptico entra en el globo ocular, atravesando la membrana esclerótica, las coroides y finalmente la retina. “Es un disco rosado que se encuentra en la parte posterior del globo ocular y está situado unos 3 mm medialmente al polo posterior del ojo. Tiene unas dimensiones de 2 x 1,5 mm.”[8]
- *Fóvea:* “Está situada a unos 2,5 mm o 17 grados del borde temporal de la papila óptica, donde la superficie de la retina está deprimida y es poco profunda.”[8]. Los vasos sanguíneos rodean a la fóvea por arriba y por abajo, mientras que dentro de ella sólo existen pequeños capilares. En el mismo centro de la fóvea, en un área de unos 0,5 mm de diámetro no existen capilares para aumentar al máximo la transparencia de la retina.
- *Ora serrata:* elemento interno que delimita la retina del área foto sensitiva y el área interna o sensible del ojo humano. Existe una ora serrata nasal o medial y una ora serrata lateral o temporal.

En la Figura 1.15, se presentan algunos de los elementos que conforman la retina

[6]El glaucoma es una enfermedad de los ojos que tiene como condición final común una neuropatía óptica que se caracteriza por la pérdida progresiva de las fibras nerviosas de la retina y cambios en el aspecto del nervio óptico.

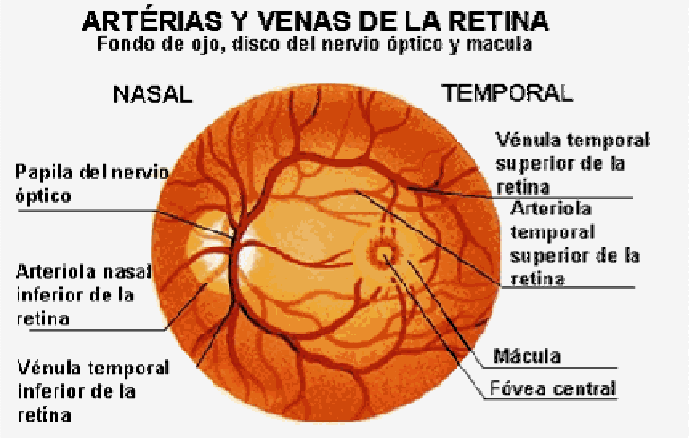

Figura 1.15. Elementos de la retina [8]

1.3.1.3.2 Reconocimiento del individuo

El escaneo de la retina puede ser sumamente preciso pero requiere que el usuario mire en un objetivo o enfoque la vista hacia un punto específico, para luego almacenar en una plantilla, si desea realizar la autenticación del individuo debe comparar los datos adquiridos con los almacenados; si la muestra coincide con la almacenada, se concluye que el usuario es quien dice ser.

Su fiabilidad para realizar la autenticación no resulta conveniente cuando el individuo utiliza lentes, ya que puede causar que los datos se distorsionen.

1.3.1.4 Geometría de la mano

Esta técnica biométrica es una de las más modernas, toma las dimensiones de la mano humana para la autenticación, como son: longitud de los dedos, ancho, espesor y curvas de los dedos; a pesar que la forma y tamaño de la mano humana permanece casi invariantes durante la etapa de la vida adulta de las personas debido a que el tamaño no tiene cambios abruptamente.

El escáner de geometría de la mano utiliza una cámara: un dispositivo de carga acoplada (CCD), diodos infrarrojos luminosos (LED) con espejos y reflectores para capturar imágenes de la silueta de la mano humana en blanco y negro. El escáner omite las huellas dactilares, líneas, cicatrices y color de la mano.

“Anatómicamente la mano posee un esqueleto óseo provisto de veintisiete huesos articulados entre sí.”[9]

Actualmente los escáneres usados no poseen la capacidad de detectar si la mano utilizada posee signos vitales o no, de tal forma es posible engañar al sistema mediante el uso de una mano falsa aplicada correctamente a la superficie lectora, siendo ésta una de las debilidades de este tipo de sistemas.

1.3.1.4.1 Elementos la mano humana

La función principal de la mano humana es sujetar objetos ya que posee pequeños huesos llamados falanges, los cuales se muestran en la figura 1.16.

Figura 1.16. Elementos de la mano humana [9]

Las falanges son huesos largos pues predomina la longitud sobre su grosor, Cada dedo humano contiene tres huesos para formar la falange a excepción del dedo pulgar que posee solamente dos huesos para formar la falange.

1.3.1.4.2 Método de reconocimiento

Para obtener los datos biométricos necesarios, se utiliza una cámara digital de baja resolución, cinco clavijas posicionadas de tal forma que ayude alinear los dedos de las manos y permita distinguir el contorno de los dedos mediante la utilización de un “espejo colocado para reflejar el perfil de la mano” [10], la mano se coloca con la palma hacia abajo sobre una superficie plana como se muestra en la Figura 1.17, para capturar la imagen de la palma de la mano y su sombra.

Una vez obtenidos los contornos del dorso y del perfil de la mano, se realizan una serie de medidas que darán como resultado el vector de características correspondiente, mostrado en la Figura 1.17.

A continuación, se describen las características a ser analizadas para realizar la autenticación del individuo.

- *Anchuras de cada uno de los dedos.* También se mide la anchura de la palma de la mano y las distancias entre ellos, en coordenadas tanto horizontales como verticales, donde los superíndices indican la coordenada tomada denotados en el gráfico como F1, F2, F3, F4, F5, F6, F7, F8, F13, F14, F15, F16 y F17.
- Alturas de los dedos tales como dedo medio, del dedo meñique, anular y de la palma de la mano, las cuales corresponden a las medidas F9, F10, F11 y F12.
- *Desviaciones estándares de los dedos* con respecto a la línea recta ideal que deberían formar las falanges. Estas distancias se miden como la distancia del punto medio del contorno del dedo (por ejemplo P12 para el caso del dedo índice) y el punto medio de la recta definida entre el punto inter dedo correspondiente (P1 en el mismo caso) y el punto más alto del contorno de ese dedo, en el que se hacen medidas (P14).

De esta forma se obtiene desviaciones estándares para cada uno de los dedos índice, medio, anular y meñique. Las desviaciones obtenidas se comparan con los datos almacenados utilizando un algoritmo matemático para determinar la similitud entre las plantillas almacenadas.

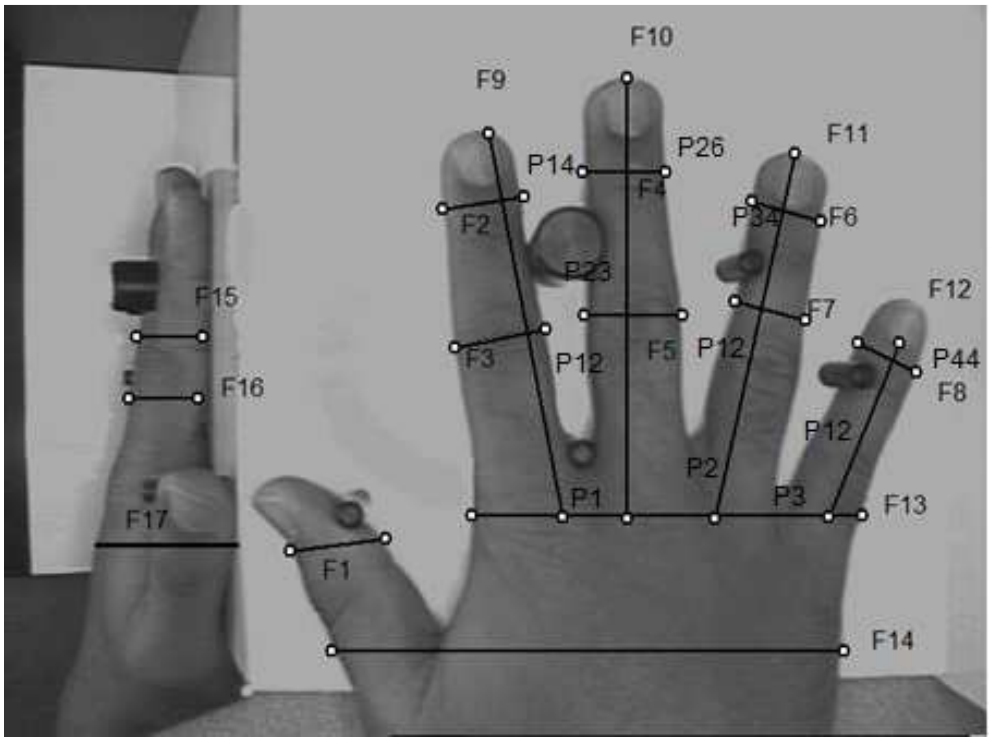

Figura 1.17. Posición de la mano para adquisición de la imagen [10]

1.3.1.5 Reconocimiento facial

A menudo el ser humano utiliza los rasgos más significativos para realizar el reconocimiento de cada individuo, es por ello que actualmente se utiliza el reconocimiento facial mediante el diseño de mecanismos para realizar esta operación. “Los primeros algoritmos de reconocimiento facial usaban modelos geométricos simples, pero en la actualidad estos procesos han mejorado tanto por sus métodos matemáticos usados como el hardware utilizado para el procesamiento.”[12]

1.3.1.5.1 Métodos de reconocimiento

Existen métodos para realizar la autenticación del individuo, los cuales han evolucionado en los últimos años, destacando los siguientes métodos.

- Análisis de componentes principales *(Principal Components Analysis, PCA)*.
- Análisis lineal discriminante *(Linear Discriminant Analysis, LDA)*.

- Correspondencia entre agrupaciones de grafos elásticos *(Elastic Bunch Graph Matching, EBGM).*

a. Análisis de componentes principales (Principal Component Analysis, PCA)

Es un método de identificación de patrones de datos y sirve para destacar tanto sus similitudes como diferencias mediante combinaciones lineales entre la imagen adquirida y la almacena. "Encontrar patrones cuando los datos a tratar son muy grandes es complicado, sobre todo cuando la calidad gráfica es baja. Entonces, PCA es una herramienta muy potente para su obtención."[12]

"Esta técnica está comúnmente usada en Eigenfaces[7], y es descrita por Kirby y Sirovich en 1988."[13] Las imágenes que trata este método deben ser normalizadas, de modo que los ojos y la boca estén alineados. Luego, realiza una compresión de la imagen quedándose con los patrones más destacados tales como formas y contornos del rostro, descartando los datos que no aportan información. Cada imagen facial puede ser representada como una suma ponderada de sus Eigenfaces. La comparación se realiza con la medida de la distancia de cada uno de los componentes de la imagen con respecto a una imagen de muestra. Esta requiere una toma de imagen frontal del individuo para poder ser comparada.

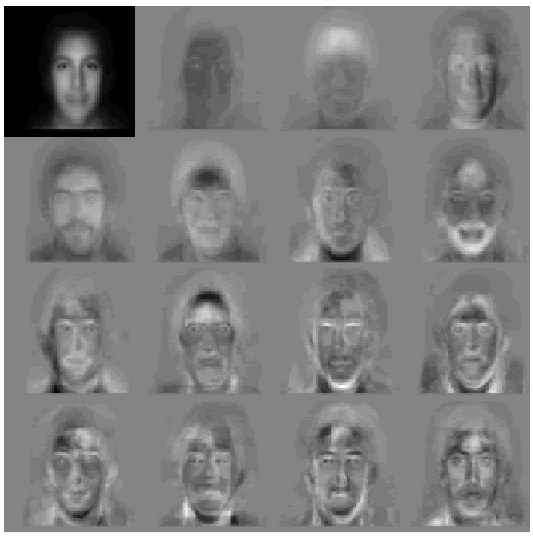

Figura 1.18. Ejemplos de muestra de Eigenfaces [12]

[7] Eigenfaces es una estructura facial con componentes ortogonales correlacionados.

b. Análisis Lineal Discriminante - LDA

“Utiliza una aproximación estadística para clasificar muestras de clases desconocidas basadas en minucias con clases conocidas” [14], mostrado en la Figura 1.19, esta técnica tiene la intención de explicar la diferencia que existen entre una imagen y un grupo de imágenes, donde cada bloque representa una clase y hay grandes variaciones entre varios individuos, pero pequeñas en por cada individuo. Este proceso de autenticación se realiza mediante una comparación estadística entre cada uno de los datos almacenados.

c. Correspondencia Entre Agrupaciones De Grafos Elásticos - EBGM

Las imágenes faciales reales tienen muchas características no lineales que no son tratadas en los métodos lineales, tales como variaciones en la iluminación de exteriores, contra luz, postura frontal y expresión de sonrisa.

Este método usa la transformación de Gabor, la cual crea una plantilla que proyecta el rostro mostrado en la Figura 1.20, el cual describe el comportamiento de la imagen alrededor de un pixel. Este resultado se la obtiene mediante una convolución de la imagen con un filtro Gabor, el cual es usado para detectar formas y extraer las características de la imagen. “Una convulsión expresa la suma de solapamientos de las funciones entre sí.” [16]

Para realizar la autenticación se procede a localizar el punto de referencia de comparación, el cual puede se puede conseguir combinando los métodos PCA y LDA.

Figura 1.19. Análisis lineal discriminante [14]

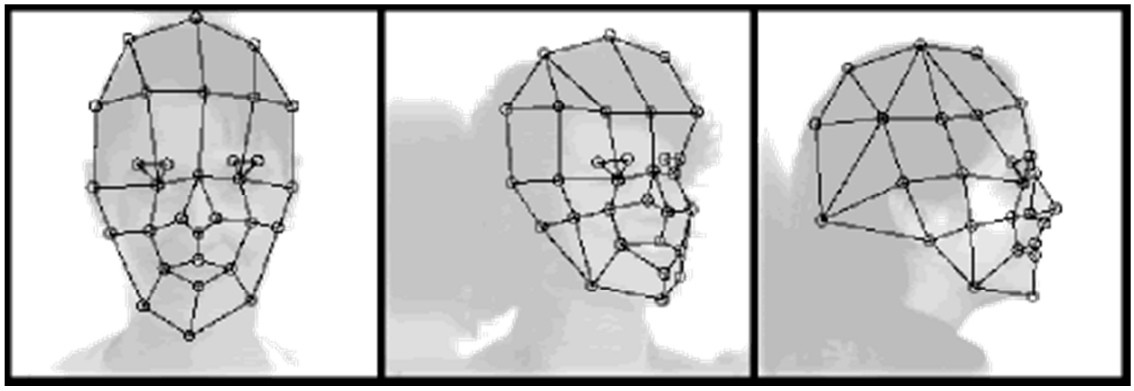

Figura 1.20. Método de correspondencia entre grafos [14]

1.3.1.6 Reconocimiento mediante el uso de termo gramas faciales

"El sistema vascular presente en el rostro genera una firma facial, única cuando el calor es emitido por la cara. Estas firmas faciales pueden ser obtenidas usando una cámara infrarroja, dando como resultado una imagen llamada termo grama facial."[17]

Un termo grama facial se considera única para cada persona y no puede ser falsificado. Ya que inclusive la cirugía plástica no puede falsificar un termo grama facial, ya que dicha cirugía no cambia el flujo de la sangre. Presenta bastantes ventajas frente al simple reconocimiento facial basado en imágenes, ya que el termo grama facial puede obtener el termo grama facial en un ambiente con poca luz e incluso en ausencia de luz debido al uso de la cámara infrarroja.

Este método tiene sus debilidades ya que el termo grama facial puede depender en una serie de factores tales como: estado emocional y temperatura del cuerpo; ya que este puede variar bruscamente y puede rechazar a un usuario legítimo.

1.3.1.7 Análisis de ADN

Es una técnica utilizada para distinguir individuos de una misma especie, utilizando la muestra de su ADN. "Se basa en que dos seres humanos tienen una gran parte de su secuencia de ADN en común" [16] y para distinguir a dos individuos se utiliza la secuencia de repetición llamada micro satélites. Mediante esta comprobación será poco probable que dos seres humanos no relacionados

tengan el mismo número de micro satélite[8], salvo en el caso de gemelos idénticos, que tendrán idénticos perfiles genéticos.

1.3.1.7.1 Enfoque en el uso del ADN

"La huella genética se utiliza en la medicina forense, para identificar a los sospechosos con muestras de sangre, cabello, saliva o semen."[16] Además se utiliza para identificar restos humanos, pruebas de paternidad y compatibilidad de órganos para donarlos.

1.3.2 MÉTODOS DE COMPORTAMIENTO

La utilización de estos métodos conlleva a que los algoritmos posean un margen de error bastante alto en comparación con los métodos físicos, debido a que el ser humano puede sufrir algún cambio permanente, ya sea por una enfermedad degenerativa o puede ser suplantado por un dispositivo o individuo.

A continuación, se consideran los siguientes métodos, los cuales han sido desarrollados y estudiados por varios años:

- ✓ Identificación por la voz.
- ✓ Reconocimiento de la firma.

1.3.2.1 Identificación por la voz

"El reconocimiento por voz o parlante, es una modalidad biométrica que utiliza la voz de un individuo," [17] este proceso de reconocimiento de voz, depende de las características del tracto vocal del individuo como también de su estado de ánimo y de la calidad del micrófono utilizado.

1.3.2.1.1 Métodos de procesamiento de la voz

Existen dos formas de realizar el procesamiento de la voz:

- ❖ Dependiente del texto (modo limitado).

[8]**Microsatelites o SSR** (*Short Sequence Repeat*) o **STR** (*Short Tandem Repeat*) por sus siglas en inglés, son secuencias de ADN en las que un fragmento (cuyo tamaño va desde uno hasta seis nucleótidos) se repite de manera consecutiva. La variación en el número de repeticiones crea diferentes alelos.

- Independiente del texto (modo ilimitado).

a. Dependiente del texto

En este tipo de sistema el individuo debe presentar una frase fija contraseña o una frase programada dentro del sistema ("Por favor diga los números: 43-42-93") mediante la utilización de un micrófono. La elección de este método facilita el procesamiento de autenticación, ya que luego de la adquisición, se realiza una conversión de un formato analógico a uno digital, para posteriormente realizar la comparación o almacenamiento de la información.

La mayoría de los sistemas de verificación dependientes del texto utilizan el concepto de Modelos Markov Ocultos (HMMs), el cual provee una representación estadística de los sonidos producidos por el individuo; mediante el análisis de comparación de variaciones subyacentes y cambios temporales a lo largo del tiempo, considerando las características de calidad, duración, intensidad dinámica y tono o nivel de voz.

b. Independiente del texto

En este tipo de métodos el usuario no posee ningún conocimiento futuro de la fase que necesita para realizar la autenticación, lo que presenta un procesamiento de la señal de voz aún más difícil.

Después de haber realizado la captura de la señal de voz del individuo, se "utiliza el modelo de Mixtura Gaussiana, el cual realiza un mapeo de estado conocido como *Hidden Markov Model* HMM[9]," [18] creando un número de vectores de estado que representan las variaciones de las formas del sonido, que son características de la fisiología y el comportamiento de un individuo.

c. Reconocimiento de la voz

Durante la fase de reconocimiento, las características de calidad, duración, volumen y tono son extraídas de la muestra tomada y se compara con las

[9] Modelo oculto de markov HMM. es un modelo estadístico en el que se asume que el sistema a modelar es un proceso de Márkov de parámetros desconocidos. El objetivo es determinar los parámetros desconocidos (u *ocultos*, de ahí el nombre) de dicha cadena a partir de los parámetros observables.

plantillas almacenadas. Estas plantillas contienen los datos de una gran variedad de individuos, se considera que una plantilla concuerda con el dato ingresado cuando contiene un "radio de similitud", similar a la identidad buscada, o supuestamente buscada. Si la voz ingresada pertenece a la identidad proclamada, el puntaje va a reflejar que la muestra presenta mayores similitudes con la identidad proclamada con el modelo.

1.3.2.1.2 Reconocimiento de la firma

En la vida diaria, la firma manuscrita es la forma más difundida que actualmente se utiliza para la acreditación personal, ya que se usa para realizar transacciones de compra venta, firma de cheques y firma de contratos; es por ello que esta técnica, debe ser robusta para disminuir la falsificación.

a. Proceso de reconocimiento

Para realizar el proceso de reconocimiento primero se debe considerar los diferentes métodos que existen para realizar la falsificación de la firma, las cuales son:

i. Aleatoria. Es aquella en que la firma se realiza sin ningún conocimiento de la firma que realiza la persona y del nombre de esta.

ii. Simple. Es aquella que se realiza conociendo el nombre de la persona pero sin ningún conocimiento de su firma.

iii. Experta. Es aquella que posee conocimiento del nombre y de la firma de la persona para realizar su suplantación.

Luego de conocer los diferentes tipos de falsificación de firma a continuación se describen los métodos utilizados para determinar la identidad de la persona.

a.1 Estáticos (off line).La firma es capturada mediante el uso de un escáner de adquisición de imagen y luego realiza el procesamiento de la imagen para verificar la identidad de la persona, este proceso de autenticación se describe a continuación.

- *Binarización:* es un proceso que realiza el cambio de la imagen a solo dos colores los cuales son blanco y negro.

- *Eliminación de Ruido:* para realizar este proceso se puede utilizar filtros pasa bajos antes o después del proceso de binarización.
- *Segmentación*: Consiste en aislar los trazos que contienen la información necesaria que caracteriza la firma. Se puede extraer toda la firma o solamente el cuerpo de la misma, eliminando los trazos estadísticos exteriores.
- *Normalización en Posición y Tamaño*: Dependiendo del algoritmo de clasificación que se utilice, puede ser necesaria la normalización en posición con respecto al punto inicial y en tamaño.
- *Comparación e identificación del individuo:* Se realiza una comparación con la muestra tomada y con la muestra almacena, si concuerdan se procede a validar al usuario.

a.2 Dinámicos (On line). Para realizar la captura de la firma generalmente se usan dispositivos digitales, estos dispositivos permiten registrar información dinámica sobre la velocidad de la escritura, presión, ángulo y posición del lápiz. Mejorando así la capacidad de identificación del individuo; a continuación se presenta el proceso para realizar la autenticación.

- *Alineamiento con respecto a la posición:* se debe encontrar el vector posición inicial de la firma mediante el cálculo de centro de masa.
- *Normalización en rotación:* se puede utilizar las siguientes normalizaciones: se puede normalizar en coordenadas polares mediante la alineación del ángulo de la trayectoria media o normalizar respecto al ángulo medio con respecto al eje de mínimo momento de inercia.
- *Normalización del Tamaño:* se suele normalizar con respecto a valores extremos de las coordenadas, rangos de variación o valores estadísticos de primer y segundo orden.
- *Comparación de los elementos.* Finalmente se compara la muestra obtenida con la muestra guardada para así realizar la identificación.

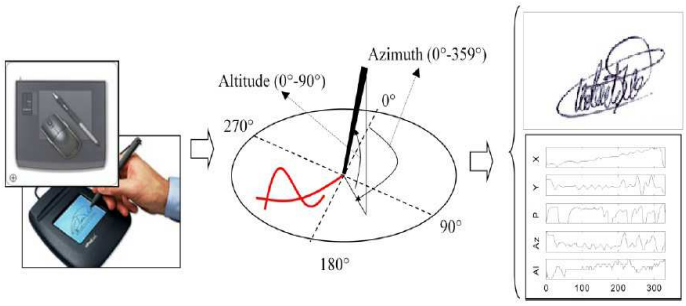

Figura 1.21. Reconocimiento de la firma [20]

1.3.3 COMPARACIÓN DE LOS SISTEMAS BIOMÉTRICOS

Todos los sistemas biométricos descritos en este capítulo muestran fortalezas como debilidades, pero básicamente tienen tres partes principales comunes; la primera es que disponen de un mecanismo automático que lee y captura la característica biométrica a procesar, ya sea que la señal de ingreso sea digital o analógica, segundo disponen mecanismos para realizar la compresión o normalización de la imagen y permite realizar el almacenamiento o comparación de los datos capturados con los guardados en una base de datos o repositorio, para finalizar, y tercero ofrecen una interfaz de comunicación entre el dispositivo biométrico y las aplicaciones que utilizan.

En la Tabla 1.2 se presenta las principales características de las tecnologías biométricas enumeradas en este capítulo para realizar la autenticación del individuo.

Debido a que el sistema biométrico de huella dactilar ha sido desarrollado y estudiado durante un período de tiempo mayor en comparación con los otros sistemas biométricos y los algoritmos que realiza la autenticación o identificación del individuo son los que poseen menos procesamiento computacional, además el costo del hardware de adquisición de imagen es menor, es por esta razón que se ha elegido la tecnología biométrica de huella dactilar para realizar el desarrollo del software de registro de ingreso y salida de empleados, ya que se desea presentar una tecnología bastante confiable debido a que el margen de error va a ser mínimo y robusta debido a que permitirá procesar peticiones de varios

dispositivos biométricos, para las empresas, que no poseen el suficiente poder económico adquisitivo.

Tecnología	Funcionamiento	Facilidad de uso	Problemas para identificar
Huella Dactilar	Capturar y comparar patrones de la huella dactilar.	Alta	Ausencia de miembro o desgaste de huella dactilar.
Geometría de la mano	Medir y comparar dimensiones de la mano y dedos.	Alta	Edad, enfermedades degenerativas en la mano o ausencia de miembro.
Retina	Capturar y comparar los patrones de distribución de los vasos sanguíneos que posee el nervio óptico.	Baja	Uso de gafas o lentes, enfermedad degenerativa en el ojo.
Iris	Capturar y comparar el comportamiento del iris.	Baja	Enfoque de luz, enfermedades degenerativas en el ojo.
Reconocimiento facial	Capturar y comparar el contorno o patrones faciales.	Baja	Edad, cambios en cabello y luz.
Termo grama Facial	Utilización de cámaras infrarrojas que detectan patrones de calor que emite el cuerpo.	Baja	Estado de ánimo del individuo, o alteraciones debido al cansancio.
Análisis de ADN	Comparar plantillas de ADN micro satélites con otras muestras.	Baja	Enfermedades degenerativas a la sangre.
Identificación por voz	Capturar y comparar el tono de la voz, mediante la utilización de un micrófono.	Media	Edad, toz o gripe pueden cambiar la voz del individuo.
Firma	Capturar y comparar el ritmo, aceleración, y presión de la firma.	Media	Edad, cambios de estado de ánimo.

Tabla 1.2. Comparación de los sistemas biométricos

1.4 ARQUITECTURA DE SOFTWARE DE N CAPAS

Es considerado como un estilo de programación, tiene como objetivo separar los diferentes funciones generales en el desarrollo de aplicaciones, tales como interfaz gráfica de presentación al usuario final, lógica de negocio y mecanismos de almacenamiento, considerando estos aspectos el programador debe realizar un análisis para el desarrollo de la aplicación, la cual considera los siguientes niveles que están representados en la Figura 1.22.

a. *Capa Presentación.* Es la interfaz gráfica que utiliza el usuario final, permite visualizar la información, mediante el envío de peticiones a la capa de negocio y recepción de datos.
b. Capa de negocio. Contiene las funciones específicas que el programa realiza, es decir en esta capa se establece la lógica que el programa puede realizar además recibe las peticiones de la capa aplicación y envía estas a la capa de acceso de datos, luego recibe los datos de la capa de datos y envía la respuesta a la capa de aplicación.
c. Capa de Acceso Datos. Contiene el método para establecer la conexión de comunicación con la base de datos.
d. Capa de Datos. Contiene los procedimientos almacenados, funciones, vistas y tablas definidas o creadas en la base de datos. La diferencia entre la capa de acceso a datos y la capa de datos es que el administrador puede acceder y modificar los datos mediante el acceso al programa de administración de la base.

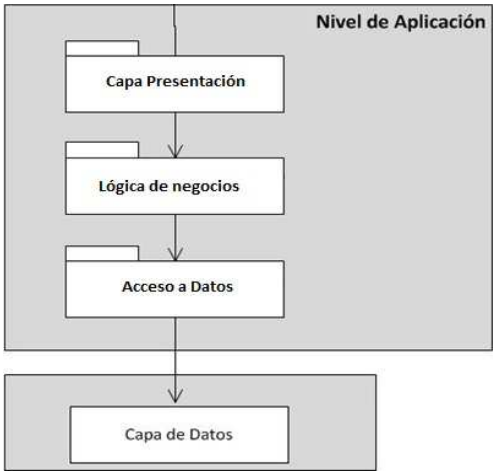

Figura 1.22. Arquitectura de software de n capas [21]

“Todas estas capas pueden residir en un único computador o varios computadores, si bien lo más usual es que posea muchos computadores para que resida cada capa, para disminuir el procesamiento y el uso de memoria.” [21]

Las capas de negocio y de datos pueden residir en el mismo computador, y dependiendo del crecimiento de las necesidades se aconseja separar estas capas. Si el tamaño o complejidad de la base de datos aumenta, se puede considerar que la capa de datos este en un solo computador. Para determinar que una capa desarrollada resida en un maquina se considera lo siguiente:

- Uso de memoria de la máquina.
- Número de peticiones que puede soportar. Ya que generalmente se desarrollan aplicaciones que realicen el procesamiento de peticiones de manera asíncrona.
- Nivel de importancia.
- Tipo de complejidad del desarrollo para el procesamiento del servicio.

1.4.1 VENTAJAS DE LA ARQUITECTURA DE SOFTWARE EN CAPAS

La arquitectura para el desarrollo de software mediante capas es una práctica muy utilizada en la actualidad, por esta razón se destacan algunas ventajas de la arquitectura de n capas.

- ✓ Si cada capa reside en una maquina diferente el procesamiento y uso de memoria se pueden distribuir, pudiendo así disminuir el uso de recursos en memoria.
- ✓ Debido a que cada capa realiza una determinada función se puede detectar fácilmente algún error generado en tiempo de ejecución.
- ✓ Se agrega un cierto nivel de seguridad debido al nivel que puede asignarse a los métodos tales como pública, privada o protegida.
- ✓ Permite realizar cambios en el software desarrollado que pueden ser casi imperceptibles para el usuario final.

1.4.2 DESVENTAJAS DE LA ARQUITECTURA DE SOFTWARE

En esta sección se describen las desventajas que se presentan al momento de desarrollar aplicaciones mediante esta arquitectura.

- ✓ Mayor costo de inversión, debido a que al realizar la distribución del procesamiento, necesariamente se utilizará varias máquinas, lo que conlleva al incremento en gastos económicos.
- ✓ La implementación del servicio en máquinas diferentes conlleva a la administración de excepciones de comunicación en cada capa, ya que provee cierta complejidad, debido a que se debe manejar protocolos de comunicación entre cada una de las capas.
- ✓ El tiempo de respuesta de procesamiento aumenta, debido a que cada petición debe pasar por cada capa.
- ✓ Si no se implementan mecanismos de redundancia en el sistema distribuido, al fallar una de las capas falla completamente el sistema o si existen problemas de comunicación entre capas, no es posible acceder al servicio.

CAPÍTULO 2
DESCRIPCIÓN DEL SISTEMA

En este capítulo se presentan los requerimientos funcionales y no funcionales necesarios para realizar el desarrollo del sistema biométrico, mediante la selección y comparación del hardware biométrico existente en el mercado, con la finalidad de escoger el más adecuado para interactuar con la aplicación a ser desarrollar, mediante la comparación de tres marcas diferentes para seleccionar un dispositivo.

2.1 REQUERIMIENTOS DEL SISTEMA

A continuación se presentan los requerimientos del sistema a implementar mediante la descripción de cada uno de ellos.

2.1.1 REQUERIMIENTOS FUNCIONALES

La aplicación que se desarrollará deberá abarcar los requerimientos de una empresa que puede contar con empleados con horarios rotativos o un establecimiento educativo en donde sus empleados cuentan con un horario fijo y pueden trabajar por horas. Considerando lo descrito anteriormente la aplicación desarrollada toma en cuenta las características generales como: registro de entrada y salida mediante la utilización de la tecnología biométrica, permisos, vacaciones y comisiones del empleado, para llevar un control de las horas del empleado para el ingreso o salida de la empresa.

2.1.1.1 Funcionalidad del sistema

En la Tabla 2.1 se describe las funciones generales que la aplicación debe realizar, para conseguir el registro de horas del empleado y administración de usuarios, empleados, horarios laborables y dispositivos biométricos.

Considerando estos requerimientos generales, en la Tabla 2.2 se describen los requerimientos específicos que el sistema va a realizar.

Con los requerimientos generales y específicos descritos en las Tablas 2.1 y 2.2 respectivamente, se presenta la matriz de requerimiento que posee el sistema biométrico, mostrado en la Tabla 2.3, la cual permite identificar la funcionalidad que va a tener el sistema biométrico.

Código requerimiento	Requerimiento	Descripción
RB001	Control de sesión	Debe permitir realizar la verificación del usuario que quiere acceder al sistema
RB002	Administración de usuarios	Debe permitir administrar todos los usuarios registrados en el sistema
RB003	Registro de Horas.	Debe permitir ingresar las horas en que el empleado realizado el registro.
RB004	Reportes	Permitir mostrar la información que almacena el sistema.
RB005	Horarios Laborables	Debe almacenar los horarios laborables del empleado.
RB006	Administración de dispositivos	Debe permitir realizar el ingreso y actualización de los dispositivos biométricos.
RB007	Configuración de servicio.	Debe permitir realizar la configuración del servicio biométrico.
RB008	Administración de empleados	Administrar los datos de los empleados registrados en el sistema.

Tabla 2.1. Requerimientos generales para el sistema biométrico

Código requerimiento especifico	Requerimiento especifico	Descripción
RE001	Autenticación de usuario.	Realiza la validación mediante el ingreso del nombre de usuario y contraseña.
RE002	Carga del grupo de acceso al sistema.	Carga los menús correspondientes al grupo que pertenece el usuario.

Tabla 2.2. Requerimientos específicos (continúa)

RE003	Autenticación de empleado.	Comparación del dato biométrico obtenido del empleado con los registros guardados.
RE004	Adquisición de la característica biométrica.	Realiza la adquisición de la característica biométrica mediante la utilización de un escáner o mediante el ingreso del nombre de usuario y contraseña.
RE005	Validación de dispositivos biométricos.	Realizar la verificación de registro del dispositivo biométrico considerando que la dirección IP, debe ser única en el sistema.
RE006	Ingreso de dispositivo.	Debe permitir realizar el ingreso previa validación del dispositivo biométrico.
RE007	Actualización de dispositivo.	Debe permitir realizar la actualización de los datos del dispositivo biométrico almacenado en el sistema, previo validación de dispositivos biométricos.
RE008	Ingreso de nuevo horario laborable.	Permite realizar el ingreso, considerando que las horas que pertenecen a un mismo horario y a un mismo día no pueden cruzar.
RE009	Actualización de un horario laborable.	Permite realizar la actualización del horario, considerando que las horas que pertenecen a un mismo horario y a un mismo día no pueden cruzar.
RE010	Ingreso / Actualización de usuario.	Permite realizar el ingreso del nuevo usuario al sistema, el cual debe pertenecer a un grupo de usuario y el nombre de usuario ingresado debe ser único en el sistema.
RE011	Actualización de datos de institución.	Permite realizar la actualización de los datos de la institución mediante como: nombre, dirección teléfono.
RE012	Ingreso / actualización de empleado.	Permite realizar el ingreso o actualización del empleado mediante el ingreso de nombres, apellidos, teléfono, documento, nombre de usuario, contraseña y registro de huella dactilar.

Tabla 2.2. Requerimientos específicos (continúa)

RE013	Reporte de horas.	Muestra la información de las horas en que el empleado ha realizado el registro, calculando las horas laborables completadas diarias.
RE014	Reporte de empleados.	Muestra los empleados registrados en el sistema.
RE015	Reporte de eventos sistema.	Muestra los eventos realizados por los usuarios en el sistema.
RE016	Ingreso / actualización de usuario.	Debe permitir realizar el ingreso, actualización de los datos del usuario, tales como reseteo de contraseña, cambio de grupo de usuario y creación de usuario.

Tabla 2.2. Requerimientos específicos

2.1.2 REQUERIMIENTOS NO FUNCIONALES

En esta sección se presenta los requisitos no funcionales que posee el sistema

- ✓ Se ha se seleccionado el lenguaje de programación C# *(C Sharp),* con la ayuda de la herramienta de programación Visual Studio C#, ya que este es un lenguaje de programación que se tiene el suficiente conocimiento para realizar aplicaciones.
- ✓ Permitir la lectura y escritura de archivos para almacenar la configuración de conexión entre aplicaciones y guardar los mensajes de eventos de errores que puede generar la aplicación.
- ✓ Manejo de roles para un usuario del sistema es un requerimiento primordial para cualquier aplicación, ya que mediante esta opción se pude restringir el acceso a la información a los usuarios que no necesariamente poseen los mismos niveles jerárquicos de accesos a los datos.
- ✓ Para almacenar la información de los usuarios, empleados, dispositivos y registros de horas de horas, se utilizará SQL Server Express 2008, el cual es un motor de base de datos, que permite realizar la administración, y manipulación de los datos, mediante un control de acceso controlado a los datos y rápido procesamiento de peticiones. Ya que permite tener

independencia lógica de los datos, acceso concurrente, integridad, compresión de los datos y seguridad mediante la administración de políticas de seguridad.

- ✓ El lector biométrico debe ser accesible para cualquier dedo y el escáner debe tener espacio para permitir la adquisición de cualquier dedo de la mano.

Req. especifico	Requerimiento General							
	RB001	RB002	RB003	RB004	RB005	RB006	RB007	RB008
RE001	X							
RE002	X							
RE003			X					
RE004			X					
RE005			X			X		
RE006						X		
RE007						X		
RE008					X			
RE009					X			
RE010	X							
RE011							X	
RE012								X
RE013				X				
RE014				X				
RE015				X				
RE016		X						

Tabla 2.3. Matriz de requerimiento para el sistema biométrico

2.2 ANÁLISIS DE HARDWARE

A continuación se va a proceder a realizar la selección del hardware necesario para realizar la adquisición de imágenes.

- La comunicación entre la aplicación y el hardware biométrico utilizado para realizar la adquisición de la imagen puede ser mediante la tecnología USB o Ethernet.
- La resolución para realizar la adquisición de la imagen debe poseer como mínimo 500 dpi puntos por pulgada (por sus siglas en ingles *dots per inch* dpi), para obtener una imagen con una calidad aceptable, para realizar la comparación de la imagen adquirida con la minucia almacenada sin ningún inconveniente según la norma cjis-rs-0010[10] (Véase Anexo E).
- Es indispensable que el dispositivo pueda trabajar sobre el sistema operativo Windows, ya que la aplicación será desarrollada sobre .Net.
- La autenticación del empleado lo puede realizar el dispositivo biométrico, cuando la información de las huellas está almacenado en el dispositivo o lo puede realizar el sistema es decir la información esta almacenada en un repositorio central.

Considerando estas características que se ha procedido a elegir los siguientes lectores de huella dactilar los cuales se describen a continuación.

2.2.1 DISPOSITIVO SECUGEN HAMSTER IV

Este dispositivo está representado en la Figura 2.1, es la versión mejorada del SecuGen, con la captura de auto encendido y empaquetado en un diseño cómodo y económico, el escáner de huella digital Hamster IV cuenta con la industria del sensor óptico más robusta y avanzada ya que utiliza la tecnología patentada de huella digital biométrica de superficie de reflexión. El escáner de huella dactilar tiene una función de encendido automático, que automáticamente comprueba la presencia de un dedo. Además posee una función de captura inteligente que asegura la calidad de escaneo de huellas dactilares, ya que ajusta

[10]Norma que establece el desempeño estándar, para la resolución de las imágenes de la huella dactilar en los dispositivos de adquisición.

automáticamente el brillo en la imagen. El Lector de huellas dactilares puede ser utilizado para las funciones de autenticación o identificación sus características principales esta mostrado en la Tabla 2.4.

Figura 2.1. Lector de huella dactilar SecugenHamster IV [21]

2.2.2 4000B READER

Figura 2.2. Lector de huella dactilar 4000B Reader [22]

Estos lectores utilizan la tecnología de exploración óptica de huellas digitales, para lograr una excelente calidad de imagen y una amplia área de captura. Poseen una capacidad de autenticación precisa y rápida, incluso de las huellas dactilares irregulares, sin importar el ángulo de colocación. El lector puede ser utilizado para integrar aplicaciones desarrolladas.

En la Tabla 2.5, se describe las características que posee este dispositivo biométrico.

Característica	**Detalle**
Dimensiones	Ancho: 2,7 cm Largo: 4 cm alto:7,3 cm
Peso	100 g.
Resolución	500 dpi
Tiempo de verificación	Menos de 1 segundo
Tipo Captura	Óptico, permite realizar la adquisición de la imagen en formato jpg o string.
Interfaz	USB
Sistemas Operativos soportados	Windows 7 / Vista/ Server 2003 / Xp / Milenium / 98.
Certificaciones	Comisión general de comunicaciones (FCC)[11] y Restricción de ciertas Sustancias Peligrosas en aparatos eléctricos y electrónicos (RoHS)[12].
Otros	Dispositivo Biométrico con librerías SDK. Compatible con Java.
Estándares soportados	Intercambio de datos basado en minucias ISO 19794-2 y INCITS 378. BioApi[13].

Tabla 2.4. Características del SECUGEN HAMSTER IV [21]

2.2.3 BIOSTART SDK

En la Figura 2.3, muestra el dispositivo BioStar SDK que contiene un kit de desarrollo de software para el control de acceso del personal, ya que permite manejar, las funciones de autenticación e identificación. Esto hace posible la integración del hardware con cualquier software de control de asistencia. El kit incluye las librerías (DLLs[14]), soporte para los diferentes lenguajes de

[11] FCC. Esta certificación se refiere a que el dispositivo no debería causar interferencias dañinas para ser humano.
[12]RoHS Especifica que el dispositivo puede ser reciclado.
[13] BioAPI Estándar utilizado en las aplicaciones, para manejar la forma de comunicación con los dispositivos biométricos y la forma en la que los datos son almacenados.
[14] DLL por sus siglas en inglés de *dynamic-link library*, es el término con el que se refiere a los archivos con código ejecutable que se cargan bajo demanda de un programa por parte del sistema operativo.

programación (Visual Basic, Visual C++, C#); estas características están representadas en la Tabla 2.6.

Característica	**Detalle**
Dimensiones	Ancho: 6,0 cm Largo: 10,3cm Alto:5,8 cm
Peso	120 g.
Resolución	512 dpi
Tipo Captura	Óptico, permite guardar la imagen en formato jpg.
Tiempo de verificación	Menos de 1 segundo
Interfaz	USB
Sistemas Operativos soportados	Windows 7 / Vista/ Server 2003 / XP y Windows Server 2000 y 2003
Certificaciones	FCC Clase B
Otros	Dispositivo Biométrico con librerías SDK, previo registro. Rechazo de huella latente, Rechazo de huella falsificada
Estándares soportados	USB, WHQL[15]

Tabla 2.5. Características del hardware de adquisición WED-USB100

Figura 2.3. BIOSTART SDK [23]

[15] Windows Hardware Quality Labs testing o WHQL Testing consiste en unas pruebas mediante unos tests ejecutados en ordenadores de varios fabricantes y los resultados de esas pruebas son enviados a Microsoft.

Características	Detalle
Tamaño	Ancho: 5,0 cm Largo: 16 cm Alto:3,7 cm
Resolución	500dpi
Velocidad	2000 comparaciones en 1 segundo
Tarjeta RF	125KHz(EM,HID)
Tipo Captura	Óptico permite almacenar la información de las huellas en el dispositivo. Máximo 1000 huellas.
Modos de Operación	Huella, Tarjeta, Huella – Tarjeta
Interface	TCP/IP, RS485
Otros	Soporta diversos lenguajes de programación (Visual Basic, Visual C++, C#)

Tabla 2.6. Especificaciones de BIOSTART SDK

2.2.4 SELECCIÓN DEL HARDWARE BIOMÉTRICO

En la Tabla 2.7 se presenta un cuadro comparativo de los dispositivos biométricos seleccionados con la finalidad de determinar el dispositivo biométrico más idóneo para el funcionamiento del sistema biométrico.

El hardware seleccionado para realizar la adquisición de la huella dactilar es el Secugen Hamster, debido a que es un hardware bastante robusto, ya posee el lenguaje soportado para la aplicación, puede almacenar la información de la huella en dos formatos diferentes, posee el lector óptico con captura automática, y es utilizado en las instituciones bancarias para autentificar a los clientes al momento de realizar un retiro. Además su facilidad de interacción con los distintos leguajes de programación como son: Visual Basic, C# *Sharp* y Java, hacen de este hardware el más completo para realizar la implementación del sistema biométrico.

Característica	SECUGEN HAMSTER	4000B READER	BIOSTAR SDK
Resolución	500 dpi	512 dpi	500 dpi
Tipo Comunicación	USB	USB	Ethernet
Autenticación	Remota	Remota	Local
Lenguajes soportados	Visual Basic, C#, java	Lenguaje C#	Visual basic, visual C++, C#
Formatos de almacenamiento de datos	JPG o String.	JPG	JPG, almacenamiento en el dispositivo
Lector	Óptico captura automática	Óptico	Óptico, captura automática

Tabla 2.7. Comparación de los dispositivos biométricos

CAPÍTULO 3
DISEÑO, DESARROLLO E IMPLEMENTACIÓN DEL SISTEMA BIOMÉTRICO

En este capítulo se realiza la descripción del sistema biométrico la cual está representada en la Figura 3.1 y considera los requerimientos descritos en el capítulo dos, para lo cual se utiliza el lenguaje unificado de modelado (UML).

Modelo de diagramas de flujo, utilizado para indicar el flujo o secuencia de una operación realizada en el sistema.

Diagramas de caso de uso el cual indica los participantes o actores involucrados en el uso del sistema y operaciones que realiza la aplicación.

Diagrama relacional de base de datos la cual es utilizado para identificar cada uno de las entidades a modelar para el almacenamiento y manipulación de la información en el sistema.

Diagrama de secuencia que muestra la interacción de un conjunto de objetos en una aplicación a través del tiempo, además se presenta el código fuente del sistema biométrico desarrollado y se describe el formato de mensaje utilizado, entre el cliente y el servidor.

Para realizar el registro de empleados mediante la autenticación de la huella dactilar o el nombre de empleado y contraseña.

3.1 ELEMENTOS DEL SISTEMA BIOMÉTRICO

Las aplicaciones a ser implementadas para el funcionamiento del sistema biométrico se describen a continuación:

- *Aplicación Servidor*.- Esta aplicación realiza el procesamiento de solicitudes de registro de autenticación de los empleados mediante la recepción de peticiones y envió de respuestas; además permite realizar la comparación de la huella dactilar o nombre de empleado y contraseña.

- *Aplicación Administrador*.- Permite realizar la administración del sistema biométrico mediante la creación de usuarios, empleados, reportes y horarios laborables. Además interactúa con el dispositivo biométrico para realizar la adquisición de la imagen de la huella dactilar del empleado para ser almacenado en el sistema.

Aplicación Cliente.- Esta aplicación interactúa con el lector biométrico para enviar las solicitudes de registro a la aplicación servidor, procesa la respuesta y muestra el resultado al empleado.

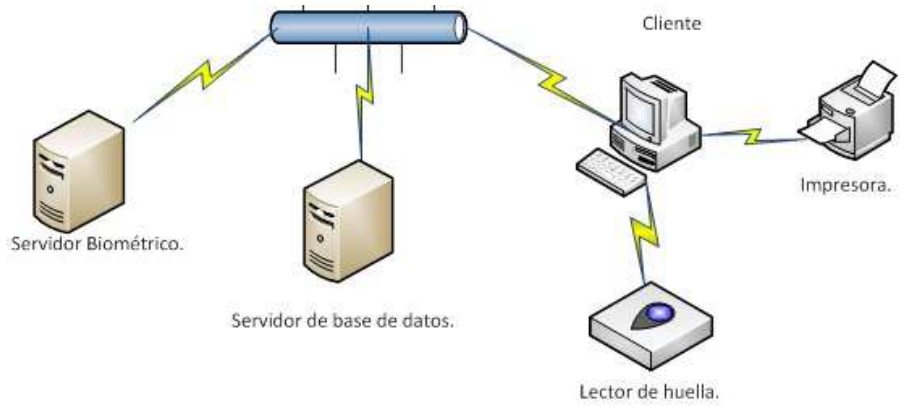

Figura 3.1. Elementos del sistema biométrico

3.2 FORMATO DE INTERCAMBIO DE MENSAJES

En esta sección se describe los campos utilizados en la trama de comunicación, para realizar la autenticación del empleado mediante el envío y recepción, entre la aplicación cliente y la aplicación servidor.

- *TIPO DE MENSAJE.* Es la cabecera de la trama utilizada, para distinguir si la información es un requerimiento o una respuesta, su tamaño es de cuatro caracteres.

  Ejemplo de asignación:

  1200 requerimiento que envía la aplicación cliente al servidor.

  1210 respuesta a la petición de requerimiento.

- *TIPO DE AUTENTICACIÓN.* Campo utilizado, para determinar si el requerimiento de autenticación es: solo huella dactilar, usuario y contraseña o huella dactilar y nombre de empleado y contraseña, su tamaño es de 4 caracteres numéricos.

  Ejemplo de asignación:

  1001 Registro con huella dactilar.

  1002 Registro con nombre de empleado y contraseña.

  1003 Registro con huella dactilar, nombre de empleado y contraseña.

- *CÓDIGO DE ERROR.* Identificado para determinar el error que se puede generar al momento de realizar la autenticación entre el cliente y el servidor, su tamaño es de tres caracteres. A continuación se describen los errores que se van a manejar en el sistema biométrico los cuales están representados en la Tabla 3.1.
- *NÚMERO DE DISPOSITIVO.* Indica el número de dispositivo biométrico asignado, para realizar la autenticación su tamaño es de cuatro caracteres.
- *DATOS.* Información enviada al servidor para realizar la autenticación del empleado, ésta puede contener la huella dactilar, nombre de empleado y contraseña, o ambos datos. La longitud de este campo depende del tipo de autenticación a utilizar, es por ello que se detalla el tamaño de los campos a enviarse.
  - *NOMBRE EMPLEADO.* Utilizado cuando la autenticación es por nombre de empleado o combinado su tamaño de 15 caracteres
  - *CONTRASEÑA.* Su tamaño es de 20 caracteres. Se envía la contraseña del empleado para realizar la autenticación.
  - *HUELLA.-* Utilizado cuando la autenticación es mediante huella dactilar o combinado, su tamaño es variable dependiendo del tamaño de la huella dactilar.

Código	Tipo Error	Descripción
000	Ok	Evento de autenticación exitoso, se procede con el registro del empleado.
001	Empleado o contraseña, no existen	Se ha recibido el nombre de empleado o contraseña incorrecto o no está registrado en el sistema.
004	No se pudo conectar con el servidor	Bloqueo de conexión entre el cliente y el servidor.
005	No se pudo conectar a la base de datos	Error producido en el servidor, al momento de realizar el acceso a la base, ya sea para realizar la administración o la autenticación.
009	Tipo de autenticación no soportada.	Recibe el campo de autenticación que no está definido por la aplicación.
010	Tipo de requerimiento inválido	Cuando el cliente o servidor reciben un tipo de mensaje o tipo de identificación diferente al que se asignó en el sistema.
013	Huella inválida	La huella capturada, no corresponde a ninguna huella de empleado almacenada en el sistema
020	Aplicación no registrada	La dirección IP de la aplicación cliente biométrico o número de aplicación no está registrada en el sistema.

Tabla 3.1. Código de errores utilizados para realizar la autenticación de empleado entre cliente y servidor

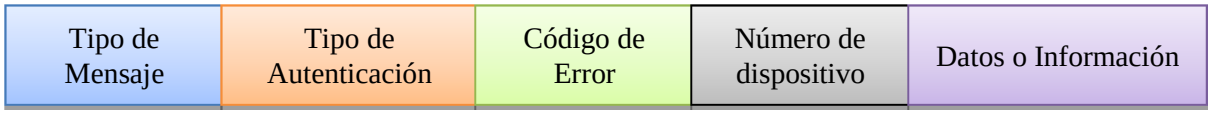

Figura 3.2. Trama de información de requerimiento

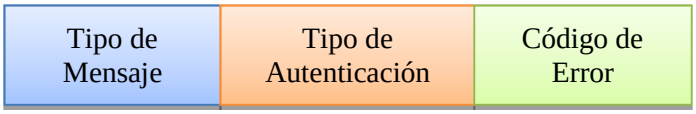

Figura 3.3. Trama de respuesta de requerimiento

Ejemplos de tramas a enviar

a. *AUTENTICACIÓN BASADA POR HUELLA DACTILAR.*

Trama de requerimiento

1200100100000001AwAAABQAAABUAwAAAQASAAMAVQAAAAAASQ….

Tipo Mensaje	1200
Tipo Autenticación	1001
Código Error	000
Número Dispositivo	0001
Información huella dactilar	AwAAABQAAABUAwAAAQASAAMAVQAAAAAASQ

Tabla 3.2. Trama de requerimiento basado en autenticación de huella dactilar

Trama de respuesta

12001001000

Tipo Mensaje	1200
Tipo Autenticación	1001
Código Error	000

Tabla 3.3. Respuesta de requerimiento

b. *AUTENTICACIÓN BASADA POR NOMBRE DE EMPLEADO Y CONTRASEÑA*

Trama de requerimiento

12001002000002lchuqui 1234

Tipo Mensaje	1200
Tipo Autenticación	1002
Código Error	000
Número Dispositivo	0002
Información nombre empleado	lchuqui
Información contraseña	1234

Tabla 3.4. Trama de requerimiento basado en autenticación de nombre de empleado y contraseña

Trama de respuesta

12001002000

Tipo Mensaje	1200
Tipo Autenticación	1002
Código Error	000

Tabla 3.5. Respuesta de requerimiento

c. *AUTENTICACIÓN MIXTA O COMBINADA*

Trama de requerimiento

12001003000001lchuqui 1234 AwAAABQAAABUAwAAAQASAAM….

Tipo Mensaje	1200
Tipo Autenticación	1003
Código Error	000
Número Dispositivo	0001
Información nombre empleado	lchuqui
Información contraseña	1234
Información huella dactilar	AwAAABQAAABUAwAAAQASAAM….

Tabla 3.6. Requerimiento de autenticación mixta

Trama de respuesta

12001003000001

Tipo Mensaje	1200
Tipo Autenticación	1002
Código Error	000

Tabla 3.7. Respuesta del requerimiento

3.3 MODELO DE CASOS DE USO DEL SISTEMA BIOMÉTRICO

Se presenta la funcionalidad del sistema biométrico tomando en consideración los actores involucrados en el sistema y los requerimientos descritos en el capítulo dos, los cuales están representados en la Tabla 3.8.

- *EMPLEADO.-* Es la persona contratada por la empresa o institución que realiza una actividad laboral específica e interactúa con la aplicación, para realizar el registro de ingreso o salida, este registro puede ser mediante la presentación de la huella dactilar o el Nick empleado[16] y contraseña.
- *USUARIO.-* Es la persona que va a administrar el sistema, mediante la creación y actualización de empleados, horarios laborables, dispositivos biométricos, usuarios y perfiles de acceso al sistema.

Figura 3.4. Actores que intervienen en el sistema biométrico

En la Figura 3.5 se presenta el diagrama de casos de uso para las entidades usuario y empleado, con las funciones que va a interactuar cada uno de estos actores con el sistema biométrico, considerando los requerimientos funcionales descritos anteriormente.

Actor	Evento	Respuesta
Usuario	Acceso al sistema.	El usuario ingresa su nombre de usuario y contraseña en un cuadro de texto. Para enviar la autenticación se va a utilizar el botón de aceptar; el sistema recibe la petición de acceso, busca el usuario con el nombre de usuario y contraseña ingresado, si este coincide con los datos almacenados se procede a enviar la respectiva respuesta y se envía el grupo de usuario y cada menú que posee. Si la autenticación es rechazada se envía la respuesta de nombre de usuario o contraseña inválidos.

Tabla 3.8. Representación de requerimientos (continúa)

[16] Nick empleado. Es el nombre de usuario del empleado que se utiliza para distinguir a los empleados.

Usuario	Creación o actualización perfiles.	El usuario selecciona la opción de actualizar o crear un nuevo perfil. Si va a ingresar un nuevo perfil se verifica que no exista el nombre en el sistema para permitir ingresar, si es una actualización el sistema carga los permisos que posee el grupo.
Usuario	Creación o actualización usuarios.	El usuario selecciona la opción de actualizar o crear un nuevo usuario. Para crear el usuario se valida que el nombre de usuario sea único en el sistema, se selecciona el perfil que desea y se asigna una clave. Si van a actualizar los datos del usuario se cargarán los usuarios registrados en el sistema para que el usuario seleccione el usuario que desea modificar, al seleccionar el usuario se procederá con la carga automática de los datos del usuario seleccionado. Cualquier creación o actualización exitoso o no, se notifica mediante mensaje.
Usuario	Creación o actualización empleado	Al seleccionar la opción de crear o modificar los datos del empleado se procede a realizar la verificación del nombre de empleado y su número de documento sea único en el sistema, para la asignación de la contraseña se debe requerir que ingrese dos veces la contraseña, para asegurar que sea la contraseña que quiere el empleado. Cualquier ingreso o creación exitoso o no, se notifica mediante un mensaje.
Usuario	Creación o actualización horarios laborables.	Para la opción de creación del horario, el usuario debe ingresar el nombre de horario y las horas de trabajo, el sistema procede a crear horario siempre y cuando el nombre del horario sea único y ninguna de las horas seleccionadas se cruce en los mismos días. Si la opción es de actualización el sistema carga los grupos de horarios disponibles, al momento de seleccionar el horario se carga las horas perteneciente al horario para que se puedan modificar las horas. Cada uno de estos eventos que se generan se debe mostrar el respectivo mensaje de notificación al usuario.

Tabla 3.8. Representación de requerimientos (continúa)

Usuario	Creación o actualización dispositivos.	El usuario al seleccionar esta opción de creación o actualización de dispositivo, debe ingresar los datos del dispositivo como es la dirección IP y la descripción del dispositivo, la dirección IP del dispositivo debe ser única para cualquiera de estas dos opciones. Cada evento generado debe mostrar un mensaje de respuesta de aceptación o rechazo.
Empleado	Registrar hora de ingreso o salida.	El empleado realiza la identificación o presentación de sus credenciales biométricas al sistema, este valida los siguientes datos: tipo de mensaje, tipo de autenticación, número de dispositivo asignado, dirección IP de origen de la petición, los cuales deben estar almacenados. Si los datos almacenados coinciden con los datos ingresados se procede a registrar la hora del empleado y se envía el mensaje de registro al empleado caso contrario se envía el respectivo mensaje de error.
Usuario	Reportes	Los reportes a mostrar al usuario son: horas de ingreso y salida, horas totales mediante la selección de los siguientes filtros seleccionados los cuales pueden ser por día, rango de fechas, por empleados o por empleado. Además debe permitir visualizar los eventos realizados en el sistema, por rango de fechas.

Tabla 3.8. Representación de requerimientos

3.4 MODELO DE CLASES

Utilizando el modelo de casos de uso se procede a realizar la abstracción de los elementos que intervienen en el sistema, con la finalidad de obtener el modelo de clases con sus relaciones entre clases, atributos y métodos los cuales muestran la función que posee cada una clase, representado en la Figura 3.6

- Empleado.
- Usuario.
- Persona.

- Dispositivo biométrico.
- Registro.
- Horario laborable.
- Biometría.
- Sector Laboral, Actividad Laboral.
- Salario.

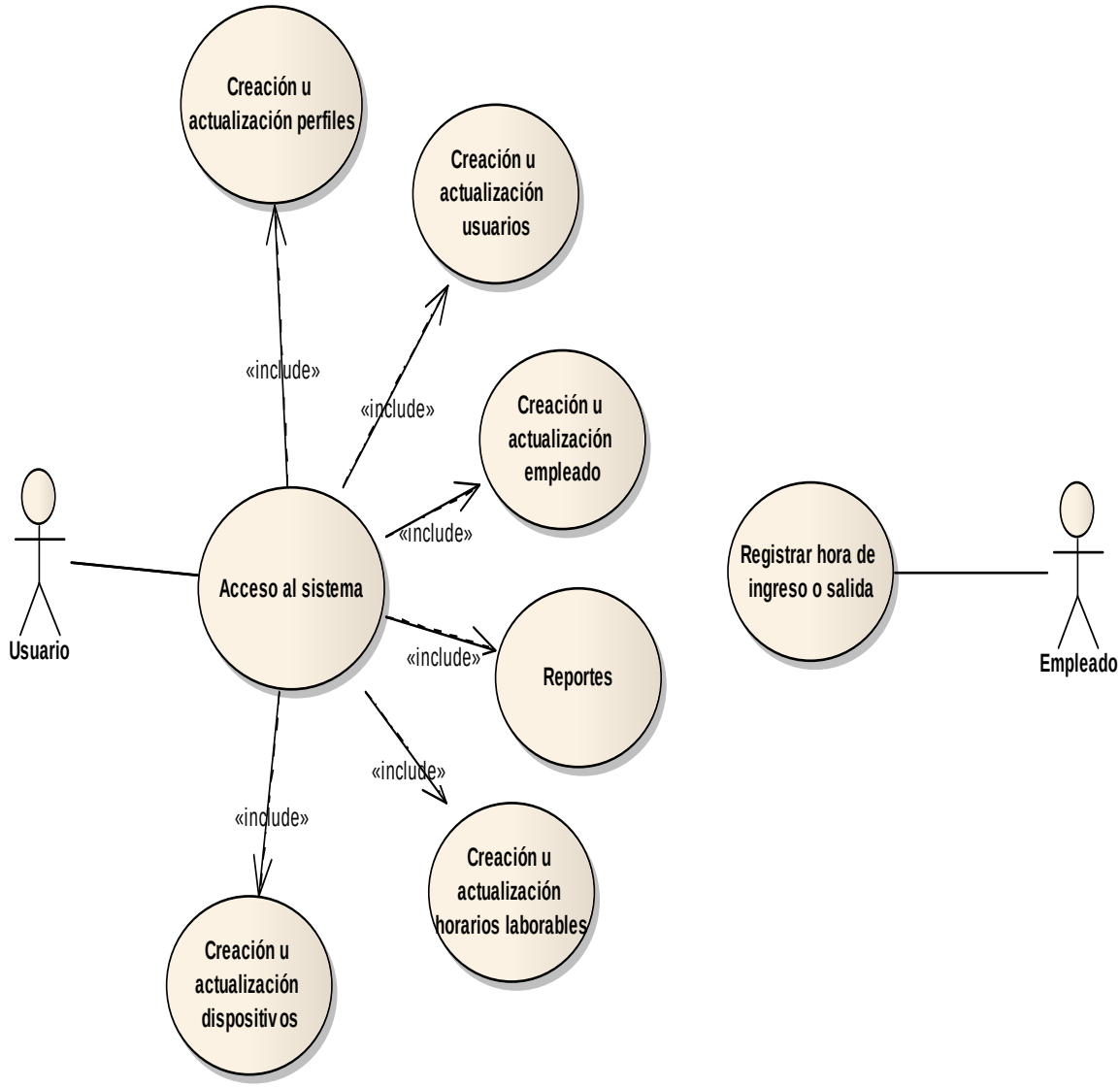

Figura 3.5. Modelo de casos de uso del sistema biométrico

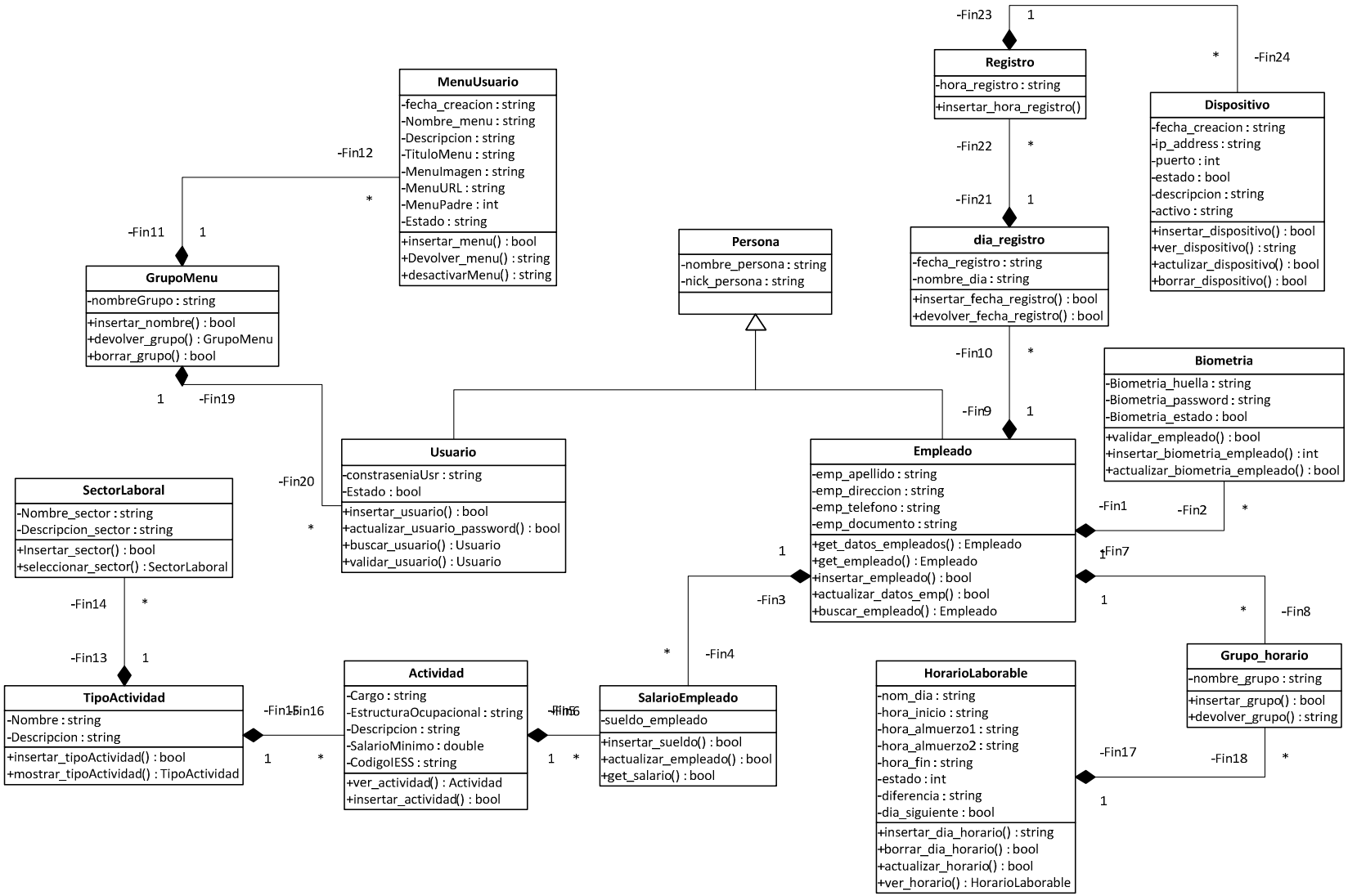

Figura 3.6. Modelo de clase del sistema biométrico

3.4.1 DESCRIPCIÓN DE LAS CLASES IMPLEMENTADAS

En esta sección se va a describir las principales clases implementadas, con sus respectivos atributos y métodos.

Clase Empleado	Permite almacenar los datos del empleado, esta clase hereda los atributos y métodos de la clase persona.
Atributos	
Emp_apellido	Atributo utilizado para almacenar el apellido del empleado.
Emp_direccion	Atributo utilizado para almacenar la dirección del empleado
Emp_telefono	Atributo utilizado para almacenar el número telefónico.
Emp_documento	Atributo utilizado para almacenar el número de documento de identidad.
Métodos	
Get_datos_empleados	Obtiene el objeto empleado.
Insertar_empleado	Realiza el ingreso de los datos del empleado
Actulizar_datos_emp	Permite realizar la actualización de los datos del empleado.
Buscar_empleado	Devuelve los datos del empleado si existe mediante el ingreso de su documento o nombres.

Tabla 3.9. Clase Empleado

Clase Biometría	Esta clase es utilizada para almacenar los datos biométricos del empleado como son: la huella dactilar y una contraseña.
Atributos	
Biometria_huella	Minucias del empleado.
Biometria_password	Almacena la contraseña del empleado. Este atributo es utilizado cuando la autenticación es realizada por nombre del empleado y contraseña.

Tabla 3.10. Clase Biometría (continúa)

Biometria_estado	Permite realizar el bloqueo de la autenticación biométrica.
Métodos	
Validar_empleado	Valida la información de la contraseña ingresada, con los datos almacenados, mediante una comparación, retorna un booleano, indicando lo siguiente: verdadero, cuando el dato capturado es igual al almacenado y falso cuando los datos ingresados no son correctos.
Validar_huella_biometria	Valida la información de la huella dactilar con los datos almacenados, mediante una comparación. Retorna un booleano, indicando lo siguiente: verdadero, cuando los datos ingresados son correctos y falso cuando los datos ingresados no son correctos.
Insertar_biometria_empleado	Inserta la huella dactilar o la contraseña del empleado.
Actualizar_biometria_empleado	Permite actualizar los datos biométricos del empleado como la huella dactilar o la contraseña

Tabla 3.10. Clase Biometría

Clase Grupo Horario	Almacena el grupo de horario, al que pertenecen los empleados.
Atributos	
Nombre_grupo	Almacena el nombre del grupo, al a que puede pertenecer el empleado.
Métodos	
Insertar_grupo	Inserta un nuevo nombre de grupo, para el horario laborable del empleado.
Devolver_grupo	Obtiene el nombre del grupo del horario.

Tabla 3.11. Grupo Horario

Clase horario Laborable	Utilizado para almacenar las horas y los días de trabajo que el empleado debe cumplir.
Atributos	
Nom_dia	Almacena el nombre del día del horario laborable.
Hora_inicio	Almacena la hora de ingreso de trabajo del empleado.
Hora_almuerzo1	Almacena la hora en que el empleado sale almorzar.
Hora_almuerzo2	Almacena la hora de entrada del empleado que llega del almuerzo.
Hora_fin	Almacena la hora de salida del empleado.
Estado	Utilizado para indicar si el día está activo o desactivo.
Diferencia	Almacena las horas totales de trabajo diario del empleado
Métodos	
Insertar_dia_horario	Inserta los datos de las horas de inicio, almuerzo entrada, almuerzo salida y salida, nombre del día. Para el grupo de horario.
Borrar_dia_horario	Elimina y desactiva el horario de un grupo de horario.
Actualizar_horario	Actualiza el horario perteneciente a un grupo.
Ver_horario	Muestra el horario del grupo de horario.

Tabla 3.12. Clase Horario Laborable

Clase Día Registro	Utilizado para almacenar la fecha del registro de ingreso o salida, del empleado.
Atributos	
Fecha_registro	Almacena la fecha en que los empleados, han realizado el registro.
Nombre_dia	Almacena el nombre del día en que los empleados, han realizado el registro.

Tabla 3.13. Clase día registro (continúa)

Métodos	
Insertar_fecha_registro.	Inserta la fecha de registro del empleado. Si ya existe, no inserta ningún valor.
Devolver_fecha_registro	Muestra o devuelve la fecha de registro, en que el empleado ha realizado el registro.

Tabla 3.13. Clase día registro

Clase Registro	Utilizada para almacenar las horas en que el empleado se ha registrado.
Atributos	
Hora_registro	Almacena la hora en la que el empleado ha realizado el registro.
Métodos	
Insertar_hora	Inserta la hora y el código de fecha en que el empleado ha realizado el registro, previo a la autenticación de la huella dactilar o el nombre de usuario y contraseña.

Tabla 3.14. Clase Registro

Clase Dispositivo	Almacena los datos del dispositivo biométrico cliente.
Atributos	
Fecha_creacion	Almacena la fecha de agregación del dispositivo al sistema.
Ip_adreess	Almacena la dirección IP que va tener el dispositivo biométrico.
Puerto	Número de puerto con que está trabajando el dispositivo biométrico.
Estado	Indica el estado de habilitación del dispositivo si esta deshabilitado no permitirá realizar el registro de usuario.
Descripción	Utiliza una descripción para el dispositivo biométrico.

Tabla 3.15. Clase Dispositivo (continúa)

Métodos	
Insertar_dispositivo	Inserta un nuevo dispositivo biométrico, tomando en consideración que la dirección IP no debe repetirse con los datos almacenados.
Ver_dispositivo	Muestra los dispositivos biométricos que están ingresados al sistema.
Actualizar_dispositivo	Actualiza los datos del dispositivo biométrico.
Borrar_dispositivo	Elimina los datos del dispositivo biométrico.

Tabla 3.15. Clase Dispositivo

Clase Usuario	Utilizado para almacenar los datos de los usuarios, que gestionan la aplicación.
Atributos	
ContraseniaUsr	Almacena la contraseña del usuario para acceder al sistema. *Estado.-* Maneja el estado del usuario si está activo o inactivo.
NombreUsr	Almacena el nombre del usuario.
PassUsr	Almacena la contraseña del usuario. Para acceder al sistema.
Métodos	
Insertar_usuario	Insertar un nuevo usuario para la aplicación.
Actualizar_usuario_password	Actualiza la contraseña del usuario.
Buscar_usuario.	Realiza una búsqueda del usuario y retorna todos los atributos de este.
Validar_usuario	Valida el usuario y la contraseña.

Tabla 3.16. Clase Usuario

Clase Menú Usuario	Utilizado para almacenar los diferentes menús de administración de usuario y sus respectivos submenús.
Atributos	
Fecha_creacion	Almacena la fecha de creación del menú.
Nombre_menu	Especificación del tipo de menú, para identificar si es principal o secundario.
Descripcion	Breve descripción del menú.
TituloMenu	Nombre que posee el menú.
MenuImagen	Dirección donde se encuentra el ícono o imagen para el menú.
MenuURL	Dirección para acceder al menú desde el menú actual.
MenuPadre	Código del menú padre al que pertenece el submenú.
Estado	Estado del menú, su estado es activo o inactivo.
Métodos	
Insertar_menu	Inserta un nuevo menú o submenú en el sistema.
Devolver_menu	Retorna los elementos del submenú que pertenecen al menú principal.
Descativar_menu	Desactiva el elemento del menú seleccionado para el grupo usuario.

Tabla 3.17. Clase menú usuario

3.5 DIAGRAMAS DE FLUJO

A continuación se presentan los diagramas de flujos de los principales procesos, que utiliza el sistema, para describir la lógica del sistema y su funcionamiento. Por lo que a continuación se enumera las funciones más importantes creadas en el sistema, para realizar la administración de usuario, empleados, horarios y dispositivos.

- Ingreso de nuevo empleado.
- Ingreso de un horario laborable.

- Ingreso de registro de hora de empleado.
- Creación de un nuevo perfil de usuario.
- Ingreso de un nuevo usuario.
- Ingreso de un nuevo dispositivo.

Se ha seleccionado el ingreso para describir el proceso que realizan, ya que estos procesos poseen más validaciones al momento de actualizar los datos.

3.5.1 DIAGRAMA DE FLUJO DE INGRESO DE NUEVO EMPLEADO

Para realizar el ingreso de un nuevo empleado el cual está representado en la Figura 3.7, se procede de la siguiente manera:

a. Solicitar los datos necesarios, tales como: nombre, apellido, dirección, teléfono, documento y nombre de empleado *(Nick).*
b. Verificar el nombre de empleado *(Nick)* y documento del empleado no se repitan en el sistema, si alguno de estos datos coinciden en el sistema, este no debe permitir realizar el ingreso del empleado y debe regresar al paso anterior y mostrar el mensaje de error, caso contrario debe pasar al siguiente paso.
c. Realizar el ingreso del nuevo empleado y luego solicitar los datos biométricos.
d. Insertar los datos biométricos y mostrar el mensaje de registro exitoso o no.

3.5.2 DIAGRAMA DE FLUJO PARA REALIZAR LA CREACIÓN DE UN HORARIO LABORABLE

En la Figura 3.8, se presenta el proceso para realizar el ingreso de un horario laborable:

a. Ingresar el nombre del horario laborable. Si ya existe el nombre, no debe permitir crear el nuevo horario y debe mostrar el mensaje de error para que el usuario pueda ingresar otro nombre.
b. Ingresar los datos de días laborables, con sus respectivas horas de trabajo tales como las horas de inicio, fin, almuerzo entrada y almuerzo salida.

c. Calcular la diferencia entre las horas de entra y salida y las horas de entrada y salida del almuerzo del empleado.
d. Verificar que la hora de almuerzo de entrada y la hora de salida no supere las dos horas laborables en el día si cumple con este requerimiento pasar al punto d, caso contrario regresar al paso b.
e. Determinar si las horas ingresadas no pertenecen al día ingresado y al grupo ingresado, si estas horas pertenecen se entiende que es una hora cruzada y se presenta el respectivo mensaje y se regresa al punto b, caso contrario se pasa al siguiente literal.
f. Insertar los datos del horario que el usuario ha ingresado y mostrar la respuesta de ingreso de horario exitoso.

3.5.3 REGISTRO DE HORAS DE EMPLEADO

En la Figura 3.9, se presenta el proceso para realizar el registro de horas de ingreso del empleado, mediante el proceso de autenticación.

3.5.3.1 Diagrama de flujo para autenticar al empleado

Se presenta en la Figura 3.9, el diagrama de flujo para realizar la autenticación del empleado mediante las opciones de autenticación de huella dactilar tales como: autenticación por nombre de empleado y contraseña, autenticación por huella dactilar, o autenticación combinada mediante la solicitud de la huella de empleado, nombre de empleado y contraseña. A continuación se describe el proceso de autenticación.

a. Verificar el tipo de autenticación recibido.
b. Validar el número del terminal con su dirección IP, con los datos almacenados, si estos datos no concuerdan enviar el mensaje de error de terminal no registrada caso contrario pasar al siguiente paso.
c. Realizar una comparación de los datos recibidos dependiendo del tipo de autenticación con los datos almacenados, si los datos concuerdan pasar al siguiente paso caso contrario retornar el mensaje de error de empleado no registrado o huella invalida dependiendo del tipo de autenticación.

d. Realizar el registro de la fecha y la hora del empleado en el sistema y retornar el mensaje de registro exitoso.

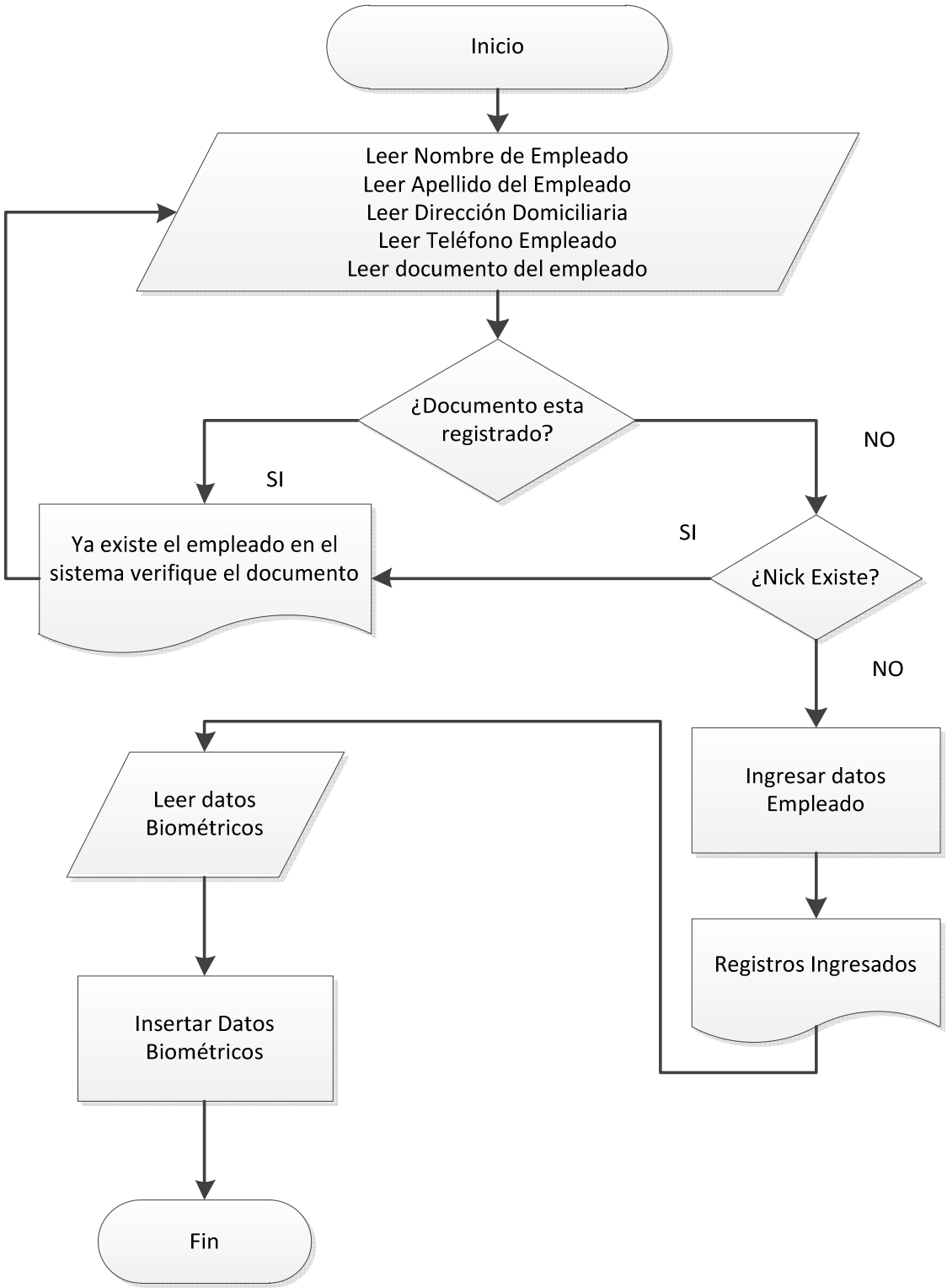

Figura 3.7. Diagrama de flujo de registro de un nuevo empleado

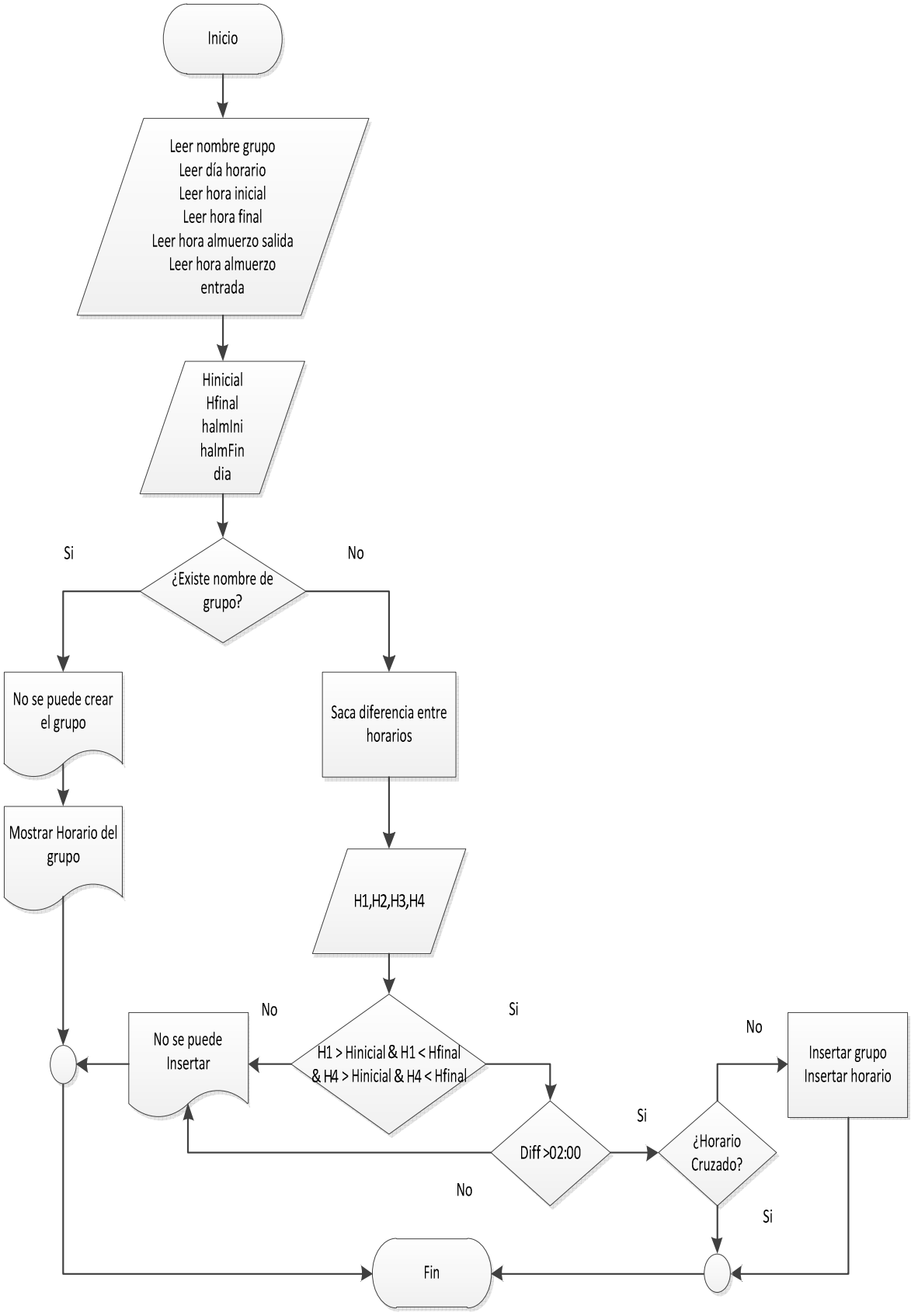

Figura 3.8. Diagrama de flujo para realizar el ingreso de un horario laborable

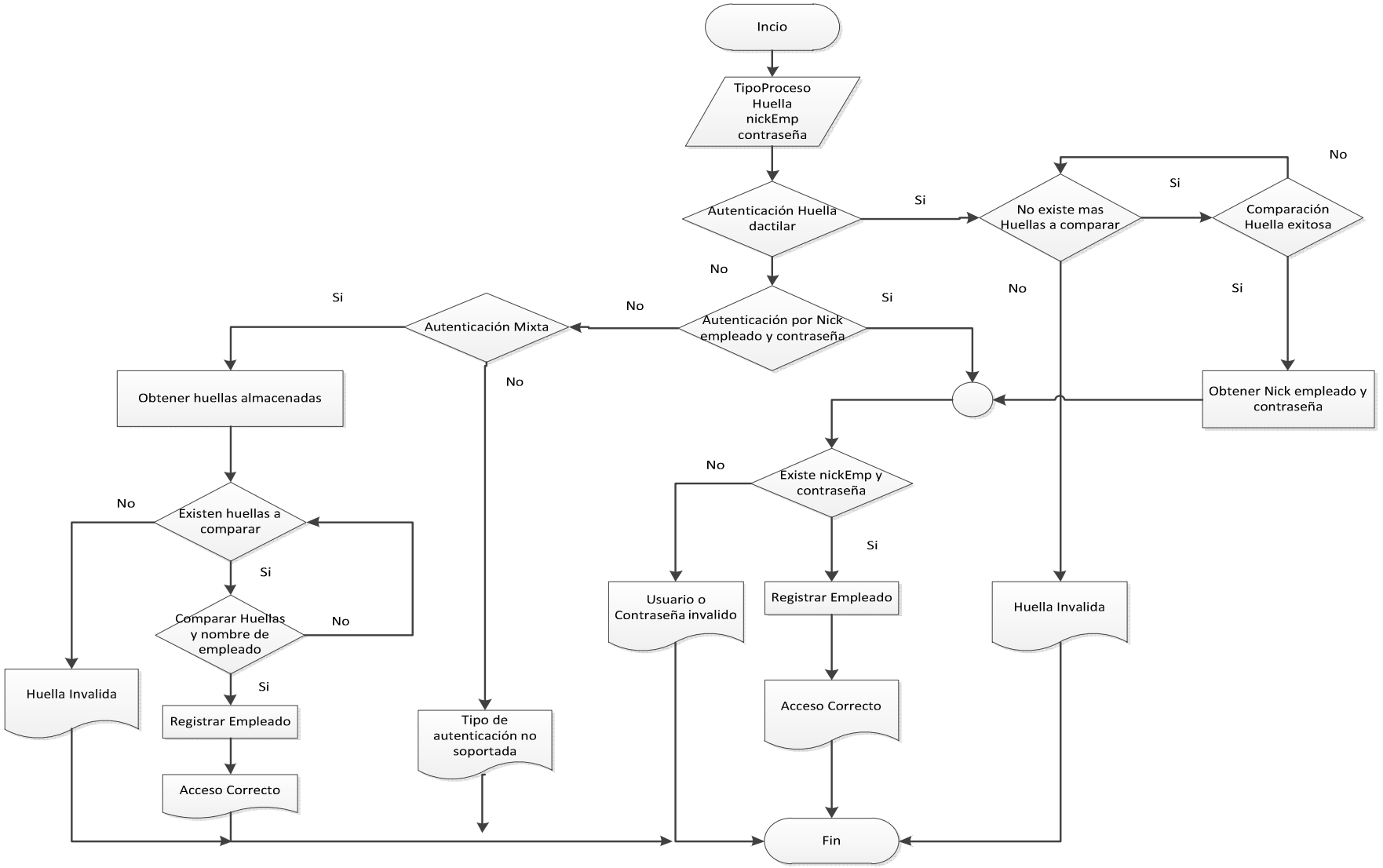

Figura 3.9 Autenticación y registro de hora de empleado

3.5.4 CREACIÓN DE UN PERFIL DE USUARIO

En esta sección se describe la opción para crear el perfil de usuario y se explica el proceso de asignación de permisos, este proceso está representado en la Figura 10 a).

a. Ingresar el nuevo nombre del perfil.
b. Seleccionar los ítems, que se desea tener acceso.
c. Valida el nombre del grupo que se encuentre disponible.
d. Insertar los datos.

Para realizar la actualización del perfil, se realiza el siguiente proceso el cual está representado en la Figura 10 b).

a. Selecciona el perfil que se desea modificar.
b. Seleccionar los ítems, que se desea tener el acceso o se desea quitar el acceso.
c. Guardar los datos actualizados en el sistema.

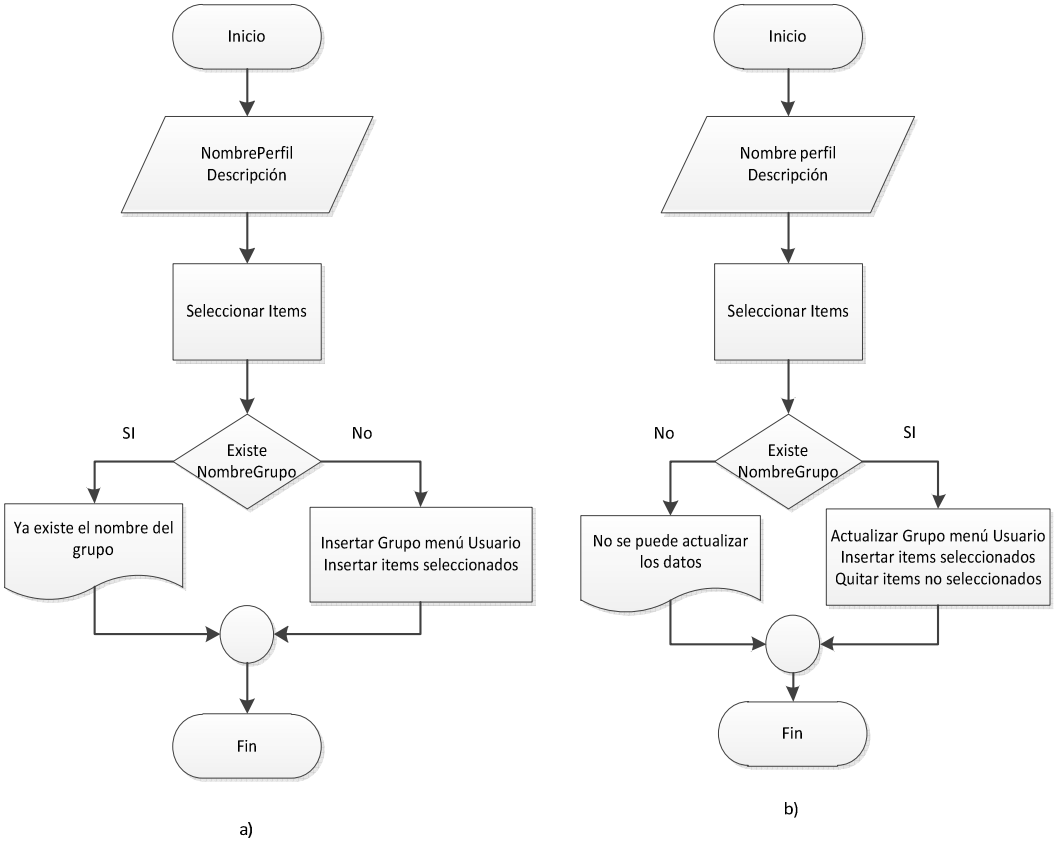

Figura 3.10 a) Creación de un perfil de usuario, b) Actualización del perfil

3.5.5 INGRESO DE USUARIO

Para este proceso se presenta el algoritmo de ingreso de un nuevo usuario el cual está representado en la Figura 3.11 a).

a. Solicitar nombre de usuario, contraseña, su nombre y apellido y finalmente seleccionar un perfil de usuario o rol, al que desea que pertenezca el usuario.
b. Verificar el nombre de usuario que no se encuentre ingresado en el sistema, si no existe en el sistema se procede al siguiente paso caso contrario regresamos al paso uno y se muestra el mensaje de nombre de usuario duplicado.
c. Ingresar los datos de usuario, y presentar el mensaje al usuario.

A continuación se describe el proceso de actualización de datos para el usuario, representado en la Figura 3.11 b).

a. Verificar el perfil que posee el usuario actual, ya que el perfil administrador es el único que permite realizar los cambios de grupos.
b. Si el usuario pertenece al grupo de administrador se procede a habilitar los usuarios a realizar el cambio, caso contrario se deshabilita esta opción. Y se selecciona por defecto al usuario que está en sesión.
c. Modificar los datos del usuario que se desea cambiar.
d. Actualizar los datos del usuario.

3.5.6 INGRESO Y ACTUALIZACIÓN DE UN DISPOSITIVO BIOMÉTRICO

El proceso de ingreso o actualización de un dispositivo biométrico se muestra en la siguiente Figura 3.12 y se describe a continuación.

a. Ingresar los siguientes datos: dirección IP, puerto y descripción.
b. Verificar que la IP asignada sea única en el sistema, si esta no está disponible mostrar el mensaje de error, caso contrario pasar al siguiente numeral.
c. Guardar los datos del dispositivo biométrico.

Para realizar la actualización del dispositivo se realiza el siguiente proceso.

a. Seleccionar el dispositivo biométrico que se desea actualizar.

b. Permitir modificar los siguientes datos: dirección IP, puerto y descripción.
c. Verificar si la IP a ser actualizada sea única en el sistema, si no lo es mostrar el mensaje de error caso contrario ir al siguiente punto.
d. Guardar los datos del dispositivo biométrico.

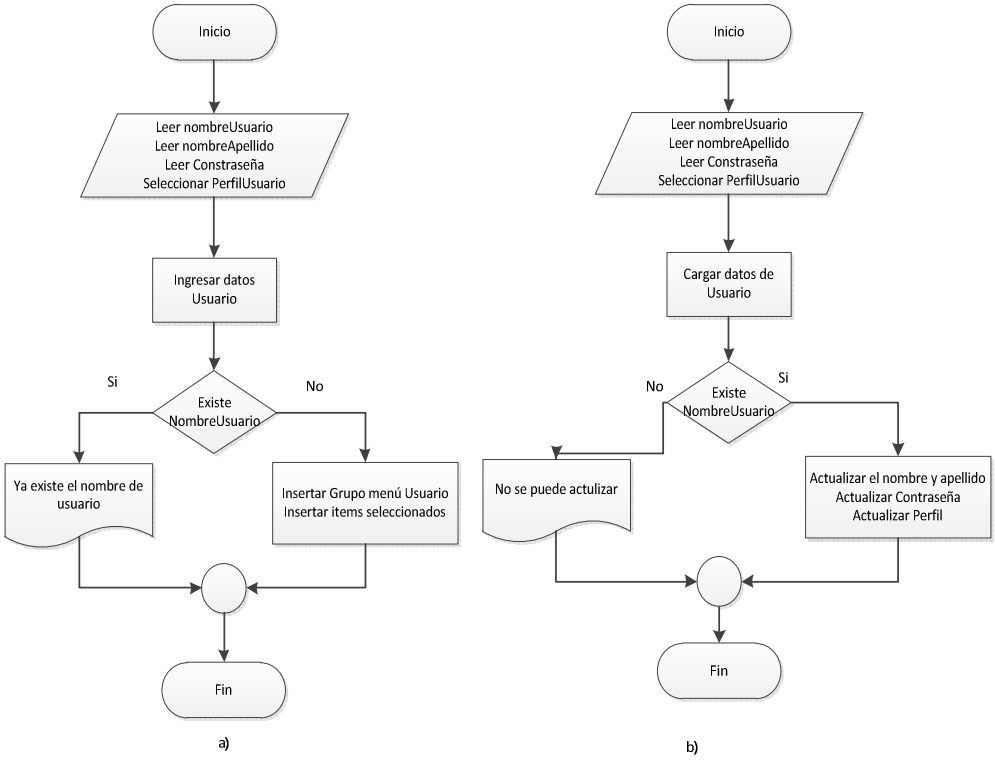

Figura 3.11. a) Ingreso de un nuevo usuario. b) Actualizar datos de usuario

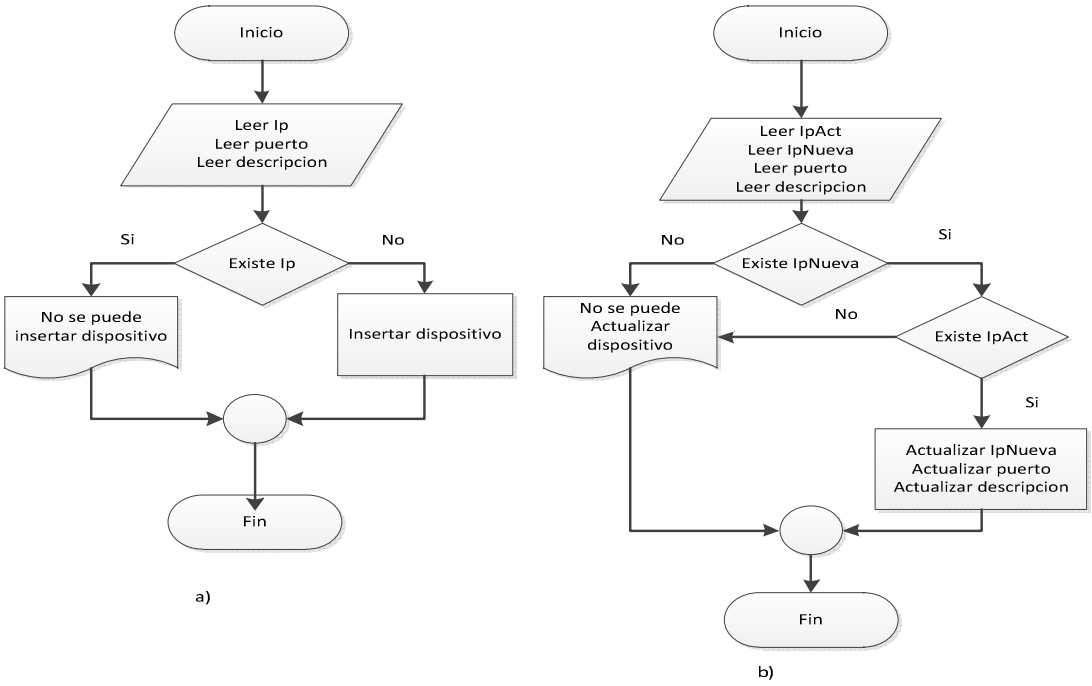

Figura 3.12. a) Ingreso de nuevo dispositivo. b) Actualización dispositivo

3.6 DIAGRAMAS DE SECUENCIA

Se procede a revisar, la secuencia de cada uno de los procesos que el usuario puede realizar, los cuales son:

- Ingreso de empleado.
- Ingreso de usuario.
- Creación de nuevo horario laborable.
- Registro de hora de empleado.

3.6.1 DIAGRAMA DE SECUENCIA DE INGRESO DE EMPLEADO

Este diagrama permite la visualización en el tiempo el ingreso de un nuevo empleado, considerando lo siguiente.

a. El usuario debe poseer en su rol o perfil, el permiso para agregar un nuevo empleado.
b. Seleccionar la opción de nuevo empleado e ingresar los datos solicitados.
c. Verificar que los datos del *Nick* y el documento del empleado, no estén ingresados en el sistema.
d. Si cumple con esta opción se procede con el ingreso del nuevo empleado.
e. Luego se procede a ingresar los datos biométricos del empleado, los que pueden ser: huella dactilar.

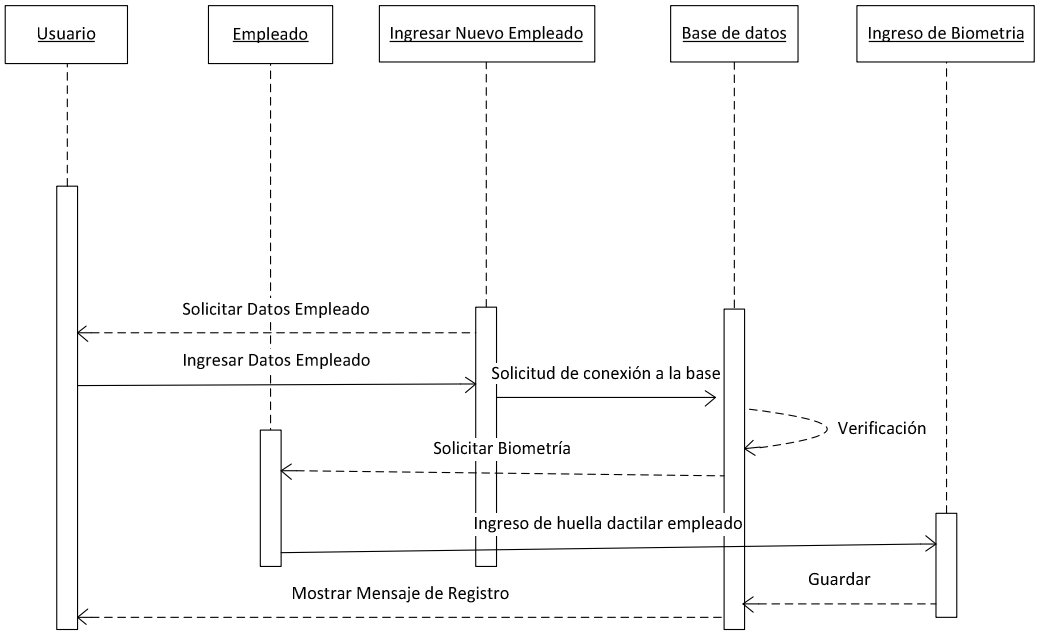

Figura 3.13. Diagrama de secuencia de ingreso de empleado

3.6.2 INGRESO DE USUARIO

Para realizar el registro de un nuevo usuario se realiza el siguiente proceso:

a. Solicitar el ingreso de los datos necesarios para el usuario.
b. Seleccionar el rol o grupo al que pertenecerá el usuario.
c. Validar el nombre de usuario, si no se repite en el sistema procede con el siguiente paso, caso contrario volver al paso inicial.
d. Proceder con el ingreso.
e. Mostrar el resultado del proceso.

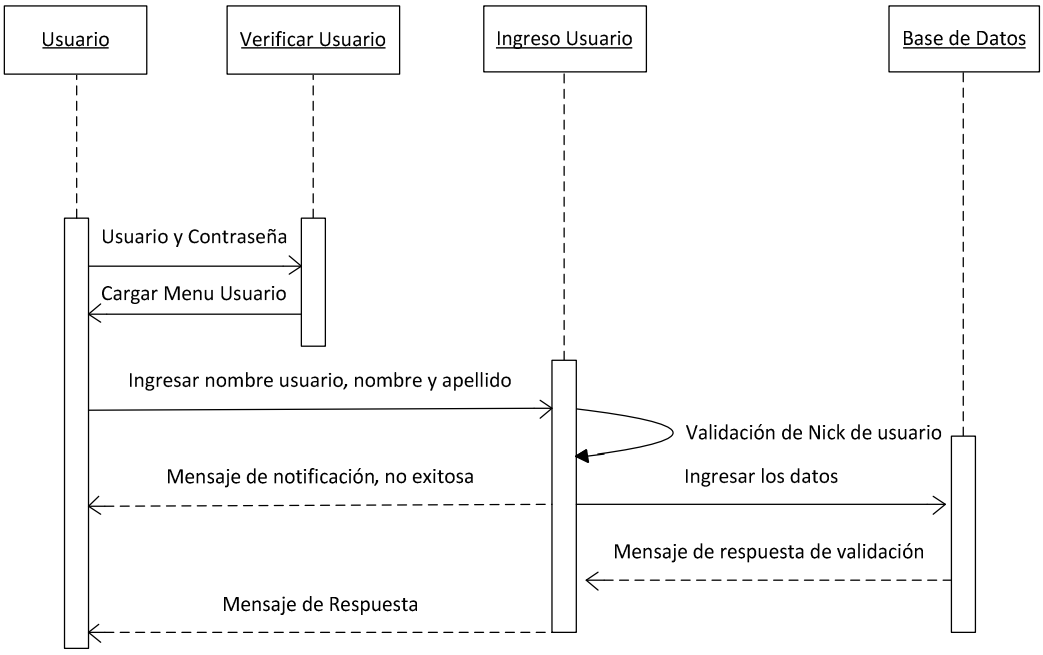

Figura 3.14. Secuencia de Ingreso de nuevo usuario

3.6.3 CREACIÓN DE UN ROL O GRUPO DE USUARIO

Para realizar la creación de un rol o grupo de usuario se procede de la siguiente manera.

a. Ingresar el nombre de grupo y una descripción
b. Seleccionar los ítems del menú que se desea que estén accesibles al grupo o rol.
c. Verificar el nombre del grupo, que no esté duplicado.
d. Si no está duplicado inserta el nombre del grupo.
e. Mostrar el resultado al usuario

Este proceso se encuentra representado en la Figura 3.15

3.6.4 CREACIÓN DE UN NUEVO HORARIO LABORABLE

A continuación se presenta el proceso para realizar la creación de un nuevo usuario, el cual se describe a continuación y está representado en la Figura 3.16.

a. Ingresar el nombre del nuevo horario.
b. Seleccionar el día e ingresar las respectivas horas como son la hora de entrada, hora de salida, hora de salida almuerzo y hora entrada almuerzo.
c. Verificar las horas ingresadas con las horas almacenadas correspondientes al día y al grupo de horario, para que no se crucen.
d. Ingresar los horarios y mostrar el resultado.

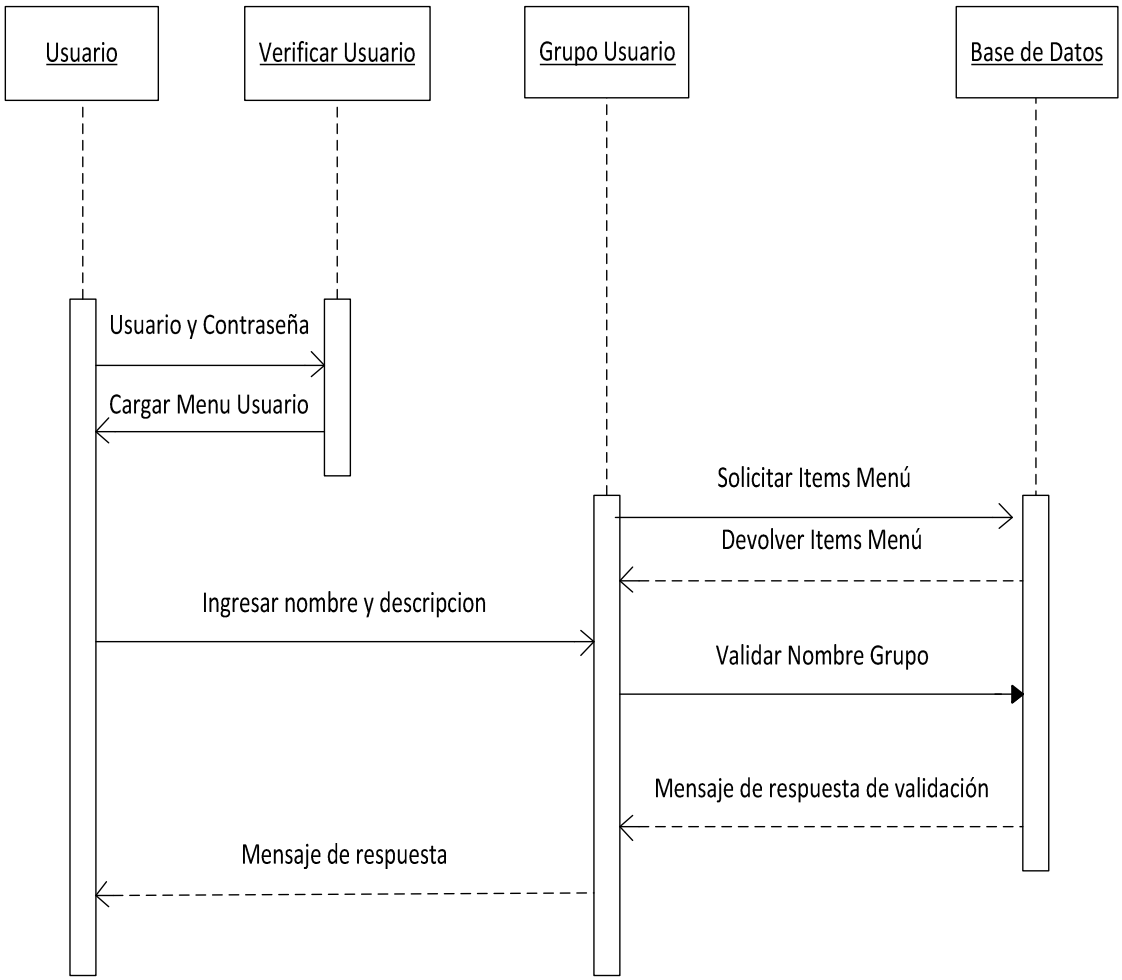

Figura 3.15. Creación de un rol de usuario

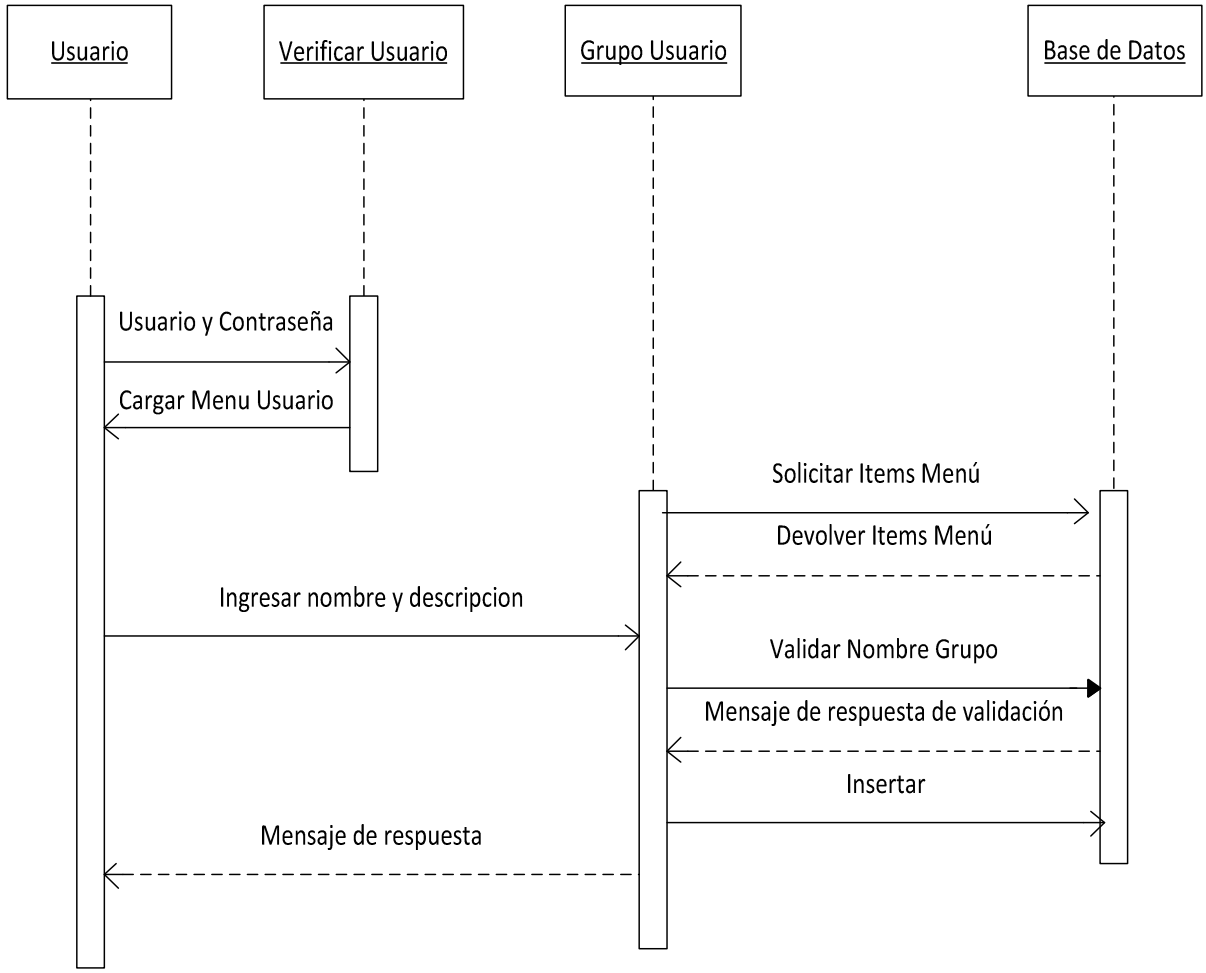

Figura 3.16. Ingreso de nuevo horario laborable

3.6.5 REGISTRO DE HORA DE EMPLEADO

Para realizar el registro de empleado el programa servidor recibe una trama de longitud variable de la aplicación cliente y debe de realizar el siguiente proceso de verificación y procesamiento de información el cual se muestra en la Figura 3.17.

a. Decodificar la información que recibe.
b. Descomponer la trama.
c. Verificar el tipo de autenticación.
d. Realizar la comparación con los datos almacenados en el sistema.
e. Realizar el registro, dependiendo de la respuesta de autenticación.
f. Construir la trama de respuesta.
g. Codificar la información y enviar.

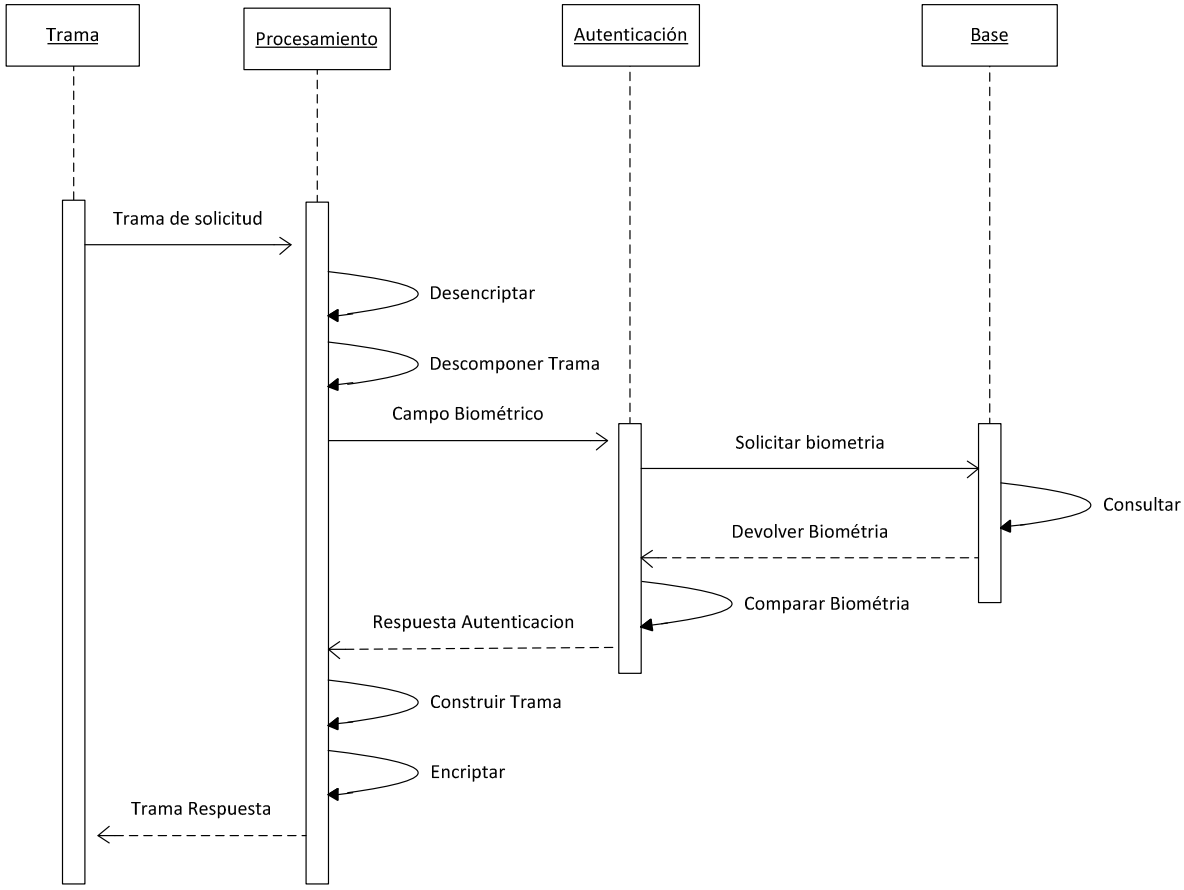

Figura 3.17. Registro de hora de empleado

3.7 DISEÑO DE LA BASE DE DATOS

La base de datos debe almacenar la siguiente información: datos de empleados, registros de timbrados, horarios laborables, usuarios del sistema, datos biométricos de los empleados como son huella dactilar o nombre de empleado y contraseña.

Se ha seleccionado la base de datos Microsoft SQL Server 2008 Express ya que esta versión de base de datos es de licencia gratuita, por ser una versión libre tienen restricciones de funciones para su uso como: recuperación en línea, replicación de datos, almacenamiento máximo de 4GB. Pero esto no afecta en la funcionalidad del sistema que se esta desarrollando.

3.7.1 MODELO DE BASE DE DATOS

A continuación se va a presentar el modelo de la base de datos implementado, el cual posee las tablas para almacenar la información necesaria de las clases descritas en el modelo de clases.

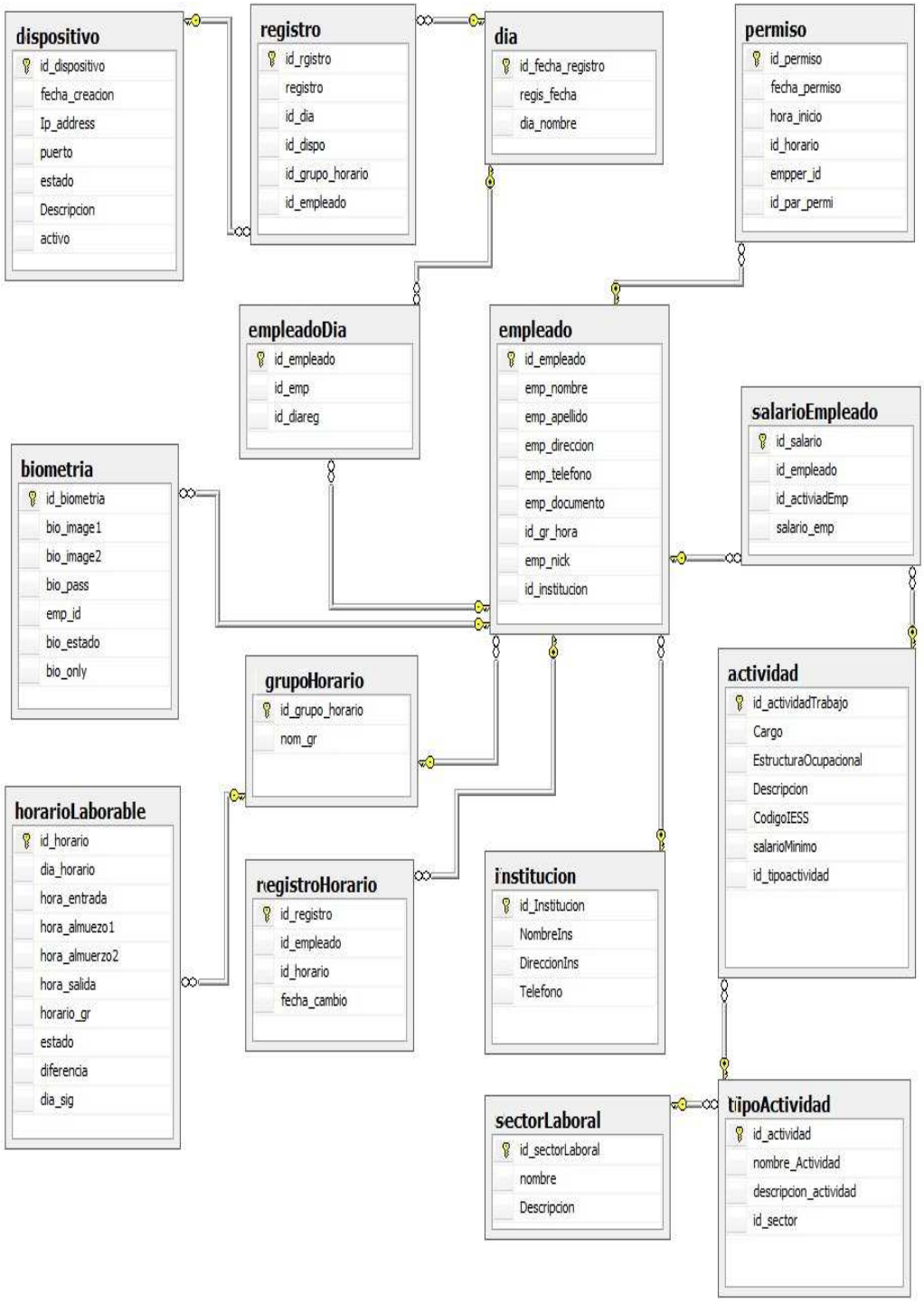

Figura 3.18. Modelo físico de la base de datos del sistema biométrico

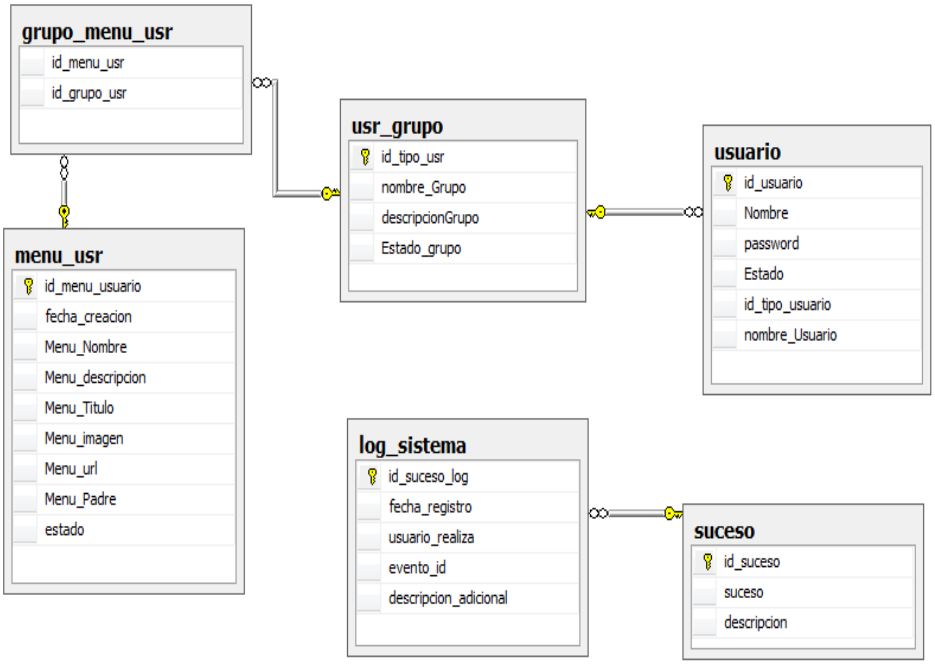

Figura 3.19. Modelo físico de datos de administración de usuarios

3.7.2 DICCIONARIO DE DATOS

A continuación se va a describir los atributos y los tipos de datos, que pertenecen a las más importantes Tablas, para el funcionamiento del sistema biométrico.

En la tabla empleado almacena la información que posee el empleado. Sus datos a almacenar se describen en la tabla 3.18.

La tabla biometría almacena la información para realizar la identificación del empleado mediante la comparación de los datos, en esta tabla se encuentra la huella dactilar y la contraseña del empleado. A continuación se presenta la descripción de los elementos en la Tabla 3.19.

En la Tabla 3.20 permiso, almacena la fecha, identificador del empleado y hace referencia a la descripción del permiso que solicito el empleado.

La tabla horario laborable, representa las horas almacenadas que puede tener un empleado, y la relación entre el empleado y los horarios se los hace mediante la tabla grupo horario y está representado en la Tabla 3.21.

Nombre Tabla	Empleado		
Atributo	**Tipo de Dato**	**Descripción**	**Permitir valores Nulos**
Id empleado	Int, auto numérico	Clave principal de la Tabla.	NO
Emp Nombre	Varchar(50)	Nombres del empleado	NO
Emp Apellido	Varchar(50)	Apellidos del empleado	NO
Emp Dirección	Varchar(50)	Dirección domiciliaria	SI
Emp Teléfono	Varchar(50)	Teléfono o número de celular del empleado	SI
Emp Documento	Varchar(13)	Número de cedula o ruc del empleado	NO
Id gr hora	Int	Grupo de horario laborable al que pertenece el empleado.	NO
Emp Nick	Varchar(50)	Nombre del empelado o sobre nombre	NO
Id Institución	Int	Identificación de la institución a la que pertenece el empleado	NO

Tabla 3.18. Tabla empleado

Nombre Tabla	Biometría		
Atributo	**Tipo de Dato**	**Descripción**	**Permitir valores Nulos**
Id biometría	Int	Identificador y clave principal de la Tabla.	NO
Bio imagen 1	Varchar(2000)	Almacenamiento de las minucias.	SI
Bio imagen 2	Varchar(2000)	Almacenamiento de las Minucias.	SI

Tabla 3.19. Tabla biometría (continúa)

Biopass	Varchar(100)	Contraseña del empleado encriptado.	SI
Emp id	Int	Identificado del empelado	NO
Bio estado	bit	Estado habilitado de los datos biométricos.	SI
Bioonly	Bit	Estado a solo huella dactilar.	SI

Tabla 3.19. Tabla biometría

Nombre Tabla	**Permiso**		
Atributo	**Tipo de Dato**	**Descripción**	**Permitir valores Nulos**
Id Permiso	Int, auto numérico	Identificador y clave principal de la Tabla.	NO
Fecha permiso	Date	Fecha de realización del permiso.	NO
Hora inicio	Time	Hora del permiso.	NO
id horario	Int	Grupo perteneciente al horario laborable.	NO
Emple id	Int	Identificador del empleado.	NO
Id par permiso	Int	Identificador de la siguiente hora fin del permiso.	NO

Tabla 3.20. Tabla permiso

La tabla registro, almacena las horas en que el empleado ha realizado la autenticación exitosa, los elementos de esta tabla están representados en la Tabla 3.22.

La tabla dispositivos permite llevar un registro de las aplicaciones biométricas permitidas para realizar el registro del empleado. Los elementos de esta tabla están enumerados en la Tabla 3.23.

Nombre Tabla	Horario Laborable		
Atributo	**Tipo de Dato**	**Descripción**	**Permitir valores Nulos**
Id horario	Int, auto numérico	Identificador y clave principal de la Tabla.	NO
Día horario	Date	Nombre del día laborable.	NO
Hora entrada	Time	Hora de ingreso.	NO
Hora almuerzo1	Time	Hora salida almuerzo.	NO
Hora almuerzo2	Time	Hora entrada almuerzo.	NO
Hora salida	Time	Hora salida.	NO
Horario gr	Int	Grupo de horario laborable.	NO
Estado	Bit	Estado de horario.	NO
Diferencia	Time	Diferencia entre hora entrada, salida y horas de almuerzo.	NO

Tabla 3.21. Tabla horario laborable

Nombre Tabla	Registro		
Atributo	**Tipo de Dato**	**Descripción**	**Permitir valores Nulos**
Id registro	Int, auto numérico	Identificador y clave principal de la Tabla.	NO
Registro	Time	Hora de realización de registro.	NO
Id día	Int	Identificador de la Tabla día.	NO
Id dispositivo	Int	Identificador del dispositivo que realizó el registro.	NO
Id grupo horario	Int	Identificador del horario laborable del empleado.	NO
Id empleado	Int	Identificador del empleado.	NO

Tabla 3.22. Tabla registro

Nombre Tabla	Dispositivo		
Atributo	**Tipo de Dato**	**Descripción**	**Permitir valores Nulos**
Id dispositivo	Int, auto numérico	Identificador y clave principal de la Tabla.	NO
Fecha creación	Date	Fecha de ingreso de dispositivo.	NO
IP address	Varchar(15)	Dirección IP del dispositivo.	NO
Puerto	Int	Número de puerto de comunicación entre el dispositivo biométrico.	NO
Estado	Varchar(10)	Estado de comunicación del dispositivo.	NO
Descripción	Varchar(50)	Lugar donde se encuentra el dispositivo	NO
Activo	Varchar(3)	Estado activo o inactivo del dispositivo	NO

Tabla 3.23. Tabla dispositivo

Tabla usuario, almacena los datos del usuario para acceder al sistema. Los elementos están representados en la Tabla 3.24.

Nombre Tabla	Usuario		
Atributo	**Tipo de Dato**	**Descripción**	**valores Nulos**
Id usuario	Int, auto numérico	Identificador y clave principal de la Tabla	NO
Nombre	Varchar(20)	Nombre usuario *nick*	NO
Password	Varchar(100)	Contraseña del usuario	NO
Estado	Bit	Estado del usuario	NO
Id tipo usuario	Int	Identificador del grupo de perfil de usuario	NO
Nombre usuario	Varchar(100)	Nombre y apellido del usuario	NO

Tabla 3.24. Tabla usuario

La Tabla 3.25 menú usuario, almacena la información de los menús que posee el sistema biométrico, para que los menús puedan ser administrados mediante la aplicación desarrollada; se ha utilizado la jerarquía de menús para distinguir el menú raíz o padre de sus menús hijos.

Nombre Tabla	**Menú usr**		
Atributo	**Tipo de Dato**	**Descripción**	**Permitir valores Nulos**
Id menú usuario	Int	Identificador de la Tabla menú, y calve principal	NO
Fecha creación	Date	Fecha de creación del menú	NO
Menú nombre	Varchar(50)	Nombre del menú si es principal o secundario.	NO
Menú descripción	Varchar(50)	Descripción de utilización del menú.	Si
Menú titulo	Varchar(50)	Título del menú	NO
Menú imagen	Varchar(50)	Dirección donde se encuentra almacenada, la imagen para mostrar.	Si
Menú URL	Varchar(50)	Dirección del menú actual.	Si
Menú padre	Int	Identificador del menú padre al que pertenece el menú.	Si
Estado	Bit	Estado del menú.	SI

Tabla 3.25. Tabla menú usuario

3.8 IMPLEMENTACIÓN CLIENTE - SERVIDOR

Para realizar estas aplicaciones se presentan las clases utilizadas para el servicio biométrico de autenticación. Describiendo sus atributos y métodos utilizados en las aplicaciones servidor biométrico y cliente, mostrada en la Figura 3.20. Mediante la utilización de comunicación por sockets, entre el cliente y servidor.

Además se utiliza la tecnología llamada servicio web[17], la cual es utilizada para realizar el intercambio de datos entre la aplicación administrador biométrico y el servidor biométrico.

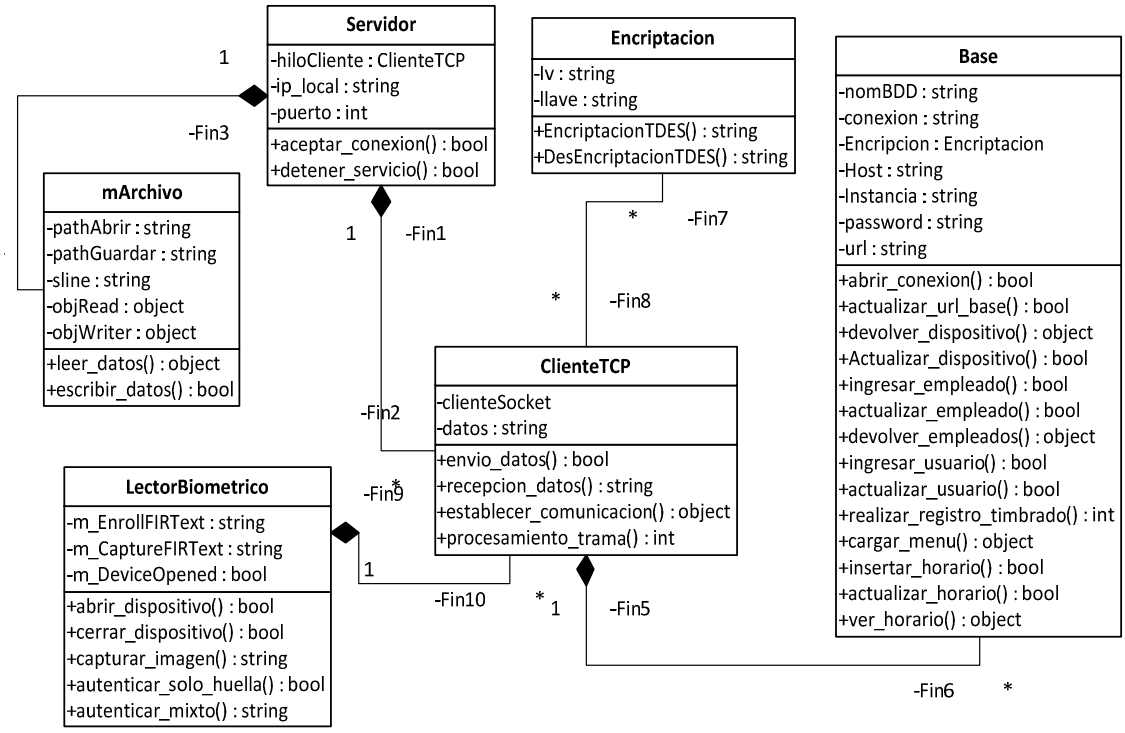

Figura 3.20. Implementación de la aplicación cliente y servidor

3.8.1 DICCIONARIO DE CLASES

A continuación se detallan las clases utilizadas, con su respectiva descripción de los objetos utilizados mostrados en las siguientes tablas.

Clase Servidor	Utilizado para procesar las peticiones de la aplicación cliente, mediante la escucha de solicitudes por un puerto especificado.
Atributos	
hiloCliente	Es un cliente TCP, el cual se encarga del procesamiento y respuesta de las solicitudes de los clientes biométricos.

Tabla 3.26. Clase servidor (continúa)

[17] Servicio web (en inglés, *Web services*) es una tecnología que utiliza un conjunto de protocolos y estándares que sirven para intercambiar datos entre aplicaciones.

Ip_local	Dirección IP local del servidor de autenticación, utilizado para atender las peticiones de los clientes biométricos por una cierta interfaz de red.
Puerto.	Número de puerto, por la que el servidor, va a atender las peticiones de los clientes biométricos.
Métodos	
Aceptar_conexion.	Inicia el servicio y escucha las peticiones, por el puerto y la dirección IP designado.
Detener_servicio	Detiene el servicio de escucha, para la autenticación.

Tabla 3.26. Clase servidor

Clase Base	Utilizado para realizar, llamadas a procedimientos almacenados y manejo de conexión a la base de datos.
Atributos	
nombreBDD.	Nombre de la base de datos, a la que se desea acceder.
Conexión	Objeto de conexión de SQL Server.
Encripción	Clase para decodificar la contraseña.
Host	Dirección IP del servidor de base de datos.
Usuario	Nombre de usuario, para acceder a la base de datos.
Instancia	Nombre de la instancia que posee la base de datos.
Password	Contraseña del usuario de la base de datos.
URL	*Cadena de caracteres de* conexión de la base de datos, constituida por el nombre de la base de datos, dirección IP de la base de datos, nombre de usuario y contraseña.
Métodos	
Abrir_conexion	Método utilizado para establecer la conexión a la base de datos.

Tabla 3.27. Clase conexión Base de datos (continúa)

Actualizar_url_base	Actualiza la URL de la base de datos.
Devolver_dispositivo	Devuelve los datos del objeto dispositivo.
Actualizar_dispositivo	Actualiza los datos del dispositivo, mediante la validación de la dirección IP, almacenada en el sistema.
Ingresar_empleado	Ingresa un nuevo empleado, mediante la validación del nombre del empleado y el documento.
Actualizar_empleado	Actualiza los datos del empleado.
Devolver_empleados	Retorna todos los datos de los empleados, registrados en el sistema.
Ingresar_usuario.	Inserta los datos de un nuevo usuario, mediante la validación del nombre de usuario.
Actualizar_usuario	Actualiza los datos del usuario del sistema.
Realizar_registro_timbrado.	Realiza el registro de horas del empleado, mediante la comparación de los datos biométricos.
Cargar_menu	Carga el menú correspondiente al perfil de usuario.
Insertar_horario	Inserta los horarios laborables del empleado.
Actualizar_horario	Actualiza los horarios laborables del empleado.
Ver_horario	Muestra los horarios, que posee el sistema biométrico.

Tabla 3.27. Clase conexión Base de datos

Clase Lector Biométrico	Utilizado para visualizar los datos del lector biométrico, que el sistema administra.
Atributos	
m_enrolFIRText.	Almacena los valores de las huellas de los empleados para realizar la autenticación mediante la comparación.
m_captureFIRText	Almacena los datos de la huella del empleado, para realizar la autenticación.
m_DeviceOpened	Muestra el estado de conexión del lector de huella.

Tabla 3.28. Lector Biométrico (continúa)

Métodos	
Abrir_dispositivo.	Establece la comunicación con el dispositivo biométrico.
Cerrar_dispositivo	Cierra la comunicación con el dispositivo biométrico.
Capturar_imagen	Realiza la captura de la huella dactilar del empleado.
Autenticar_solo_huella	Realiza la autenticación del empleado mediante la huella dactilar, y las compara con cada una de las huellas almacenadas en el sistema.
Autenticar_mixto	Realiza la autenticación del empleado mediante la huella dactilar y el nombre de usuario y contraseña.

Tabla 3.28. Lector Biométrico

3.8.2 DIAGRAMA DE FLUJO PARA EL PROCESO DE SOLICITUDES DE AUTENTICACIÓN

Para realizar el proceso de autenticación de lectura biométrica, el servidor debe estar escuchando por un puerto estático seleccionado, de preferencia mayor a 1024, ya que por el puerto configurado al momento de recibir una petición creará un hilo de ejecución, el cual realizará el procesamiento de la solicitud y enviará la respuesta de solicitud al cliente biométrico. Este proceso se lo representa en la Figura 3.21.

3.8.3 DIAGRAMA DE SECUENCIA PARA LA AUTENTICACIÓN DE EMPLEADO

En la Figura 3.22 se presenta el modelo de secuencia de comunicación entre el cliente y el servidor, para realizar la autenticación del empleado y registro de horas, el empleado envía una solicitud de registro con sus datos biométricos al servidor este crea un hilo de ejecución y procesa los datos recibidos para luego enviar una respuesta de aceptación o rechazo al registro.

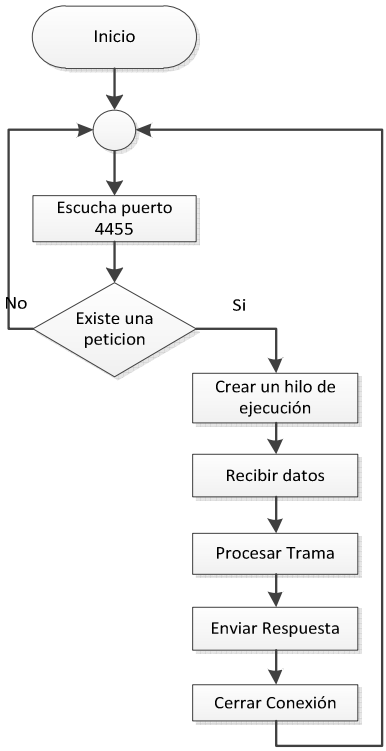

Figura 3.21. Diagrama de flujo para receptar la solicitud de los clientes

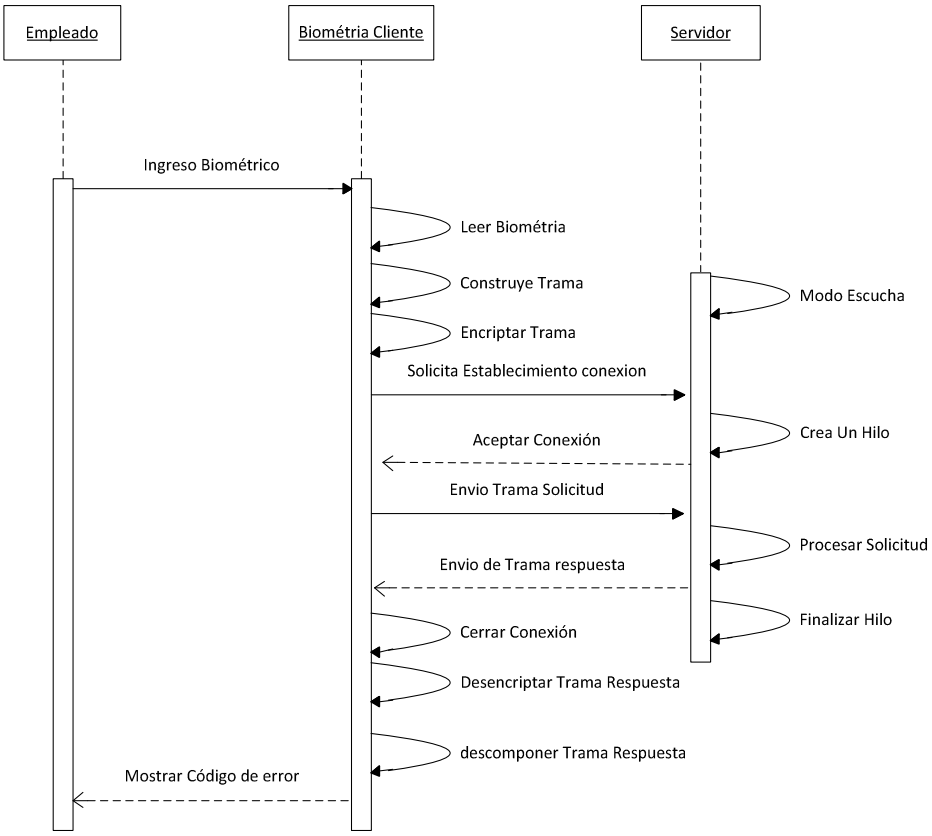

Figura 3.22. Autenticación entre el cliente y el servidor

3.9 INTERFACES GRÁFICAS

En esta sección se presentan, las interfaces gráficas diseñadas como son: administración del sistema, cliente biométrico y servidor de autenticación.

A continuación se presenta el diseño y las funciones que realiza cada una de estas interfaces gráficas empezando por la interfaz de administración del sistema.

3.9.1 INTERFAZ GRÁFICA DE ADMINISTRACIÓN EMPLEADOS

Esta interfaz permite realizar la administración de sistema biométrico, como son creación y modificación de empleados, usuarios, horarios laborables, perfiles y dispositivos biométricos.

3.9.1.1 Acceso al sistema

Esta interfaz es utilizada, para realizar la validación de usuario y está representada en la Figura 3.23. El usuario ingresara el nombre de usuario y la contraseña para validar sus datos, si esta validación es exitosa se cargará el menú correspondiente al perfil que posee el usuario. Caso contrario se muestra el mensaje de error correspondiente.

Figura 3.23. Interfaz para realizar el inicio de sesión

3.9.1.2 Menú usuario

Permite realizar la administración de usuario, mediante la selección de opciones de creación de usuario y perfil.

3.9.1.2.1 Sub menú nuevo usuario

Permite realizar el ingreso de un nuevo usuario al sistema, como se observa en la Figura 3.24, los datos que se deben ingresar son los siguientes: Nombre de usuario, contraseña, Nick de usuario y el perfil al que va a pertenecer.

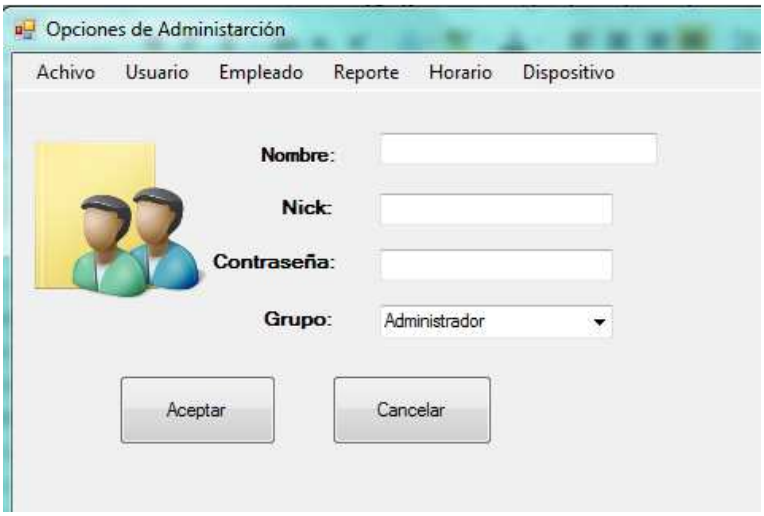

Figura 3.24. Ingreso de un nuevo usuario

3.9.1.2.2 Sub menú actualizar usuario

Permite realizar: el reseteo de contraseña, actualización de perfil y bloqueo de usuario para acceder al sistema. Esta interfaz está representada en la Figura 3.25.

Figura 3.25. Sub-Menú Actualizar Usuario

3.9.1.2.3 Sub menú crear nuevo grupo o rol de usuario

Permite realizar la creación de un nuevo grupo de acceso, para administrar el sistema. La cual se muestra en la Figura 3.26.

3.9.1.2.4 Sub menú actualización de grupo de usuario

Permite realizar la modificación y elección de submenú de grupo de usuario. Estas opciones son activadas con un cuadro seleccionador. La cual esta mostrada en la Figura 3.27, estos valores cambian dependiendo del perfil seleccionado.

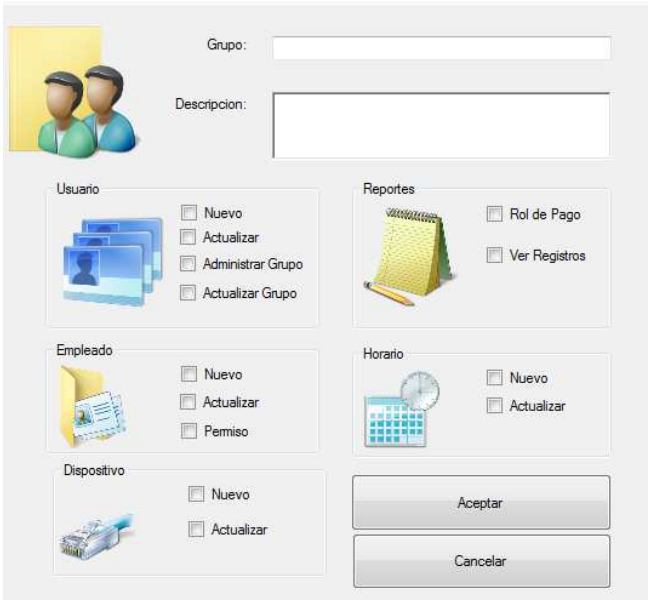

Figura 3.26. Crear un nuevo grupo de acceso

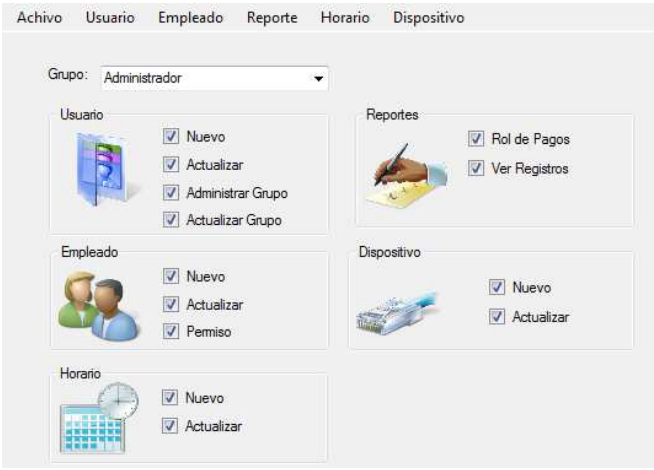

Figura 3.27. Actualización de grupo de usuario

3.9.1.3 Menú empleado

Permite realizar la administración de los empleados, mediante la creación y actualización de los datos del empleado y sus datos biométricos.

3.9.1.3.1 Sub menú nuevo empleado

Permite realizar el ingreso de un nuevo empleado al sistema y el registro biométrico de éste. El registro biométrico puede realizarse, mediante la utilización del lector biométrico o solamente por el nombre de usuario y contraseña.

Los campos requeridos para el ingreso del empleado son el nombre del empleado *(Nick)*, el número de documento, nombre y apellido, cargo y salario, estos datos se los presenta Figura 3.28.

3.9.1.3.2 Sub menú actualizar datos de empleado

Permite realizar la actualización de los datos del empleado. Para seleccionar un empleado se puede buscar mediante el siguiente filtro: número de documento o por el nombre y apellido del empleado. Esta opción está representada en la Figura 3.29.

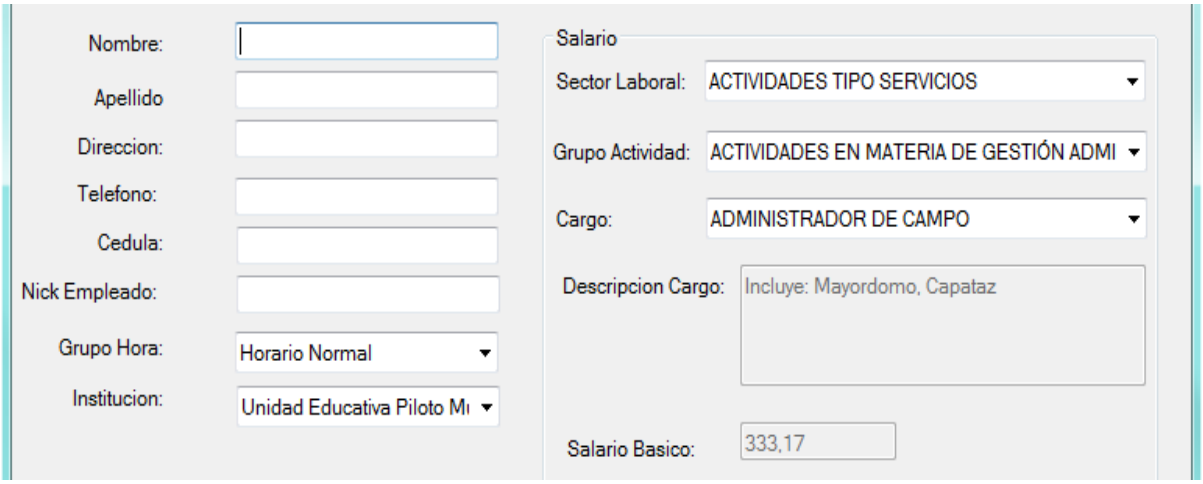

Figura 3.28. Ingreso de un nuevo empleado

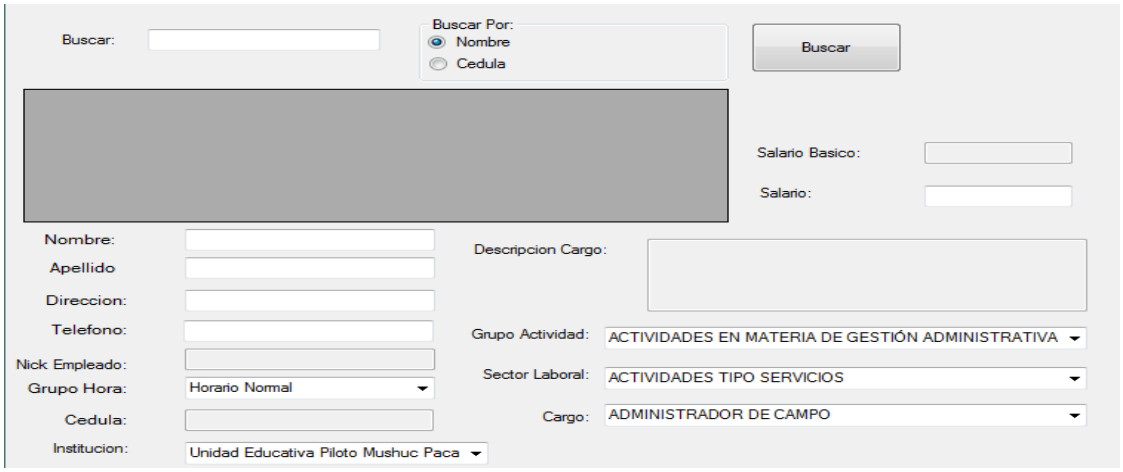

Figura 3.29. Actualización de los datos del empleado

3.9.1.3.3 Sub menú administración de permisos

Permite realizar el ingreso de: permisos, vacaciones o comisiones. Para realizar el registro hay las siguientes opciones:

1. Registrar a un solo empleado.
2. Registrar a todos los empleados que están en el sistema.
3. Seleccionar el rango de permiso por día, rango de fechas y las horas en que solicita el permiso.

Para realizar el registro el sistema compara la fecha de ingreso con el horario laborable que posee el empleado, si existe algún error se muestra en un cuadro de texto el error este mensaje, esta interfaz se muestra en la Figura 3.30.

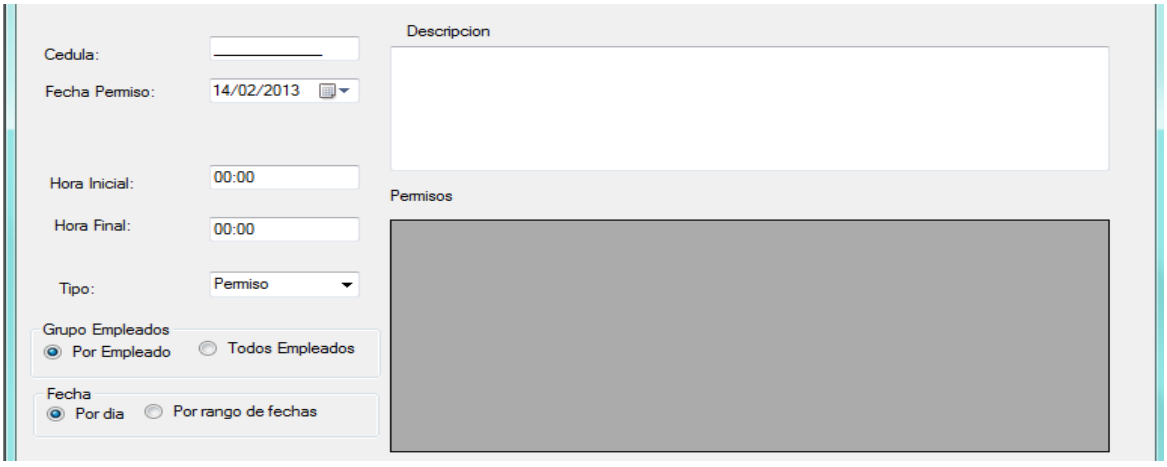

Figura 3.30. Administración de permisos

3.9.1.4 Menú ver reporte

Permite ver los reportes de los días en que el empleado ha registrado su huella dactilar, o los cambios realizados que el usuario ha realizado en el sistema este reporte puede ser generado por el usuario registrado en el sistema, mediante la mediante la selección de rangos de fechas.

3.9.1.4.1 Sub menú registros de ingresos

Presenta los días y las horas en que el empleado se ha registrado en la Figura 3.31. En este reporte interviene el módulo de compensación de horas. Si un empleado ha llegado tarde y ha salido después de las horas de trabajo, se compensan estas horas, con la finalidad de cumplir la jornada de trabajo establecida en el sistema.

Figura 3.31. Reporte de registro de empleado

3.9.1.4.2 Sub menú entrada salida

Muestra las horas inicial y final en que el empleado ha sido registrado, en este reporte no realiza ningún cálculo de horas. Solamente saca el registro de horas mínimo y máximo. En este reporte se puede visualizar por empleados, día, mes.

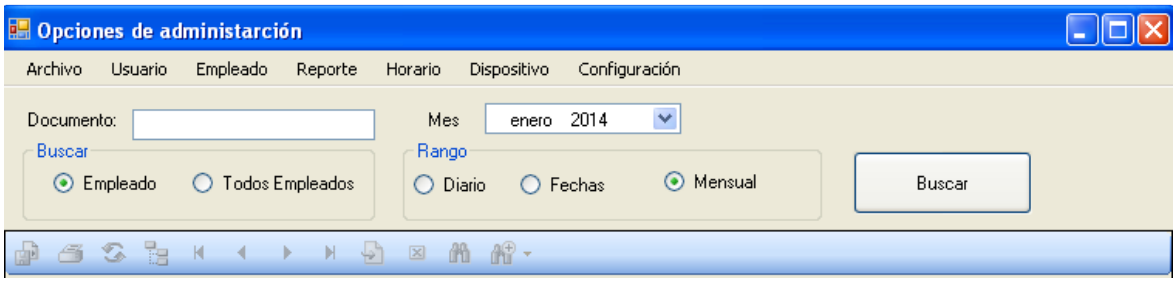

Figura 3.32. Reporte de Sub menú entrada y salida

3.9.1.4.3 Sub menú ver empleados registrados

En la Figura 3.33, se muestra todos los empleados registrados en el sistema, con los siguientes datos, número de cédula, nombres y apellidos, cargo, fecha de registro y el usuario que realizó el registro el empleado.

Figura 3.33. Reporte de empleados registrados en el sistema

3.9.1.4.4 Sub menú eventos del sistema

La Figura 3.34, se muestra los eventos que el usuario realiza en el sistema, mediante el registro de los cambios que el usuario puede realizar en el sistema tales como ingreso actualización de datos de empleado, creación de grupo, creación de horarios, etc.

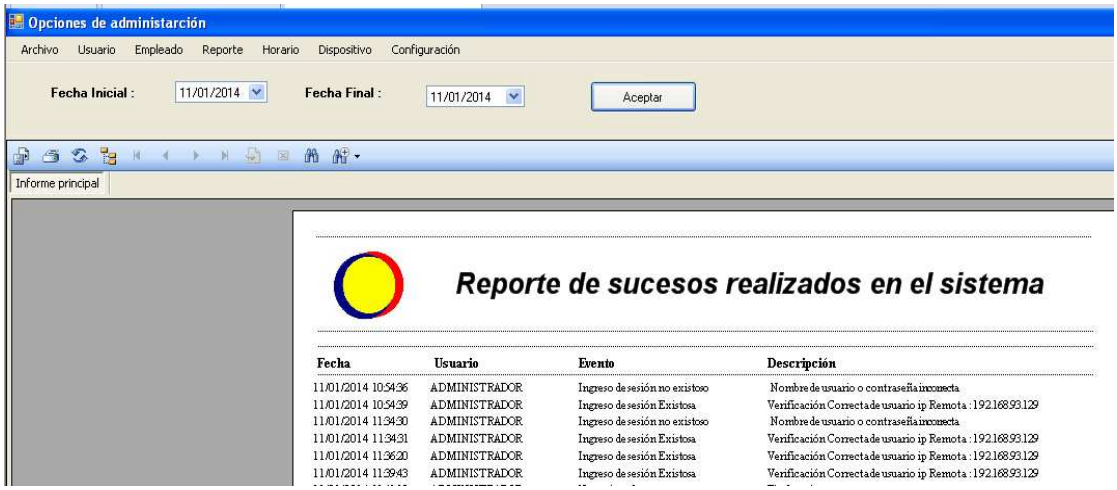

Figura 3.34. Reporte de eventos del sistema

3.9.1.5 Menú horario

Permite realizar la administración de los horarios laborables para los empleados.

3.9.1.5.1 Sub menú nuevo horario

Permite realizar la creación de un nuevo horario de trabajo para los empleados, mediante el ingreso de horas de los empleados con su respectivo día, la cual está representada en la Figura 3.35, en este módulo al momento de ingresar las horas, el sistema debe verificar que no se crucen las horas ingresadas con otras ingresadas anteriormente y que pertenezca al mismo grupo y al mismo día.

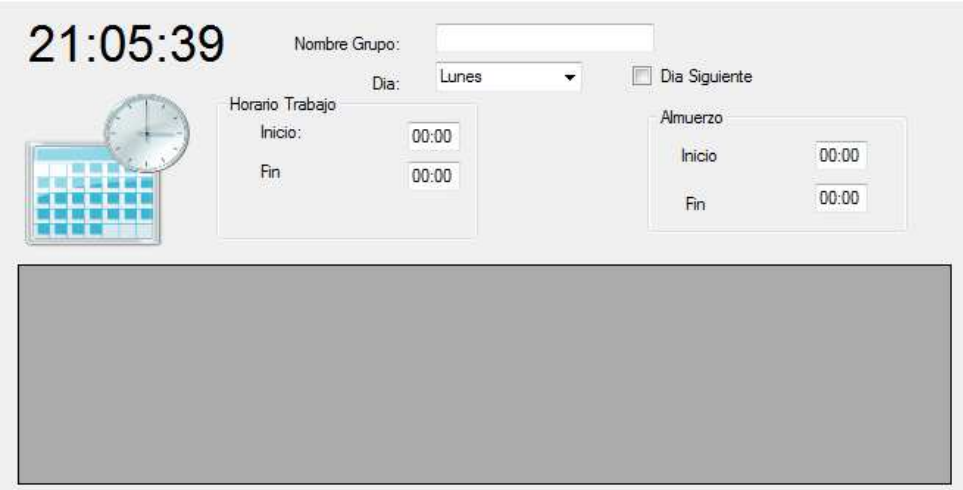

Figura 3.35. Creación de un nuevo horario

3.9.1.5.2 Actualizar horario

Permite realizar la actualización de los horarios laborables, mediante la adición o eliminación de los horarios de los empleados. Esta interfaz está representada en la Figura 3.36.

En este módulo al momento de ingresar o actualizar las horas debe verificar que las horas, no se crucen con otras horas ingresadas anteriormente correspondientes al mismo grupo y al mismo día.

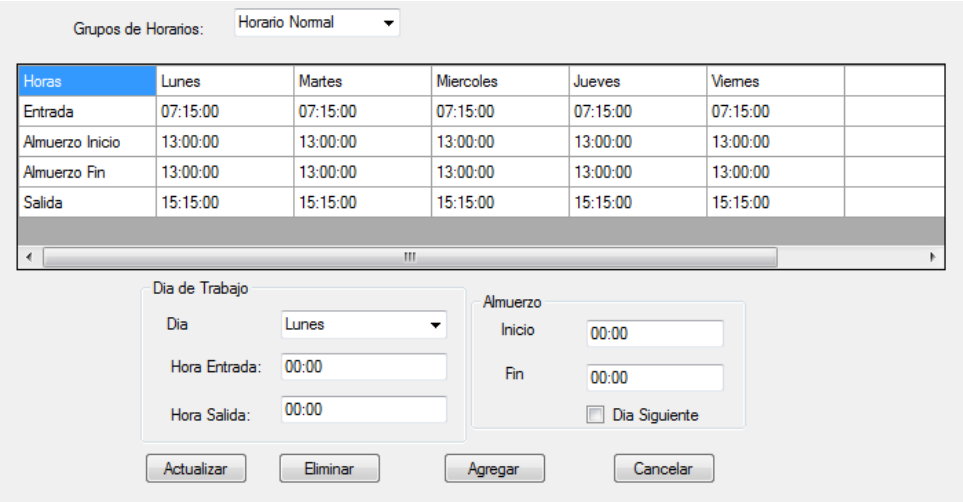

Figura 3.36. Actualización de un horario laborable

3.9.1.6 Menú dispositivo

Permite realizar la administración de los dispositivos biométricos que están conectados al servidor para realizar la autenticación del empleado.

3.9.1.6.1 Nuevo cliente biométrico

La interfaz gráfica está representada en la Figura 3.37 y permite la creación de nuevo un nuevo dispositivo biométrico asignando un código numérico de identificación de dispositivo al momento de realizar el ingreso. Al momento de realizar la creación, el sistema valida que esa dirección IP asignada al dispositivo no esté almacenada anteriormente en el sistema. Los datos a ingresar son: dirección IP, el número de puerto y la descripción del equipo.

Figura 3.37. Ingreso de un cliente biométrico

3.9.1.6.2 Actualizar dispositivo

Realiza la actualización de los datos del dispositivo biométrico, tales como dirección IP, número de puerto y descripción. Para realizar la actualización de la dirección IP el sistema validará la nueva dirección que no esté almacenada en el sistema y esta mostrado en la Figura 3.38.

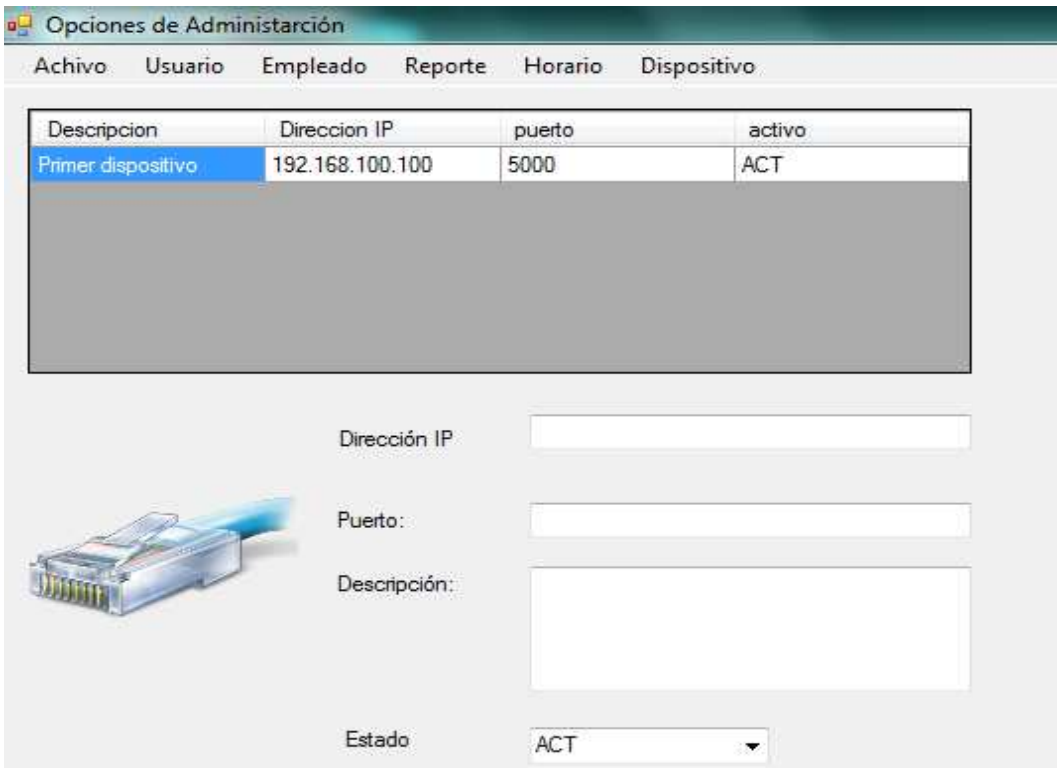

Figura 3.38. Actualización del dispositivo biométrico

3.9.1.7 Menú configuración

Permite administrar los cargos que puede ocupar un empleado en la empresa o institución y los datos de la institución.

3.9.1.7.1 Configuración manual

Permite realizar el registro de la institución mediante la solicitud de nombre, dirección y teléfono, además permite realizar el ingreso o actualización de las actividades que puede ocupar el empleado mediante el ingreso del sector laboral, tipo de actividad y la actividad económica.

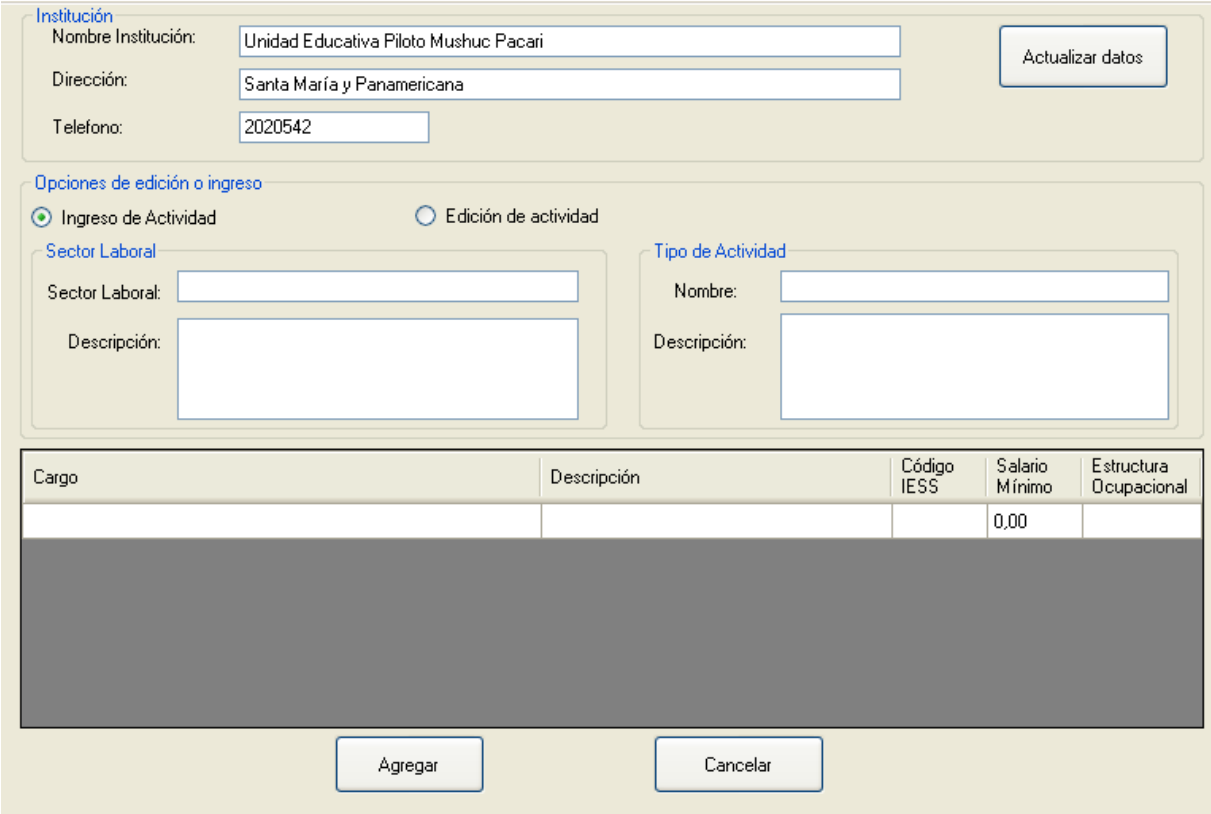

Figura 3.39. Sub menú configuración manual

3.9.2 INTERFAZ GRÁFICA DE CLIENTE BIOMÉTRICO

Envía el requerimiento de registro del empleado hacia el servidor de autenticación, mediante la captura de la huella dactilar o el ingreso de datos del empleado, esta opción está representada en la Figura 3.40.

Figura 3.40. Interfaz gráfica para realizar el registro de empleado

A continuacion se muestra los modos de operación utilizados para el proceso de autenticacion, el cual se presenta en la siguiente Figura 3.41.

Figura 3.41. Tipo de autenticación biométrica

3.9.3 INTERFAZ GRÁFICA DEL SERVIDOR DE AUTENTICACIÓN

A continuación se presenta la interfaz gráfica mostrada en la Figura 3.42, la cual muestra las operaciones de peticiones y respuesta de autenticación de los empleados. Además permite visualizar el estado de conexión de las aplicaciones biométrica, mostrada en la Figura 3.43.

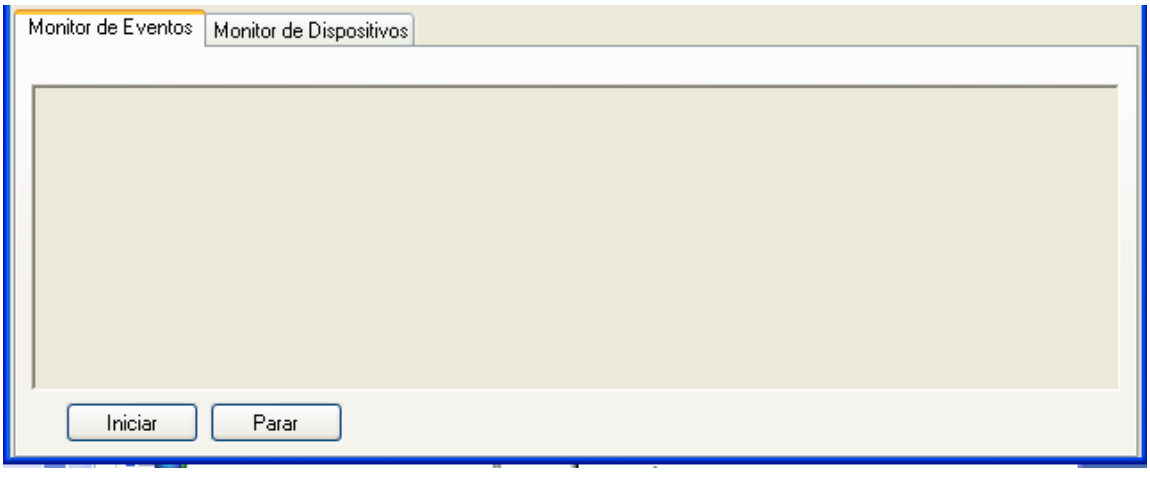

Figura 3.42. Monitor de eventos, para el servicio de autenticación

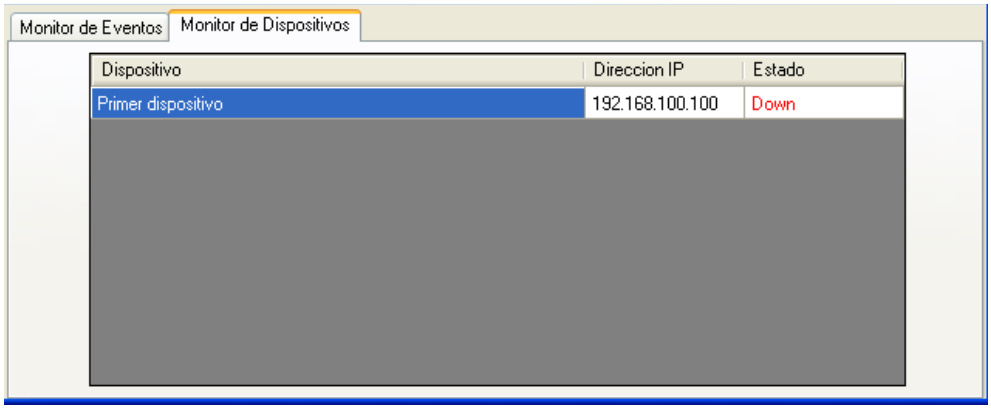

Figura 3.43. Monitor del canal para dispositivos

Finalmente para realizar la configuración de este servicio, se presenta la Figura 3.44, los parámetros de ingreso, los cuales son los siguientes ítems: puerto del servicio, Dirección IP del servicio de autenticación, Dirección IP del servidor de Base de datos, nombre de usuario y contraseña para acceder a la base.

Figura 3.44. Configuración del servicio de autenticación

CAPÍTULO 4
PRUEBAS, RESULTADOS Y COSTOS

En este capítulo se presenta la descripción de las pruebas unitarias realizadas del sistema biométrico mostrado en la Figura 4.1. Mediante la descripción de los siguientes elementos que interactúan.

- Descripción de etiquetas utilizadas en el sistema biométrico, para la identificación de los equipos.
- Descripción de pruebas funcionales, para verificar el funcionamiento de los métodos descritos en el capítulo tres, correspondiente a los casos de usos.
- Instalación de paquetes necesarios para el funcionamiento de las aplicaciones cliente, servidor y administrador de empleados.
- Configuración del servicio de autenticación y publicación del servicio web, el cual es utilizado para realizar el intercambio de información con la aplicación administrador, proceso descrito en el Anexo J.
- Configuración de la aplicación administrador de empleados y configuración del servicio de autenticación, proceso descrito en el Anexo K.

Además se presentan los resultados obtenidos en las pruebas realizadas para el servicio biométrico, modificaciones realizadas en la aplicación, características de hardware utilizado para albergar el sistema biométrico y costo total del sistema.

4.1 DESCRIPCIÓN DE ETIQUETAS DEL SISTEMA BIOMÉTRICO

Es necesario llevar un registro de etiquetas del sistema biométrico ya que cada uno realiza una tarea específica, ya sea para realizar la adquisición de la huella, realizar el proceso de identificación de empleado o administraran los datos, es por ello que a continuación se describen las etiquetas a ser utilizadas.

Servidor biométrico.- Este servidor alberga la lógica de negocio del sistema tanto para el servicio biométrico como para el administrador biométrico, es por esta razón que se ha asignado la ética *logicnet*.

Servidor Base de datos.- Utilizado para almacenar la información de los empleados y sus respectivos registros de entrada y salida, para identificar a este servidor se utiliza la etiqueta *dbnet.*

Para los clientes como el administrador de empleados y cliente biométrico, no se les asigna ninguna etiqueta debido a que estas aplicaciones deben conectarse al servidor *logicnet.*

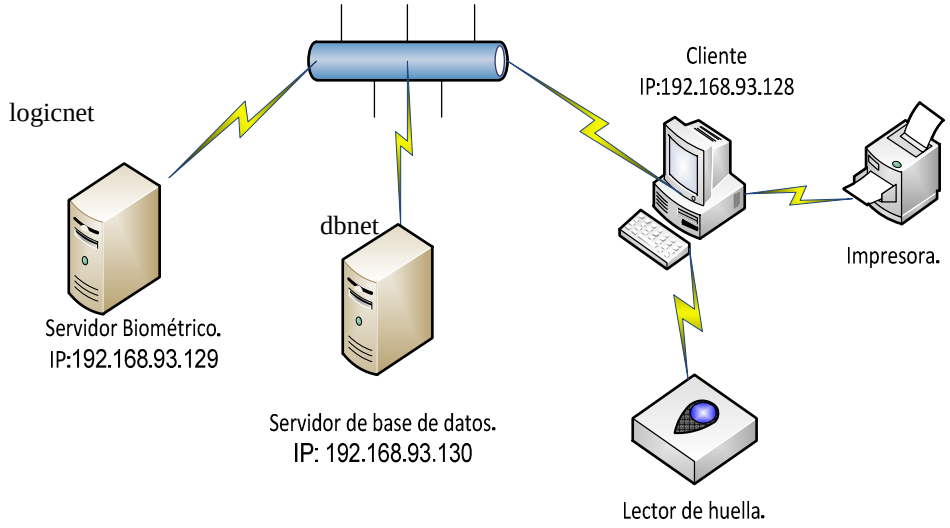

Figura 4.1. Elementos de red del servicio biométrico a instalar y configurar

4.2 DESCRIPCIÓN DE PRUEBAS FUNCIONALES REALIZADAS

A continuación se describen las pruebas funcionales realizadas en cada aplicación desarrollada, las cuales ese ha obtenido mediante los diagramas de casos de uso y los diagramas de secuencia analizados en el capítulo tres.

Para la aplicación administrador de empleados se ha realizado el siguiente set de validaciones el cual está indicado en la Tabla 4.1.

Evento	**Descripción**	**Posibles Eventos Considerados**	**Resultado esperado**
Acceso al sistema	El usuario ingresa el nombre de usuario y contraseña.	Usuario no registrado	Muestra el mensaje de no existe usuario.

Tabla 4.1. Pruebas funcionales para el administrador de empleados (continúa)

		Contraseña no corresponde.	Envía la respuesta de contraseña inválida.
		Ingreso correcto de los datos del usuario.	Carga el perfil de menú que tiene el usuario.
		Otros eventos no considerados	Muestra el mensaje de error generado.
Ingreso de nuevo usuario	Ingreso de los datos del usuario.	El nombre de usuario Nick ya existe en el sistema.	Muestra el mensaje al usuario que debe escoger otro Nick.
		No ingresa ningún dato requerido	Muestra el mensaje que debe llenar por lo menos los datos requeridos.
		Ingreso correcto de datos del nuevo usuario.	Muestra el mensaje que el usuario se ingresó correctamente al sistema
Actualización de datos de usuario.	Reseteo de contraseña. Mediante el ingreso de la nueva contraseña en dos cuadros de textos diferentes.	La nueva contraseña no corresponde en cada uno de los cuadros de texto.	No permite realizar la actualización y muestra el respectivo mensaje de error.
		Reseteo de contraseña correcto	Actualiza los datos de la contraseña del empleado.
Actualización de datos de usuario.	Cambio de perfil o cambio de Nick de usuario.	No se puede cambiar de perfil	Debido a que solamente usuario con perfil de administrador pueden realizar el cambio.
		No permite realizar el cambio de Nick.	El Nick de empleado posee otro empleado en el sistema.
		Cambio de datos.	Se muestra el mensaje de actualización de datos.

Tabla 4.1. Pruebas funcionales para el administrador de empleados (continúa)

Actualización de perfil.	Quita los permisos de acceso al sistema.	Error presentado en la actualización de datos.	Muestra la excepción generada.
		Actualización correcta.	Muestra el mensaje al usuario.
Registro de nuevo empleado.	Realiza el ingreso de acceso al empleado y su registro biométrico.	El número de documento o el Nick del empleado ya existen.	Muestra el mensaje de error presentado.
		No se ha ingresado los campos requeridos como número de documento, Nick nombres y salario.	Muestra un mensaje de notificación indicando los campos requeridos para proceder con el registro.
		Ingreso correcto.	Muestra el mensaje de ingreso correcto
Ingreso de permisos	Realizar el ingreso de permisos, comisiones o vacaciones del empleado.	Ingreso del permiso sin la descripción.	Muestra el mensaje que debe ingresar una descripción.
		Ingreso de permisos que no corresponden a los días laborables.	Muestra el mensaje que no se puede insertar debido a que el día de permiso no corresponde con el tipo de permiso a ingresar.
		Ingreso correcto	Muestra el mensaje que el permiso está ingresado.
		Permiso, comisión o vacación duplicado.	Muestra el mensaje que ya existe ingresado un permiso. En ese día. Y en esas horas.
Agregar Nuevo Horario Y Actualizar Horario	Permite realizar la creación de un nuevo horario laborable.	Horas duplicadas en el mismo día.	Muestra el mensaje que no se permite ingresar.

Tabla 4.1. Pruebas funcionales para el administrador de empleados (continúa)

		Horas que pertenecen a un horario ingresado anteriormente y que pertenezca al mismo grupo y día.	No permite ingresar e indica el mensaje correspondiente.
Añadir dispositivo y Actualizar dispositivo.	Permite realizar el ingreso y actualización de los datos. De los dispositivos.	La dirección IP no está disponible.	Muestra el mensaje de que debe ingresar otra dirección IP.
		Ingreso de datos exitoso.	Muestra el mensaje de ingreso exitoso al sistema.

Tabla 4.1. Pruebas funcionales para el administrador de empleados

En la Tabla 4.2, se indica las pruebas funcionales para la aplicación cliente biométrico.

Evento	**Descripción**	**Posibles Eventos Considerados**	**Resultado esperado**
Lectura de huella.	Inicia el proceso de adquisición mediante el establecimiento de conexión al lector biométrico, para luego enviar los datos al servidor de autenticación y mostrar la respuesta de esta validación.	No permite establecer la comunicación con el lector.	Muestra el mensaje de error y para el proceso de lectura.
		No existe conexión al servidor de autenticación.	Muestra el mensaje de error de no poder establecer la comunicación con el servidor.
		Lectura normal de huella	Empieza a esperar la lectura de la huella.

Tabla 4.2. Pruebas funcionales para el cliente biométrico

Estas pruebas funcionales se han realizado para verificar el funcionamiento del sistema biométrico. En la Tabla 4.3, se describen las pruebas funcionales realizadas en el servidor de autenticación, El cual ha sido verificado y probado considerando los diferentes tipos de autenticación que puede soportar el sistema.

Evento	Descripción	Posibles Eventos Considerados	Resultado esperado
Procesamiento de peticiones.	Ingresa una petición para poder realizar el registro del empleado.	El tipo de mensaje de requerimiento no concuerda con el establecido en el capítulo tres.	Almacena en el log el mensaje de ingreso y cierra la conexión, no responde a estos mensajes.
		El número de dispositivo biométrico y su dirección IP no están registrados.	Envía el mensaje de respuesta con el código de error 020 aplicación no registrada.
		Huella dactilar no está almacenada en el sistema o el empleado ingreso incorrectamente la huella.	El sistema responde con código de error 013.
		Autenticación exitosa.	Responde con código de error 000, que significa que se procesó correctamente.

Tabla 4.3. Pruebas unitarias para el servidor biométrico

4.3 INSTALACIÓN DE PAQUETES NECESARIOS PARA EL FUNCIONAMIENTO DEL SISTEMA

Para el funcionamiento de las aplicaciones desarrolladas como son: cliente biométrico, administrador de empleados y servidor de biométrico los cuales están indicados en el Capítulo 3.1, es necesario que estén instalados los siguientes paquetes en el sistema operativo los cuales están descritos en la Tabla 4.4.

En esta sección se explica la función que realizan cada uno de estos paquetes para el funcionamiento del sistema biométrico.

Framework 3.5.- Este paquete es necesario para mostrar las ventanas del sistema biométrico y correr los métodos desarrollados, ya que el Framework es un

middleware[18], utilizado para interpretar la sintaxis de cada uno de los lenguajes de programación que maneja Microsoft como son: C *Sharp*, *C++, Visual Basic* y *Asp Net*.

CRRedist2008.- Esta aplicación es utilizada para visualizar los reportes que posee la aplicación administrador biométrico.

SecuBSP SDK Pro.- Esta librería es necesaria para las aplicaciones desarrolladas debido a que se utilizan los métodos para realizar la adquisición y comparación de las huellas.

Internet Information Services.- permite realizar la publicación de la lógica de negocios y los métodos que posee el sistema biométrico mediante la utilización del protocolo de comunicación http, para la aplicación administrador de empleados.

Paquete	Cliente Biométrico.	Administrador de Empleados.	Servidor Biométrico.
FrameWork 3.5	X	X	X
CRRedist2008 (Librerias)		X	
SecuBSP SDK Pro	X	X	X
Internet Information Services 6 o superior			X

Tabla 4.4. Paquetes necesarios para el funcionamiento del sistema biométrico

4.4 RESULTADOS DE LAS PRUEBAS REALIZADAS

En esta sección se presenta el resultado de las pruebas de autenticación realizadas del sistema biométrico en tiempo real, para obtener estos datos se utiliza el *log* de eventos del servicio de autenticación, el cual almacena los resultados de autenticación realizado para los empleados en el sistema.

Los datos a mostrar son aquellos tomados para un rango de fechas, para ello se va a utilizar el sistema de registro en todo el mes de febrero, el cual está representado en la Tabla 4.5, considerando como un registro exitoso que la huella

[18] Middleware es un software que asiste a una aplicación para interactuar o comunicarse con otras aplicaciones, software, redes, hardware y/o sistemas operativos.

dactilar esta almacenada en el sistema y pertenece al empleado que realizo el timbrado, mientras que un registro fallido es cuando el empleado ha ingresado una huella que no está registrado en el sistema o puso incorrectamente la huella en el lector y no concuerda con la huella almacenada en la base.

Fecha	Registro Exitoso		Registro Fallido		Permisos registrados		
	Entrada	Salida	Entrada	Salida	Permiso	Vacación	Comisión
01/02/2013	24	25	0	2	0	0	1
02/02/2013	0	0	0	0	0	0	0
03/02/2013	0	0	0	0	0	0	0
04/02/2013	0	0	0	0	0	27	0
05/02/2013	0	0	0	0	0	27	0
06/02/2013	0	0	0	0	0	27	0
07/02/2013	0	0	0	0	0	27	0
08/02/2013	0	0	0	0	0	27	0
09/02/2013	0	0	0	0	0	0	0
10/02/2013	0	0	0	0	0	0	0
11/02/2013	23	24	3	1	0	0	1
12/02/2013	26	24	5	0	0	0	2
13/02/2013	27	26	0	2	1	0	0
14/02/2013	25	24	2	1	0	0	1
15/02/2013	24	27	1	3	1	0	0
16/02/2013	0	0	0	0	0	0	0
17/02/2013	0	0	0	0	0	0	0
18/02/2013	21	21	1	0	1	0	1
19/02/2013	24	24	3	0	0	0	0

Tabla 4.5. Resumen de registro de empleados en el mes de febrero (continúa)

20/02/2013	**27**	**27**	**4**	**1**	**0**	**0**	**2**
21/02/2013	25	23	3	0	1	0	0
22/02/2013	22	25	2	0	0	0	0
23/02/2013	0	0	0	0	0	0	0
24/02/2013	0	0	0	0	0	0	0
25/02/2013	23	22	2	0	0	0	1
26/02/2013	27	25	0	1	0	0	0
27/02/2013	27	25	1	1	0	0	0
28/02/2013	27	27	1	1	0	0	1
01/03/2013	27	27	0	0	0	0	0

Tabla 4.5. Resumen de registro de empleados en el mes de febrero

El principal inconveniente detectado del sistema, fue la manipulación de las aplicaciones por parte del personal encargado, debido a que cada aplicación diseñada, se la debe iniciar manualmente y el personal encargado, aún no estaba familiarizado con el manejo de las aplicaciones. Esto fue disminuyendo mientras el personal encargado y el empleado se familiarizan con el sistema y las opciones que posee.

Por parte de los empleados se detecta, que al momento de realizar el registro con la huella dactilar, se registra en más de una ocasión debido a que el empleado no está familiarizado en el proceso de autenticación para el registro de hora, ya que mantiene el dedo en el lector y hasta esperar el mensaje de notificación de respuesta se envía la solicitud en más de una ocasión. Esto influye en el cálculo de horas de trabajo porque el sistema calcula las horas de trabajo diarias del empleado mediante una diferencia de horas pares. Para corregir este inconveniente el servidor biométrico autoriza el tiempo mínimo para que el empleado pueda realizar otro registró el cual está configurado con un valor de un minuto, y se agregó sonidos de notificación para indicar al empleado que retire su dedo del lector.

Se detecta que algunos empleados, no realizan el registro o timbrado en su horario de trabajo utilizando el servicio biométrico. Puede ser por que el sistema no está disponible debido a falla de energía eléctrica o la persona encargada no se encuentra en su puesto de trabajo para iniciar la aplicación cliente. Para ello se ha indicado al personal encargado que la aplicación cliente biométrico puede correr en segundo plano, es decir se puede dejar iniciado en la computadora para que los empleados puedan utilizar el lector biométrico.

Los registros fallidos se pueden producir cuando el empleado ha ingresado el dedo incorrecto el cual no ha sido registrado en el sistema, o porque su huella dactilar está demasiado desgastada y disminuye la posibilidad de poder identificar la identidad de la persona.

4.5 COSTO TOTAL DEL SISTEMA

Para realizar el cálculo del costo total del sistema biométrico, se utiliza el método de *Constructive Cost Model COCOMO*. “Este modelo permite realizar estimaciones de tiempo de desarrollo y número de personas necesarias para realizar el desarrollo de software, además se considera el tamaño del software desarrollado mediante la definición los siguientes modelos” [21] descritos en la Tabla 4.6.

Para realizar el cálculo de costo de desarrollo de software se ha seleccionado el modelo intermedio, ya que calcula los datos partiendo desde la selección de los elementos del sistema biométrico desarrollado. Además el desarrollo del sistema es desde cero y se ha procedido a evaluar el hardware que puede utilizar. Para realizar el cálculo del costo mediante el modelo intermedio es necesario seguir los siguientes pasos:

1. Determinar la cantidad de número de líneas de código total que posee cada aplicación, considerando el lenguaje de programación con el cual fue desarrollado. La cantidad de líneas de código se obtiene mediante la Ecuación 4.1.

$$KDLC = \frac{PF * Lineas\ de\ código\ por\ cada\ PF}{1000}$$

Ecuación 4.1. Cálculo del número de Kilo líneas de código [20]

Donde, *KLDC* es la ponderación de cantidad de miles de líneas de código que posee el sistema en un determinado lenguaje de programación por sus puntos de función.

PF puntos de función, es el número de miles de líneas de código que posee la aplicación.

Líneas de código por cada PF, valor constante que depende del tipo de lenguaje de programación con el que se está realizando la aplicación, estos valores se muestran en la Tabla 4.7.

2. Calcular el esfuerzo, tiempo de desarrollo y el número de personas necesarias mediante la utilización de las siguientes formulas.

$$E = a\ KLDC^{e} * FAE \text{ (persona x mes)}$$

Ecuación 4.2. Cálculo del esfuerzo [20]

$$T = c\ E^{d} \text{ (meses)}$$

Ecuación 4.3. Cálculo del tiempo [20]

$$P = E/T \text{ (personas)}$$

Ecuación 4.4. Cálculo del número de personas [20]

Dónde:

E es el esfuerzo necesario para realizar el proyecto.

Las variables *a, e, c y d* son constantes de valoración, que depende del valor de KDLC, estos valores están indicados en la Tabla 4.8.

FAE es el factor de ajuste de esfuerzo obtenido de acuerdo a las características del proyecto. Este factor se lo obtiene mediante la multiplicación de los diferentes valores del sistema a ser desarrollado, descritos en la Tabla 4.9.

T es el tiempo de duración del desarrollo de la aplicación.

P es el número de personas necesarias para realizar la aplicación.

Nivel.	Descripción.
Modelo básico.	Se basa en el tamaño expresado en LDC[19], es utilizado en los proyectos de software en fase de prototipo.
Modelo intermedio.	Evalúa las alternativas de hardware y software, para el desarrollo de un proyecto.
Modelo avanzado.	Define la arquitectura del sistema, y es utilizado en la etapa de mantenimiento.

Tabla 4.6. Modelos del sistema de COCOMO [21]

LENGUAJE	LDC/PF
Ensamblador	320
C#	150
COBOL	105
Pascal	91
Prolog/LISP	64
C++	64
Visual Basic	32
SQL	12

Tabla 4.7. Valores utilizados de LDC/PF, para los distintos lenguajes de programación [21]

[19] LDC.- Unidad de líneas de código.

PROYECTO SOFTWARE	A	E	C	D	Consideración
Normal	3,2	1,05	2,5	0,38	KDLC <50
Intermedio	3	1,12	2,5	0,35	50<=KDLC<=300
Avanzado	2,8	1,2	2,5	0,32	KDLC >300

Tabla 4.8. Valores de constantes asignados según el valor de número de líneas KDLC [21]

A continuación se describen cualidades del sistema a desarrollar las cuales se menciona en la Tabla 4.9, y poseen un puntaje de estimación para realizar el cálculo del factor de ajuste de esfuerzo.

a. Cualidades de producto

Fiabilidad requerida del software.- Utilizado para valorar si todavía existen defectos en el software. Un valor muy bajo indica que solamente hace falta eliminar los defectos sin ninguna otra consecuencia.

Tamaño de la base de datos.- Mide el tamaño de almacenamiento de información que va almacenar debido al uso de la aplicación, se considera un valor bajo si el almacenamiento es poco y alto cuando se van almacenar datos de gran tamaño.

Complejidad del producto.- Indica la complejidad de cada módulo que posee el sistema. Por lo que la puntuación puede variar de *muy bajo* si el módulo está compuesto de funciones simples y *alto* para módulos que utilizan muchos recursos de procesamiento.

b. Cualidades del hardware

Restricciones del tiempo de ejecución.- Siempre será más exigente para un programador escribir un programa que tiene una restricción o uso del CPU[20] en tiempo de ejecución. Es *bajo* cuando el porcentaje es del 50%, y *alto* cuando la restricción es del 95%.

[20] CPU.- Unidad central de proceso.- es el componente principal de la computadora y otros dispositivos programables, que interpreta las instrucciones contenidas en los programas y procesa datos.

Restricciones del almacenamiento principal.- Se espera que un cierto porcentaje del almacenamiento principal sea utilizado por el programa. El esfuerzo de programación se incremente si el programa tiene que correr en un volumen menor del almacenamiento principal. Si el requerimiento por el uso del CPU es mayor se lo considera como extremadamente alto, y bajo si no hay restricciones.

Volatilidad del ambiente virtual de la máquina.- Durante el desarrollo del software la máquina en la que desarrolla puede sufrir algunos cambios como reducción de espacio en el disco o uso de CPU. Si existe muchos cambios se lo refleja como alto.

Tiempo de respuesta del ordenador.- Mide el tiempo de respuesta del procesamiento de una función específica implementada. Cuanto mayor sea el tiempo de respuesta, más alto será el esfuerzo humano. Y se considerará como alto.

c. Cualidades del personal

Capacidad del analista.- califica el esfuerzo humano del desarrollador, considerando la habilidad de análisis, eficiencia y capacidad para cooperar en un grupo. Cuanto más capaz, menos esfuerzo será necesario.

Experiencia en la aplicación.- La experiencia del grupo de programadores en una aplicación similar tiene una gran influencia en el esfuerzo. Puede variar desde muy bajo cuando no posee experiencia a muy alto cuando posee experiencia en proyectos similares.

Capacidad de los programadores.- La cuantificación es similar a la capacidad de analista, pero en este caso relacionado con los programadores. Se califica al grupo de programadores.

Experiencia en el S.O. utilizado.- Cuanto mayor sea la experiencia del grupo de programación con el uso del SO en el procesador, menor será el esfuerzo necesario.

Experiencia del lenguaje de programación.- Un grupo de programadores con amplia experiencia en un lenguaje determinado programará de una manera mucho más segura, generando un menor número de defectos.

d. Cualidades del proyecto

Prácticas de programación modernas.- Utilización de modernas prácticas de programación. Estas prácticas incluyen, por ejemplo, programación estructurada y desarrollo

Utilización de herramientas software.- El uso correcto de herramientas desarrollo es un valor alto de productividad. Este valor varía desde muy bajo cuando sólo se utilizan herramientas básicas, a muy alto cuando se utilizan herramientas específicas.

Horario requerido del desarrollo.- Tiempo utilizado para realizar cierta actividad. Cualquier apresuramiento se le asigna como muy bajo o retraso se le asigna como alto, demandarán más esfuerzo.

En la Tabla 4.9 se presenta los valores de costo para calcular el factor ajuste.

a). Estimación del costo total del sistema

Para calcular el valor KDLC, se describe en la siguiente Tabla 4.10 las clases creadas en el proyecto librería tomando en cuenta el total de líneas de código, que es la suma líneas de código y comentarios. Este proyecto maneja la conexión y manipulación de los datos de la base de datos, realiza la codificación y decodificación de la información, administra las conexiones TCP/IP mediante sockets tanto para el cliente como para el servidor, maneja lectura y escritura de archivos y realiza la validación de identidad del empleado en el servidor.

En la Tabla 4.11, se presenta la cantidad de líneas utilizadas para realizar la interfaz de usuario servidor biométrico. Esta aplicación utiliza las librerías creadas para acceder al servicio, muestra el resultado de la autenticación del empleado en un cuadro de texto y permite iniciar y para el servicio de autenticación biométrico.

En la Tabla 4.12, se presenta la cantidad de líneas de código utilizadas para la aplicación usuario biométrico.

CONDUCTORES DE COSTO	VALORACIÓN					
	Muy bajo	*Bajo*	*Normal*	*Alto*	*Muy alto*	*Extra alto*
Fiabilidad requerida del software	0,75	0,88	1.00	1,15	1,4	-
Tamaño de la base de datos	-	0,94	1.00	1,08	1,16	-
Complejidad del producto	0,7	0,85	1.00	1,15	1,3	1,65
Restricciones del tiempo de ejecución	-	-	1.00	1,11	1,3	1,66
Restricciones del almacenamiento principal	-	-	1.00	1,06	1,21	1,56
Volatilidad del ambiente virtual de la máquina.	-	0,87	1.00	1,15	1,3	-
Tiempo de respuesta del ordenador	-	0,87	1.00	1,07	1,15	-
Capacidad del analista	1,46	1,19	1.00	0,86	0,71	-
Experiencia en la aplicación	1,29	1,13	1.00	0,91	0,82	-
Capacidad de los programadores	1,42	1,17	1.00	0,86	0,7	-
Experiencia en S.O. utilizado	1,21	1,1	1.00	0,9	-	-
Experiencia en el lenguaje de programación	1,14	1,07	1.00	0,95	-	-
Prácticas de programación modernas	1,24	1,1	1.00	0,91	0,82	-
Utilización de herramientas software	1,24	1,1	1.00	0,91	0,83	-
Horario requerido del desarrollo.	1,23	1,08	1.00	1,04	1,1	-

Tabla 4.9. Coeficientes de ajuste de esfuerzo [20]

Para calcular el valor de KDLC para la base de datos, se muestra en la Tabla 4.14 el número de líneas utilizadas en la creación de la base de datos como: Tablas, procedimientos almacenados y funciones.

Archivos	Descripción	Total líneas	Líneas de código
msgMostrar.cs	Maneja los mensajes de aviso y de error de la aplicación	63	53
mArchivo.cs	Manejo de lectura y escritura de archivos.	238	196
Base.cs	Manejo de Conexión a la base de datos.	1968	1751
Encriptacion.cs	Manejo de codificación y decodificación de la información	51	42
Administracion.cs	Administración de mensajes ICMP, para dispositivos.	96	89
ClienteTCP.cs	Cliente TCPIP, procesamiento de peticiones.	299	237
ConexionServ.cs	Servidor, para recepción de peticiones.	107	95
dispositivoBiometrico.cs	Administración de dispositivo biométrico, Secugen.	22	19
	Total	2844	2482

Tabla 4.10. Tabla de descripción de líneas de código del proyecto de librerías

En la Tabla 4.15 se presenta las líneas de código utilizadas en el proyecto biométrico, el cual nos indica la cantidad de puntos de función del sistema desarrollado el cual será utilizado para calcular el valor KDLC.

Archivos	Descripción	Total líneas	Líneas de código
ConexionCon.cs	Ventana para establecer los parámetros de conexión para el servicio.	135	114
ConexionCon. Designer.cs	Contiene los objetos utilizados en la ventana.	251	183
Dispositivo Biometrico.cs	Ventana para realizar el monitoreo de dispositivos biométricos.	224	191
Dispositivo Biometrico.Designer.cs	Contiene los objetos utilizados en la ventana.	239	171
Monitor.cs	Administración del servicio biométrico y visor de sucesos.	304	264
Monitor.Designer.cs	Contiene los objetos utilizados en la ventana.	256	186
	Total	1409	1109

Tabla 4.11. Número de líneas del servicio de autenticación biométrica

Nombre de Archivo	Descripción	Líneas Totales	Líneas de código
Conexion.cs	Ventana utilizada para visualizar la configuración de comunicación del servicio.	43	35
Conexion.Designer.cs	Contiene los objetos de la ventana.	120	82
Config.cs	Ventana utilizada para visualizar la configuración del servicio de autenticación.	82	72
Config.Designer.cs	Contiene los objetos de la ventana.	145	104
Form1.cs	Ventana para realizar la interacción entre el hardware y la aplicación	269	231
Form1.Designer.cs	Contiene los objetos de la ventana.	243	171

Tabla 4.12. Aplicación usuario biométrico (continúa)

Sonido.cs	**Maneja reproducción de sonidos, dependiendo de la respuesta de autenticación.**	**25**	**22**
Trama.cs	Construye y procesa las tramas que van del cliente hacia el servidor.	168	160
	Total	1095	877

Tabla 4.12. Aplicación usuario biométrico

En la Tabla 4.13, se muestra la cantidad de líneas de código utilizadas para realizar la aplicación administrador biométrico.

Nombre de Archivo	Descripción	Líneas Totales	Líneas de código
empleadosAnio.cs	Ventana de administrador de empleado	185	136
Form1.cs	Ventana utilizada para presentar las opciones del usuario.	382	337
Form1.Designer.cs	Contiene los objetos de la ventana	111	74
login.cs	Ventana de ingreso de sesión de usuario.	100	87
login.Designer.cs	Contiene los objetos de la ventana	163	116
ReporteEmple.cs	Ventana para visualizar los datos de las horas.	169	122
reporteGeneral.cs	Ventana para visualizar el cálculo de horas.	169	122
Modificar Dispositivo.cs	Ventana para modificar los dispositivos biométricos del sistema.	72	65

Tabla 4.13 Número de código de líneas para la aplicación administrador biométrico (continúa)

ModificarDispositivo. Designer.cs	Contiene los objetos utilizados en la ventana.	204	148
NuevoDispo.cs	Ventana para crear un nuevo dispositivo.	39	36
NuevoDispo.Designer.cs	Contiene los objetos utilizados en la ventana.	156	109
ActulizarEmp.cs	Ventana para actualizar los datos del empleado.	297	249
ActulizarEmp.Designer.cs	Contiene los objetos utilizados en la ventana.	520	386
AgregarEmp.cs	Ventana para agregar un empleado.	204	174
AgregarEmp. Designer.cs	Contiene los objetos utilizados en la ventana.	457	335
BorrarPermiso.cs	Ventana para actualizar y borrar permisos de empleado.	35	32
BorrarPermiso. Designer.cs	Contiene los objetos utilizados en la ventana.	228	163
ingresoBiometria.cs	Ventana para insertar o actualizar los datos biométricos.	108	99
ingresoBiometria .Designer.cs	Contiene los objetos utilizados en la ventana.	196	143
IngresoEmpleado.cs	Ventana utilizada para ingresar un nuevo empleado.	19	18
IngresoEmpleado .Designer.cs	Contiene los objetos utilizados en la ventana.	46	27
permiso.cs	Ventana utilizada para ingresar un nuevo permiso.	400	364
permiso.Designer.cs	Contiene los objetos utilizados en la ventana.	381	286

Tabla 4.13 Número de código de líneas para la aplicación administrador biométrico (continúa)

RegistrosNo Ingresados.cs	Ventana utilizada para visualizar los errores al momento de ingresar permisos.	71	60
RegistrosNo Ingresados. Designer.cs	Contiene los objetos utilizados en la ventana.	105	72
ds_empledoc.cs	*Data set*[21] utilizado para almacenar los datos del empleado.	6	4
ds_empledoc .Designer.cs	Contiene los atributos de la *data set.*	1479	1263
ds_repor_gener.cs	Data set utilizado para almacenar el registro de horas del empleado.	6	4
ds_repor_gener .Designer.cs	Contiene los atributos del *data set.*	2199	1871
registroEmple.cs	Ventana utilizada para mostrar los datos de registro.	13	9
registroEmple .Designer.cs	Contiene los objetos de la ventana	782	666
ReporteGeneral Emp.cs	Ventana utilizada para mostrar los registro de horas.	385	324
ReporteGeneral Emp.Designer.cs	Contiene los objetos de la ventana	132	94
reporteprueba.cs	Ventana para mostrar los reportes de horas.	1062	820
reporteprueba. Designer.cs	Contiene los objetos de la ventana	304	226
ActualizarUsr.cs	Ventana utilizada para actualizar los datos del usuario.	141	125
ActualizarUsr .Designer.cs	Contiene los objetos de la ventana	203	147

Tabla 4.13 Número de código de líneas para la aplicación administrador biométrico (continúa)

[21] Data set es un grupo de clases que describen una simple base de datos relacional en memoria.

cambircontraseña.cs	Ventana para cambiar la contraseña del usuario.	51	48
Cambircontraseña .Designer.cs	Contiene los objetos de la ventana	137	96
NuevoGrupo Usuario.cs	Ventana utilizada para crear un nuevo grupo de usuario	93	86
NuevoGrupo Usuario.Designer.cs	Contiene los objetos utilizados de la ventana.	467	354
NuevoUsuario.cs	Ventana utilizada para agregar a un nuevo usuario.	81	72
NuevoUsuario .Designer.cs	Contiene los objetos de la ventana	185	130
peermisoMenu.cs	Ventana utilizada para actualizar permiso al empleado.	296	284
peermiso Menu.Designer.cs	Contiene los objetos de la ventana	435	331
ActualizarHorario.cs	Ventana utilizada para actualizar los datos del horario laborable.	206	188
ActualizarHorario. Designer.cs	Contiene los objetos de la ventana	321	238
NuevoHorario.cs	Ventana utilizada para crear un nuevo horario laborable.	148	131
NuevoHorario .Designer.cs	Contiene los objetos de la ventana	327	239
Reference.cs	Maneja la comunicación entre la aplicación y el servidor mediante la invocación al servicio web.	4226	3012
	Total	18502	14522

Tabla 4.13. Número de código de líneas para la aplicación administrador biométrico

Nombre de Archivo	Descripción	Líneas Totales	Líneas de código
ScriptBase	Script utilizado para la creación de base de datos, Tablas , procedimientos almacenados y funciones	2572	2360

Tabla 4.14. Número de líneas de código para la creación de la base de datos

Aplicación	Líneas de código total	Líneas de código
Librería	2844	2482
Servidor de autenticación	1409	1109
Usuario biométrico	1095	877
Administrador biométrico	18502	14522
Total líneas de código	23850	18990

Tabla 4.15. Líneas de código totales del sistema biométrico

Para obtener el valor de KDLC mediante la Ecuación 4.1 es necesario saber la cantidad de puntos de función que es el total de líneas que utilizamos para desarrollar la aplicación y el lenguaje de programación utilizado estos valores están representados en la Tabla 4.15 y 4.7 respectivamente. Para ello se va a separar el sistema entre la creación base de datos que está realizado en SQL server y las aplicaciones que están realizadas en C#, mediante la ayuda del IDE[22] Visual Studio 2008. A continuación se va a presentar el cálculo de KDLC realizado para la lógica de negocio y capa aplicación.

Tomando en consideración los siguientes datos para el cálculo:

- El número de líneas por punto de función PF: 18,990, valor que es tomando de la Tabla 4.15.

[22] IDE.- es un entorno de programación que ha sido empaquetado como un programa de aplicación; es decir, consiste en un editor de código, un compilador, un depurador y un constructor de interfaz gráfica (GUI).

- El lenguaje de programación utilizado es C# *(C Sharp)*, por lo que se toma el siguiente valor de líneas de código por cada PF 150 de acuerdo a la Tabla 4.6. y se aplica la Ecuación 4.1 para realizar el cálculo del número de líneas.

$$KDLC = \frac{PF * Lineas\ de\ código\ por\ cada\ PF}{1000}$$

$$KDLC = \frac{18{,}99 * 150}{1000}$$

$$KDLC = 2{,}849\ KDLC$$

Ya que el valor de KDLC, no fue mayor a 50 KDLC, se va a seleccionar los siguientes valores de las constantes según la Tabla 4.8.

a = 3,2, e =1,05, c = 2,5 y d = 0,38.

Luego de obtener el valor KDLC y el valor de las constantes se calcula el factor de ajuste de esfuerzo FAE mediante la selección de los coeficientes de coste los cuales están indicados el valor de selección en la Tabla 4.16.

FAE =
1,15*1,00*0,85*1,00*1,00*1,00*1,00*1,00*1,00*0,86*1,00*0,95*0,91*0,91*1,04

FAE = 0,69

Con el cálculo del factor de ajuste se obtiene el valor del esfuerzo, mediante la aplicación de la Ecuación 4.2

E = a KLDC ^{e} * FAE (persona x mes)

E = 3,2*(2,849)^{1,05}*0,69

E = 6,63 personas*mes.

Luego se calcula el tiempo de desarrollo mediante la Ecuación 4.3.

T = c Esfuerzo ^{d}

$T= 2,5 * (6,63)^{0,38} = 5,13$ meses

Personal promedio mediante la Ecuación 4.4

$P = E/T$

$P = 6,63/5,13 = 1,29 \approx 2$ personas

Con estos cálculos se concluye, que son necesarias dos personas para realizar la programación de la aplicación en aproximadamente cinco meses. Ahora se considera que una sola persona realiza el mismo trabajo mediante la utilización de la Ecuación 4.4 se obtiene el valor de 6,82 meses ya que se despeja el tiempo y se toma el mismo esfuerzo.

Se va a realizar el cálculo de estimación de personas necesarias y el tiempo requerido para realizar la creación de la base de datos el cual sigue la misma lógica mostrada en el cálculo anterior.

Utilizando la Ecuación 4.1 y el valor de número de líneas por punto de función PF: en la Tabla 4.15 se toma este valor de 2,36 y el valor para el lenguaje de programación SQL, el cual muestra en la Tabla 4.8 el valor de 12 PF.

Aplicando la Ecuación 4.1

KLDC = (2,36*12)/1000 = 0,028 KDLC

Ya que el valor de KDLC, no fue mayor a 50 KDLC se selecciona los valores de las siguientes constantes según la Tabla 4.8

$$a = 3,2,\ e =1,05,\ c = 2,5 \text{ y } d = 0,38.$$

Luego se considera los mismos valores del factor de ajuste de esfuerzo descrito en la Tabla 4.16, calculados anteriormente.

FAE = 0,69.

Factor	Elección	Justificación
Fiabilidad requerida del software	Alto. Valor 1,15	El valor seleccionado es alto, ya que el sistema abarca los requerimientos descritos en el capítulo dos.
Tamaño de la base de datos	Normal. Valor 1,00	La información que almacena es muy pequeña en comparación con otros sistemas por esta razón se ha elegido el valor normal.
Complejidad del producto	Bajo. Valor 0.85	La aplicación no va a realizar cálculos complejos.
Restricciones del tiempo de ejecución	Normal. Valor 1,00	El tiempo de respuesta entre aplicaciones está considerado hasta máximo 10 segundos.
Restricciones del almacenamiento principal	Normal. Valor 1,00	No existe restricción para el uso de la memoria para el servicio ya que el servidor cumple con las especificaciones dadas en el capítulo dos.
Volatilidad del ambiente virtual de la máquina.	Normal. Valor 1,00	No se han realizados cambios significativos en la maquina donde se desarrollo es por esta razón que se ha seleccionado el valor normal.
Tiempo de respuesta del computador	Normal. Valor 1,00	Tiempo de respuesta debe ser normal. Para que sea interactivo con el usuario.
Capacidad del analista	Normal. Valor 1,00	El conocimiento para estructurar la aplicación es medio, por esta razón se ha seleccionado este valor.
Experiencia en la aplicación	Normal. Valor 1,00	La experiencia en el desarrollo de aplicaciones es baja, pero se coloca en nivel normal ya que se tiene conocimientos en los lenguajes de programación utilizados en el sistema.

Tabla 4.16. Elección de valores para calcular FAE (continúa)

Capacidad de los programadores	Alto. Valor 0,86	Se selecciona este valor ya que se posee un conocimiento general del funcionamiento del sistema y cálculos a realizar.
Experiencia en S.O. utilizado	Normal. Valor 1,00	Manejo básico del procesamiento de los recursos para los sistemas operativos Windows XP, Windows 7 o Windows Server 2003 o 2008.
Experiencia en el lenguaje de programación	Alto. Valor 0,95	Se selecciona este valor debido a que posee nociones medias del lenguaje de programación.
Prácticas de programación modernas	Alto. Valor 0,91	Se selecciona este valor ya que el sistema está utilizando el modelo de programación de capas, para las aplicaciones distribuidas.
Utilización de herramientas software	Alto. Valor 0,91	Se usarán herramientas estándares como es el IDE.
Horario requerido del desarrollo.	Bajo, Valor 1,04	El software no fue desarrollado con forme al tiempo indicado y fue un retraso es por esta razón que se selecciona este valor.

Tabla 4.16. Elección de valores para calcular FAE

Y a continuación se procede a calcular el esfuerzo para realizar la programación de la base de datos mediante la Ecuación 4.2.

$E = 3,2*(0,028)^{1,05}*0,69$

E = 0,05 personas/mes.

Calculo del tiempo de desarrollo mediante la utilización de la Ecuación 4.3.

$T = 2,5 * (0,05)^{0,38} = 0,8$ meses

Personal promedio mediante la utilización de la Ecuación 4.4.

$P = E/T = 0,05 / 0,8 = 0,06 \approx 1$ personas

Con estos datos obtenidos en el desarrollo de la base de datos se puede concluir que se necesita una persona para realizar la programación de la base de datos en dos semanas.

Tomando en consideración los cálculos realizados tanto para la aplicación como para la el desarrollo de la base de datos se concluye con lo siguiente.

Para realizar el desarrollo de la aplicación con una sola persona, el tiempo estimado para terminar el desarrollo de la aplicación y la programación de la base de datos es de aproximadamente siete meses este tiempo calculado mediante la suma de los tiempos calculados para realizar la base de datos y la aplicación, con un costo total de desarrollo de 3500 dólares, este valor se obtiene, ya que se considera el costo de la hora laborable del empleado de dos dólares con cincuenta centavos, este precio no incluye el valor del hardware.

El costo del hardware seleccionado SECUGEN, tiene un costo en el mercado alrededor de 120 dólares. Por consiguiente el costo total del desarrollo del sistema con el dispositivo biométrico es de 3620 dólares.

CAPÍTULO 5

5.1 CONCLUSIONES

✓ En comparación con las otras técnicas de reconocimiento biométrico, La técnica de autenticación por huella dactilar tiene mayor penetración en el mercado, debido a que ha sido desarrollada e investigada por largo tiempo, por su bajo costo y su confiabilidad para la identificación del individuo.

✓ La aplicación con el modelo de capas desarrollado, permite procesar varias peticiones por aplicaciones de clientes biométricos, ya que posee un hilo de ejecución maestro que atiende las peticiones y crea un hilo hijo para que este se encargue de realizar el procesamiento.

✓ Los tipos de datos que permite almacenar y comparar minucias mediante el dispositivo biométrico *Secugen* es: cadena de caracteres *String* o Imagen *Image*, debido a que permite almacenar estos tipos de datos, se ha elegido el tipo String para guardar en la base de datos. Ya que al momento de guardar una imagen en la base se debe realizar un cambio de tipo de dato a binario y este cambio causa que se pierdan o alteren las minucias.

✓ La arquitectura modular de n capas implementado, permite dividir el procesamiento entre varios computadores, el inconveniente surge debido a que se necesita implementar mecanismos de redundancia tales como un servidor de respaldo tanto para la capa lógica como para la capa de accesos a datos, con la finalidad de mantener las comunicaciones entre las diferentes capas; ya que, si una capa falla el sistema queda totalmente inoperante.

✓ Se ha desarrollado el sistema biométrico con la interfaz gráfica para aplicaciones de escritorio, debido a que este modelo permite manejar el estado y el valor de las variables en comparación con una aplicación web que necesita establecer mecanismos para permitir la ejecución de subprogramas y manejar los estados de las variables.

✓ El intercambio de mensajes utilizado, para distinguir una solicitud de una respuesta, entre el cliente y el servidor, se usa para tener un control ordenado del flujo de mensajes e identificar los posibles errores de respuesta que pueden presentarse al momento de realizar la autenticación.

✓ Se procedió a realizar la publicación de las librerías, para el funcionamiento de las aplicaciones por dos métodos. La primera es el método que llama a las librerías que residen en el mismo programa que ejecuta la aplicación, como ejemplo es la aplicación servidor biométrico y cliente biométrico. La segunda es mediante la invocación de métodos publicados en un servidor web, el cual necesita que estas librerías residan solamente en una máquina. A este tipo de método se lo conoce como servicio web y utiliza la aplicación administrador biométrico y su uso permite transportar grandes cantidades de información a través de la capa aplicación según el modelo OSI.

✓ El número de autenticaciones negativas detectadas por la aplicación, se debió a que el empleado ingresó otra huella dactilar que no estaba registrada en el sistema o colocó incorrectamente el dedo en el lector o la huella registrada poseía desgaste en sus crestas y valles.

✓ El método COCOMO es utilizado para estimar el esfuerzo, tiempo y número de personas requeridas para realizar el proyecto para así determinar el costo que se necesita para realizar la implementación de este. Pero también se puede realizar la estimación, mediante la utilización de COCOMO II, ya que permite realizar los cálculos, considerando las características de mejoramiento continuo y la reutilización del código fuente o funciones de la aplicación.

5.2 RECOMENDACIONES

✓ Investigar el intercambio de mensajes de comunicación para los dispositivos de huella dactilar, para luego realizar la implementación de interpretación de mensajes entre la aplicación y el dispositivo biométrico, con la finalidad de administrar cualquier tipo de dispositivo de huella dactilar.

- ✓ Al momento de realizar la adquisición de la huella dactilar mediante el dispositivo USB, se debe considerar el estado del puerto USB utilizado, ya que si no, se tiene una administración un correcto control el puerto de trabajo del dispositivo puede quedar abierto y no permitirá realizar la adquisición de las imágenes.

- ✓ Por el modelo de desarrollo de la aplicación se puede añadir otras funcionalidades, como el cálculo de rol de pagos de los empleados, ingreso de llamadas de atención y cálculo de liquidaciones con la finalidad de centralizar todos los datos de los empleados en esta aplicación.

- ✓ Verificar los paquetes necesarios instalados, antes de realizar la ejecución de cada una de las aplicaciones, ya que si uno de estos paquetes no están instalados, puede generar una ejecución incorrecta o puede generar una excepción.

- ✓ La aplicación permite administrar el acceso a la información almacenada, por lo que se recomienda que se creen perfiles a los usuarios que van a utilizar la aplicación administrador biométrico.

- ✓ Al momento de realizar el registro del empleado en el sistema, se recomienda almacenar la contraseña del empleado y la huella dactilar con un número mínimo de dos huellas por empleado, para aumentar la probabilidad de registro exitoso.

- ✓ Para realizar el registro de autenticación se deben considerar que el empleado se encuentre registrado en el sistema, con su respectiva característica biométrica y además la aplicación cliente biométrico, debe estar registrada en el sistema, caso contrario no permitirá el registro del empleado.

BIBLIOGRAFÍA

[1] Juan Carlos Santamaría O. Reconocimiento y validación de huellas dactilares utilizando una red neuronal. Recuperado el julio 2008, de Repositorio digital uelbosque.edu.co

[2] Garcia, J. L. (s.f.). Algoritmo para la identificación de personas basado en huellas dactilares. Recuperado el 20 de Marzo de 2012, de Repositorio digital upcommons.upc.edu: http://upcommons.upc.edu/pfc/bitstream/2099.1/8082/1/Mem %C3%B2ria.pdf

[3] UNAM. (s.f.). redyseguridad.fi-p.unam.mx. Recuperado el Marzo de 2012, de UNAM: http://redyseguridad.fi-p.unam.mx/proyectos/biometria/clasificacionsistemas/ procesamientohuella.html

[4] Juan Carlos Santamaría O. Reconocimiento y validación de huellas dactilares utilizando una red neuronal. Recuperado el julio 2008, de Repositorio digital uelbosque.edu.co

[5] UNAM. (s.f.). redyseguridad.fi-p.unam.mx. Recuperado el Marzo de 2012, de UNAM: http://redyseguridad.fi-p.unam.mx/proyectos/biometria/clasificacionsistemas/ clasificaciontipo.html

[6] Dougman, J. (2004). How iris recognition works. IEEE.

[7] Daugman, J. (2002). High confidence visual recognition of person by a test of statiscal independence. IEEE Computer Society.

[8] Laura Florian Cruz, F. C. (2006). Reconocimiento del iris. Universidad nacional de Trujillo.

[9] Harvey, S. (2011). La persepción sensorial. Limusa Wiley.

[10] Anónimo. (Mayo de 2009). UNAM- Facultad de Ingeniería Biometría Informática . Recuperado el Mayo de 2012, de Geometría de la mano: http://redyseguridad.fi-p.unam.mx/proyectos/biometria/clasificacionsistemas/recomano.html

[11] Anónimo. (Mayo de 2009). UNAM- Facultad de Ingeniería Biometría Informática . Recuperado el Mayo de 2012, de Geometría de la mano:

http://redyseguridad.fi-p.unam.mx/proyectos/biometria/clasificacionsistemas /capturamano.html.

[12] Gaensslen's, L. a. (2001). Advances in Fingerprint Technology, Second Edition. CRC Express.

[13] República de Argentina. (s.f.). Congreso internacional de Biométria. Recuperado el Agosto de 2012, de Biométria: http://www.biometrics.gov/Standards/facial.aspx

[14] José Zuñiga, M. M. (2009). Sistemas y Técnicas de autenticación. Tesis.

[15] Anónimo (2010), Sistemas de seguridad basados en biometria., Recuperado el Junio de 2012 de Red de Revistas Científicas de América Latina y el Caribe, España y Portugal: http://www.redalyc.org/articulo.oa?id=84920977016

[16] República de Argentina. (s.f.). Congreso internacional de Biométria. Recuperado el Agosto de 2012, de Biométria: http://www.biometria.gov.ar/metodos-biometricos/voz.aspx

[17] Aitor Mendaza Ormaza, O. M. (2009). Estudio de un sistema de reconocimiento biométrico mediante firma manuscrita online basado en SVN. Grupo Universitario de Tecnologías de Identificación.

[18] Anónimo. (Diciembre de 2010). Blog de desarrollo de software y aplicaciones web. Recuperado el Agosto de 2012, de Software y Aplicaciones Web: http://www.jtentor.com.ar/post/Arquitectura-de-N-Capas-y-N-Niveles.aspx

[19] Ratha, N. K. (2008). Advances in Biometrics Sensors, Algorithms and Systems. Venu.

[20] Technology, N. I. (2000). American National Standard for Information Systems Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo (SMT) Information. NIST.

[21] Villarreal, B. (2007). Estimación de esfuerzo y costo en la producción de software hecho en Venezuela. Universidad de los andes.

[22] Pressman, R. S. (2002). Ingeniría del software un enfoque práctico. Concepción Fernández Madrid.

[23] SecuGen Corporation (2013). SecuGen® USB Fingerprint Reader User Guide. Hecho en United States.

[24] Bioidentidad (2010), BioSuprema BioEntry Plus. Terminal biométrico dactilar compacto para control e identificacion de personas, Recuperado el Junio de 2012 de Lima Peru: http://www.biosuprema.com/bioentry_plus.html

[25] Lector de huellas (2012). U 4000B Reader. Hecho en United States.

ANEXOS

ANEXO A: CÓDIGO FUENTE DE LA APLICACIÓN

- ✓ Este Código se encuentra en cd del proyecto de titulación.

ANEXO B: CÓDIGO FUENTE DE LA BASE DE DATOS

- ✓ Este Código se encuentra en cd del proyecto de titulación.

ANEXO C: CERTIFICADO DE INSTALACIÓN Y FUNCIONAMIENTO

ANEXO D: MANUAL DE USUARIO

ANEXO E: SECUGEN FINGER PRINT READER GUIDE

ANEXO F: FINGER U4000B READER

ANEXO G: TABLAS DE ACTIVIDADES LABORABLES EN EL ECUADOR

ANEXO H: DIAGRAMAS DE CLASES Y DE SECUENCIA DEL SISTEMA BIOMÉTRICO

ANEXO I: INSTALACIÓN Y CONFIGURACIÓN DEL SERVICIO WEB

ANEXO J: INSTALACIÓN DE APLICACIONES DESARROLLADAS