

**Documento de Diseño “Sistema de Ingreso por Reconocimiento Biométrico en la  
Universidad del Cauca”**



**Universidad  
del Cauca**

**Luis Miguel Ortiz Muñoz**

**Carlos Daniel Collazos Zambrano**

**Cristian Felipe Bolaños Ortega**

**Jefferson Danilo Noguera**

**Mary Cristina Carrascal Reyes**

**Hermes Fabian Vargas Rosero**

**Facultad de Ingeniería Electrónica y Telecomunicaciones**

**Ingeniería Electrónica y Telecomunicaciones**

**Laboratorio 4 de electrónica.**

**Popayán, septiembre de 2024**

# Índice

<b>1. INTRODUCCIÓN</b>	4
1.1 Contexto	4
1.2 Problema para resolver	4
1.3 Relevancia o justificación	5
<b>2. REQUERIMIENTOS</b>	5
2.1. Requerimientos Funcionales	5
2.2. Requerimientos No Funcionales	6
2.3. Requerimientos Legales y Normativos	7
<b>3. ARQUITECTURA</b>	7
3.1 Hardware	7
3.2 Software	10
<b>4. CASOS DE USO (HISTORIAS DE USUARIO)</b>	12
4.1 Diagrama de casos de uso inmerso en un sistema institucional como la Universidad del Cauca	12
4.2 Descripción extendida	12
4.3 Mockups historias de usuario	15
4.4 Diagramas de secuencia	17
<b>4.5.1 Integrante de la institución</b>	17
<b>4.5.2 Funcionario administrativo de la institución</b>	18
<b>4.5.3 Sistema de control de acceso</b>	19
<b>5. ALCANCE DE LOS PROTOTIPOS</b>	20
5.1 Primer prototipo	20
5.2 Segundo prototipo	20
5.3 Tercer prototipo	21
5.4 Entrega final	22
<b>6. AVANCE EN LA DOCUMENTACIÓN DE LOS DISPOSITIVOS HARDWARE</b>	22
6.1. Sensor dactilar capacitivo Simlug(bpnwמר81u)	22
6.2. Microcontrolador WT32-ETH01	23

<b>7. BIBLIOGRAFIA.....</b>	<b>24</b>
-----------------------------	-----------

# 1. INTRODUCCIÓN

## 1.1 Contexto

En las universidades, como la Universidad del Cauca, circula una gran cantidad de personas, entre estudiantes, docentes, administrativos y otros miembros de la comunidad universitaria. Esta alta afluencia plantea un desafío significativo en términos de seguridad, ya que se necesita identificar de manera efectiva quiénes pertenecen a la institución. Este reto se acentúa en universidades con un gran número de personas.

Para abordar este problema, la Universidad del Cauca implementó hace algún tiempo un sistema de control de acceso mediante carnets con tecnología NFC. Este sistema permitía, a través de sensores, registrar tanto la entrada como la salida de las personas, mejorando la seguridad y aliviando la carga laboral de los vigilantes en las porterías. Sin embargo, el sistema presentaba una limitación importante: la necesidad de portar siempre el carnet. La realidad es que muchas personas olvidan, pierden o no llevan consigo el carnet, lo que obliga a recurrir nuevamente a métodos manuales para verificar la pertenencia a la universidad, como mostrar un horario o acceso a plataformas internas como SIMCA, regresando así al problema original.

A pesar de que este sistema de control fue efectivo, la universidad decidió no renovar el contrato con el proveedor del sistema hace unos años, volviendo al método tradicional de verificación con carnet o documentos equivalentes. Este retroceso ha reintroducido las dificultades en el control de acceso, por lo que es necesario buscar una solución más moderna y eficiente.

## 1.2 Problema para resolver

El sistema actual de control de acceso de la Universidad del Cauca depende principalmente de la verificación manual de documentos físicos por parte de los vigilantes, lo que genera ineficiencias y retrasos, especialmente cuando un usuario ha olvidado o perdido su credencial. Este problema se agrava debido al alto volumen de usuarios diarios, lo que aumenta el riesgo de accesos no autorizados o ineficiencias en la validación. Esto se debe a la dependencia del factor humano en la verificación de los documentos físicos, lo cual puede generar errores o falsificaciones, afectando la seguridad general de las instalaciones. Por lo que en un contexto donde la tecnología de autenticación biométrica ha evolucionado significativamente, surge la oportunidad de innovar y modernizar el sistema de ingreso, implementando una solución basada en el uso de huellas dactilares. Esto no solo mejora la eficiencia, sino que también incrementa la seguridad, al eliminar la necesidad de portar una credencia física para ingresar al campus.

### 1.3 Relevancia o justificación

La implementación de un sistema de ingreso biométrico basado en huellas dactilares ofrece varias ventajas que lo convierten en una solución idónea para la Universidad del Cauca:

- **Seguridad Mejorada:** El uso de huellas dactilares, una característica única e intransferible de cada persona, elimina el riesgo de falsificación o pérdida de credenciales de acceso como los carnets.
- **Eficiencia Operativa:** La biometría permite una autenticación rápida y precisa, reduciendo los tiempos de espera en los puntos de acceso, lo que facilita el flujo de personas, especialmente en momentos de alta demanda.
- **Escalabilidad y Modernización:** El sistema propuesto es escalable, lo que significa que puede adaptarse al crecimiento futuro de la universidad en términos de usuarios. Además, posiciona a la Universidad del Cauca como una institución moderna que adopta tecnologías avanzadas para mejorar su gestión operativa y de seguridad.

## 2. REQUERIMIENTOS

A continuación, se detallan los requerimientos funcionales y no funcionales para el sistema de ingreso biométrico basado en huellas dactilares para la Universidad del Cauca:

### 2.1. Requerimientos Funcionales

- ***Captura de Huellas Dactilares:***
  - El sistema debe permitir la captura de huellas dactilares de los usuarios en los puntos de acceso distribuidos en todo el campus.
  - Los sensores de huellas dactilares deben poder capturar imágenes de alta calidad y enviar estos datos al microcontrolador para su posterior transmisión al servidor central.
- ***Autenticación Biométrica***
  - El sistema debe procesar la huella dactilar enviada desde el microcontrolador a un servidor central para realizar la verificación e identificación biométrica mediante un algoritmo de machine learning.
  - El sistema debe permitir la autenticación en muy poco tiempo, garantizando fluidez en los puntos de acceso.
- ***Transmisión de Datos***

- Los microcontroladores (ESP32) deben poder transmitir las imágenes de las huellas dactilares al servidor a través de una red Ethernet.
- El sistema debe ser capaz de enviar y recibir datos de autenticación desde y hacia el servidor en tiempo real.
- **Gestión de Usuarios**
  - El sistema debe contar con una aplicación web que permita registrar nuevos usuarios, capturando y almacenando sus huellas dactilares, junto con otros datos personales, en la base de datos.
  - La aplicación debe permitir la modificación o eliminación de usuarios existentes en el sistema.

- **Monitoreo en Tiempo Real**

La aplicación web debe permitir a los administradores del sistema monitorear en tiempo real las entradas y salidas de los usuarios en los diferentes puntos de acceso del campus.

- **Escalabilidad**

El sistema debe ser escalable para poder manejar el crecimiento de la universidad, permitiendo agregar nuevos puntos de acceso y usuarios sin afectar el rendimiento.

- **Almacenamiento y Gestión de Huellas Dactilares**

El sistema debe almacenar las huellas dactilares de al menos 5,000 usuarios en una base de datos centralizada que permita la búsqueda y comparación eficiente de las huellas.

- **Manejo de Fallas**

El sistema debe gestionar adecuadamente los fallos en la red o la desconexión de los dispositivos. En caso de fallo en la conexión Ethernet, los dispositivos deben intentar reconectarse automáticamente.

## 2.2. Requerimientos No Funcionales

- **Seguridad**
  - El sistema debe garantizar la seguridad de los datos biométricos mediante cifrado tanto en la transmisión como en el almacenamiento de las huellas dactilares.

- Solo personal autorizado debe tener acceso a la base de datos y a la aplicación de escritorio para la gestión de usuarios.
- ***Disponibilidad y Confiabilidad***
  - El sistema debe garantizar una alta disponibilidad (al menos 99.5%) en los puntos de acceso para evitar bloqueos o interrupciones en el flujo de personas.
  - Debe contar con un sistema de respaldo de datos que garantice la integridad de la información en caso de fallo del servidor.
- ***Compatibilidad***

La aplicación web debe ser compatible con los navegadores más usados.
- ***Facilidad de Uso***
  - La interfaz de la aplicación de escritorio debe ser intuitiva y fácil de usar, permitiendo a los administradores registrar y monitorear usuarios sin conocimientos técnicos avanzados.
  - La experiencia de usuario en los puntos de acceso debe ser fluida y sencilla, sin requerir acciones complejas por parte de los usuarios.

### **2.3. Requerimientos Legales y Normativos**

- El sistema debe cumplir con las normativas de protección de datos, como lo es la Ley de Protección de Datos Personales (Ley 1581 de 2012 de Colombia), asegurando que los datos biométricos y personales de los usuarios estén debidamente protegidos y almacenados de manera segura.
- Los usuarios deben estar informados y dar su consentimiento para el uso de sus datos biométricos en el sistema.

## **3. ARQUITECTURA**

### **3.1 Hardware**

El sistema de ingreso biométrico está compuesto por varios componentes de hardware distribuidos a lo largo del campus de la Universidad del Cauca. Estos componentes se encargan de capturar, procesar y transmitir la información

biométrica (huellas dactilares) de los usuarios hacia un servidor central para su validación. A continuación, se describe la arquitectura de hardware propuesta.

### **3.1.1. Puntos de Acceso Biométrico**

Cada punto de acceso del campus estará compuesto por los siguientes elementos:

#### **3.1.1.1. Sensor de huella dactilar capacitivo con interfaz de comunicación I2C o UART**

- *Función:* El sensor de huellas dactilares captura la imagen de la huella del usuario cuando éste coloca su dedo sobre el lector. Utiliza tecnología capacitiva para obtener una imagen precisa de la huella.
- *Comunicación:* El sensor se comunica con el microcontrolador a través de UART o I2C, dependiendo del modelo utilizado.
- *Relevancia:* Los sensores capacitivos garantizan una captura precisa y rápida de las huellas, lo que es crucial para la eficiencia del sistema en puntos de alto tráfico.

#### **3.1.1.2. Microcontrolador WT32-ETH01 con Ethernet Integrado**

- *Función:* Este microcontrolador es el núcleo de control en cada punto de acceso. Se encarga de recibir la imagen de la huella dactilar desde el sensor y enviarla al servidor central mediante la red Ethernet.
- *Conectividad:* El WT32-ETH01 incluye un puerto Ethernet integrado, eliminando la necesidad de módulos adicionales y garantizando una transmisión rápida y confiable de los datos.
- *Características:*
  - Procesador basado en el ESP32, con doble núcleo para manejar múltiples tareas.
  - Memoria RAM y flash adecuadas para almacenar temporalmente las imágenes de huellas antes de enviarlas al servidor.



- Interfaz UART e I2C para comunicarse con el sensor de huellas dactilares y Ethernet para la transmisión de datos.

#### 3.1.1.3. Indicador LED

- Función: Proporciona retroalimentación visual al usuario sobre el estado de la autenticación. El LED se ilumina en verde si la huella dactilar es aceptada, y en rojo si es rechazada.
- Interfaz: El microcontrolador WT32-ETH01 controla el LED mediante pines GPIO, emitiendo señales para encender o apagar el LED en función de los resultados de la autenticación.

### 3.1.2. Servidor Central

- Función: El servidor central es responsable de recibir los datos de huellas dactilares desde los puntos de acceso, procesar las huellas mediante un algoritmo de machine learning, y emitir una respuesta de autenticación (permitir o denegar el acceso).
- Características Requeridas:
  - Procesador: Un procesador multi-núcleo, con al menos 8 a 12 núcleos, para manejar múltiples solicitudes de autenticación en paralelo.
  - Memoria RAM: Se recomienda 32GB de RAM o más, para garantizar un procesamiento fluido y evitar cuellos de botella cuando haya picos de solicitudes simultáneas. La memoria RAM se utilizará para almacenar temporalmente los datos de las huellas dactilares en proceso, así como para manejar los algoritmos de machine learning que identifican las huellas.
  - Almacenamiento: Discos SSD de al menos 1TB para almacenar la base de datos de huellas y los registros de acceso.
  - Conectividad: Conectividad Gigabit Ethernet (1Gbps). La transmisión de imágenes de huellas dactilares desde varios módulos implica un tráfico constante de datos. La red debe soportar este tráfico sin retrasos, por lo que se recomienda una red Ethernet de 1Gbps para el servidor.

### **3.1.3. Red cableada Ethernet**

- Función: La red Ethernet interconecta todos los puntos de acceso biométrico con el servidor central. La transmisión de los datos de huellas se realiza de manera rápida y estable a través de esta red.
- Velocidad: Se recomienda una red de al menos 1Gbps para garantizar que los datos se transmitan sin demoras.

### **3.1.4. Computadora para la página web de administración**

- Función: Los administradores del sistema utilizarán una computadora de escritorio o portátil conectada a la red local para monitorear los puntos de acceso, gestionar los usuarios, y realizar registros de nuevas huellas dactilares.
- Requerimientos mínimos de Hardware:
  - Procesador: Intel i3 de 8<sup>th</sup> generación o equivalente.
  - Memoria RAM: 4GB para ejecutar la página web de monitoreo y registro
  - Tener un navegador reconocido instalado, como Chrome o Microsoft Edge
  - Conectividad: Puerto Ethernet o conectividad Wi-Fi para acceder al servidor central y la base de datos.

## **3.2 Software**

El software del sistema de control de acceso biométrico para la Universidad del Cauca está diseñado para integrar eficientemente los componentes de hardware y proporcionar una gestión robusta y segura del acceso al campus. Esta integración del software se implementará con diferentes componentes para lograr el funcionamiento requerido.

### **3.2.1 Plataforma Web**

La plataforma web actuará como la interfaz principal para los administradores podrán monitorear en tiempo real el flujo de personas, incluyendo entradas y salidas en los diversos puntos de acceso del campus, gracias a la conexión continua con la base de datos. Además, la interfaz de usuario debe ser intuitiva y de fácil uso para los administradores, minimizando la necesidad de conocimientos técnicos avanzados y permitiendo una gestión eficaz.

### **3.2.2 La base de datos**

Esta desempeñará un papel crucial al almacenar toda la información relacionada con los accesos y salidas de los usuarios, así como sus datos biométricos. Esta base de datos debe ser capaz de gestionar y almacenar de manera segura la información de huellas dactilares de al menos 5.000 usuarios, asegurando la integridad y privacidad de los datos mediante cifrado tanto en tránsito como en reposo. El sistema de backend procesará las imágenes de huellas dactilares enviadas desde los microcontroladores ubicados en los puntos de acceso, utilizando algoritmos avanzados de aprendizaje automático para la verificación biométrica. La solución debe garantizar una alta disponibilidad del servicio y debe ser compatible con los navegadores web más comunes para asegurar una accesibilidad amplia.

## 4. CASOS DE USO (HISTORIAS DE USUARIO)

### 4.1 Diagrama de casos de uso inmerso en un sistema institucional como la Universidad del Cauca

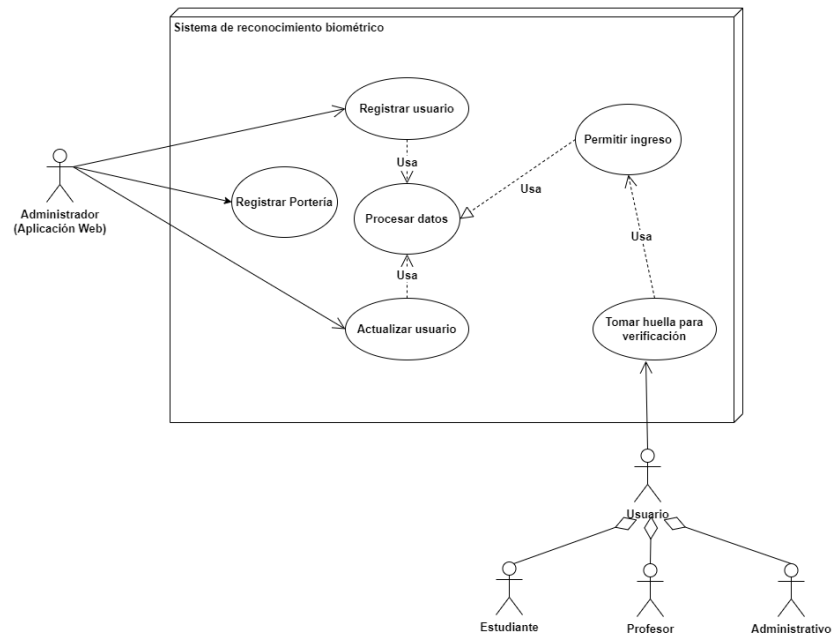


Figura 1. Diagrama de casos de uso del sistema

### 4.2 Descripción extendida

Identificador (ID) de la historia	HU1
Iniciador	Usuario (Estudiante, Docente, Administrativo, etc.)
Título	Verificación de Huella para Ingreso
Propósito	Validar la huella dactilar del usuario para permitir el acceso al campus universitario de manera segura y rápida.
Resumen	Como usuario de la universidad, necesito poder verificar mi identidad utilizando mi huella dactilar en los puntos de acceso del campus, para ingresar de forma eficiente y segura sin necesidad de una credencial física.
Flujo principal	<p>El usuario se acerca a un punto de acceso con un lector de huellas dactilares.</p> <p>El usuario coloca su dedo en el sensor de huellas.</p> <p>El sistema captura la huella y envía la información al servidor central para su verificación.</p> <p>Si la huella es validada correctamente, el LED se enciende en verde, indicando que el acceso ha sido autorizado.</p> <p>La puerta de acceso se desbloquea, permitiendo al usuario ingresar al campus.</p> <p>Si la huella no es reconocida o es incorrecta, el LED se enciende en rojo, indicando que el acceso ha sido denegado y la puerta permanece bloqueada.</p>

Identificador (ID) de la historia	HU2
Iniciador	Administrador del sistema
Título	Registro de Usuario
Propósito	Registrar un nuevo usuario en el sistema de control de acceso biométrico con sus datos personales y su huella dactilar.
Resumen	Como administrador del sistema, necesito registrar nuevos usuarios capturando sus huellas dactilares y datos personales en la base de datos, para permitirles el acceso al campus universitario.
Flujo principal	<p>El administrador inicia sesión en la aplicación web del sistema de control de acceso. Accede a la interfaz de registro de usuarios.</p> <p>Introduce los datos personales del nuevo usuario (nombre, identificación, etc.).</p> <p>Captura la huella dactilar del usuario utilizando un lector de huellas.</p> <p>Guarda la información en la base de datos central.</p> <p>La huella dactilar y los datos personales del usuario se almacenan de forma segura en la base de datos, permitiendo su autenticación en los puntos de acceso.</p>

Identificador (ID) de la historia	HU3
Iniciador	Administrador del sistema
Título	Registro de Portería
Propósito	Registrar y configurar un nuevo punto de acceso (portería) en el sistema para la autenticación biométrica.
Resumen	Como administrador del sistema, necesito registrar y configurar nuevas porterías en el sistema de control de acceso, para ampliar la cobertura de autenticación biométrica en el campus universitario.
Flujo principal	<p>El administrador inicia sesión en la aplicación web del sistema de control de acceso. Accede a la interfaz de gestión de puntos de acceso.</p> <p>Introduce los datos del nuevo punto de acceso (ubicación, identificación de hardware, etc.).</p> <p>Configura la comunicación con el microcontrolador y el lector de huellas del nuevo punto de acceso.</p> <p>Guarda la información y el nuevo punto de acceso queda registrado en el sistema, listo para operar.</p>

Identificador (ID) de la historia	HU4
Iniciador	Administrador del sistema
Título	Actualización del sistema
Propósito	Modificar la información personal o biométrica de un usuario registrado en el sistema.
Resumen	Como administrador del sistema, necesito actualizar los datos personales o la huella dactilar de los usuarios existentes en el sistema, para mantener la información al día y garantizar el acceso seguro al campus.
Flujo principal	El administrador inicia sesión en la aplicación web del sistema de control de acceso. Accede a la interfaz de gestión de usuarios. Busca al usuario por su identificación o nombre. Modifica los datos personales o vuelve a capturar la huella dactilar del usuario. Guarda los cambios en la base de datos. La información actualizada se almacena de forma segura en la base de datos central.

Identificador (ID) de la historia	HU5
Iniciador	Administrador del sistema
Título	Generación de Reportes de Acceso
Propósito	Generar reportes de accesos de usuarios en determinados periodos de tiempo.
Resumen	Como administrador del sistema, necesito generar reportes de accesos diarios, semanales, o mensuales, para monitorear la actividad en el campus.
Flujo principal	El administrador accede al sistema de generación de reportes. Selecciona el rango de fechas para el reporte. El sistema muestra los registros de accesos para el periodo seleccionado. El administrador puede exportar el reporte en diferentes formatos (PDF, Excel, etc.).

Identificador (ID) de la historia	HU6
Iniciador	Administrador del sistema
Título	Eliminación de Usuario
Propósito	Eliminar la información de un usuario del sistema cuando ya no sea necesario que tenga acceso.
Resumen	Como administrador del sistema, necesito eliminar usuarios que ya no requieren acceso al campus universitario, para mantener la base de datos actualizada y segura.
Flujo principal	El administrador accede al sistema de gestión de acceso. Busca al usuario por identificación. Selecciona la opción de eliminar. Confirma la eliminación del usuario.

### 4.3 Mockups historias de usuario

HU2: ingreso del administrador

The mockup shows a login interface with a dark blue background. In the top left corner is the University of Cauca logo and name. In the top right corner, it says 'Sistema biometrico para el ingreso al campus de Unicauca'. The main heading is 'INICIAR SESION'. Below it are two input fields labeled 'Usuario' and 'Contraseña', followed by a green 'ENTRAR' button. On the right side, there is a large white fingerprint icon.

Figura 2. Inicio de sesión

The mockup shows an administrator menu interface with a dark blue background. In the top left corner is the University of Cauca logo and name. In the top right corner, it says 'Sistema biometrico para el ingreso al campus de Unicauca'. The main heading is 'MENU ADMINISTRADOR'. Below it are five buttons: 'REGISTRO DE USUARIO', 'REGISTRO DE PORTERIA', 'ELIMINAR USUARIOS', 'ACTUALIZACION DE DATOS', and 'GENERACION DE REPORTES'. On the right side, there is a large white fingerprint icon. In the bottom left corner, it displays 'Usuario: ADMIN' and 'Fecha de ingreso: xx/xx/xxxx'.

Figura 3. Menú administrador



Universidad

del Cauca

Sistema biometrico

para el ingreso al

campus de Unicauca

REGISTRO DE USUARIO

NOMBRE

CARGO

PROGRAMA

Usuario: ADMIN

Fecha de ingreso:

xx/xx/xxxx



Figura 4. Registro de usuario.

HU3:



Universidad

del Cauca

Sistema biometrico

para el ingreso al

campus de Unicauca

REGISTRO DE PORTERIA

FACULTAD

PUERTA No

UBICACION

Usuario: ADMIN


Fecha de ingreso:

xx/xx/xxxx



Figura 5. Registro de portería.

HU4:



Universidad

del Cauca

Sistema biometrico

para el ingreso al

campus de Unicauca

ACTUALIZACION DEL SISTEMA

USUARIOS REGISTRADOS

Usuario: ADMIN

Fecha de ingreso:

xx/xx/xxxx





Figura 6. Actualización datos del sistema.

HU5:

The screenshot shows a web interface for the Universidad del Cauca. At the top left is the university's logo and name. At the top right, it says 'Sistema biometrico para el ingreso al campus de Unicauca'. The main title is 'GENERACION DE REPORTES'. Below this, there are four columns of input fields: 'USUARIO', 'FECHA', 'HORA DE INGRESO', and 'HORA DE SALIDA'. Each column has four empty rounded rectangular boxes for data entry. To the right of these fields is a large white fingerprint icon on a dark blue background. At the bottom left, it displays 'Usuario: ADMIN' and 'Fecha de ingreso: xx/xx/xxxx'.

Figura 7. Generación de reportes.

HU6:

The screenshot shows a web interface for the Universidad del Cauca. At the top left is the university's logo and name. At the top right, it says 'Sistema biometrico para el ingreso al campus de Unicauca'. The main title is 'ELIMINACION DE USUARIO'. Below this, there are two columns of input fields: 'USUARIO' and 'FACULTAD'. Each column has three empty rounded rectangular boxes for data entry. To the right of these fields is a large white fingerprint icon on a dark blue background. At the bottom left, it displays 'Usuario: ADMIN' and 'Fecha de ingreso: xx/xx/xxxx'.

Figura 8. Eliminación de usuario.

## 4.4 Diagramas de secuencia

### 4.5.1 Integrante de la institución

El integrante perteneciente a la institución (estudiante, docente, administrativo, etc.) debe colocar su dedo índice (principal) en el dispositivo en la ubicación correcta sobre el lector de huellas dactilares. Si la autenticación es exitosa, se activará un led o señal de retroalimentación para que la persona sepa que puede ingresar, al mismo tiempo, la puerta se desbloquea y permite el acceso al campus (en caso de una autenticación fallida, también se notificará con una señal de retroalimentación y se mantendrá el bloqueo).

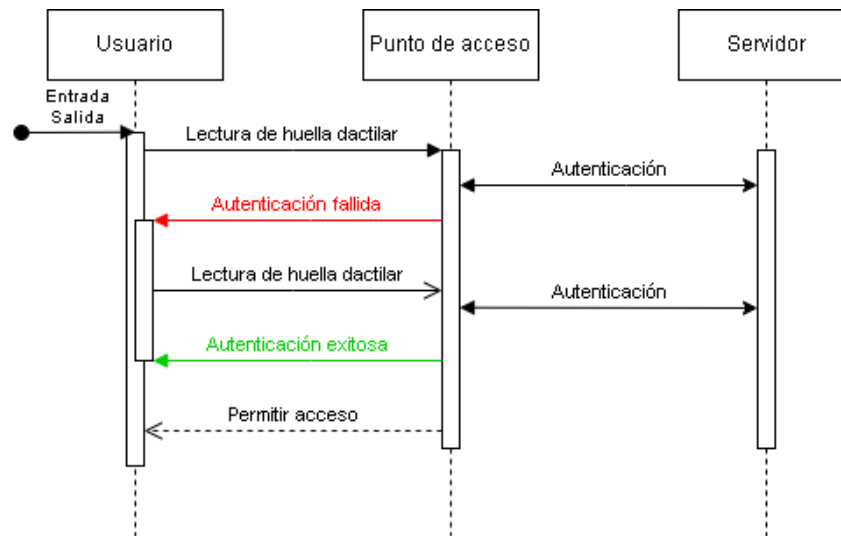


Figura 9. Diagrama de secuencia del proceso de usuario en el sistema de acceso

#### 4.5.2 Funcionario administrativo de la institución

Un funcionario de la institución educativa con acceso al aplicativo web del sistema debe realizar el registro de datos biométricos y personales del usuario de la institución educativa, solamente los datos necesarios para identificar correctamente al usuario. Debe contar con un lector de huella dactilar que grabe correctamente las características de la huella, actualizar y guardar los datos, por lo cual, este administrador va a tener acceso a la base de datos, sin embargo, este acceso es limitado a solo observación.

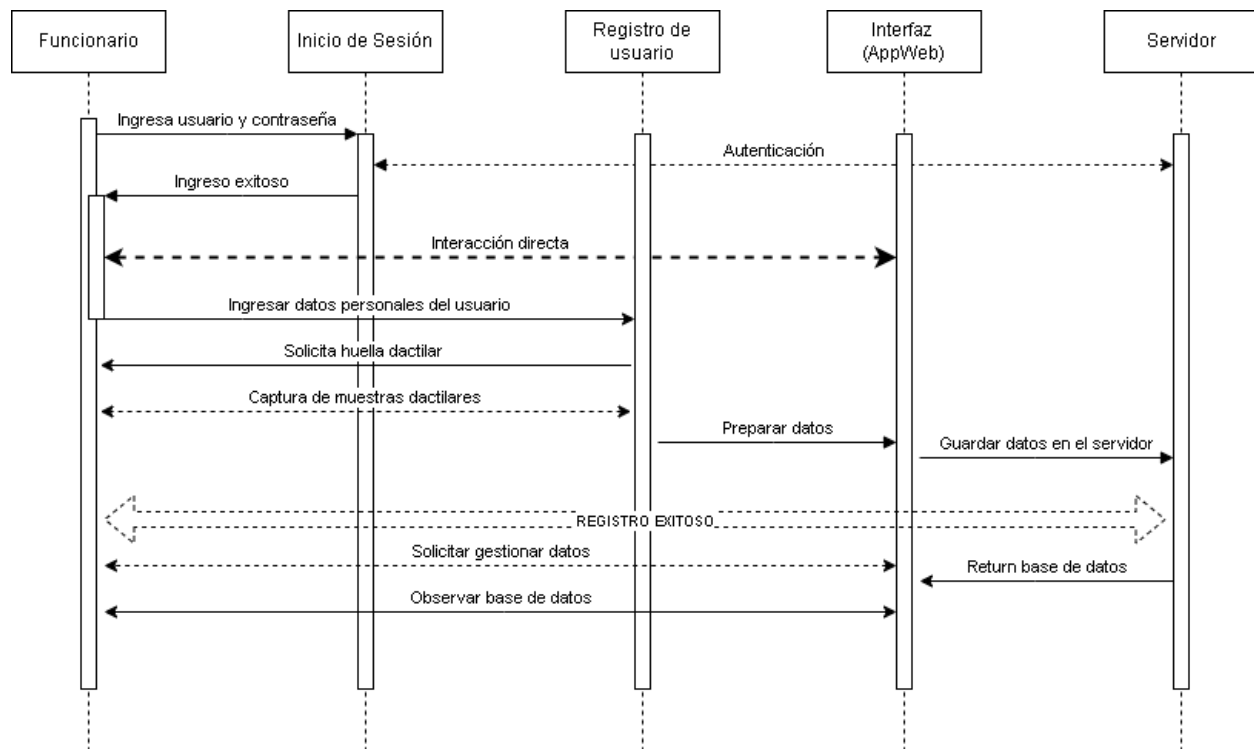


Figura 10. Diagrama de secuencia de los procesos en el aplicativo web del sistema

#### 4.5.3 Sistema de control de acceso

El sistema de control de acceso hace parte de los actores involucrados en el sistema, por lo que se hace necesario realizar un diagrama de secuencia desde el punto de vista del sistema en general más allá de los actores humanos que participan en el proceso. El usuario coloca su dedo en el lector, que extrae las características biométricas y las envía al servidor. El servidor recibe los datos y los compara con las huellas almacenadas en la base de datos. Posteriormente, dependiendo de si la huella coincide o no, el sistema permitirá o denegará el acceso.

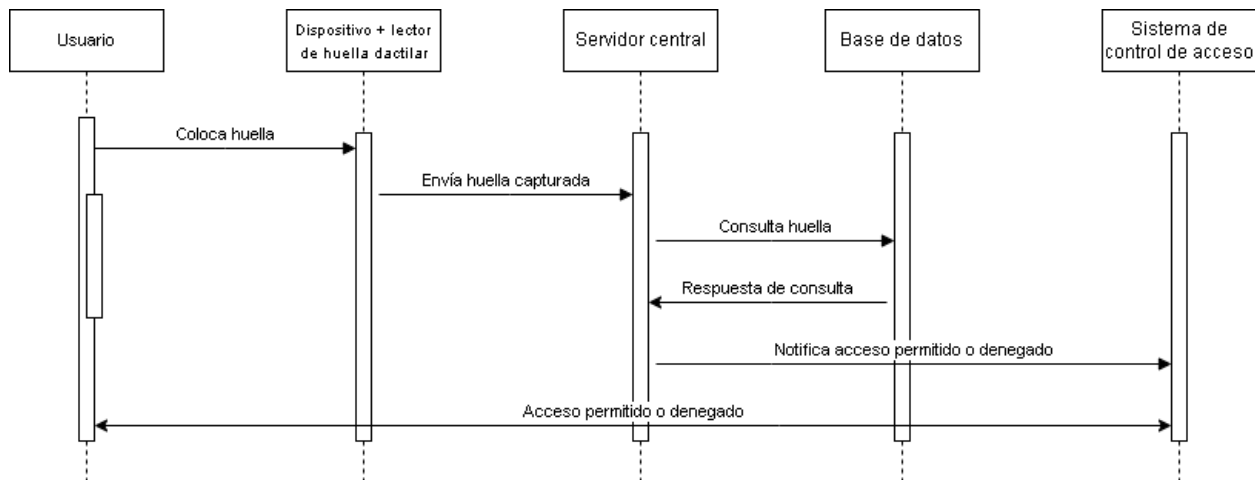


Figura 11. Diagrama de secuencia del proceso del sistema de acceso en general

## 5. ALCANCE DE LOS PROTOTIPOS

### 5.1 Primer prototipo

Constará a nivel software:

- **Interfaz de inicio de sesión** para el administrador del sistema que en este caso sería un funcionario administrativo de la división correspondiente dentro de la institución.
- **Interfaz de registro de datos biométricos y personales** para que el administrador pueda registrar ordenadamente todas las huellas (simuladas) y datos que identifiquen a cada integrante de la institución.
- **Interfaz de administrador** que permite la visualización de los accesos permitidos y denegados (simulados), así como el estado de los lectores de huella instalados.
- **Diseño de la base de datos** y configuración inicial para almacenar las plantillas de huellas y los datos de los usuarios.

#### Funcionalidad:

- El aplicativo deberá funcionar sin el uso del lector de huellas por el momento, debido al tiempo que se necesita para obtener los dispositivos hardware del sistema, por lo que en el primer prototipo solamente se verán avances con funcionalidad solamente de software.
- Estructura de la base de datos para registrar usuarios y guardar las huellas dactilares (en forma de imágenes o templates).
- Conexión a un servidor de pruebas (local) para simular la autenticación de datos.

## 5.2 Segundo prototipo

Constará a nivel software y hardware:

- **Configuración y programación de los lectores de huellas dactilares:** Conectar y configurar los lectores para capturar huellas reales.
- **Implementación del microcontrolador:** Programación para comunicarse con los lectores de huellas y enviar datos al servidor central vía Ethernet.
- **Ajustes para captura real de huellas:** Modificar la lógica de captura y comparación para utilizar datos reales de los lectores.
- **Captura y registro de huellas dactilares reales:** Registrar huellas de usuarios en el sistema utilizando los lectores físicos.

### Funcionalidad:

- Permitir a los usuarios registrar sus huellas dactilares en el sistema a través de los lectores.
- Los usuarios podrán autenticarse en el punto de acceso y el sistema procesará las huellas en el servidor central.
- Registro y visualización de accesos reales en el sistema, incluyendo fecha, hora y punto de acceso.
- Mejoras en el rendimiento y la seguridad basadas en las pruebas realizadas con hardware real.

## 5.3 Tercer prototipo

Integración completa del sistema, constará a nivel software y hardware:

- **Sistema funcional con hardware y software integrados:** El lector de huellas y el microcontrolador estarán completamente operativos, con una interfaz fácil de usar para la gestión de usuarios y autenticaciones.
- **Optimización del sistema para uso diario:** Refinar el código y la interfaz para mejorar el rendimiento y la fiabilidad del sistema.
- **Pruebas de campo (aproximación):** El sistema se probará en un entorno real para asegurar su funcionamiento en condiciones cotidianas.
- **Optimización del tiempo de respuesta:** Asegurar que el sistema funcione de manera fluida, con un tiempo de respuesta óptimo para la autenticación.

### Funcionalidad:

- Los usuarios podrán autenticarse de manera rápida y segura, accediendo a las áreas permitidas según el sistema.

- Implementar un sistema de monitoreo básico para registrar los intentos de acceso, y generar reportes simples de actividad.
- El sistema estará diseñado de manera modular, permitiendo que se agreguen más lectores de huellas en diferentes puntos de acceso del campus si se decide escalar el proyecto.

## 5.4 Entrega final

- **Sistema completamente funcional y operativo:** Entrega de un prototipo completamente funcional, con integración de hardware y software.
- **Documentación técnica y de usuario:** Se entregará documentación técnica sobre la implementación para la operación básica del sistema.
- **Preparación para escalabilidad:** El sistema estará listo para ser escalado en el futuro, si se decide implementar más lectores de huellas y mejorar la infraestructura.

## 6. AVANCE EN LA DOCUMENTACIÓN DE LOS DISPOSITIVOS HARDWARE

A continuación, se detalla un avance en la información adquirida acerca de los dispositivos hardware a implementar.

### 6.1. Sensor dactilar capacitivo Simlug(bpnwmrd81u)

Después de una búsqueda exhaustiva se optó por usar este sensor que se observa en la Figura 12, ya que posee muchas características que van en pro del proyecto.

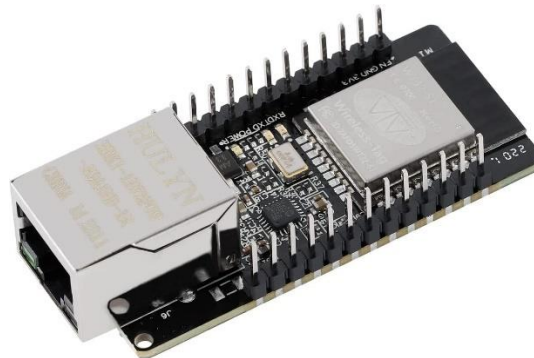


Figura 12. Sensor dactilar capacitivo Simlug(bpnwmrd81u)

### **Características:**

- Comunicación RS232 compatible con la interfaz UART del microcontrolador WT32-ETH01
- Voltaje alimentación: 3.3V. Con esto se elimina la necesidad de un regulador de voltaje ya que el microcontrolador posee este mismo voltaje de operación. También cabe recalcar que el sensor al tener 3.3V en su interfaz serial RS232, su señal de transmisión y recepción estará dentro del rango que el WT32-ETH01 puede manejar directamente, por lo que tampoco sería necesario un adaptador de niveles de voltaje.
- Sensor Capacitivo: Este es uno de los aspectos más importantes que se necesitaba para el proyecto, debido a que estos sensores son mas robustos y resistentes a condiciones de suciedad, humedad y entre otros. Lo cual lo hace idóneo para situarlo en un sitio de alta congestión como lo es una portería de la Universidad del Cauca.
- Costo: 27.5 dólares. Entre tantas opciones que existen en el mercado, esta referencia es bastante accesible sobre todo para la creación de un prototipo a pequeña escala. Cabe recalcar que existen sensores mucho mejor que este, pero de igual forma su precio es proporcional a esto, por lo que para la implementación real del proyecto lo ideal sería adquirir sensores de mayor calidad y duración.

## **6.2. Microcontrolador WT32-ETH01**



*Figura 13. Microcontrolador WT32-ETH01*

El microcontrolador WT32-ETH01, ilustrado en la Figura 13, destaca por combinar las capacidades del procesador ESP32 con un puerto Ethernet integrado, lo que lo convierte en una opción altamente versátil para este proyecto. Entre sus características más relevantes se encuentran:

- Protocolos de comunicación: TCP, UDP, IP, DHCP. Gracias a estos protocolos integrados, el WT32-ETH01 facilita la comunicación con el servidor de manera óptima. Por ejemplo, a través del protocolo DHCP, el microcontrolador puede obtener automáticamente su dirección IP, y mediante TCP o UDP, establecerse como cliente para interactuar con otros dispositivos en la red. Este conjunto de protocolos permite que el microcontrolador funcione de manera similar a una PC, ya que puede conectarse a la red y transmitir datos al servidor de forma eficiente, tanto en redes LAN como WAN, utilizando los protocolos necesarios para la transmisión y recepción de datos.
- Comunicación UART. Esta interfaz es esencial para la comunicación directa con el sensor de huellas dactilares, garantizando un flujo de datos eficiente entre el sensor y el microcontrolador.

## 7. BIBLIOGRAFIA

- (<https://support.microsoft.com/es-es/topic/crear-un-diagrama-de-casos-de-uso-uml-92cc948d-fc74-466c-9457-e82d62ee1298#:~:text=Los%20diagramas%20de%20casos%20de,s.f.>)
- <https://en.wireless-tag.com/product-item-2.html>