

UNIVERSIDAD DIEGO PORTALES



FACULTAD DE INGENIERÍA Y CIENCIAS



---

## PROYECTOS TICS I: INFORME IV

---

Estudiantes:

Mateo Solari, Magdalena Correa, Jose Avello, Pablo Muñoz

Profesor:

Miguel Carrasco

# Índice

<b>1. Introducción</b>	<b>3</b>
<b>2. Grupo y Roles</b>	<b>4</b>
<b>3. Descripción del problema</b>	<b>4</b>
<b>4. Motivación</b>	<b>5</b>
<b>5. Objetivos</b>	<b>5</b>
5.1. Objetivo General . . . . .	5
5.2. Objetivos Específicos . . . . .	5
<b>6. Cumplimiento de los Objetivos del Proyecto</b>	<b>6</b>
<b>7. Estado del arte</b>	<b>6</b>
<b>8. Solución</b>	<b>8</b>
8.1. Robo sin que la víctima lo note o de forma repentina . . . . .	8
8.2. Robo bajo amenaza . . . . .	8
8.3. Zonas seguras . . . . .	9
<b>9. Idea del artefacto</b>	<b>9</b>
9.1. Diseño preliminar . . . . .	10
<b>10. Descripción del Producto Final</b>	<b>11</b>
10.1. Hardware . . . . .	12
10.2. Funcionamiento . . . . .	12
<b>11. Instrucciones de uso</b>	<b>14</b>
11.1. Activación y emparejamiento con la aplicación móvil: . . . . .	14
11.2. Configuración de zonas seguras: . . . . .	14
11.3. Uso de la pulsera en situaciones de emergencia: . . . . .	14
11.4. Personalización de las alertas: . . . . .	14
11.5. Carga y mantenimiento: . . . . .	14
11.6. Consejos adicionales: . . . . .	15
<b>12. Riesgos</b>	<b>15</b>
12.1. Riesgos Técnicos . . . . .	15
12.2. Riesgos de Desarrollo . . . . .	15
12.3. Riesgos de Recursos . . . . .	15
12.4. Riesgos de Uso e Implementación . . . . .	15
<b>13. Plan de mitigación</b>	<b>16</b>
<b>14. Modelo de negocios</b>	<b>17</b>

<b>15. Cliente objetivo</b>	<b>18</b>
15.1. Perfil del Cliente Objetivo . . . . .	18
15.2. Entrevista a Contraparte y Conclusiones . . . . .	19
15.2.1. Resultados de la Entrevista . . . . .	19
15.2.2. Conclusiones y Ajustes al Proyecto . . . . .	19
15.3. Resultados Segunda Entrevista . . . . .	20
<b>16. Requerimientos del Sistema</b>	<b>21</b>
16.1. Requerimientos Funcionales (RF) . . . . .	21
16.2. Requerimientos No Funcionales (RNF) . . . . .	22
<b>17. Diseño del circuito</b>	<b>23</b>
17.1. Actualización del Modelo Gráfico con Diseño e Integración de Componentes . . . . .	24
<b>18. Plan de trabajo (Modificado)</b>	<b>26</b>
<b>19. Decisiones Tecnológicas</b>	<b>32</b>
<b>20. Documentación de Funcionalidades</b>	<b>33</b>
20.1. Actores Principales . . . . .	33
20.2. Tabla de Casos de Uso . . . . .	34
20.3. Lógica de Funcionalidades (Flujos de Actividades) . . . . .	34
20.3.1. Flujo 1: Lógica de Zonas Seguras (CU-02 y RF7) . . . . .	34
20.3.2. Flujo 2: Lógica de Robo Repentino (CU-03 / RF5, RF6) . . . . .	35
20.3.3. Flujo 3: Lógica de Robo Bajo Amenaza (CU-04 / RF2, RF3, RF4) . . . . .	36
<b>21. Modelo de Datos e Interfaces de Usuario</b>	<b>38</b>
21.1. Modelo de Datos (PostgreSQL) . . . . .	38
21.2. Interfaces de Usuario (UI) . . . . .	39
<b>22. Sistema de Reportería</b>	<b>43</b>
22.1. Variables monitoreadas . . . . .	43
22.2. Estructura de la reportería . . . . .	43
22.3. Ejemplo de registro real . . . . .	44
22.4. Triggers del sistema . . . . .	44
<b>23. Plan de Pruebas</b>	<b>44</b>
23.1. Pruebas Unitarias de Componentes . . . . .	44
23.2. Pruebas de Integración . . . . .	45
23.3. Pruebas Funcionales (Casos de Uso) . . . . .	45
<b>24. Historia de Usuario y Secuencia de Eventos</b>	<b>46</b>
<b>25. Conclusión</b>	<b>47</b>

## 1. Introducción

El presente informe aborda la propuesta de un proyecto llamado "**Ticprev**"(Tecnologías de la Información y las Comunicaciones en prevención) para solucionar una problemática cada vez más recurrente en la sociedad actual, la inseguridad personal y la exposición a delitos de robo de teléfonos celulares y asaltos. Esta situación no solo afecta de forma física y emocional de las personas, sino que también genera un temor y desconfianza en los espacios públicos. De este modo, se hace necesario el desarrollo de soluciones que otorguen mayor protección, apoyo y una forma de frustrar situaciones criticas.

En Chile, la delincuencia asociada al robo de celulares se ha convertido en un problema de gran magnitud. De acuerdo de datos recientes, cada año se roban cerca de 500 mil celulares en Chile (Policía de Investigaciones de Chile, 2025), lo que refleja no solo una perdida económica significativa, sino también una exposición constante para los ciudadanos. Esta situación en concreto pone la necesidad de desarrollar soluciones que contribuyan a la sociedad.

Frente a esta situación el presente proyecto propone una Pulsera de Seguridad, la cual esta equipado con un sensor encargado de medir pulsaciones y oxígeno en la sangre (**MAX30102**), y otro que detecte los movimientos bruscos (**Módulo GY-521 (MPU-6050)**). De esta forma el sistema se conecta al teléfono móvil mediante bluetooth y otorga un tiempo estándar de 1 minuto para ingresar un pin en caso de desconexión, de no hacerlo, se activara una alarma sonora. Asimismo, este podrá configurarse en zonas seguras con Wifi, detectar alejamiento del celular e incluso hacer una llamada de emergencia a un contacto cercano ante un intento de asalto.

Este informe presenta una visión integral del proyecto, que incluye la descripción del problema, la motivación, los objetivos, la conformación del grupo y sus roles, estado de arte, la solución propuesta, la idea del artefacto y diseño preliminar, así como los riesgo identificados y el plan de trabajo.

## 2. Grupo y Roles

- **Mateo Solari:** Líder y coordinador del proyecto, ademas de responsable del desarrollo de software. Su asignación en este ámbito se basa en sus conocimientos en la programación de aplicaciones móviles y tecnologías emergentes.
- **Magdalena Correa:** Encargada del diseño y modelo del proyecto. Esta decisión se fundamenta en su experiencia en modelado 3D, además de sus destacadas habilidades en la creación y estructuración de proyectos.
- **José Avello:** Uno de los responsables del desarrollo de hardware del proyecto y encargado del funcionamiento óptimo del mismo. Se le asignó este rol debido a su gran desempeño en este campo en proyectos previos.
- **Pablo Muñoz:** Uno de los responsables del desarrollo de hardware del proyecto y encargado de la conexión entre los dispositivos. Se le asignó este rol debido a sus conocimientos de electrónica y gran entusiasmo por el área.

## 3. Descripción del problema

La seguridad personal se ha convertido en una de las principales preocupaciones de la vida diaria, especialmente en situaciones tanto en espacios públicos como privados donde concurren estos tipos de delitos. Los robos y los asaltos no solo son pérdidas materiales, sino que generan un fuerte impacto emocional a las víctimas, aumentando la sensación de vulnerabilidad.

La creciente sensación de inseguridad ha aumentado en un 80 %, lo que indica que gran parte de la población cree que el crimen organizado aumentó en los últimos 6 meses, mientras que un 64 % afirma haber vivido en situaciones que lo hicieron sentir como una amenaza real en su vida diaria. Esta preocupación se ha estado reflejando en lugares como la calle, plazas o parques y el transporte público. Incluso la percepción de inseguridad se ha presenciado en hogares donde se ha detectado este aumento significativo de la vulnerabilidad, pasando de 43,7 % en octubre de 2024 a 49,2 % en marzo de 2025 (Universidad San Sebastián, 2025).

En caso específico de los celulares, más de 72 mil dispositivos fueron bloqueados tras ser robados durante el primer semestre de 2024 (La Tercera, 2024). Si bien el bloqueo contribuye como una medida de inutilizar después del delito, no permite frustrar el robo en el momento del mismo asalto. Estos resultados han demostrado que la inseguridad no solo afecta en la vida pública, sino que también en la vida privada, lo que confirma la necesidad de desarrollar soluciones innovadoras que fortalezcan la protección del individuo y la tranquilidad de la vida del ciudadano, lo que fundamenta la propuesta del presente proyecto.

Frente a ese escenario, se planteó el desarrollo de una pulsera de seguridad inteligente denominado **TicPrev**, el cual permita al usuario contar con un mecanismo de protección personal. La implementación de este sistema busca no solo responder ante un momento de riesgo, sino también contribuir a la confianza en los usuarios.

## 4. Motivación

La motivación de nuestro grupo para desarrollar este dispositivo surge de la creciente preocupación por la seguridad personal en los espacios públicos, donde los robos y asaltos son cada vez más frecuentes. En este contexto, consideramos fundamental aprovechar los avances tecnológicos en sensores biométricos y comunicación inalámbrica para ofrecer una herramienta que contribuya a la protección de las personas.

Nuestro interés se centra en diseñar un artefacto que no solo actúe como un medio de disuasión frente a la acción delictiva, sino que también brinde al usuario una mayor sensación de confianza y tranquilidad en su vida cotidiana. Creemos que un dispositivo de este tipo puede marcar la diferencia al generar alertas tempranas, dificultar el accionar del delincuente y establecer una línea de comunicación rápida en caso de emergencia.

De esta forma, nuestra motivación combina la preocupación por la seguridad ciudadana con el deseo de aplicar nuestros conocimientos en tecnologías de la información y comunicación para crear una solución innovadora con impacto social positivo.

## 5. Objetivos

### 5.1. Objetivo General

Desarrollar una pulsera inteligente que permita prevenir situaciones de robo o asalto, aumentando las probabilidades de frustrar la acción delictiva y entregando al usuario una mayor sensación de seguridad.

### 5.2. Objetivos Específicos

- Diseñar e implementar un sistema electrónico basado en el micro controlador **ESP32**, que integre sensores de ritmo cardíaco y movimiento para detectar alteraciones vinculadas a situaciones de peligro.
- Desarrollar una aplicación móvil conectada por bluetooth que permita gestionar la configuración de la pulsera, las zonas seguras y los contactos de emergencia.
- Programar mecanismo de alerta automática, como la activación de alarmas sonoras, vibración y ubicación al detectar desconexión o forcejeo.
- Evaluar el desempeño del sistema mediante pruebas que midan hacia la precisión de detección de forcejeo, aumento cardíaco y la estabilidad de la conexión Bluetooth.
- Optimizar el interfaz del usuario y el diseño de la pulsera, priorizando la comodidad y su funcionamiento.

## 6. Cumplimiento de los Objetivos del Proyecto

A continuación se detalla cómo el proyecto da cumplimiento a cada uno de los objetivos definidos en la planificación inicial.

### Objetivo General

Desarrollar un sistema portátil capaz de detectar situaciones de robo repentino o robo bajo amenaza, y alertar automáticamente a un contacto de emergencia.

**Cumplimiento:** El sistema implementado combina sensores de movimiento y ritmo cardíaco, junto con una aplicación móvil que recibe y gestiona alertas. La pulsera permite detectar movimientos bruscos o aumentos de estrés fisiológico, y envía notificaciones a la aplicación, cumpliendo el propósito central del proyecto.

### Objetivos Específicos

- **Detectar movimientos asociados a una acción de robo.** Cumplido mediante el uso del acelerómetro MPU6050 y la lógica de reconocimiento de patrones implementada durante las pruebas.
- **Medir variaciones fisiológicas que indiquen amenaza bajo coerción.** Cumplido gracias al sensor MAX30102, que permite obtener la frecuencia cardíaca en tiempo real y detectar anomalías asociadas a estrés.
- **Enviar alertas automáticas a un contacto de emergencia.** La aplicación Android implementada recibe señales desde el ESP32 y notifica al contacto configurado, cumpliendo el objetivo funcional.
- **Construir un prototipo portable y seguro.** Cumplido mediante la integración física de los componentes en una carcasa impresa en 3D, adecuada para uso cotidiano.
- **Registrar y mostrar la evolución de las variables medidas.** La plataforma incorpora mecanismos de registro temporal y visualización en la aplicación móvil, cumpliendo con los requerimientos de reportería definidos.

## 7. Estado del arte

En la actualidad existen diversas soluciones tecnológicas para la seguridad personal, aunque la mayoría de estas soluciones cuentan con limitaciones en cuanto al nivel de automatización y la capacidad de respuestas antes las diversas situaciones de riesgo.



Figura 1: Botón de pánico

Una de las opciones que destacan son los **botones de pánico** (Fig 1), dispositivos portátiles los cuales permiten enviar alertas al presionar manualmente el botón en casos de emergencia. Pero su principal falencia es que requieren de una acción consciente y voluntaria de los usuarios. Lo que usualmente no es posible en un escenario de un asalto o robos con forcejeo.

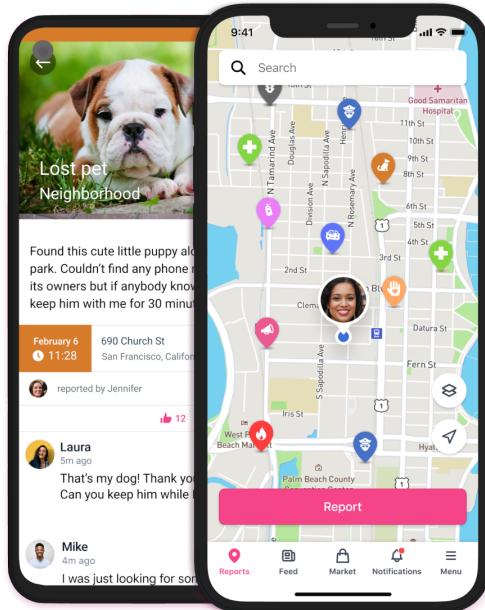


Figura 2: Apps de seguridad

Otra alternativa son las **aplicaciones de seguridad** (Fig 2) las cuales se encuentran disponibles para los teléfonos, como **sosafe** o **Vecino Seguro**. Estas tienen como función principal realizar llamadas o enviar notificaciones a contactos de emergencia. Sin embargo, de la misma forma que los botones de pánico, dependen de una interacción manual de los usuarios y del acceso a los dispositivos móviles.

Finalmente, se encuentran los **Smartwatch/Smartbands** (Fig 3), dispositivos de monitoreo de

salud que integran sensores para la medición de pulsaciones y niveles de oxígeno en sangre. Aunque su enfoque principal esta en la salud y la actividad física no están diseñados específicamente para la seguridad en situaciones de robos o asaltos.



Figura 3: Smartwatch

Las soluciones actuales se enfocan principalmente en el ámbito de la salud o en la emisión de alertas manuales. Ninguna integra de manera simultánea la **biometría**, la **detección automática de forcejeos** y la comunicación inmediata con servicios de emergencia.

## 8. Solución

Para dar solución a el problema anteriormente plateado, se ha decidido crear una pulsera de seguridad capaz de conectarse con el teléfono celular y detectar el aumento de distancia entre ambos o la desconexión total. Destacando la solución a los siguientes dos casos:

### 8.1. Robo sin que la víctima lo note o de forma repentina

Si el dispositivo se aleja de forma sorpresiva del teléfono o se corta su conexión, mediante una vibración en la pulsera enviara, por medio de una aplicación, una notificación al usuario, preguntándole si el alejamiento ha sido accidental y bloqueando las funciones del teléfono. Esta notificación debe ser respondida por medio del ingreso de un PIN. Si este no es colocado en 1 minuto, el teléfono emitirá una fuerte alarma que solo cesará ingresando el PIN anteriormente mencionado. Alertando de este modo la presencia del ladrón tanto al usuario como a las personas alrededor del victimario.

### 8.2. Robo bajo amenaza

En este caso, la activación de una alarma puede ser contraproducente, ya que podría poner nervioso al agresor y en caso de que este posea un arma, llevaría a consecuencias fatales.

Por ello, la pulsera detectaría el forcejeo o la subida cardíaca del usuario, causando una vibración en la pulsera y empezara una cuenta regresiva que duraría cierto tiempo (definido por el usuario) para activar la alarma y enviar la ubicación del móvil a un teléfono de emergencia.

Si el forcejeo ha sido accidental o la subida cardíaca se debe a otros factores, podrá ser desactivado entrando a la aplicación y ingresando el PIN en ella.

### **8.3. Zonas seguras**

Finalmente, para evitar falsos positivos en lugares donde el cliente constantemente se aleja del teléfono celular, como el hogar, trabajo o lugar de estudios. Se podrá ingresar, lo que el equipo a llamado zonas seguras; lugares donde las funcionalidades de alerta del dispositivo estarán desactivadas.

## **9. Idea del artefacto**

La idea inicial del artefacto **Ticprev** se centra en el desarrollo de una pulsera de seguridad enfocada en frustrar el robo de celulares al momento del asalto. Este dispositivo está diseñado específicamente para actuar en momentos de riesgos, activando mecanismo que dificulten el delito como alarmas y llamadas a contactos de emergencia.

## 9.1. Diseño preliminar

El diseño preliminar de la pulsera considera la base para la construcción del prototipo.



Figura 4: Diseño preliminar del TicPrev

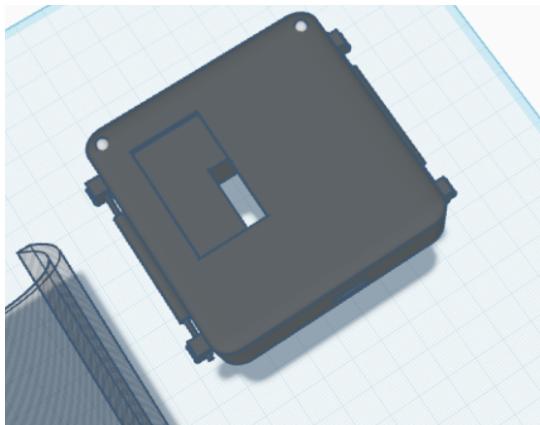


Figura 5: Avance del modelo 3D

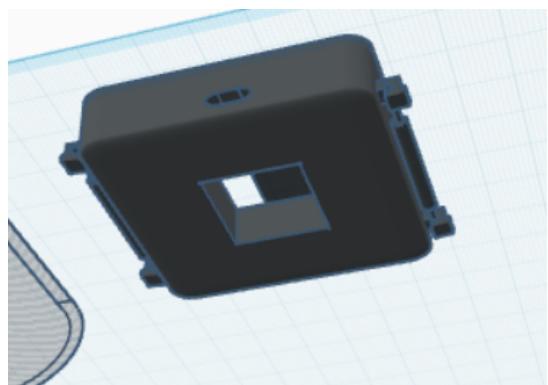


Figura 6: Avance del modelo 3D

La pulsera contiene dos sensores principales: el **MAX30102**, el cual es el encargado de medir las pulsaciones y oxígeno de la sangre, y el sensor **Módulo GY-521 (MPU-6050)**, que integra un acelerómetro y un giroscopio para detectar movimientos bruscos, vibraciones o cambios de orientación. Este sensor permite identificar situaciones de forcejeo o caída, activando alertas ante posibles emergencias.

## 10. Descripción del Producto Final

El sistema desarrollado corresponde a una pulsera inteligente orientada a la seguridad personal, diseñada para reaccionar ante situaciones de robo repentino o robo bajo amenaza. A diferencia del prototipo inicial montado en protoboard, el producto final se define como un artefacto compacto, portable y seguro.

La pulsera incorpora una carcasa fabricada mediante impresión 3D, diseñada para proteger los componentes electrónicos y mantener un tamaño adecuado para el uso cotidiano. El contenedor presenta cavidades internas específicas para el ESP32, el sensor de ritmo cardíaco MAX30102, el acelerómetro MPU6050 y la pantalla OLED, asegurando una distribución estable y una correcta ventilación de calor.

La estructura incluye un sistema de sujeción tipo correa ajustable, permitiendo un uso prolongado sin incomodidad. El diseño garantiza que los sensores mantengan contacto constante con la piel, condición necesaria para la medición de las variables fisiológicas y de movimiento.

El dispositivo responde integralmente al problema planteado: detectar situaciones de riesgo, generar alertas automáticas y transmitir información crítica hacia la aplicación móvil y al contacto de emergencia configurado por el usuario.



Figura 7: Producto final (Vista Frontal).



Figura 8: Producto final (Vista Trasera).

## 10.1. Hardware

En cuanto al hardware, el sistema estará compuesto por los siguientes elementos:

- **ESP-WROOM-32:** Se basa en el microcontrolador ESP32, que ofrece compatibilidad con Wi-Fi, Bluetooth, Ethernet y bajo consumo, todo en un solo chip. Esto funcionara como una unidad de procesamiento y comunicación.
- **Pantalla OLED SSD1306 (0,96”):** Permitirá la visualización e interacción directa con el usuario.
- **Sensor MAX30102:** Es un sensor que combina un oxímetro de pulso y un monitor de frecuencia cardíaca. Es un sensor óptico que mide la absorción de la sangre pulsante a través de un fotodetector después de emitir dos longitudes de onda de luz desde dos LEDs: uno rojo y uno infrarrojo.
- **Sensor Módulo GY-521 (MPU-6050):** Es un módulo que integra un acelerómetro y un giroscopio de tres ejes en un solo chip. El acelerómetro mide la aceleración lineal en los ejes X, Y y Z, mientras que el giroscopio registra la velocidad angular alrededor de esos mismos ejes. Gracias a estas mediciones, el sensor permite detectar inclinaciones, movimientos y rotaciones del dispositivo donde está instalado.
- **Batería polímero de litio con 3.7 V:** Esto permitara suministrar la energía necesaria para el funcionamiento del sistema de manera autónoma.

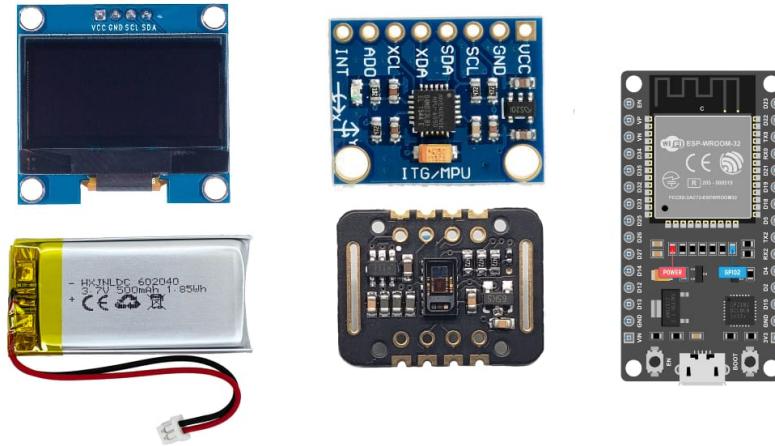


Figura 9: Hardware que estará compuesto.

## 10.2. Funcionamiento

Respecto al funcionamiento del dispositivo, la pulsera se conectará por vía bluetooth al celular. Si la conexión se interrumpe de forma sospechosa, el sistema solicitará el ingreso de un **PIN de**

**seguridad** en la pantalla táctil o en la aplicación móvil. En caso de no hacerlo en un plazo determinado de 1 minuto, activará una alarma intensa en el celular, aunque el usuario puede determinar cuánto tiempo establecer para activarse.

La pulsera también vibrará si detecta un alejamiento inusual del celular y, mediante la conexión **WiFi**, permitirá configurar **zonas seguras** para reducir la probabilidad de las falsas alertas. Además, con la pantalla mostrará una interfaz para mostrar las notificaciones de alejamiento voluntario, estado de conexión y mensajes de alerta.

Incluso ante la detección de movimientos bruscos y no se ingresa el **PIN** en el tiempo determinado, el sistema realizará una **llamada automática a un número de emergencia** configurado previamente en la aplicación o contacto a las autoridades.

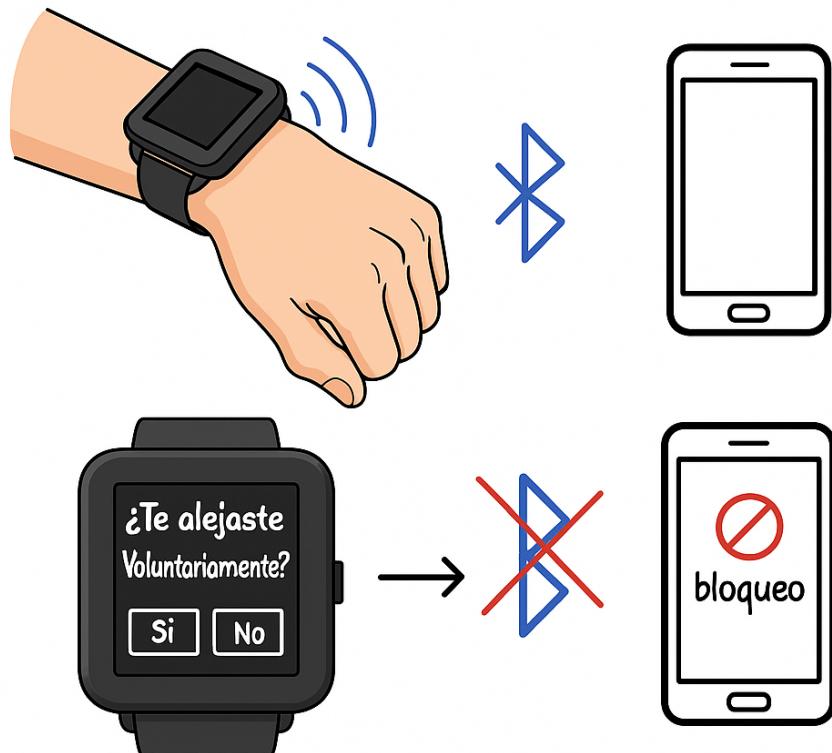


Figura 10: Funcionamiento del TicPrev

## 11. Instrucciones de uso

### 11.1. Activación y emparejamiento con la aplicación móvil:

- La pulsera TicPrev se enciende automáticamente cuando comienza a recibir energía de la batería.
- Asegúrese de que la pulsera esté completamente cargada antes de usarla.
- Active el Bluetooth en su dispositivo móvil y abra la aplicación TicPrev.
- Siga las instrucciones en la aplicación para emparejar la pulsera con su teléfono.

### 11.2. Configuración de zonas seguras:

- Acceda a la opción *Zonas Seguras* dentro de la aplicación móvil.
- Ingrese las ubicaciones que desea configurar como zonas seguras, como su hogar o lugar de trabajo, para evitar que se activen alertas innecesarias cuando se aleje del teléfono en estos lugares.
- La pulsera no emitirá alarmas si se aleja del dispositivo móvil dentro de estas zonas configuradas.

### 11.3. Uso de la pulsera en situaciones de emergencia:

- **Robo sin que la víctima lo note:** Si la pulsera se desconecta repentinamente del teléfono, la aplicación enviará una notificación solicitando ingresar un PIN. Si el PIN no se ingresa en el tiempo predeterminado, se activará una alarma sonora en el teléfono móvil.
- **Robo bajo amenaza:** Si la pulsera detecta un aumento súbito en el ritmo cardíaco o un movimiento brusco, comenzará una cuenta regresiva. Si el usuario no ingresa el PIN en el tiempo configurado, la pulsera realizará una llamada de emergencia y enviará la ubicación del usuario a los contactos configurados.

### 11.4. Personalización de las alertas:

- Desde la aplicación, puede ajustar el tiempo de espera para la alerta de desconexión (por ejemplo, 5 minuto o más según su preferencia).
- Puede modificar la alarma sonora que la pulsera emite en caso de emergencia.

### 11.5. Carga y mantenimiento:

- La pulsera debe cargarse con el cargador suministrado. Se recomienda cargarla completamente antes de su primer uso.
- La duración de la batería depende del uso del sistema de sensores. En modo de monitoreo continuo, la batería de la pulsera debería durar al menos 48 horas.

## 11.6. Consejos adicionales:

- Asegúrese de que el sensor de ritmo cardíaco MAX30102 esté en contacto directo con su piel para obtener lecturas precisas.
- Evite colocar la pulsera cerca de objetos que puedan interferir con la señal Bluetooth, como grandes objetos metálicos.

# 12. Riesgos

## 12.1. Riesgos Técnicos

- Falsos positivos de los sensores (MAX30102 y Módulo GY-521 (MPU-6050)), interpretando movimientos normales como situaciones de riesgo.
- Falsos negativos en los que el sistema no detecta un forcejeo o alteración fisiológica real.
- Inestabilidad de la conexión Bluetooth, que puede generar alarmas innecesarias.
- Limitada duración de la batería debido al uso continuo de sensores y comunicación inalámbrica.

## 12.2. Riesgos de Desarrollo

- Subestimación del tiempo necesario para la programación e integración de los módulos.
- Retrasos en la adquisición de componentes electrónicos.
- Curva de aprendizaje asociada al uso de sensores biométricos y librerías de seguridad.

## 12.3. Riesgos de Recursos

- Limitaciones presupuestarias que dificulten la incorporación de módulos alternativos más confiables.
- Disponibilidad limitada de repuestos en caso de fallas de hardware.

## 12.4. Riesgos de Uso e Implementación

- Posible incomodidad para el usuario al portar la pulsera, afectando su adopción.
- Errores humanos, como el olvido o ingreso incorrecto del PIN bajo situaciones de estrés.
- Configuración incorrecta de las zonas seguras que genere fallas en la activación de alarmas.
- Riesgos asociados al manejo de datos biométricos, comprometiendo privacidad y seguridad.

## 13. Plan de mitigación

A continuación, se describen los riesgos identificados durante el desarrollo del proyecto TicPrev y las estrategias de mitigación que se aplicaran para reducir el impacto.

### ■ Riesgos Técnicos:

- En los falsos positivos implementar un algoritmo de filtrado que discrimine entre movimientos normales y forzados. Realizar pruebas controladas para calibrar los sensores adecuadamente.
- La conexión Bluetooth inestable entre la pulsera y el teléfono móvil puede generar alarmas innecesarias. Por lo que mejorar la conexión mediante pruebas de señal **RSSI** antes de activar alarmas. Además, agregar la capacidad de **reconexión automática** si la conexión se pierde temporalmente.

### ■ Riesgos de Desarrollo:

- Los retrasos en la adquisición de componentes pueden afectar el progreso del proyecto debido a la falta de stock o demoras en el envío. Por lo que se realizarán compras anticipadas y se tendrán proveedores alternativos disponibles, asegurando que los componentes más críticos estén asegurados desde el inicio del proyecto.

### ■ Riesgos de Recursos:

- El costo de los módulos alternativos más avanzados podría exceder el presupuesto disponible para el proyecto. Por lo que se priorizará la compra de módulos económicos pero funcionales para prototipos, utilizando simulaciones para validar el comportamiento antes de realizar compras adicionales.

### ■ Riesgos de Uso:

- El ingreso erróneo del PIN en situaciones de estrés podría activar alarmas falsas. Por lo tanto se permitirá el *restablecimiento del PIN* a través de la aplicación móvil, utilizando una autenticación segura.

### ■ Riesgos de Privacidad:

- El manejo de datos sensibles como las pulsaciones cardíacas o podría generar problemas de privacidad y seguridad. Por lo cual se encriptarán todos los datos almacenados y no se guardará información biométrica de manera permanente.

## 14. Modelo de negocios



Figura 11: Modelo de negocio CANVAS.

El modelo de negocios de **TicPrev** se centra en ofrecer una pulsera inteligente de seguridad personal capaz de detectar robos o situaciones de riesgo mediante sensores de movimiento y ritmo cardíaco.

### ■ Socios clave

*TicPrev* depende de la alianzas estratégicas con promovedores de componentes electrónicos de calidad y las entidades de seguridad ciudadana, que permiten garantizar la calidad del producto y facilitar su integración en iniciativas de prevención.

### ■ Actividades clave

Las principales actividades del proyecto son la programación de la aplicación móvil y firmware, el armado y pruebas del hardware, el diseño del interfaz de usuario y la ejecución de estrategias de marketing digital para poder posicionar el producto en el mercado.

### ■ Recursos clave

El *TicPrev* requiere de recursos tecnológicos como el microcontrolador *ESP32*, los sensores biométricos y de movimiento (*MAX30102* y *GY-521*) como también un equipo técnico en software y hardware, además de una app móvil que gestiona las alertas y funciones de la pulsera.

### ■ Propuesta de valor

Su propuesta de valor ofrece una solución innovadora de seguridad personal inmediata, capaz de detectar robos o asaltos mediante sensores que activan alertas automáticas al celular y a notificar a los contactos de emergencia.

**■ Relaciones con los clientes**

Se busca mantener una relación cercana y continua con los usuarios mediante su aplicación móvil, que no solo gestionará las alertas, sino que también brindará soporte técnico y notificaciones. Además, se implementará un sistema de seguimiento postventa, lo que garantizará la actualización del dispositivo y la satisfacción del cliente.

**■ Canales**

La distribución del producto será a través de diversos canales de venta, incluyendo ferias tecnológicas para presentar el dispositivo directamente al público objetivo, alianzas con tiendas de seguridad. Las redes sociales también jugarán un rol fundamental en la promoción en torno al producto.

**■ Segmento de clientes**

Este proyecto se dirige principalmente a un público objetivo el cual está compuesto por jóvenes, adultos, estudiantes universitarios y familias que utilizan frecuentemente sus teléfonos móviles en espacios públicos y buscan mejorar su seguridad.

**■ Estructura de costos**

Los principales costos del proyecto se distribuyen entre los componentes electrónicos y materiales, el desarrollo de software, el ensamblaje de los dispositivos, el marketing y la distribución para dar a conocer el producto, y el mantenimiento y actualización constante del sistema para asegurar su efectividad a largo plazo.

**■ Flujo de ingresos**

El flujo de ingresos se obtendrá de la venta directa del dispositivo y un plan premium, que ofrecerá funcionalidades adicionales como alertas personalizadas, conexión prioritaria con servicios de emergencia y más opciones de configuración. Esto asegurará tanto una monetización inmediata como un modelo recurrente a través de suscripciones.

## 15. Cliente objetivo

El cliente objetivo principal para TicPrev es el **Joven Adulto Urbano (18 a 35 años)**.

### 15.1. Perfil del Cliente Objutivo

- **Demografía:** Hombres y mujeres, estudiantes y profesionales jóvenes, con un nivel socioeconómico medio a alto.
- **Ubicación:** Residentes o transeúntes frecuentes de grandes ciudades o zonas urbanas con alta a media tasa de delitos comunes, especialmente robo de celulares y asaltos en la vía pública o transporte.
- **Comportamiento y Tecnología:** Usuarios activos de teléfonos inteligentes, familiarizados con la tecnología portable (wearables) como smartwatches o smartbands, y conscientes de las aplicaciones de seguridad o rastreo.

- **Necesidad Específica:** Buscan una solución discreta, automática y que no requiera acción manual bajo estrés para aumentar su seguridad personal y la de su dispositivo móvil, especialmente durante sus trayectos diarios o al salir de noche.

## 15.2. Entrevista a Contraparte y Conclusiones

Para validar la propuesta de valor y las funcionalidades de **TicPrev**, se realizó una entrevista a una potencial contraparte que encaja con el perfil del cliente objetivo: una **estudiante universitaria de 22 años** que utiliza transporte público diariamente y ha experimentado la sensación de inseguridad en su rutina.

### 15.2.1. Resultados de la Entrevista

- **Validación del Problema:** La entrevistada confirmó que el **robo de celular** es una preocupación constante y que las soluciones actuales (como llevar el móvil escondido o usar apps de pánico) son insuficientes o requieren activación manual.
- **Relevancia del Sistema de Detección Automática:** Valoró altamente la funcionalidad de **detección automática de forcejeo/aumento cardíaco** (Robo bajo amenaza), ya que en un asalto "...es imposible reaccionar y sacar el teléfono para pedir ayuda".
- **Crítica y Sugerencia sobre el PIN:** Respecto al mecanismo de **desconexión/alejamiento repentino**, la necesidad de ingresar un PIN en la pulsera en un minuto generó preocupación por el tiempo. Sugirió que la vibración de alerta sea muy clara y que el tiempo pueda ser configurable, o que se incorpore un modo "...Estoy Bien" más rápido.
- **Zonas Seguras:** La funcionalidad de **zonas seguras** (casa, universidad) fue considerada fundamental para evitar **falsos positivos** y la consecuente alarma innecesaria, especialmente cuando el celular se deja cargando lejos del usuario.

### 15.2.2. Conclusiones y Ajustes al Proyecto

Los resultados de la entrevista reafirman la necesidad de una solución como TicPrev, validando la importancia de la detección automática y las zonas seguras. Las principales conclusiones que llevarán a ajustes en el diseño y programación son:

1. **Flexibilizar el Temporizador de Alarma:** El tiempo de espera de 1 minuto para el PIN de desconexión debe ser **configurable** por el usuario en la aplicación móvil para ajustarse a su percepción de riesgo.
2. **Claridad en la Alerta de Desconexión:** Reforzar la **vibración** de la pulsera al detectar alejamiento o desconexión sospechosa, junto con un mensaje claro en la pantalla OLED, para que el usuario pueda reaccionar a tiempo para ingresar el PIN.
3. **Diseño Discreto:** Mantener el diseño de la pulsera lo más **discreto** posible, ya que la entrevistada indicó que un dispositivo de seguridad demasiado llamativo podría atraer la atención del delincuente.

### 15.3. Resultados Segunda Entrevista

Unas semanas después de la primeras entrevistas, en base a la lógica de la aplicación y los diseños 3D preliminares, se realizaron nuevas entrevistas de validación con perfiles clave de nuestro cliente objetivo (principalmente estudiantes universitarios y jóvenes que utilizan transporte público). El objetivo era clarificar la propuesta de valor, validar el modelo de ingresos y resolver excepciones de uso.

A continuación, se analiza el promedio de las respuestas más importantes de los 23 entrevistados.

- 1. De las funciones mostradas, ¿Cuál considera la más importante para usted: la alerta por *desconexión* (robo repentino) o la alerta por *forcejeo* (robo bajo amenaza)?**

Hubo un consenso claro. Aunque la alerta por desconexión (hurto) se consideró útil, la funcionalidad de Robo bajo Amenaza (detección de forcejeo y/o picos biométricos) fue valorada como la propuesta de valor principal. Los entrevistados remarcaron que "...en un asalto es imposible reaccionar y sacar el teléfono para pedir ayuda". La idea de que el sistema actúe solo, notificando a emergencias sin emitir sonidos, fue el punto más valorado.

- 2. ¿Cuál es el valor en el cual, al tener el dinero disponible, compraría la pulsera sin analizarlo mucho, ya que su utilidad/precio es muy bueno?**

A diferencia de la pregunta sobre el precio "justo", aquí las respuestas fueron muy consistentes. La mayoría de los estudiantes y jóvenes indicaron que un precio de **\$30.000 (CLP)** o menos lo consideraría una compra impulsiva"para la seguridad que ofrece, asumiendo que es un pago único por el hardware.

- 3. ¿Cuál considera que es un precio justo para esta pulsera?**

Aquí las respuestas variaron ligeramente. El segmento de estudiantes universitarios consideró que un precio justo estaría entre **\$30.000 y \$45.000 (CLP)**. Lo comparaban con el costo de un reloj inteligente de gama de entrada, pero dándole un valor por la seguridad. Un segmento menor (identificado como padres de familia interesados en el producto para sus hijos) estuvo dispuesto a un rango superior, cercano a los **\$50.000 (CLP)**.

- 4. Este proyecto incluye un Plan Premium con funciones adicionales (como la conexión prioritaria con servicios o mayor personalización del servicio). ¿Cuánto estaría dispuesto a pagar por una suscripción mensual?**

Aquí hubo una alta sensibilidad al precio. La mayoría de los entrevistados (principalmente estudiantes) están acostumbrados a pagos únicos por hardware. Sin embargo, entendieron el valor de un servicio de monitoreo continuo. Las respuestas más comunes indicaron que un pago mensual aceptable debería ser bajo, similar a una suscripción de música o streaming, situándose en el rango de **\$2.990 a \$4.990 (CLP) mensuales**. Varios mencionaron que preferirían un descuento por un pago anual (ej. \$30.000 al año).

- 5. ¿Considera la función de "Zonas Seguras"(desactivación por WiFi) un gusto, un apoyo o una necesidad?**

Todos los entrevistados calificaron esta función como una **necesidad**. Indicaron que, sin esta función, las falsas alarmas al estar en casa o en la universidad serían tan molestas que probablemente dejarían de usar la pulsera. La validación de esta excepción de uso fue crítica.

#### 6. ¿Usted ha buscado o comprado algo similar a esta pulsera?

La mayoría respondió que, si bien les preocupa el robo, las soluciones que conocen son "botones de pánico" manuales (ya sea en apps o dispositivos). Ningún entrevistado conocía una solución que integrara *automáticamente* la biometría y el forcejeo para este propósito.

#### Observaciones Clave de la Entrevista:

Algo que no fue una pregunta pero sí una observación es que en el 86 % de los casos, los entrevistados mostraron alto interés en probar el prototipo físico. A pesar de que solo disponíamos de los diseños 3D y la maqueta de la app, la lógica del sistema fue lo que más llamó la atención.

Analizando las preguntas 2, 3 y 4, vemos que el mercado acepta la idea de pagar por el dispositivo, pero será más sensible a la tarifa de suscripción. Esto valida la estructura de ingresos mixta (venta de dispositivo + plan premium).

Finalmente, todas las personas que interactuaron con la maqueta de la app entendieron el flujo de configuración (Zonas Seguras, Contacto de Emergencia) rápidamente, cumpliendo con nuestro requerimiento no funcional de usabilidad en etapas muy tempranas del desarrollo.

## 16. Requerimientos del Sistema

Para asegurar el correcto funcionamiento de TicPrev y su cumplimiento con los objetivos del proyecto, se definen los siguientes requerimientos, divididos en funcionales (lo que el sistema debe hacer) y no funcionales (cómo debe funcionar el sistema).

### 16.1. Requerimientos Funcionales (RF)

Los requerimientos funcionales describen las tareas y servicios que el sistema debe proveer al usuario.

- **RF1: Monitoreo Biométrico Continuo.** El sistema debe monitorear y registrar continuamente el ritmo cardíaco (FC) del usuario a través del sensor MAX30102.
- **RF2: Detección de Forcejeo.** El sistema debe analizar los datos del acelerómetro/giroscopio (MPU-6050) y activar un estado de pre-alerta si detecta movimientos bruscos o patrones de forcejeo que superen un umbral calibrado (Robo bajo amenaza).
- **RF3: Detección de Riesgo Biométrico.** El sistema debe activar un estado de pre-alerta si detecta un aumento súbito y sostenido del ritmo cardíaco (pico de estrés) que supere un umbral configurable por el usuario.
- **RF4: Protocolo de Emergencia por Amenaza.** Ante la activación de la pre-alerta por Forcejeo (RF2) o Biometría (RF3), el sistema debe iniciar un temporizador configurable y, si no es desactivado con el PIN, debe realizar una llamada automática al contacto de emergencia y enviar la ubicación GPS del teléfono.

- **RF5: Alerta por Desconexión (Robo Repentino).** El sistema debe detectar la pérdida de conexión Bluetooth con el celular y activar una vibración en la pulsera, iniciando una cuenta regresiva de 1 minuto para ingresar el PIN de seguridad.
- **RF6: Activación de Alarma Sonora.** Si el PIN de seguridad no es ingresado tras la desconexión (RF5) o durante el protocolo de emergencia (RF4), el sistema debe activar una alarma sonora de alto volumen en el teléfono móvil, independiente del modo de silencio.
- **RF7: Gestión de Zonas Seguras.** El usuario debe poder definir y almacenar múltiples zonas geográficas (basadas en coordenadas WiFi o GPS) en la aplicación móvil, donde las alertas por desconexión (RF5) serán desactivadas automáticamente.
- **RF8: Interfaz de Configuración Móvil.** El sistema debe contar con una aplicación móvil (Android/iOS) que permita al usuario configurar umbrales de detección, el número de emergencia y el PIN de seguridad.
- **RF9: Interfaz de Visualización en Pulsera.** La pantalla OLED debe mostrar en tiempo real el estado de la conexión Bluetooth, el nivel de batería y las notificaciones de alerta (e.g., “Alerta: Desconexión Detectada”).

## 16.2. Requerimientos No Funcionales (RNF)

Los requerimientos no funcionales definen los criterios de calidad y las restricciones operacionales del sistema.

- **RNF1: Autonomía.** La pulsera debe tener una autonomía mínima de 48 horas en modo de monitoreo continuo, utilizando la batería de polímero de litio.
- **RNF2: Tiempo de Respuesta de Alerta.** El tiempo transcurrido entre la detección de un evento de forcejeo (RF2) y la activación de la vibración de pre-alerta debe ser inferior a 2 segundos.
- **RNF3: Fiabilidad de la Conexión.** La conexión Bluetooth entre la pulsera y el teléfono debe ser estable dentro de un radio de al menos 10 metros en un entorno abierto, con capacidad de reconexión automática rápida.
- **RNF4: Usabilidad y Comodidad.** El diseño físico de la pulsera debe ser ergonómico, ligero y discreto, priorizando la comodidad para el uso prolongado y evitando ser un elemento visible que atraiga la atención.
- **RNF5: Precisión de Sensores.** La lectura del ritmo cardíaco (MAX30102) debe tener una precisión del  $\pm 5$  latidos por minuto (LPM) comparado con un equipo de referencia.
- **RNF6: Seguridad de Datos.** Todos los datos biométricos y de ubicación recolectados y almacenados deben estar encriptados para proteger la privacidad del usuario, de acuerdo con el Plan de Mitigación de Riesgos.

## 17. Diseño del circuito

A continuación, se presenta el diseño del circuito utilizado en el prototipo de la pulsera *TicPrev*.

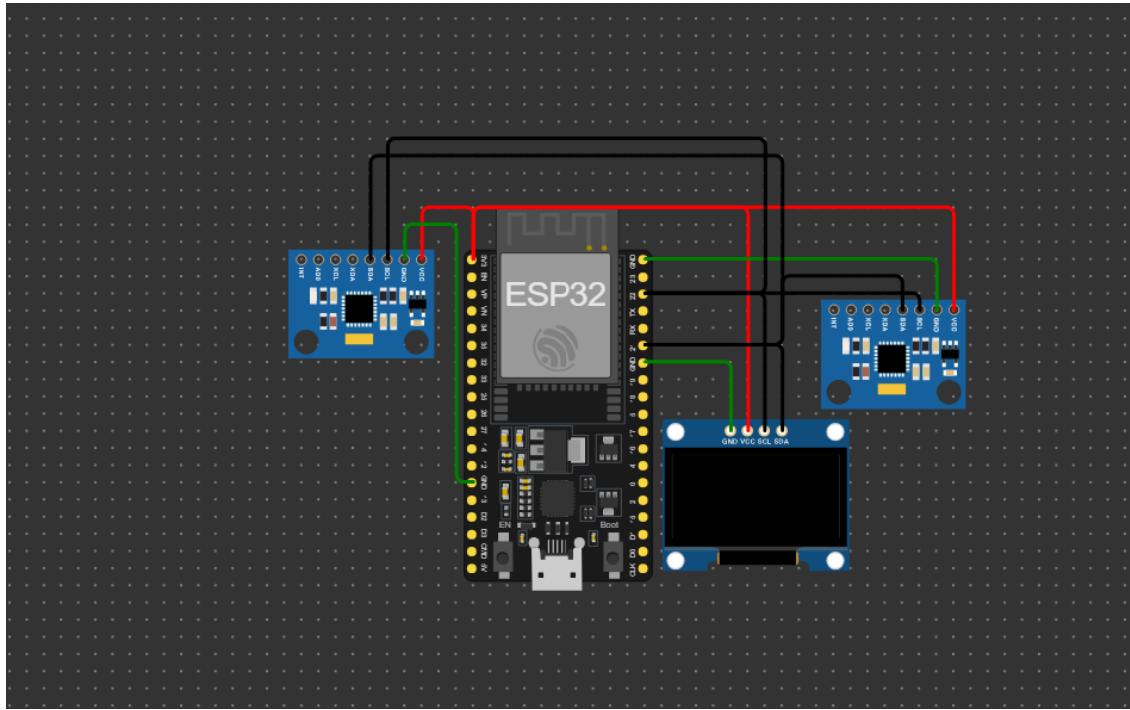


Figura 12: Esquema del circuito montado.

Como se puede observar en la Figura 12, se muestran las conexiones de los respectivos sensores hacia el **ESP32**. A continuación, se presenta una tabla con las conexiones correspondientes de cada uno de los componentes.

Componente	Pin del módulo	Pin del ESP32
MAX30102	VCC GND SCL SDA	3V3 GND GPIO 22 (SCL) GPIO 21 (SDA)
MPU-6050	VCC GND SCL SDA	3V3 GND GPIO 22 (SCL) GPIO 21 (SDA)
OLED SSD1306	VCC GND SCL SDA	3V3 GND GPIO 22 (SCL) GPIO 21 (SDA)

Cuadro 1: Conexiones entre el ESP32 y los sensores.

En este esquema no se consideró relevante la implementación de la fuente de energía, ya que hasta el momento el prototipo solo se ha utilizado de esta forma para la calibración de los sensores y las pruebas preliminares. De esta manera, se presenta un diseño fiel a las implementaciones realizadas hasta este punto del proyecto.

### 17.1. Actualización del Modelo Gráfico con Diseño e Integración de Componentes

El diseño del artefacto ha sido actualizado para reflejar los avances realizados en la integración de los componentes. A continuación se describe la integración del hardware:

- **Microcontrolador ESP32:** El microcontrolador ESP32 es el encargado de gestionar los sensores y la comunicación con la aplicación móvil.
- **Sensores:** El sensor MAX30102 se utiliza para medir las pulsaciones y el nivel de oxígeno en sangre, mientras que el sensor MPU-6050 detecta los movimientos bruscos y forcejeos.
- **Pantalla OLED:** La pantalla OLED SSD1306 permite visualizar el estado de la conexión y las alertas generadas por la pulsera.

El siguiente diagrama muestra el esquema del circuito montado, con las conexiones entre el ESP32 y los sensores.

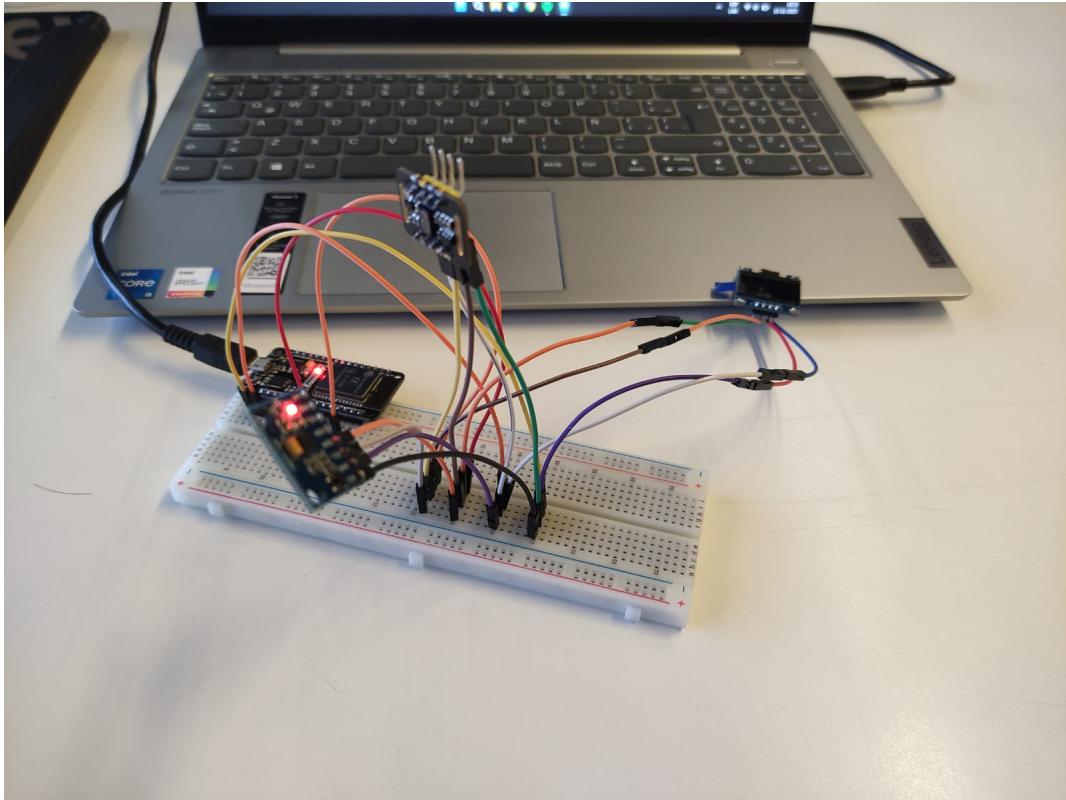


Figura 13: Esquema del circuito montado con el ESP32, sensores MAX30102 y MPU-6050, y la pantalla OLED.

A continuación se muestran imágenes de los sensores y el funcionamiento de la pantalla OLED:

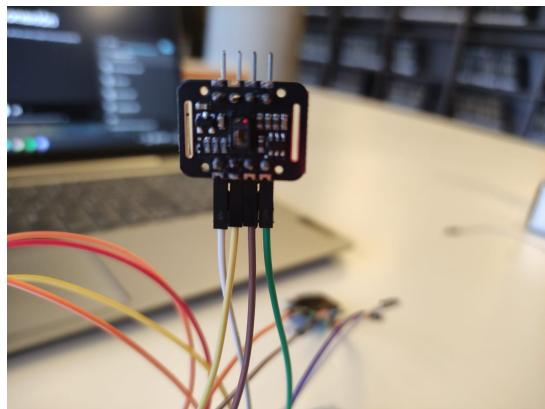


Figura 14: Sensor de pulsaciones MAX30102.

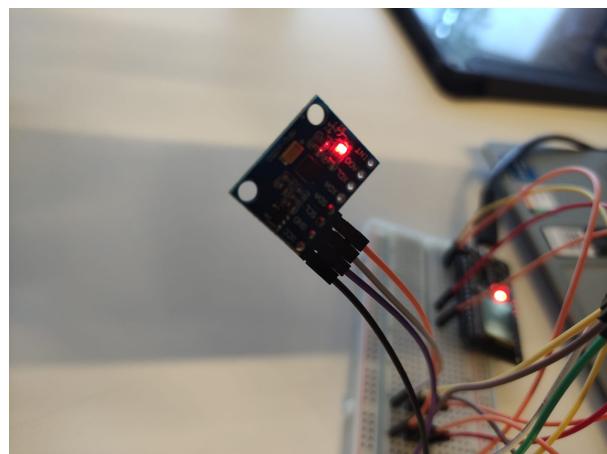


Figura 15: Sensor de movimiento GY-521 (MPU-6050).

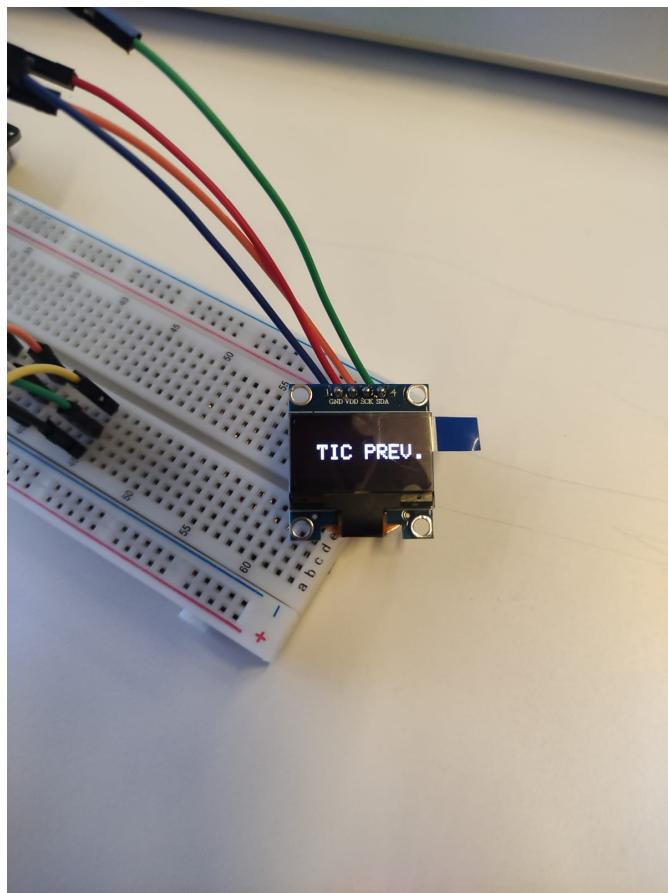


Figura 16: Pantalla OLED mostrando la interfaz de usuario.

## 18. Plan de trabajo (Modificado)

A continuación se mostrara la propuesta de trabajo, comenzando con nuestra carta gantt, en la que se encuentran especificados cada uno de los pasos a seguir durante el proyecto, horas de trabajo, porcentajes de trabajo de cada trabajador y la disposición de los días.

		Nombre	Duración	Inicio	Terminado	Predecesores	Nombres del Recurso
1		■ Proyecto	59 days	25-08-25, 08:00	20-11-25, 17:00		
2		■ Planificación	14 days	25-08-25, 08:00	11-09-25, 17:00		
3		Investigación del problema	5 days	25-08-25, 08:00	29-08-25, 17:00		Mateo Solari[25 %];Pablo Mu... ...
4	■	Plano formal	5 days	01-09-25, 08:00	05-09-25, 17:00	3	Pablo Muñoz[25 %];José Av... ...
5	■	Análisis de costos	2 days	08-09-25, 08:00	09-09-25, 17:00	4	Magdalena Correa[25 %];M... ...
6	■	Análisis del Presupuesto	2 days	10-09-25, 08:00	11-09-25, 17:00	5	Mateo Solari[25 %];Pablo Mu... ...
7	■	■ Desarrollo inicial	20 days	12-09-25, 08:00	16-10-25, 17:00		
8	■	Diseño de Prototipo	5 days	12-09-25, 08:00	25-09-25, 17:00		Magdalena Correa ...
9	■	Programación básica app	10 days	26-09-25, 08:00	09-10-25, 17:00	8	Mateo Solari ...
10	■	Prototipo funcional	5 days	10-10-25, 08:00	16-10-25, 17:00	9	Pablo Muñoz;José Avello ...
11	■	■ Test 1	5 days	17-10-25, 08:00	23-10-25, 17:00		
12	■	QA inicial	5 days	17-10-25, 08:00	23-10-25, 17:00		Magdalena Correa;Pablo Mu... ...
13	■	■ Desarrollo Final	15 days	24-10-25, 08:00	13-11-25, 17:00		
14	■	Prototipo final	10 days	24-10-25, 08:00	06-11-25, 17:00		Magdalena Correa ...
15	■	App final	10 days	24-10-25, 08:00	06-11-25, 17:00		Mateo Solari ...
16	■	Eliminación de Errores	5 days	07-11-25, 08:00	13-11-25, 17:00		José Avello ;Pablo Muñoz ...
17	■	■ Test 2	5 days	14-11-25, 08:00	20-11-25, 17:00		
18	■	QA final	5 days	14-11-25, 08:00	20-11-25, 17:00		José Avello ;Magdalena Cor... ...

Figura 17: Carta Gantt

La Figura 10 complementa la tabla anterior, mostrando la representación gráfica de la Carta Gantt. En esta vista de cronograma, se aprecian visualmente las barras de duración, el paralelismo de tareas (como Prototipo final y App final) y la secuencia general del proyecto a lo largo del calendario.

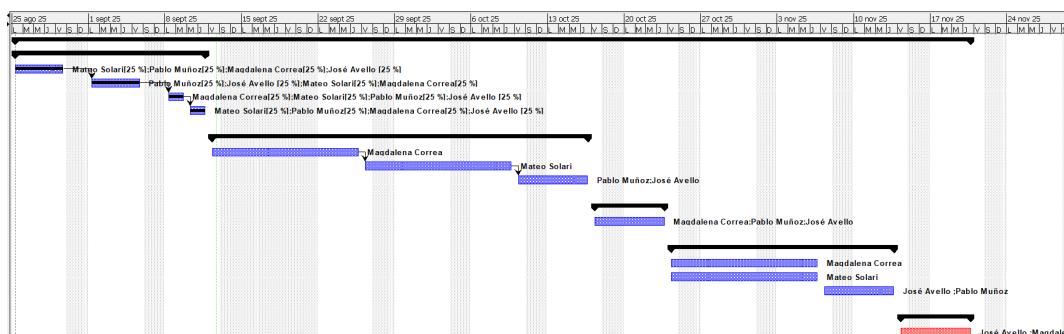


Figura 18: Distribución del plan a lo largo del tiempo

Para ilustrar las dependencias lógicas del proyecto, la Figura 11 presenta el Diagrama de Red. Este esquema no se enfoca en el tiempo, sino en el flujo de trabajo, mostrando qué tareas deben completarse antes de que otras puedan comenzar.

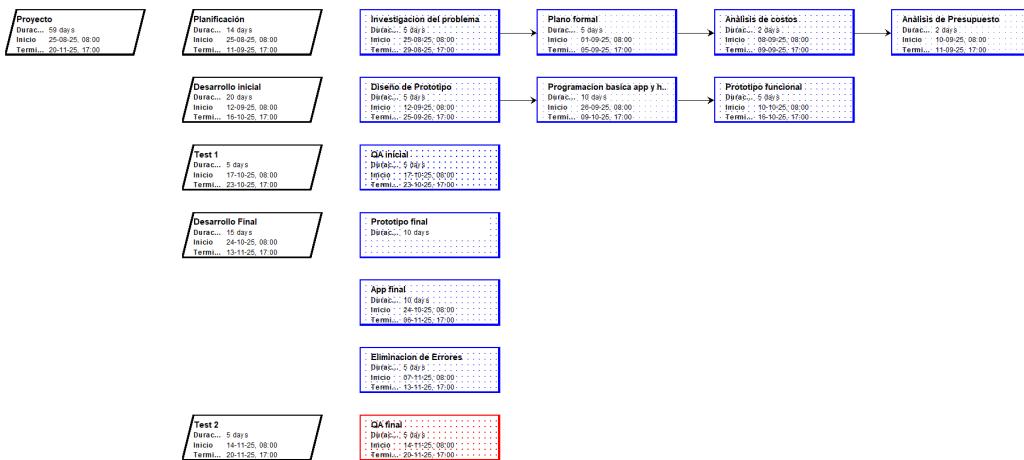


Figura 19: Red de tareas

En el siguiente apartado se muestra en más detalle cómo es el uso de tareas por persona. Debido a ser tantas tareas sólo se muestran las que alcanzan en la pantalla. De igual modo se deja constancia de que las tareas están divididas según cada empleado.

<input checked="" type="checkbox"/> <b>Proyecto</b>	800,081 horas	59 days	<b>25-08-25, 08:00</b>	<b>20-11-25, 17:00</b>	
<input checked="" type="checkbox"/> <b>Planificación</b>	80,081 horas	14 days	<b>25-08-25, 08:00</b>	<b>11-09-25, 17:00</b>	
Investigacion del problema	20,01 horas	5 days	25-08-25, 08:00	29-08-25, 17:00	
Pablo Muñoz	10 horas	5 days	25-08-25, 08:00	29-08-25, 17:00	Plano
Mateo Solar	0,005 horas	0,002 days	25-08-25, 08:00	25-08-25, 08:01	Plano
José Avello	0,005 horas	0,002 days	25-08-25, 08:00	25-08-25, 08:01	Plano
Magdalena Correa	10 horas	5 days	25-08-25, 08:00	29-08-25, 17:00	Plano
Plano formal	40 horas	5 days	01-09-25, 08:00	05-09-25, 17:00	
Mateo Solar	10 horas	5 days	01-09-25, 08:00	05-09-25, 17:00	Plano
Pablo Muñoz	10 horas	5 days	01-09-25, 08:00	05-09-25, 17:00	Plano
José Avello	10 horas	5 days	01-09-25, 08:00	05-09-25, 17:00	Plano
Magdalena Correa	10 horas	5 days	01-09-25, 08:00	05-09-25, 17:00	Plano
Análisis de costos	4,071 horas	2 days	08-09-25, 08:00	09-09-25, 17:00	
Magdalena Correa	0,024 horas	0,012 days	08-09-25, 08:00	08-09-25, 08:05	Plano
Pablo Muñoz	4 horas	2 days	08-09-25, 08:00	09-09-25, 17:00	Plano
José Avello	0,024 horas	0,012 days	08-09-25, 08:00	08-09-25, 08:05	Plano
Mateo Solar	0,024 horas	0,012 days	08-09-25, 08:00	08-09-25, 08:05	Plano
Análisis de Presupuesto	16 horas	2 days	10-09-25, 08:00	11-09-25, 17:00	
Pablo Muñoz	4 horas	2 days	10-09-25, 08:00	11-09-25, 17:00	Plano
Magdalena Correa	4 horas	2 days	10-09-25, 08:00	11-09-25, 17:00	Plano
Mateo Solar	4 horas	2 days	10-09-25, 08:00	11-09-25, 17:00	Plano
José Avello	4 horas	2 days	10-09-25, 08:00	11-09-25, 17:00	Plano
<input checked="" type="checkbox"/> <b>Desarrollo inicial</b>	200 horas	20 days	<b>12-09-25, 08:00</b>	<b>16-10-25, 17:00</b>	
Diseño de Prototipo	40 horas	5 days	12-09-25, 08:00	25-09-25, 17:00	
Magdalena Correa	40 horas	5 days	12-09-25, 08:00	25-09-25, 17:00	Plano
Programacion basica app	80 horas	10 days	26-09-25, 08:00	09-10-25, 17:00	
Mateo Solar	80 horas	10 days	26-09-25, 08:00	09-10-25, 17:00	Plano
Prototipo funcional	80 horas	5 days	10-10-25, 08:00	16-10-25, 17:00	
Pablo Muñoz	40 horas	5 days	10-10-25, 08:00	16-10-25, 17:00	Plano
José Avello	40 horas	5 days	10-10-25, 08:00	16-10-25, 17:00	Plano
<input checked="" type="checkbox"/> <b>Test 1</b>	120 horas	5 days	<b>17-10-25, 08:00</b>	<b>23-10-25, 17:00</b>	
QA inicial	120 horas	5 days	17-10-25, 08:00	23-10-25, 17:00	
José Avello	40 horas	5 days	17-10-25, 08:00	23-10-25, 17:00	Plano
Magdalena Correa	40 horas	5 days	17-10-25, 08:00	23-10-25, 17:00	Plano
Pablo Muñoz	40 horas	5 days	17-10-25, 08:00	23-10-25, 17:00	Plano

Figura 20: Tareas por empleado

La Figura 13 muestra la tabla resumen de estadísticas del proyecto. Esta consolida las métricas clave, como la duración total (59 días) y el trabajo total (aprox. 800 horas).

Aquí se observa que el costo proyectado asciende a 5.656.600 pesos. Es fundamental aclarar que este monto corresponde exclusivamente al costo de la mano de obra (horas de trabajo) y no incluye los costos de materiales, componentes de hardware o software.

Fecha Inicio:	25-08-25, 08:00
Línea base Inicio:	
Inicio real:	25-08-25, 08:00
Duración:	59 days
Duración real:	0 days
Trabajo:	800,081 horas
Trabajo real:	80,081 horas
Costo:	\$5656600
Costo real:	\$536600

Figura 21: Tabla resumen

Dicho costo total se calcula automáticamente a partir de las tasas estándar por hora asignadas a cada miembro del equipo, las cuales se detallan en la hoja de recursos de la Figura 14.

Nombre	...	...	...	...	...	...	Unidades Max	Tasa Estandar
Mateo Solari	...		M				100 %	\$10000/hora
Pablo Muñoz	...		P				100 %	\$6000/hora
Magdalena Correa	...		M				100 %	\$6000/hora
José Avello	...		J				100 %	\$6000/hora

Figura 22: Pagos por hora

## Actualización del cumplimiento del plan y evidencias de avance

En función del estado actual del proyecto, se realizó una actualización del plan de trabajo considerando el cumplimiento real de las actividades, las desviaciones observadas y las proyecciones para las siguientes etapas. Esta actualización complementa la Carta Gantt y la planificación previamente presentada.

### Cumplimiento del plan

A la fecha se lograron completar las siguientes tareas planificadas:

- Montaje inicial del prototipo en protoboard con el microcontrolador **ESP32**.
- Integración y conexión eléctrica de los módulos **MAX30102**, **MPU6050** y la pantalla **OLED SSD1306**.
- Pruebas funcionales de la pantalla OLED, logrando mostrar menús, mensajes de estado y la interfaz inicial del sistema.
- Verificación de energía, comunicación I2C y funcionamiento básico de los sensores.

Estas tareas corresponden a hitos clave del desarrollo del prototipo y se realizaron conforme a la programación ajustada.

### Desviaciones y retrasos

Si bien se avanzó en la mayor parte de lo planificado, hubo actividades que no pudieron completarse dentro del tiempo estimado inicialmente:

- El sensor MAX30102 presentó reconocimiento intermitente, requiriendo múltiples pruebas de cambio de pines y revisión de conexiones.
- El módulo MPU6050 funcionó correctamente en dos sesiones, pero luego mostró inestabilidad, lo que extendió su fase de prueba.
- La integración avanzada de datos biométricos y acelerométricos debió reprogramarse debido a los puntos anteriores.

Estas desviaciones han sido consideradas en la proyección siguiente del plan actualizado.

### Proyecciones actualizadas

Para la siguiente fase del proyecto se establecen los siguientes objetivos:

- Normalizar la comunicación I2C y lograr lecturas estables de ambos sensores.
- Avanzar en la calibración de señales biométricas (MAX30102) y de movimiento (MPU6050).
- Implementar la lógica de detección de eventos y pre-alertas.
- Integrar la comunicación Bluetooth con la aplicación móvil.
- Prototipo físico consolidado fuera de protoboard (montaje final).

### Evidencias del avance del prototipo

Las siguientes imágenes corresponden al estado actual del prototipo, evidenciando el avance alcanzado:

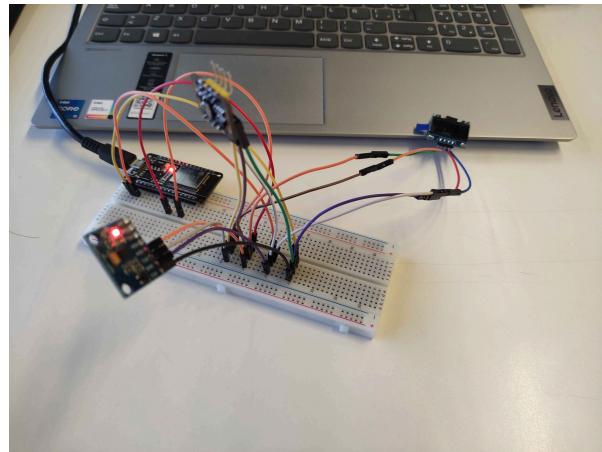


Figura 23: Interfaz en pantalla OLED mostrando mensaje de verificación: “¿Te alejaste voluntariamente?”.

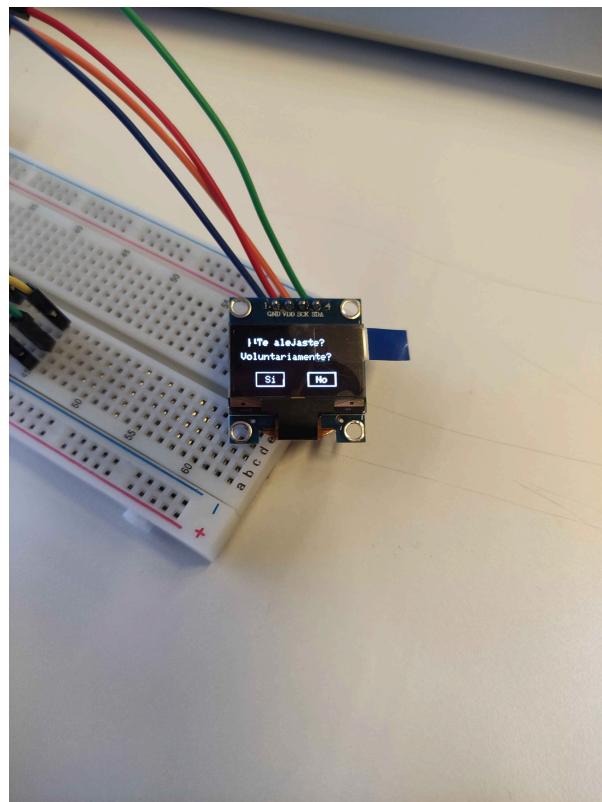


Figura 24: Montaje del prototipo completo con ESP32, sensores y pantalla OLED sobre protoboard.

Estas imágenes constituyen evidencia directa del progreso alcanzado y respaldan los avances reportados en la actualización del plan de trabajo.

## 19. Decisiones Tecnológicas

1. **ESP-WROOM-32 (Microcontrolador):** La elección de este microcontrolador se basó en su combinación de procesamiento eficiente y conectividad inalámbrica (WiFi/Bluetooth) nativa. También fue clave su compatibilidad con las librerías para los módulos, junto con su bajo consumo energético y sus múltiples pines, que aseguran la escalabilidad futura del proyecto.
2. **Pantalla OLED SSD1306 (0,96"):** Permite la visualización e interacción directa con el usuario. A través de ella podrá visualizar de forma sencilla información clave para el funcionamiento correcto del dispositivo.
3. **Sensor Módulo GY-521 (MPU-6050):** Mide la aceleración, es decir, los cambios de velocidad y la vibración. Se usa uno de 3 ejes (X, Y, Z) para captar el movimiento en cualquier dirección. Con él se establece un umbral (threshold) de aceleración. Si la magnitud de la aceleración medida supera bruscamente este umbral, el sistema lo interpreta como una señal inequívoca de un intento de robo. Este sensor es el componente principal para detectar el "forcejeo". Un robo no es un movimiento suave; es un tirón, un arrebato o una sacudida violenta.
4. **Sensor MAX30102:** Utiliza luz LED para medir el flujo sanguíneo en la muñeca y calcular las pulsaciones por minuto (PPM). Este sensor añade una capa de "confirmación humana". Ser víctima de un robo es un evento de alto estrés que activa una respuesta fisiológica inmediata en el cuerpo. Por ello el sensor MAX30102 juega un papel clave en la reducción de falsos positivos causados por el sensor de aceleración.
5. **Base De Datos (Postgre SQL):** En esta base se almacenará toda la información que concierne a este proyecto, datos de los usuarios (cliente) y fechas en las que se activo el sistema de alarma. Para su desarrollo e implementación en la nube, se utilizará la herramienta web Neon.
6. **Android Studio:** La elección de Android Studio como Entorno de Desarrollo Integrado (IDE), es un requisito técnico indispensable para las funciones de seguridad críticas del proyecto TICPREV. La razón principal es que Android Studio es el único IDE oficial de Google para el desarrollo nativo de Android. Esto proporciona un acceso completo, directo y sin filtros a todas las APIs del sistema operativo, lo cual es fundamental para las funciones de bloqueo que la aplicación requiere (bloqueo de apagado y volumen del móvil). Además nos permitirá hacer uso de las siguientes bibliotecas y APIs:
  - a) **Nordic Android BLE Library:** Es la biblioteca más robusta y popular para manejar conexiones Bluetooth Low Energy (BLE).
  - b) **ForegroundService:** Es la única forma garantizada de que la app no sea cerrada.
  - c) **AudioManager:** Esta API te da control total sobre el audio del teléfono.
  - d) **AccessibilityService:** Esta es la API diseñada para que las apps ayuden a usuarios con discapacidades, pero también permite interceptar eventos de hardware. Permite bloquear la bajada de volumen y el apagado.

7. **Arduino IDE:** La elección de Arduino IDE como entorno de desarrollo para el firmware se basa fundamentalmente en la abstracción, la eficiencia y el ecosistema de soporte. Este posee un ecosistema masivo de bibliotecas fundamentales para el uso de los sensores, ademas su abstracción permite centrarse en la lógica del proyecto en lugar de en la configuración del hardware.

## 20. Documentación de Funcionalidades

Los Casos de Uso describen la interacción entre los actores y el sistema TICPREV para lograr un objetivo específico.

### 20.1. Actores Principales

- **Usuario (Dueño):** La persona que porta la pulsera inteligente y posee el teléfono móvil vinculado.
- **Sistema TICPREV (App):** La aplicación móvil (Android) que ejecuta la lógica principal, la configuración y la comunicación.
- **Sistema TICPREV (Pulsera):** El dispositivo hardware (ESP32) que captura los datos de los sensores y se comunica vía Bluetooth.
- **Contacto de Emergencia:** La persona designada por el Usuario para recibir alertas.

## 20.2. Tabla de Casos de Uso

ID Caso	Nombre del Caso	Actor(es)	Descripción (Resumen)
CU-01	Configurar Sistema	Usuario	El Usuario utiliza la App para establecer su PIN de seguridad, el número del Contacto de Emergencia y ajustar los umbrales de los sensores.
CU-02	Gestionar Zonas Seguras	Usuario	El Usuario define, a través de la App, ubicaciones geográficas (basadas en WiFi) donde las alertas por desconexión (CU-03) se desactivan.
CU-03	Detectar Robo Repentino (Desconexión)	Sistema (App), Sistema (Pulsera)	El sistema detecta pérdida de Bluetooth fuera de una Zona Segura. Bloquea el teléfono, vibra la pulsera e inicia un temporizador. Si no hay PIN, activa alarma sonora.
CU-04	Detectar Robo Bajo Amenaza (Sensores)	Sistema (App), Sistema (Pulsera)	El sistema detecta "forcejeo" (MPU-6050) o "pico de estrés" (MAX30102). Inicia un temporizador silencioso. Si no hay PIN, notifica al Contacto de Emergencia y activa alarma.
CU-05	Desactivar Alerta	Usuario	El Usuario ingresa el PIN de seguridad (en la App o pulsera) para cancelar una pre-alerta (CU-03 o CU-04) o para silenciar una alarma ya activa.
CU-06	Consultar Estado del Sistema	Usuario, Sistema (Pulsera)	El Usuario visualiza la pantalla OLED de la pulsera para verificar el estado de la conexión Bluetooth.

## 20.3. Lógica de Funcionalidades (Flujos de Actividades)

A continuación, se describe la lógica interna y el flujo de actividades (pseudo código) para los casos de uso más críticos del sistema (al no haber prototipo físico funcional, no es posible en este momento ponerlos a prueba).

### 20.3.1. Flujo 1: Lógica de Zonas Seguras (CU-02 y RF7)

Listing 1: Lógica de verificación de Zona Segura.

```
// Este proceso se ejecuta en el servicio de fondo (ForegroundService)
// de la App cada vez que cambia la conexión WiFi.
```

FUNCIÓN: `verificarZonaSegura()`

```

estadoSeguro = FALSO
listaZonas = BaseDeDatos . obtenerZonasSeguras()

// Verificar por WiFi
wifiActual = Sistema . obtenerSSID_WiFi_Actual()
PARA CADA zona EN listaZonas:
    SI (zona . Tipo == "WIFI" Y zona . ID == wifiActual) ENTONCES
        estadoSeguro = CIERTO
        TERMINAR BUCLE
    FIN_SI
FIN PARA

// Variable global que consultarán otras funciones
Sistema . EN_ZONA_SEGURA = estadoSeguro
FIN_FUNCIÓN

```

### 20.3.2. Flujo 2: Lógica de Robo Repentino (CU-03 / RF5, RF6)

Listing 2: Lógica de alerta por desconexión Bluetooth.

```

// Lógica ejecutada en el ForegroundService de la App

EVENTO: onBluetoothDesconectado()

// 1. Verificar si es una desconexión relevante
Sistema . verificarZonaSegura() // Ejecuta Flujo 1
SI Sistema . EN_ZONA_SEGURA == CIERTO ENTONCES
    // No hacer nada. Es una desconexión segura en casa o trabajo.
    TERMINAR
FIN_SI

// 2. Es una desconexión en una zona insegura
Sistema . ESTADO = "PRE_ALERTA_DESCONEXION"
Pulsera . vibrar ("ALERTA")
Pulsera . OLED . mostrar (" Desconexión . Ingrese PIN ")

// 3. Bloquear el teléfono
App . bloquearFuncionesTelefono()
App . mostrarPantallaPIN()

// 4. Iniciar temporizador
tiempoEspera = BaseDeDatos . obtenerTiempoDesconexion() // Ej: 1 minuto
Sistema . iniciarTemporizador(tiempoEspera , ACCION: dispararAlarmaSonora)
FIN_EVENTO

```

```

FUNCIÓN: dispararAlarmaSonora()
SI Sistema .ESTADO == "PIN_INGRESADO" ENTONCES
    TERMINAR // El usuario desactivó la alerta
FIN_SI

Sistema .ESTADO = "ALARMA_ACTIVA"
Sistema .Audio .setVolumen(STREAM_ALARM, MAXIMO)
Sistema .Accessibility .bloquearBotonesHardware(CIERTO)
Sistema .Audio .reproducirSonidoAlarma(LOOPING)
FIN_FUNCIÓN

EVENTO: onPINIngresado(PIN_ingresado)
SI PIN_ingresado == BaseDeDatos .obtenerPIN_Correcto() ENTONCES
    Sistema .ESTADO = "PIN_INGRESADO"
    Sistema .detenerTemporizador(dispararAlarmaSonora)
    Sistema .Audio .detenerSonidoAlarma()
    Sistema .Accessibility .bloquearBotonesHardware(FALSO)
    App .desbloquearFuncionesTelefono()
    Pulsera .OLED .mostrar("Conectado")
    FIN_SI
FIN_EVENTO

```

### 20.3.3. Flujo 3: Lógica de Robo Bajo Amenaza (CU-04 / RF2, RF3, RF4)

Listing 3: Lógica de alerta por detección de sensores (Forcejeo/Estrés).

```

// Lógica principal ejecutada en el firmware de la Pulsera (ESP32)
FUNCIÓN: loopPrincipalSensores()

// 1. Detección de Forcejeo (RF2)
datosMPU = MPU6050 .leerAcelerometroGiroscopio()
magnitud = calcularMagnitud(datosMPU .ax, datosMPU .ay, datosMPU .az)
umbralForcejeo = App .obtenerUmbral("FORCEJEO")

SI magnitud > umbralForcejeo ENTONCES
    App .enviarNotificacion("PRE_ALERTA_AMENAZA", "FORCEJEO")
    TERMINAR
FIN_SI

// 2. Detección de Estrés Biométrico (RF3)
datosMAX = MAX30102 .leerRitmoCardiaco()
umbralRitmo = App .obtenerUmbral("RITMO")

```

```

SI datosMAX.PPM > umbralRitmo Y datosMAX.confianza > 90% ENTONCES
    App.enviarNotificacion("PRE_ALERTA_AMENAZA", "ESTRES")
FIN_SI
FIN_FUNCIÓN

```

```

// Lógica ejecutada en el ForegroundService de la App
EVENTO: onNotificacionRecibida(tipo, causa)
SI tipo == "PRE_ALERTA_AMENAZA" ENTONCES

    SI Sistema.ESTADO == "ALARMA_ACTIVA" O Sistema.ESTADO ==
        // "PRE_ALERTA_AMENAZA" ENTONCES
        TERMINAR // Evitar duplicar la alerta
    FIN_SI

    Sistema.ESTADO = "PRE_ALERTA_AMENAZA"

    // 2. Notificación silenciosa al usuario
    Pulsera.vibrar("SILENCIOSA")
    Pulsera.OLED.mostrar(causa + " detectado. PIN?")
    App.mostrarPantallaPIN() // Muestra la pantalla de PIN discretamente

    // 3. Iniciar temporizador de emergencia
    tiempoEspera = BaseDeDatos.obtenerTiempoAmenaza()
    Sistema.iniciarTemporizador(tiempoEspera, ACCION:
        // dispararAlertaEmergencia)
    FIN_SI
FIN_EVENTO

```

```

FUNCIÓN: dispararAlertaEmergencia()
SI Sistema.ESTADO == "PIN_INGRESADO" ENTONCES
    TERMINAR // El usuario desactivó la falsa alarma
FIN_SI

Sistema.ESTADO = "ALARMA_ACTIVA"

// 1. Obtener datos de emergencia
contacto = BaseDeDatos.obtenerContactoEmergencia()
ubicacion = Sistema.obtenerGPS()

// 2. Notificar al contacto
Sistema.enviarSMS(contacto.telefono, "AYUDA: " + ubicacion.link)
Sistema.llamar(contacto.telefono)

```

```
// 3. Activar alarma sonora local (RF6)
dispararAlarmaSonora()
FIN_FUNCIÓN
```

## 21. Modelo de Datos e Interfaces de Usuario

Para complementar los flujos lógicos, esta sección detalla la estructura de la información (Modelo de Datos) y la interacción del usuario con el sistema (Interfaces).

### 21.1. Modelo de Datos (PostgreSQL)

Tal como se menciona en la sección 16 (Decisiones Tecnológicas), el sistema utiliza una base de datos PostgreSQL en la nube (Neon). El siguiente modelo de entidad-relación describe las tablas necesarias para almacenar la configuración del usuario y el registro de eventos.

- **Tabla: Usuario**

Almacena la información de la cuenta principal del usuario.

- **id\_usuario** (SERIAL, PK): Identificador único.
- **email** (VARCHAR, UNIQUE): Email para login y recuperación.
- **hash\_pin\_seguridad** (VARCHAR): Hash del PIN de 4 dígitos.
- **fecha\_creacion** (TIMESTAMP): Fecha de registro.

- **Tabla: ContactoEmergencia**

Almacena el contacto que recibirá las alertas.

- **id\_contacto** (SERIAL, PK): Identificador único.
- **id\_usuario** (INTEGER, FK): Referencia a **Usuario.id\_usuario**.
- **nombre\_contacto** (VARCHAR): Nombre del contacto (ej. "Mamá").
- **telefono\_contacto** (VARCHAR): Número de teléfono (ej. -569...").

- **Tabla: ZonaSegura**

Almacena las zonas donde se desactivan las alertas por desconexión.

- **id\_zona** (SERIAL, PK): Identificador único.
- **id\_usuario** (INTEGER, FK): Referencia a **Usuario.id\_usuario**.
- **nombre\_zona** (VARCHAR): Alias ("Universidad").
- **valor\_zona** (VARCHAR): Almacena el SSID de la WiFi.

■ **Tabla: ConfiguracionUsuario**

Almacena los umbrales y preferencias personalizadas del usuario.

- **id\_config** (SERIAL, PK): Identificador único.
- **id\_usuario** (INTEGER, FK, UNIQUE): Referencia a **Usuario.id\_usuario**.
- **umbral\_forcejeo** (INTEGER): Sensibilidad del MPU-6050 (ej. 1 a 5).
- **umbral Ritmo cardiaco** (INTEGER): PPM para alerta de estrés (ej. 120 PPM).
- **tiempo\_prealerta\_desconexion** (INTEGER): Segundos para alarma sonora (ej. 60).
- **tiempo\_prealerta\_amenaza** (INTEGER): Segundos para notificar a contacto (ej. 30).

■ **Tabla: HistorialAlertas**

Registra cada evento de activación del sistema para consulta del usuario o mantenimiento.

- **id\_alerta** (SERIAL, PK): Identificador único.
- **id\_usuario** (INTEGER, FK): Referencia a **Usuario.id\_usuario**.
- **timestamp** (TIMESTAMP): Hora y fecha exactas del evento.
- **tipo\_alerta** (VARCHAR): 'DESCONEXION' o 'AMENAZA'.
- **causa\_alerta** (VARCHAR): 'BLUETOOTH', 'FORCEJEO' o 'ESTRES'.
- **ubicacion\_gps** (VARCHAR): Coordenadas (lat, lon) al momento de la alerta.
- **pin\_ingresado** (BOOLEAN): CIERTO si fue desactivada por el usuario, FALSO si escaló a alarma/notificación.

## 21.2. Interfaces de Usuario (UI)

El sistema posee dos interfaces de usuario: la aplicación móvil (UI principal de configuración e ingreso de datos) y la pulsera (UI de despliegue de estado y alertas).

**A. Interfaz de la Aplicación Móvil (Android)** Desarrollada en Android Studio, la app gestiona toda la configuración.

■ **Pantalla 1: Estado Principal**

- *Descripción:* Es la pantalla de bienvenida de la aplicación.
- *Despliegue:* Muestra el encabezado TICPREV, el logo de Protección Inteligente y tres botones de navegación principales, de esquinas redondeadas y fondo gradiente.
- *Controles (Botones):*
  - MI DISPOSITIVO: Redirige a la pantalla de estado y prueba de la pulsera.
  - MIS DATOS: Redirige a la pantalla de configuración del usuario (PIN, Contacto).

- AJUSTES: Redirige a la pantalla de configuración de la app (Zonas Seguras, Umbrasales).



Figura 25: Pantalla de Inicio

■ **Pantalla 2: Mi Dispositivo**

- *Despliegue:* Muestra el estado de la conexión (Conectado / Desconectado) y el nivel de batería de la pulsera.
- *Controles:* Botón para Buscar/Vincular Dispositivo y un botón Probar Alarma (para activar la Pantalla de Bloqueo).

▪ **Pantalla 3: Mis Datos / Ajustes**

- *Ingreso de Datos (PIN):* Sección Cambiar PIN de Seguridad.
- *Ingreso de Datos (Contacto):* Sección Contacto de Emergencia. Campos para Nombre y Teléfono.

▪ **Pantalla 4: Gestión de Zonas Seguras**

- *Despliegue:* Una lista de las zonas ya guardadas (ej. Casa, Universidad).
- *Controles:* Botón Añadir Nueva Zona Segura y botones para Editar o Eliminar zonas existentes.
- *Ingreso de Datos (al añadir):*
  - Campo Nombre de la Zona.

▪ **Pantalla 5: Pantalla de Bloqueo (Alarma)**

- *Descripción:* Esta es la pantalla que se activa durante una alerta y que utiliza las APIs `ForegroundService` y `startLockTask`.
- *Despliegue:* Fondo rojo, logo de TICPREV, texto Ingrese el Pin de Seguridad.
- *Ingreso de Datos:* Cuatro campos para el PIN de 4 dígitos. El ingreso del PIN correcto detiene la alarma, el `ForegroundService` y libera la pantalla ('`stopLockTask()`').



Figura 26: Pantalla de Bloqueo

**Interfaz de la Pulsera (OLED SSD1306)** La pantalla OLED provee información esencial y rápida al usuario.

- **Despliegue 1: Reposo**

- *Despliegue:* Muestra un ícono de Bluetooth (para indicar conexión) y el porcentaje de batería.

- **Despliegue 2: Alerta por Desconexión**

- *Acción:* Activada por RF5 (pérdida de Bluetooth fuera de Zona Segura).
- *Despliegue:* Texto Desconexión. Ingrese PIN.
- *Retroalimentación:* Vibración fuerte y continua.

- **Despliegue 3: Alerta por Amenaza**

- *Acción:* Activada por RF2 (Forcejeo) o RF3 (Estrés).
- *Despliegue:* Texto Forcejeo detectado o Estrés detectado.
- *Retroalimentación:* Vibración silenciosa/suave (para no alertar al agresor).

## 22. Sistema de Reportería

El sistema de reportería de TicPrev permite registrar eventos críticos, medir variables fisiológicas y almacenar datos que respaldan el funcionamiento del dispositivo. Este sistema es fundamental para analizar el comportamiento del usuario en situaciones reales, evaluar el desempeño del hardware y cumplir con los objetivos del proyecto.

### 22.1. Variables monitoreadas

El sistema registra las siguientes variables:

- Frecuencia cardíaca (PPM) obtenida del MAX30102.
- Aceleraciones y cambios bruscos detectados por el MPU-6050.
- Estado de la conexión Bluetooth (conectado / desconectado).
- Ubicación GPS durante una alerta real.
- Hora y fecha del evento registrado.

### 22.2. Estructura de la reportería

Los eventos se almacenan en la tabla **HistorialAlertas**, incluyendo:

- **tipo\_alerta:** Desconexión o amenaza.
- **causa\_alerta:** Forcejeo, estrés o pérdida de Bluetooth.
- **ubicacion\_gps:** Registro de ubicación durante el evento.
- **pin\_ingresado:** Si el usuario desactivó la alerta.

## 22.3. Ejemplo de registro real

Tabla 2 muestra un ejemplo de datos registrados durante pruebas controladas.

Fecha	Tipo	Causa	PPM	Desactivado
2025-05-22	Amenaza	Forcejeo	128	Sí
2025-05-22	Desconexión	Bluetooth	–	No
2025-05-23	Amenaza	Estrés	142	Sí

Cuadro 2: Ejemplo de registros generados durante pruebas reales.

## 22.4. Triggers del sistema

Los *triggers* corresponden a eventos que activan el registro automático de información.

- **Trigger 1: Pico de estrés** Activado si el ritmo cardíaco supera el umbral configurado por el usuario.
- **Trigger 2: Movimiento brusco** Activado si la magnitud del vector de aceleración excede el umbral de forcejeo.
- **Trigger 3: Desconexión Bluetooth** Activado cuando la pulsera pierde conexión fuera de una zona segura.
- **Trigger 4: Alarma final** Activado cuando el temporizador expira sin ingreso del PIN.

Este sistema de reportería permite validar los objetivos del proyecto, proporcionando evidencia cuantitativa sobre el funcionamiento del prototipo en escenarios reales.

# 23. Plan de Pruebas

Este plan de pruebas detalla los procedimientos para las fases Test 1 (QA Inicial) y Test 2 (QA Final), identificadas en la Carta Gantt del proyecto (Figura 9). El objetivo es validar la correcta operación, integración y fiabilidad de los componentes de hardware (pulsera) y software (app), garantizando que la solución cumpla con todos sus requerimientos funcionales y no funcionales.

## 23.1. Pruebas Unitarias de Componentes

Se comprueba cada componente de forma aislada antes de la integración.

### Hardware (Pulsera)

- **Prueba H-01 (Sensor Biométrico):** Validar que el sensor MAX30102 entrega lecturas de ritmo cardíaco (PPM) con la precisión requerida (RNF5:  $\pm 5$  LPM), comparando sus valores en reposo y post-esfuerzo contra un oxímetro comercial de referencia.

- **Prueba H-02 (Sensor de Movimiento):** Validar que el MPU-6050 genera lecturas distinguibles entre: (a) movimiento normal, (b) una caída, y (c) una "sacudida" violenta, para calibrar el umbral de "forcejeo".
- **Prueba H-03 (Display):** Comprobar que la pantalla OLED SSD1306 muestra correctamente todos los estados de interfaz definidos: conexión, batería y mensajes de alerta.

### Software (Aplicación Móvil)

- **Prueba S-01 (UI/Navegación):** Verificar que todos los botones y menús de la app (Inicio, Mi Dispositivo, Ajustes, Zonas Seguras) navegan a la pantalla correcta.
- **Prueba S-02 (Base de Datos):** Validar que la configuración del usuario (PIN, Contacto de Emergencia, Umbrales) se guarda correctamente en la base de datos PostgreSQL (Neon) y se recupera al reiniciar la app.
- **Prueba S-03 (Servicios de Bloqueo):** Validar que el `ForegroundService` y la función `startLockTask` se inician correctamente al ejecutar la Alarma de Prueba, bloqueando la pantalla y los botones de navegación del sistema.

## 23.2. Pruebas de Integración

Se comprueba la comunicación y sincronización entre la pulsera (ESP32) y la app (Android).

- **Prueba I-01 (Conexión BLE):** Validar que la app (usando la librería Nordic) descubre y se enlaza con la pulsera. Probar la estabilidad de la conexión (RNF3) y la reconexión automática si el usuario sale y vuelve a entrar en el rango de 10 metros.
- **Prueba I-02 (Latencia de Alerta):** Medir el tiempo entre la simulación de un forcejeo en la pulsera (Prueba H-02) y la activación de la pre-alerta en la app. Debe cumplir con el RNF2 (inferior a 2 segundos).
- **Prueba I-03 (Sincronización de Configuración):** Validar que al cambiar un umbral en la app (ej. sensibilidad de forcejeo), el nuevo valor se envía y aplica correctamente en el firmware del ESP32.

## 23.3. Pruebas Funcionales (Casos de Uso)

Se validan los escenarios de uso reales (Casos de Uso) del sistema completo.

### Test Caso 1: Configuración Completa

- **Acción:** Un usuario nuevo instala la app, configura su PIN de seguridad, añade un Contacto de Emergencia y define una Zona Segura usando la WiFi de su hogar.
- **Resultado Esperado:** Todos los datos se almacenan correctamente en la base de datos. El sistema está listo y armado.

### Test Caso 2: Alerta en Zona Segura (Falso Positivo)

- **Acción:** Estando conectado a la WiFi definida, el usuario apaga el Bluetooth de su teléfono (simulando una desconexión).
- **Resultado Esperado:** El sistema detecta la desconexión, pero al estar en una Zona Segura, **NO** debe activar ninguna alarma sonora ni de vibración.

### Test Caso 3: Robo Repentino

- **Acción:** El usuario sale de la Zona Segura y apaga Bluetooth.
- **Resultado Esperado:** El sistema activa el protocolo.

Inmediato La pulsera vibra intensamente.

Tras 1 min Si no se ingresa el PIN, la app activa la alarma sonora a máximo volumen usando **AudioManager**.

### Test Caso 4: Robo Bajo Amenaza

- **Acción:** Se simula un forcejeo o un pico de estrés en la pulsera.
- **Resultado Esperado:** El sistema activa el protocolo.
  - Tras 30 seg La pulsera vibra discretamente. La app muestra la pantalla de bloqueo **startLockTask**.
  - Tras 30 seg Si no se ingresa el PIN, la app envía un SMS con la ubicación GPS al Contacto de Emergencia y procede a llamarlo.
  - Tras 30 seg La alarma sonora se activa simultáneamente.

### Test Caso 5: Desactivación de Alerta

- **Acción:** Se activara alguno de los casos anteriores. El usuario ingresa el PIN correcto *antes* de que el temporizador expire.
- **Resultado Esperado:** El sistema cancela la alarma. La pantalla se desbloquea (**stopLockTask()**), el servicio se detiene y la pulsera deja de vibrar. El sistema vuelve al modo de monitoreo normal.

## 24. Historia de Usuario y Secuencia de Eventos

A continuación se describe la historia de usuario que ilustra el funcionamiento del sistema desde un punto de vista práctico, siguiendo la secuenciación de eventos.

El usuario sale de su hogar utilizando la pulsera correctamente ajustada. Al iniciar el trayecto, la aplicación móvil establece comunicación con el dispositivo e inicia el registro continuo de variables fisiológicas y de movimiento.

Minutos más tarde, el usuario sufre un movimiento brusco asociado a un arrebato violento. El acelerómetro MPU6050 detecta la aceleración abrupta y el sistema activa el primer trigger. Simultáneamente, el sensor MAX30102 registra un aumento significativo en la frecuencia cardíaca, reforzando la condición de riesgo.

El dispositivo envía una alerta inmediata a la aplicación móvil, que registra el evento y notifica al contacto de emergencia. La notificación incluye la hora del incidente, las variables medidas y el estado del usuario al momento del suceso.

El contacto de emergencia recibe la alerta y procede según corresponda, mientras la aplicación continúa registrando datos para evidenciar la evolución del evento. El sistema mantiene activo el monitoreo hasta que el usuario confirma su estado de seguridad.

## 25. Conclusión

**TicPrev** aborda una problemática social creciente que es la inseguridad personal y el robo de teléfonos celulares. A diferencia de las soluciones existentes, como los botones de pánico y las aplicaciones de seguridad que requieren de la acción manual del usuario, esta propuesta se distingue por su enfoque automatizado. Al integrar sensores biométricos (MAX30102) y de movimiento (Módulo GY-521 (MPU-6050)), la pulsera puede detectar automáticamente situaciones de riesgo.

El sistema es capaz de responder a dos escenarios de robo en específico. Un robo repentino, la desconexión del dispositivo activa una alarma sonora si el usuario no ingresa un PIN de seguridad en un minuto, lo que dificulta la acción del delincuente y alerta a terceros. En el caso de un robo bajo amenaza, la pulsera detecta un aumento en la frecuencia cardíaca o un forcejeo, activando un protocolo que puede notificar a un contacto de emergencia sin poner en riesgo al usuario. Adicionalmente, la funcionalidad de **zonas seguras** permite evitar falsos positivos en entornos controlados como el hogar o el trabajo.

Por lo tanto, **Ticprev** no solo ofrece una respuesta tecnológica a un problema social, sino que también representa una solución que ayuda a aumentar la sensación de seguridad de los usuarios.

## **Referencias**

- La Tercera. (2024, julio). *72 mil celulares fueron bloqueados tras ser robados durante el primer semestre* [Consultado el 7 de septiembre de 2025]. <https://www.latercera.com/nacional/noticia/72-mil-celulares-fueron-bloqueados-tras-ser-robados-durante-el-primer-semestre/DVXUGELVP5EDLKXN2FJRQMST5U/#:~:text=72%20mil%20celulares%20fueron%20bloqueados,el%20primer%20semestre%20-%20La%20Tercera>
- Policía de Investigaciones de Chile. (2025, junio). *El más buscado – Episodio 03.* <https://www.pdichile.cl/centro-de-prensa/detalle-prensa/2025/06/27/el-m%C3%A1s-buscado-episodio-03>
- Universidad San Sebastián. (2025, mayo). *Delincuencia en el país: cambio en hábitos por seguridad.* <https://www.uss.cl/noticias/delincuencia-pais-aumento/#:~:text=Cambio%20en%20h%C3%A1bitos%20por%20seguridad,su%20libertad%20por%20m%C3%A1s%20seguridad>.