

**UNIVERSIDAD NACIONAL  
TORIBIO RODRÍGUEZ DE MENDOZA DE AMAZONAS**



**FACULTAD DE INGENIERÍA DE SISTEMAS Y MECÁNICA  
ELÉCTRICA  
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS**

**TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE  
INGENIERO DE SISTEMAS**

**TÍTULO DE LA TESIS**

**“SISTEMA DE MONITOREO Y CONTROL PARA LA  
SEGURIDAD PERSONAL UTILIZANDO DISPOSITIVOS  
WEARABLES”**

**Autor : Bach. Natalio Oswaldo Salinas Ponce**

**Asesor : Mg. Carlos Luis Lobatón Arenas**

**Registro : \_\_\_\_\_**

**CHACHAPOYAS – PERÚ**

**2023**



ANEXO 3-H

AUTORIZACIÓN DE PUBLICACIÓN DE LA TESIS EN EL REPOSITORIO INSTITUCIONAL DE LA UNTRM

1. Datos de autor 1

Apellidos y nombres (tener en cuenta las tildes): SACINAS PONCE NATALIO OSWALDO
DNI N°: 01317837
Correo electrónico: 0131783741@untrm.edu.pe
Facultad: Ingeniería de Sistemas y Mecánica Eléctrica
Escuela Profesional: Ingeniería de sistemas

Datos de autor 2

Apellidos y nombres (tener en cuenta las tildes):
DNI N°:
Correo electrónico:
Facultad:
Escuela Profesional:

2. Título de la tesis para obtener el Título Profesional

Sistema de Monitoreo y control para la seguridad personal utilizando dispositivos wearables.

3. Datos de asesor 1

Apellidos y nombres:
DNI, Pasaporte, C.E N°:
Open Research and Contributor-ORCID (https://orcid.org/0000-0002-9670-0970)

Datos de asesor 2

Apellidos y nombres: LOBATÓN ARENAS CARLOS LUIS
DNI, Pasaporte, C.E N°: 17614582
Open Research and Contributor-ORCID (https://orcid.org/0000-0002-9670-0970) 0000-0002-0209-9337

4. Campo del conocimiento según la Organización para la Cooperación y el Desarrollo Económicos- OCDE (ejemplo: Ciencias médicas, Ciencias de la Salud-Medicina básica-Immunología)

https://catalogos.concytec.gob.pe/vocabulario/ocde\_ford.html
2,00.00 - Ingeniería Tecnológica

5. Originalidad del Trabajo

Con la presentación de esta ficha, el(la) autor(a) o autores(as) señalan expresamente que la obra es original, ya que sus contenidos son producto de su directa contribución intelectual. Se reconoce también que todos los datos y las referencias a materiales ya publicados están debidamente identificados con su respectivo crédito e incluidos en las notas bibliográficas y en las citas que se destacan como tal.

6. Autorización de publicación

El(los) titular(es) de los derechos de autor otorga a la Universidad Nacional Toribio Rodríguez de Mendoza de Amazonas (UNTRM), la autorización para la publicación del documento indicado en el punto 2, bajo la Licencia creative commons de tipo BY-NC: Licencia que permite distribuir, remezclar, retocar, y crear a partir de su obra de forma no comercial por lo que la Universidad deberá publicar la obra poniéndola en acceso libre en el repositorio institucional de la UNTRM y a su vez en el Registro Nacional de Trabajos de Investigación-RENATI, dejando constancia que el archivo digital que se está entregando, contiene la versión final del documento sustentado y aprobado por el Jurado Evaluador.

Chachapoyas, 05.11.2023



Firma del autor 1
Firma del Asesor 1

Firma del autor 2
Firma del Asesor 2

## **Dedicatoria**

### **MI FAMILIA**

*Mi hija, Angela y hermana, por su cariño de siempre, en todos estos años que permitieron mi formación profesional*

## **Agradecimiento**

*Agradezco a Dios por consagrar mi vida, por guiarme y darme fuerza día a día a continuar en aquellos momentos de dificultad y debilidad.*

*Agradezco también a mi familia, por ser los principales generadores para lograr esta meta y por contar siempre con su apoyo moral incondicional.*

*A mi asesor, Ing. Carlos Lobatón Arenas, por las oportunidades para culminar esta tesis, cuya orientación, conocimiento, enseñanza y colaboración me permitieron desarrollar esta investigación.*

*A los docentes integrantes del jurado, por sus contribuciones y recomendaciones para la mejora del informe final.*

AUTORIDADES DE LA UNIVERSIDAD NACIONAL TORIBIO RODRÍGUEZ DE  
MENDOZA DE AMAZONAS

**Ph.D. Jorge Luis Maicelo Quintana**

Rector

**Dr. Oscar Andrés Gamarra Torres**

Vicerrector Académico

**Dra. María Nelly Lujan Espinoza**

Vicerrectora de Investigación

**Dr. Italo Maldonado Ramírez**

Decano de la Facultad de Ingeniería de Sistemas y Mecánica Eléctrica



## ANEXO 3-L

### VISTO BUENO DEL ASESOR DE TESIS PARA OBTENER EL TÍTULO PROFESIONAL

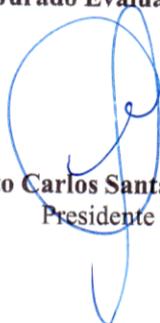
El que suscribe el presente, docente de la UNTRM (x)/Profesional externo ( ), hace constar que ha asesorado la realización de la Tesis titulada Sistema de monitoreo y control para la Seguridad Personal utilizando dispositivos wearables; del egresado Natalio Oswaldo Salinas Ponce de la Facultad de Ingeniería de sistemas y Mecánica eléctrica Escuela Profesional de Ingeniería de sistemas de esta Casa Superior de Estudios.

El suscrito da el Visto Bueno a la Tesis mencionada, dándole pase para que sea sometida a la revisión por el Jurado Evaluador, comprometiéndose a supervisar el levantamiento de observaciones que formulen en Acta en conjunto, y estar presente en la sustentación.

Chachapoyas, 12 de Octubre de 2022

Firma y nombre completo del Asesor

**Jurado Evaluador**



**Mg. Roberto Carlos Santa Cruz Acosta.**  
Presidente



**Dr. Carlos Alberto Rios Campos**  
Secretario



**Mg. Eder Nicanor Figueroa Piscoya**  
Vocal



ANEXO 3-Q

CONSTANCIA DE ORIGINALIDAD DE LA TESIS PARA OBTENER EL TÍTULO PROFESIONAL

Los suscritos, miembros del Jurado Evaluador de la Tesis titulada:

SISTEMA DE MONITOREO Y CONTROL PARA LA SEGURIDAD PERSONAL UTILIZANDO DISPOSITIVOS WEARABLES

presentada por el estudiante ( )/egresado (X) NATALIO OSWALDO SALINAS PONCE

de la Escuela Profesional de INGENIERÍA DE SISTEMAS

con correo electrónico institucional 0131783741@untrm.edu.pe

después de revisar con el software Turnitin el contenido de la citada Tesis, acordamos:

- a) La citada Tesis tiene 20 % de similitud, según el reporte del software Turnitin que se adjunta a la presente, el que es menor (X) / igual ( ) al 25% de similitud que es el máximo permitido en la UNTRM.
- b) La citada Tesis tiene \_\_\_\_\_ % de similitud, según el reporte del software Turnitin que se adjunta a la presente, el que es mayor al 25% de similitud que es el máximo permitido en la UNTRM, por lo que el aspirante debe revisar su Tesis para corregir la redacción de acuerdo al Informe Turnitin que se adjunta a la presente. Debe presentar al Presidente del Jurado Evaluador su Tesis corregida para nueva revisión con el software Turnitin.



Chachapoyas, 10 de MAYO del 2023

[Signature]  
SECRETARIO

[Signature]  
PRESIDENTE

[Signature]  
VOCAL

OBSERVACIONES:

.....  
.....



ANEXO 3-5

ACTA DE SUSTENTACIÓN DE TESIS PARA OBTENER EL TÍTULO PROFESIONAL

En la ciudad de Chachapoyas, el día 25 de Julio del año 2023, siendo las 10:00 horas, el aspirante: Natalio Oswaldo Salinas Ponce, asesorado por Mg. Carlos Luis Lobaton Arenas defiende en sesión pública presencial (  ) / a distancia (  ) la Tesis titulada: Sistema de Monitoreo y Control para la Seguridad Personal Utilizando Dispositivos Wearables, para obtener el Título Profesional de Ingeniero de Sistemas, a ser otorgado por la Universidad Nacional Toribio Rodríguez de Mendoza de Amazonas; ante el Jurado Evaluador, constituido por:

Presidente: Mag. Roberto Carlos Santa Cruz Acosta

Secretario: Dr. Carlos Alberto Ríos Campos

Vocal: Mgg. Eder Nicanor Figueroa Piscoya

Procedió el aspirante a hacer la exposición de la Introducción, Material y métodos, Resultados, Discusión y Conclusiones, haciendo especial mención de sus aportaciones originales. Terminada la defensa de la Tesis presentada, los miembros del Jurado Evaluador pasaron a exponer su opinión sobre la misma, formulando cuantas cuestiones y objeciones consideraron oportunas, las cuales fueron contestadas por el aspirante.

Tras la intervención de los miembros del Jurado Evaluador y las oportunas respuestas del aspirante, el Presidente abre un turno de intervenciones para los presentes en el acto de sustentación, para que formulen las cuestiones u objeciones que consideren pertinentes.

Seguidamente, a puerta cerrada, el Jurado Evaluador determinó la calificación global concedida a la sustentación de la Tesis para obtener el Título Profesional, en términos de:

Aprobado (  ) por Unanimidad (  ) / Mayoría (  ) Desaprobado (  )

Otorgada la calificación, el Secretario del Jurado Evaluador lee la presente Acta en esta misma sesión pública. A continuación se levanta la sesión.

Siendo las 11:00 horas del mismo día y fecha, el Jurado Evaluador concluye el acto de sustentación de la Tesis para obtener el Título Profesional.

[Signature]  
SECRETARIO

[Signature]  
VOCAL

[Signature]  
PRESIDENTE

OBSERVACIONES:

.....

## Índice

Índice .....	x
Índice de Tablas .....	xiii
Índice de Figuras .....	xiv
Resumen .....	xviii
Abstract .....	xix
I. INTRODUCCIÓN .....	20
1.1. Motivación .....	20
1.2. Objetivos .....	22
1.2.1 Objetivo general .....	22
1.2.2 Objetivos específicos .....	22
1.3. Metodología .....	22
II. MATERIALES Y METODOS .....	24
2.1. Población .....	24
2.2. Muestra .....	24
2.3. PROCEDIMIENTOS .....	24
2.3.1 DISEÑO DE TÉCNICAS DE RECOLECCIÓN DE LA INFORMACIÓN .....	24
2.3.2 TÉCNICAS E INSTRUMENTOS .....	25
2.3. Variables de estudio .....	25
2.4. Métodos .....	25
2.4.1 Indicadores .....	25
III. RESULTADOS .....	26
3.1 Objetivo 1: Determinar las fuentes de información tanto cuantitativas como cualitativas que permitan profundizar en el estudio de la seguridad personal. ....	26
3.1.1 Introducción .....	26
3.1.2 Plan Nacional de Seguridad Ciudadana 2019 – 2023 .....	27
3.1.3 Alineamiento Estratégico .....	28
3.2. Objetivo 2: Estudiar y analizar los diferentes tipos de dispositivos wearables, así como los protocolos de comunicación utilizados. ....	31
3.2.1 Wearables inteligentes .....	31
3.2.2 Reconocimiento de emociones .....	32
3.2.3 Tele monitorización pasiva .....	33
3.2.4 Variables a monitorizar para detectar una situación de agresión .....	34
3.2.5 Movimientos abruptos .....	34
3.2.6 Respiración .....	35

3.2.7 Actividad del corazón.....	35
3.2.8 Presión sanguínea.....	36
3.2.8 Glicemia .....	36
3.2.9 La temperatura.....	36
3.2.10 La transpiración.....	37
3.2.11 Conductancia de la piel.....	37
3.2.12 Actividad cerebral .....	37
3.2.13 Tensión muscular .....	38
3.2.14 Voz, sonido ambiental .....	38
3.2.15 Variables biológicas adicionales.....	38
3.2.16 Parámetros de medición.....	39
3.2.17 Dispositivos de activación de la alerta.....	39
3.3. Objetivo 3: Estudiar y analizar los diferentes sistemas de monitorización basados en seguridad personal, que mejor se adapten al proyecto. ....	40
3.3.1 Sistemas de monitorización y control .....	40
3.3.2 Sistemas de activación autónoma .....	40
3.3.3 Sistemas de activación manual .....	41
3.3.4 Sistemas de activación autónoma - manual .....	42
3.3.5 Sistemas de seguridad personal en el mercado .....	43
3.4. Objetivo 4: Seleccionar los mecanismos de reconocimiento de la agresión física del usuario en base al análisis de los diferentes tipos de dispositivos wearables que porta el usuario, las distintas técnicas de captación de la información, los medios utilizados para recoger dicha información y almacenarla en una plataforma. ....	49
3.4.1 Posibles arquitecturas y tecnologías utilizadas en la plataforma a desarrollar ....	49
3.4.2 Arquitectura.....	49
3.4.3 Eventos.....	50
3.4.3.1 <i>Generador de evento</i> .....	50
3.4.3.2 <i>Canales de evento</i> .....	50
3.4.4 Estilo arquitectónico REST. ....	50
3.4.4 Tecnologías usadas en el proyecto.....	53
3.5 Objetivo 5 Determinar las herramientas para el diseño y modelado; así como la arquitectura del sistema para el desarrollo de la plataforma de este proyecto. ....	56
3.5.1 Android .....	56
3.5.2 Gestores de Bases de Datos .....	59
3.5.3 JAVA .....	60
3.5.4 JERSEY.....	60
3.6 Objetivo 6: Seleccionar los dispositivos wearables, la tecnología de comunicación y dispositivos móviles más adecuados al proyecto, en base a los datos que pueden proporcionar	

en él envió de la alerta.....	61
3.6.1    Los dispositivos wearables .....	61
3.6.2    Wearables para monitorear la seguridad personal.....	62
3.6.3    Relojes (Smart Watch).....	62
3.6.4    Pulseras (Smart Bands).....	63
3.6.5    Anillos (Smart Ring) .....	64
3.6.6    Hearables .....	64
3.6.7    Ropa inteligente (Smart Clothes).....	65
3.7 Objetivo 7: Realizar pruebas unitarias del sistema para evaluar el buen funcionamiento, conforme a los requisitos establecidos. ....	68
3.7.1    Especificaciones técnicas para el despliegue de la plataforma.....	68
3.7.2    Descripción de la plataforma .....	69
3.7.3    Requerimientos de la plataforma .....	70
3.8 Objetivo 8: Preparar un piloto del sistema con voluntarios, para evaluar el grado de aceptación del sistema. ....	97
3.8.1    Análisis del sistema .....	97
3.8.1.1    Selección de los parámetros para medir la actividad física .....	97
3.8.2    Selección del wearables para la implementación .....	98
3.8.3    Modelo conceptual del sistema.....	98
3.8.4    Diseño de la plataforma.....	101
3.8.5    Diseño de interfaces gráficas de la plataforma.....	103
3.8.6    Modelo relacional de la base de datos .....	112
3.8.7    Implementación .....	115
3.8.8    Implementación a nivel de captura de datos .....	121
3.8.9    Implementación a nivel de percepción de datos.....	132
3.8.10    Conectividad con los diferentes wearables. ....	133
3.8.11    Implementación con Xioami Mi Band 6.....	133
3.8.12    Resultados de la implementación.....	136
3.8.13    Resultados del servicio rest. ....	138
3.8.14    Casos de prueba realizados en la plataforma. ....	138
IV.    DISCUSIÓN .....	142
4.1    Análisis del Despliegue del sistema de monitoreo y control para la seguridad personal utilizando dispositivos wearables propuesto.....	144
4.2    Análisis de la validación del sistema de monitoreo y control para la seguridad personal utilizando dispositivos wearables propuesto .....	144
V.    CONCLUSIONES .....	147
VI.    RECOMENDACIONES .....	149

VII. REFERENCIAS BIBLIOGRAFICAS .....	150
ANEXO N° 01 .....	156
ANEXO N° 02 .....	157
ANEXO N° 03 .....	158

### **Índice de Tablas**

Tabla 1. Estadística del total de horas y total de tareas .....	23
Tabla 2. Alineamiento Estratégico del PNSC 2019 – 2023 .....	29
Tabla 3. Factores de Riesgo.....	30
Tabla 4. Comparativa de los dispositivos de seguridad personal en el mercado .....	48
Tabla 5. Wearables para monitorear los sobrevivientes de violencia.....	67
Tabla 6. Crear cuenta.....	73
Tabla 7. Iniciar Sesión.....	74
Tabla 8. Configurar lista de contactos .....	76
Tabla 9. Configurar comandos de reconocimiento de voz.....	77
Tabla 10. Analizar Datos Biológicos.....	78
Tabla 11. Programar cuenta atrás .....	80
Tabla 12. Activar cuenta atrás .....	81
Tabla 13. Desactivar cuenta atrás .....	82
Tabla 14. Activar modo supervisión.....	83
Tabla 15. Desactivar modo supervisión.....	84
Tabla 16. Efectuar alerta .....	85
Tabla 17. Enviar alerta .....	86
Tabla 18. Grabar audio del entorno .....	87
Tabla 19. Obtener información del entorno .....	88
Tabla 20. Tomar foto.....	89
Tabla 21. Rastreo de ubicación por GPS .....	90
Tabla 22. Ver historial de alertas .....	91
Tabla 23. Ver historial de rastreo por ubicación GPS.....	92
Tabla 24. Emparejar dispositivos .....	93
Tabla 25. Actualizar aplicación instalada .....	94
Tabla 26. Registrar perfil.....	95
Tabla 27. Consultar perfil.....	95
Tabla 28. Actualizar perfil.....	96
Tabla 29. Descripción de las clases de la plataforma.....	101
Tabla 30. Descripción de la funcionalidad al iniciar sesión.....	139

Tabla 31.	Descripción de la funcionalidad al crear usuario. ....	139
Tabla 32.	Descripción de la funcionalidad ver perfil. ....	140
Tabla 33.	Descripción de la funcionalidad editar usuario. ....	141
Tabla 34.	Descripción de la funcionalidad emparejar dispositivo. ....	141
Tabla 35.	Descripción de los servicios de monitorización. ....	141
Tabla 36.	Descripción de la funcionalidad en la supervisión. ....	142
Tabla 37.	Relevancia Final de cada atributo del sistema de monitoreo y control para la seguridad personal. ....	145
Tabla 38.	Opinión antes del análisis de verificación del sistema por el experto y opinión después del análisis de verificación del sistema por el experto. ....	146
Tabla 39.	Formato de encuesta al atributo conformidad del sistema. ....	156
Tabla 40.	Formato de encuesta al atributo amigabilidad del sistema. ....	157
Tabla 41.	Formato de encuesta al atributo tiempo de respuesta a un incidente. ....	157
Tabla 42.	Resultado de encuestas de evaluación del sistema en conformidad. ....	157
Tabla 43.	Resultado de encuestas de evaluación del sistema en amigabilidad. ....	158
Tabla 44.	Resultado de encuestas de evaluación del sistema en tiempo de respuesta a un incidente. ....	158
Tabla 45.	Herramientas y tecnologías utilizadas. ....	159

### **Índice de Figuras**

Figura 1.	Porcentaje del número de tareas por tipo. ....	24
Figura 2.	Porcentaje del número de horas por tipo. ....	24
Figura 3.	Mapa Estratégico PNSC 2019 - 2023. ....	31
Figura 4.	Sistema de alarma autónomo para sobrevivientes de violencia basado en Monitoreo Pasivo. ....	34
Figura 5.	Flujo para el Procesamiento de un Evento. ....	50
Figura 6.	Arquitectura REST. ....	51
Figura 7.	Niveles de la Arquitectura REST. ....	52
Figura 8.	Arquitectura de un Dispositivo Wearable con BLE. ....	54
Figura 9.	Jerarquía de Perfiles GATT. ....	56
Figura 10.	Arquitectura del Sistema Operativo Android. ....	57
Figura 11.	Apple Watch Series 7. ....	63
Figura 12.	Fitbit Charge 5. ....	64
Figura 13.	Anillo Motiv. ....	64
Figura 14.	Audífonos BeHeard. ....	64
Figura 15.	Smart Clothes Athos. ....	65
Figura 16.	Diagrama General de Casos de Uso. ....	71

Figura 17.	Gestión de Contactos .....	72
Figura 18.	Gestión del Aprendizaje Automático .....	76
Figura 19.	Gestión del modo cuenta atrás .....	79
Figura 20.	Gestión del modo supervisión.....	82
Figura 21.	Gestión de alertas .....	84
Figura 22.	Gestión del administrador.....	93
Figura 23.	Mi Smart Band 6 .....	98
Figura 24.	Modelo conceptual de la plataforma.....	99
Figura 25.	Arquitectura principal de la plataforma .....	102
Figura 26.	Arquitectura por capas de la aplicación móvil .....	103
Figura 27.	prototipo de la interfaz Iniciar sesión.....	104
Figura 28.	Prototipo crear cuenta.....	104
Figura 29.	Prototipo crear cuenta registrando teléfono .....	105
Figura 30.	Prototipo crear cuenta validando teléfono.....	105
Figura 31.	Prototipo configurar lista de contactos.....	105
Figura 32.	Prototipo importar contactos existentes .....	106
Figura 33.	Prototipo registrar contacto nuevo .....	106
Figura 34.	Prototipo para seleccionar contacto existente a editar.....	106
Figura 35.	Prototipo para editar contacto existente .....	107
Figura 36.	Prototipo para configurar los comandos de voz .....	107
Figura 37.	Prototipo para programar cuenta atrás. ....	107
Figura 38.	Prototipo para programar supervisión de actividad.....	108
Figura 39.	Prototipo para registrar nueva actividad .....	108
Figura 40.	Prototipo para iniciar supervisión de actividad .....	108
Figura 41.	Prototipo para rastrear ubicación GPS de la actividad .....	109
Figura 42.	Prototipo para finalizar supervisión de actividad .....	109
Figura 43.	Prototipo para activar el botón de pánico.....	109
Figura 44.	Prototipo para enviar alerta de pánico.....	110
Figura 45.	Prototipo para cancelar alerta de pánico .....	110
Figura 46.	Prototipo para mostrar el menú principal.....	110
Figura 47.	Prototipo de registrar perfil.....	111
Figura 48.	Prototipo de emparejar dispositivos.....	111
Figura 49.	Prototipo de historial de alertas .....	111
Figura 50.	Prototipo de ajustes avanzados .....	112
Figura 51.	Información adicional.....	112
Figura 52.	Modelo relacional de Base de Datos.....	113

Figura 53.	Despliegue del nivel de persistencia de datos .....	115
Figura 54.	Diagrama de paquetes del servicio Rest .....	116
Figura 55.	Clases del paquete model.....	117
Figura 56.	Clases del paquete dao.....	118
Figura 57.	Parámetros de configuración de la base de datos en web.xml.....	118
Figura 58.	Clases del paquete logic. ....	119
Figura 59.	Clases del paquete request. ....	119
Figura 60.	Clases del paquete response.....	120
Figura 61.	jar para utilizar Jersey.....	120
Figura 62.	configuración de Jersey en el web.xml. ....	121
Figura 63.	Clases del paquete resource. ....	121
Figura 64.	diagrama de despliegue del nivel de captura de datos.....	121
Figura 65.	constructor para generar la conexión con SQLite. ....	122
Figura 66.	método para crear las tablas en SQLite.....	123
Figura 67.	método para actualizar las estructuras de las tablas. ....	123
Figura 68.	variables para la creación de una tabla en SQLite.....	124
Figura 69.	insertar valores por defecto en tablas básicas.....	124
Figura 70.	diagrama de paquetes de la aplicación móvil.....	125
Figura 71.	clases del paquete ConnectionManager. ....	126
Figura 72.	clases del paquete clienteRest.....	126
Figura 73.	clases del paquete model. ....	127
Figura 74.	clases del paquete dao.....	128
Figura 75.	clases del paquete logic. ....	128
Figura 76.	clases del paquete request. ....	129
Figura 77.	clases del paquete response .....	129
Figura 78.	funcionamiento de actividades y fragmentos .....	130
Figura 79.	despliegue del nivel de percepción de datos .....	132
Figura 80.	conexión Bluetooth con la pulsera. ....	133
Figura 81.	obteniendo el dispositivo a través de la MAC.....	134
Figura 82.	conexión a los servicios gatt de un dispositivo. ....	135
Figura 83.	método que detecta un cambio en la conexión con la gatt del dispositivo. ....	135
Figura 84.	método que permite escribir en cualquier servicio y característica un array de bytes. ....	136
Figura 85.	método para enviar una notificación a la pulsera Mi band 6.....	136
Figura 86.	iniciar sesión del participante. ....	137
Figura 87.	registrar participante. ....	137

Figura 88.	emparejar dispositivos.....	138
Figura 89.	Promedio de los indicadores del análisis de opinión.....	146

## Resumen

Propuesta de un sistema de monitoreo y control para la seguridad personal utilizando dispositivos wearables.

La tesis propone el diseño y desarrolló de una plataforma software que monitoriza y controla de forma continua la seguridad personal a través de dispositivos wearables con la cual se va a poder, por un lado, enviar señales de alerta de manera manual o de forma automática si el sistema detecta que los signos vitales del usuario se encuentran alterados en caso exista violencia física. Al enviar la alerta, el sistema proporciona información del usuario a sus contactos predefinidos, con el objetivo de actuar de inmediato para prevenir y acudir frente a cualquier atentado contra su integridad física del usuario.

Para el desarrollo del proyecto se optó por una metodología establecida con el método científico apoyándonos en la planificación de las tareas a realizar con la metodología SCRUM (marco de trabajo para desarrollo ágil de software), que permite llevar a cabo el proceso de investigación mediante el desarrollo de tareas de corta duración.

Además, por el hecho de que se cuenta con una vasta cartera tecnológica en el mercado y a bajo costo que nos facilita implementar la arquitectura para una propuesta factible a implementar en la localidad de Bagua.

Por lo que, la propuesta permite mejorar la seguridad, personal de los usuarios mediante el uso de dispositivos wearables inteligentes configuradas y desarrollados en la plataforma Android.

**Palabras clave:** Wearable, violencia física, aplicación móvil, servicio rest, aprendizaje automático.

## Abstract

Proposal for a monitoring and control system for personal security using wearable devices.

The thesis proposes the design and development of a software platform that continuously monitors and controls personal security through wearable devices with which it will be possible, on the one hand, to send alert signals manually or automatically if the system detects that the user's vital signs are altered in the event of physical violence. By sending the alert, the system provides user information to its predefined contacts, with the aim of acting immediately to prevent and respond to any attack against the user's physical integrity.

For the development of the project, a methodology established with the scientific method was chosen, supporting us in the planning of the tasks to be carried out with the SCRUM methodology (framework for agile software development), which allows carrying out the research process through the development of short duration tasks.

In addition, due to the fact that there is a vast technological portfolio in the market and at a low cost that makes it easier for us to implement the architecture for a feasible proposal to be implemented in the town of Bagua.

Therefore, the proposal allows users to improve personal security through the use of smart wearable devices configured and developed on the Android platform.

**Keywords:** Wearable, physical violence, mobile application, rest service, machine learning.

## **I.INTRODUCCIÓN**

La seguridad y bienestar de la sociedad ha sido siempre un tema esencial para el estado peruano y no es ajeno a ello la localidad de Bagua, que con el paso del tiempo son testigos o víctimas de actos delictivos, como lo son los ataques personales dentro o fuera de un área laboral o del domicilio de residencia.

Actualmente, existe una gran variedad de sistemas de vigilancia, muchos de los cuales son dispositivos móviles, dispositivos biométricos y de reconocimiento facial, pero el costo de adquirirlos es alto, lo que los residentes de áreas propensas a la delincuencia no pueden pagar, lo que limita su seguridad en estas áreas.

Al encontrarnos en una era de digitalización donde la tecnología está en su auge, es de necesidad diseñar e implementar un sistema de seguridad personal de bajo costo con dispositivos wearables de seguimiento pasivo del usuario que lo porta en tiempo real.

Así, se presenta un panorama general del proyecto de investigación, el motivo y necesidad que motivó el desarrollo de esta investigación, y los objetivos a alcanzar. También se examina la metodología utilizada para lograr los objetivos y la estructura de montaje de un sistema de seguridad personal utilizando dispositivos wearables.

### **1.1.Motivación**

Actualmente existen grandes avances tecnológicos con respecto a los dispositivos wearables que permiten monitorizar y supervisar a una persona a través de envío de señales de alerta. Muchos de estos dispositivos tienen un bajo costo lo que facilita acceder a ellos sin restricciones. Además, si comparamos los costos y los beneficios que brindan los dispositivos se obtiene que el costo es considerablemente barato a comparación con los grandes beneficios que brinda en la mejora de la seguridad de las personas usuarias.

Los dispositivos wearables actuales tienen grandes ventajas, como lo es la supervisión constante de los parámetros fisiológicos. Lo que permite al sistema enviar señales de alerta en caso de que los signos vitales se encuentran alterados. Otra de las ventajas de los dispositivos es su inmersión, ya que estarán conectados a las personas sin causar ningún tipo de molestia y con el transcurrir del tiempo se olvidarán que llevan consigo un dispositivo que se encuentra obteniendo información permanentemente de los signos vitales del usuario.

Dentro de las aplicaciones de los dispositivos wearables se encuentra un sistema de alarma autónomo que se encarga de garantizar la seguridad personal basado en el monitoreo pasivo continuo a través de biosensores y técnicas de aprendizaje automático para inferir si se está produciendo una situación anormal relacionada con la violencia de género, activando en este caso una alarma. (Rodríguez-Rodríguez I. a.-V.-M.-G., 2020).

Dado que los delitos sobre todo contra las mujeres que van en aumento a diario, es necesario que los gobiernos implementen más medidas preventivas que permitan a las mujeres sentirse seguras en todo momento del día, por tal razón se requiere un sistema que esté disponible las 24 horas del día, los 7 días de la semana para evitar situaciones desafortunadas. Por este motivo se cuenta con un sistema donde el usuario pueda activar manualmente a través de una banda, presionando el botón de activación o de manera automática a través de un sensor de micrófono, si el usuario está hablando (Chaudhari, Archana and Patel, Jahnavi and Savla, Krishi and Shetty, Akshitha and Shah, Vrushika, 2020). Por otro lado, el Banco Interamericano de Desarrollo (BID) sostiene que América Latina y el Caribe (ALC) vienen librando una guerra de baja intensidad, pero de alta mortalidad y de enormes costos económicos, sociales y políticos. Estas condiciones han creado zozobra social al punto que alrededor del 43% de la población tiene miedo de ser víctima de un delito, y la seguridad pública se ha convertido en una de las preocupaciones más apremiantes para los ciudadanos. (Chinchilla, Laura and Vorndran, Doreen, 2018). Perú cuenta con el Plan Nacional de Seguridad Ciudadana 2019-2023 fortalece la seguridad de la población frente a los delitos en el territorio del país, el cual incluye medidas que coadyuven a fortalecer el precepto, la paz y la seguridad en el país.

Varios dispositivos de uso externo como es el caso de los wearables vienen implementados con los mecanismos para realizar mediciones de la temperatura corporal, la frecuencia cardíaca, el movimiento muscular, la actividad física y otros datos críticos a través de sensores incorporados, permitiendo tener información de los parámetros fisiológicos de los seres humanos de forma continua. (Mukhopadhyay, Subhas Chandra, 2014). También, la tecnología de comunicación de campo cercano (NFC) permitirá la conectividad e intercambio de datos con los teléfonos inteligentes (Kulkarni, 2021). Por otro lado, se han desarrollado diferentes tipos de aplicaciones de seguridad personal, sin embargo, hay poca

investigación sobre como las personas pueden responder en diferentes situaciones de seguridad personal y como estas aplicaciones pueden contribuir a su respuesta. (Just, 2019).

## **1.2.Objetivos**

### **1.2.1 Objetivo general**

Diseño y desarrollo de una plataforma que permita monitorizar y controlar de forma continua la seguridad personal, mediante la utilización de dispositivos wearables en la localidad de Bagua.

### **1.2.2 Objetivos específicos**

- Determinar las fuentes de información tanto cuantitativas como cualitativas que permitan profundizar en el estudio de la seguridad personal.
- Estudiar y analizar los diferentes tipos de dispositivos wearables, así como los protocolos de comunicación utilizados.
- Estudiar y analizar los diferentes sistemas de monitorización basados en seguridad personal, que mejor se adapten al proyecto.
- Seleccionar los mecanismos de reconocimiento de la agresión física del usuario en base al análisis de los diferentes tipos de dispositivos wearables y dispositivo móvil que porta el usuario, las distintas técnicas de captación de la información, los medios utilizados para recoger dicha información y almacenarla en la plataforma.
- Determinar las herramientas para el diseño y modelado; así como la arquitectura del sistema para el desarrollo de la plataforma de este proyecto.
- Seleccionar los dispositivos wearables, la tecnología de comunicación y dispositivos móviles más adecuados al proyecto, en base a los datos que pueden proporcionar en el envío de la alerta.
- Realizar pruebas unitarias del sistema para evaluar el buen funcionamiento, conforme a los requisitos establecidos.
- Preparar un piloto del sistema con voluntarios, para evaluar el grado de aceptación del sistema.

## **1.3.Metodología**

Para el desarrollo del proyecto se optó por una metodología basada en el método científico, estableciendo una hipótesis de partida que se probará a partir del estudio de los trabajos

académicos relacionados con dicho tema de investigación y las distintas soluciones comerciales actualmente disponibles, utilizando diversos tipos de fuentes basados en búsqueda por Internet, artículos científicos, artículos de revisión, ponencias en congresos, secciones de libros, patentes, etc. Se planificaron las tareas a realizar siguiendo una metodología SCRUM (marco de trabajo para desarrollo ágil de software), que permite llevar a cabo el proceso de investigación mediante el desarrollo de tareas de corta duración que, de manera incremental, se irán abordando en los distintos aspectos del tema de investigación. El progreso del proyecto de investigación se va determinado en los Sprints que se realizaron en coordinación con el asesor del proyecto.

Como resultado del trabajo, y para comprobar la factibilidad de la investigación realizada, se realizó un piloto con usuarios a los que se le solicitó un consentimiento informado.

Como hipótesis de partida se consideró que el usuario cuente con un dispositivo wearable (pulsera de actividad) y un dispositivo móvil para la captación de información y envío de la alerta. La plataforma desarrollada podrá ser utilizada por cualquier tipo de usuario.

Seguidamente, se presenta el porcentaje de desarrollo de las tareas tanto de implementación de la plataforma, como de trabajo de investigación. Partiendo como fecha inicial el mes de noviembre del año 2021 y culminando en el mes de setiembre del año 2022.

En la **tabla 1**, se presenta una estadística del total de horas y el total de tareas

	<b>Número de tareas</b>	<b>Horas trabajadas</b>
Sprints	14	195
Investigación	08	155
Implementación	01	10
<b>Total</b>	<b>23</b>	<b>360</b>

*Tabla 1. Estadística del total de horas y total de tareas*

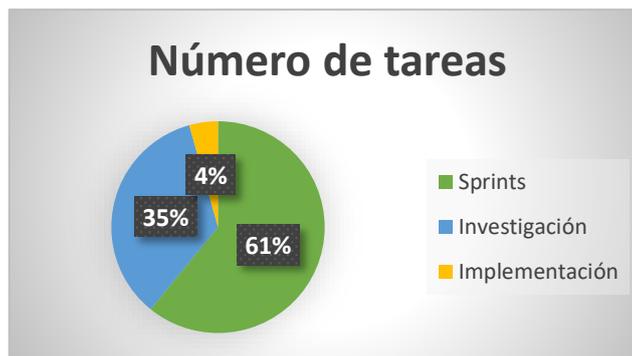


Figura 1. Porcentaje del número de tareas por tipo



Figura 2. Porcentaje del número de horas por tipo

## II. MATERIALES Y METODOS

### 2.1. Población

Como población se consideró a los ciudadanos del distrito de Bagua (ciudad) que corresponde a personas con mayoría de edad conformada por varones y mujeres de manera indeterminada.

### 2.2. Muestra

Caso de estudio del sistema de seguridad personal de bajo costo con dispositivos wearables de seguimiento pasivo que permita monitorear y controlar permanentemente a los usuarios en el periodo mayo 2022 a setiembre 2022

#### Unidad de análisis

Proceso de análisis de indicadores de seguridad personal con dispositivos wearables en el periodo mayo 2022 - setiembre 2022.

## 2.3 PROCEDIMIENTOS

### 2.3.1 DISEÑO DE TÉCNICAS DE RECOLECCIÓN DE LA INFORMACIÓN

Tipo de Estudio: Experimental

Diseño del estudio: Pre Experimental

## **2.3.2 TÉCNICAS E INSTRUMENTOS**

### *2.3.2.1 Técnicas e Instrumentos de recolección de datos:*

Las técnicas de recolección de datos usada: Observación para las etapas en la realización de pruebas del sistema de seguridad personal en el distrito de Bagua (ciudad): Lista de cotejo y el Tablero para observaciones respectivamente.

### *2.3.2.2 Técnicas e Instrumentos de Procesamiento y análisis de datos*

Se realizó la prueba no paramétrica con la prueba de Wilcoxon y usando el software Minitab 19.

### *2.3.2.3 Consideraciones éticas:*

Pedir permiso para obtener información. Proteger los datos utilizados.

## **2.3. Variables de estudio**

Variable independiente: sistema de monitoreo y control

Variable dependiente: seguridad personal

## **2.4. Métodos**

Se describe la metodología utilizada, en la que se trabajó siguiendo los siguientes pasos:

- Investigar sobre sistemas de seguridad existentes con el uso de dispositivos wearables.
- Diseñar un sistema para el monitoreo y control de la seguridad personal con dispositivos wearables.
- Realizar pruebas del sistema de seguridad personal en usuarios en el periodo mayo del 2022-setiembre del 2022.
- Evaluar el nivel de aceptación antes y después de las pruebas realizadas con el sistema
- Procesado y discusión de resultados
- Elaboración de conclusiones y recomendaciones.

### **2.4.1 Indicadores**

- Conformidad del sistema
- Amigabilidad del sistema
- Tiempo de desarrollo del sistema

- La granularidad en los reportes de alerta
- Tiempos de respuesta en los reportes de alerta

### **III.RESULTADOS**

A continuación, se analiza cada uno de los objetivos específicos planteados en esta investigación.

#### **3.1 Objetivo 1: Determinar las fuentes de información tanto cuantitativas como cualitativas que permitan profundizar en el estudio de la seguridad personal.**

##### **3.1.1 Introducción**

Según el (Programa de las Naciones Unidas para el Desarrollo, 2014) La seguridad ciudadana es el proceso de creación, fortalecimiento y protección de un orden civil democrático, eliminando la amenaza de violencia entre la población y posibilitando la convivencia segura y pacífica. Se considera un bien público y exige la tutela efectiva de los derechos humanos, en especial el derecho a la vida, a la intimidad, al domicilio y a la libre circulación en los lugares públicos.

La seguridad de los ciudadanos no se trata sólo de reducir la delincuencia, sino de una estrategia integral y versátil para mejorar la calidad de vida de la población, las actividades comunitarias para prevenir el delito, la disponibilidad de un sistema legal efectivo y la educación basada en valores, el respeto por la persona por la ley y tolerancia.

Más de 1500 millones de personas viven en países afectados por la violencia, el conflicto o la delincuencia grave, y más de 526 000 personas mueren de forma violenta cada año, o poco más de una por minuto. Aunque muchos factores han reducido la violencia y el crimen en muchos países desarrollados y pacíficos en las últimas décadas, esta no es una tendencia universal. Muchos países en desarrollo sufren un aumento alarmante de la violencia y la delincuencia, lo que socava los cimientos de la democracia y supone una enorme carga social, cultural y económica para las sociedades que menos tienen y que pueden permitírselo debido a su precaria seguridad.

Las instituciones de justicia y seguridad están en crisis en muchos países de África, América Latina y el Caribe. La inseguridad se ha convertido en uno de los problemas de desarrollo más importantes a los que se enfrentan los ciudadanos.

Las causas de la violencia y la inseguridad son diversas y complejas, pero suelen incluir:

- Problemas internos como el alto desempleo juvenil, la economía de guerra, la creciente desigualdad de ingresos y la injusticia flagrante.

- Problemas externos como la disponibilidad de armas de fuego ilegales, los movimientos de población, el crecimiento del crimen organizado, la existencia de redes de narcotráfico o los conflictos territoriales entre grupos criminales.
- Un desarrollo urbano rápido o mal planificado y la pobreza urbana.
- Tensiones subyacentes y conflictos por diferencias políticas, religiosas o étnicas, inequidad e injusta en la asignación de recursos.
- Una cultura de impunidad, de instituciones de seguridad no responsables, de corrupción o de un estado de derecho deficiente.
- Una crisis en la gobernanza e instituciones débiles como la policía, el sistema judicial y los servicios de seguridad que no pueden hacer frente o prevenir estos problemas.
- El crimen y la violencia tienen un impacto negativo en las economías en desarrollo y socavan la confianza empresarial porque causan altos costos y, en ocasiones, la pérdida de ciudadanos educados debido a la migración masiva.

Es importante señalar que combatir el crimen y la violencia a través de la intervención policial con medidas de seguridad mejoradas desvía recursos de otros importantes servicios de desarrollo como la salud y la educación.

En muchos países, la falta de seguridad de los ciudadanos puede ser el mayor obstáculo para el desarrollo económico, social y político. La prevención y el control eficaz de los delitos son un requisito previo para el desarrollo y la erradicación de la pobreza.

### **3.1.2 Plan Nacional de Seguridad Ciudadana 2019 – 2023**

Mediante Ley N° 27933, Ley del Sistema Nacional de Seguridad Ciudadana, modificada mediante Decreto Legislativo N° 1454, se crea el Sistema Nacional de Seguridad Ciudadana (SINASEC), como un sistema práctico encargado de asegurar el cumplimiento de las políticas públicas que orientan la intervención del Estado en materia de seguridad ciudadana para garantizar la seguridad, la paz, la tranquilidad, el cumplimiento y el respeto de las garantías individuales y sociales a nivel nacional para lograr una situación de paz social y protección de libre ejercicio de los derechos y libertades, en el marco de lo dispuesto en la Ley Orgánica del Poder Ejecutivo. La Ley N° 27933, Ley del Sistema Nacional de Seguridad Ciudadana, define a la seguridad ciudadana como “la acción integrada y articulada que desarrolla el Estado, en sus tres niveles de gobierno, con la participación del sector privado, la sociedad civil organizada y la ciudadanía, destinada a asegurar la convivencia pacífica, la erradicación de la violencia y la utilización pacífica de las vías y espacios públicos. Del mismo modo, contribuir a la prevención de la comisión de delitos y faltas”.

En el artículo 5 de la Ley N° 27933, se crea el Consejo Nacional de Seguridad Ciudadana (CONASEC), como el máximo organismo del SINASEC, encargado de la formulación, conducción y evaluación de las políticas de seguridad ciudadana, con autonomía funcional y técnica. Conforme al literal a) del artículo 9 de la Ley N° 27933, se pone de manifiesto que es función del CONASEC proponer ante la Presidencia del Consejo de Ministros la aprobación del Plan Nacional de Seguridad Ciudadana, elaborado bajo un enfoque descentralizado, de gestión por resultados e intercultural; En el artículo 4 del Decreto Legislativo N°1266, Ley de Organización y Funciones del Ministerio del Interior, y el artículo 3-A de la Ley N° 27933, Ley del Sistema Nacional de Seguridad Ciudadana, el Ministerio del Interior ejerce la rectoría del SINASEC; En ese contexto, el Ministerio del Interior se constituye como la autoridad técnico normativa de alcance nacional encargada de dictar normas, establecer los procedimientos relacionados con la implementación de las políticas nacionales y coordinar su operación técnica, así como las formas de articulación entre las diversas entidades involucradas, asumiendo la responsabilidad de su correcto funcionamiento.

Mediante resolución suprema N° 017-2018-IN se crea la comisión Multisectorial de carácter temporal encargada de elaborar la propuesta de “Plan Nacional de Seguridad Ciudadana 2019 - 2023” (PNSC) como principal instrumento orientador en esta materia, conformada por los diversos representantes de los distintos sectores y entidades públicas involucrados del Poder Ejecutivo; quienes concluyeron con el proceso de elaboración de la propuesta del citado Plan Nacional. En sesión de fecha 19 de diciembre del 2018, el CONOSEC aprobó el “Plan Nacional de Seguridad Ciudadana 2019 - 2023”; la propuesta del “Plan Nacional de Seguridad Ciudadana 2019 - 2023” ha sido presentada ante la Presidencia del Consejo de Ministros, siendo necesario su aprobación; documento de gestión que se constituirá en el principal instrumento del Estado Peruano para fortalecer la seguridad de la población frente a un conjunto de delitos en el territorio nacional y que incluye medidas que coadyuvarán a reforzar el orden, la paz y la seguridad en el País.

El Ministerio del Interior, a través de la Dirección General de Seguridad Ciudadana, tiene a su cargo la implementación, el monitoreo y la evaluación del “Plan Nacional de Seguridad Ciudadana 2019 - 2023”.

### **3.1.3 Alineamiento Estratégico**

El PNSC 2019-2023 se alinea a un conjunto de importantes instrumentos internacionales y nacionales. En el primer nivel, se alinea con: a) la Agenda 2030 para el Desarrollo Sostenible, b) el Índice para una Vida Mejor de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) y c) el Índice de Competitividad Global del Foro Económico Mundial. En el nivel nacional, el PNSC 2019-2023 se alinea con: d) el Acuerdo Nacional, e) el Plan Estratégico de Desarrollo Nacional y f) la Política General de Gobierno.

<b>Internacional</b>	(A) ODS de la Agenda 2030	(B) Índice para una Vida Mejor de la OCDE	(C) Índice de Competitividad Global del Foro Económico Mundial
<b>Nacional</b>	(D) Políticas de Estado del Acuerdo Nacional	(E) Plan Estratégico de Desarrollo Nacional	(F) Política General de Gobierno al 2021
Plan Nacional de Seguridad Ciudadana 2019 – 2023			

Tabla 2. *Alineamiento Estratégico del PNSC 2019 – 2023<sup>1</sup>*

El PNSC 2019-2023 reconoce cuatro fenómenos que amenazan la seguridad ciudadana. Estos fenómenos están agrupados de la siguiente manera: i) muerte violenta, representado por delitos asociados a homicidios y muertes en accidentes de tránsito; ii) delitos contra las mujeres, niños, niñas y adolescentes, materializado en feminicidios, violencia sexual, trata de personas, violencia doméstica y violencia contra niños, niñas y adolescentes; iii) delitos patrimoniales en espacios públicos, compuestos por actos de robo, hurto y estafas, micro comercialización; y iv) delitos cometidos por bandas criminales, expuesto en extorsiones, amenazas, intimidaciones y micro comercialización de drogas.

En respuesta a estos fenómenos, el Estado desarrolla medidas destinadas a proteger a los ciudadanos a través del orden público. Por lo tanto, el PNSC 2019-2023 asume un enfoque que reduce los factores de riesgo, pero no ignora que algunos de estos fenómenos tienen causas estructurales en la sociedad.

Factores estructurales	<ul style="list-style-type: none"> <li>• Exclusión social</li> <li>• Desigualdad</li> <li>• Pobreza</li> </ul>
Factores ambientales	<ul style="list-style-type: none"> <li>• Diseño urbano, espacios públicos y alumbrado público</li> <li>• Hacinamiento</li> </ul>
Factores individuales	<ul style="list-style-type: none"> <li>• Género</li> <li>• Edad</li> <li>• Edad de inicio de conducta delictiva</li> <li>• Consumo de alcohol y otras drogas</li> <li>• Abstencionismo y abandono escolar</li> <li>• Abuso físico en niñez</li> <li>• Uso indebido del tiempo libre</li> </ul>
Factores del hogar	<ul style="list-style-type: none"> <li>• Historia de violencia familiar</li> <li>• Normas internas del hogar</li> <li>• Roles ejercidos en el hogar</li> </ul>

<sup>1</sup> Fuente: Ministerio del Interior

	<ul style="list-style-type: none"> <li>• Ingreso per cápita del hogar</li> </ul>
Factores sociales y comunitarios	<ul style="list-style-type: none"> <li>• Disponibilidad de armas</li> <li>• Débiles controles institucionales</li> <li>• Conductas antisociales de los padres</li> <li>• Normas culturales (legitimidad social de la violencia)</li> <li>• Niveles de pobreza y desigualdad</li> <li>• Historial de violencia</li> <li>• Conductas antisociales de los amigos</li> <li>• Falta de oportunidades laborales</li> </ul>

Tabla 3. Factores de Riesgo<sup>2</sup>

Este entendimiento de la seguridad ciudadana permite, por un lado, focalizar las amenazas que cuentan con mayor prevalencia y, por el otro, propone intervenciones a partir de los problemas que afectan directamente a la ciudadanía. Ello implica formas de prevención, mecanismos de disuasión y reducción de la oportunidad delictiva (Cornish, Derek Blaikie y Clarke, Ronald V, 2003).

El PNSC 2019-2023 sirve de orientación y alineamiento a los diseños de los Planes de Acción Regionales, Provinciales y Distritales de Seguridad Ciudadana, según la Ley del Sistema Nacional de Seguridad Ciudadana - Ley N.º 27933, modificada por Decreto Legislativo N° 1454.

Esta orientación y alineamiento se desarrollan a fin de fortalecer tres aspectos. El primero, el eje de descentralización efectiva para el desarrollo, según lo indica la Política General de Gobierno al 2021. El segundo, la articulación de los diferentes niveles de gobierno, las entidades públicas y privadas, la sociedad civil bajo un enfoque intercultural y descentralizado de gestión por resultados. El tercero, el fortalecimiento y mejora de los equipos técnicos regionales, provinciales y locales. A continuación, se presenta el mapa estratégico del Plan Nacional de Seguridad Ciudadana 2019 – 2023.

---

<sup>2</sup> Fuente: (Redondo, 2008; Hilterman & Andrés-Pueyo, 2007; Farrington, 2003)

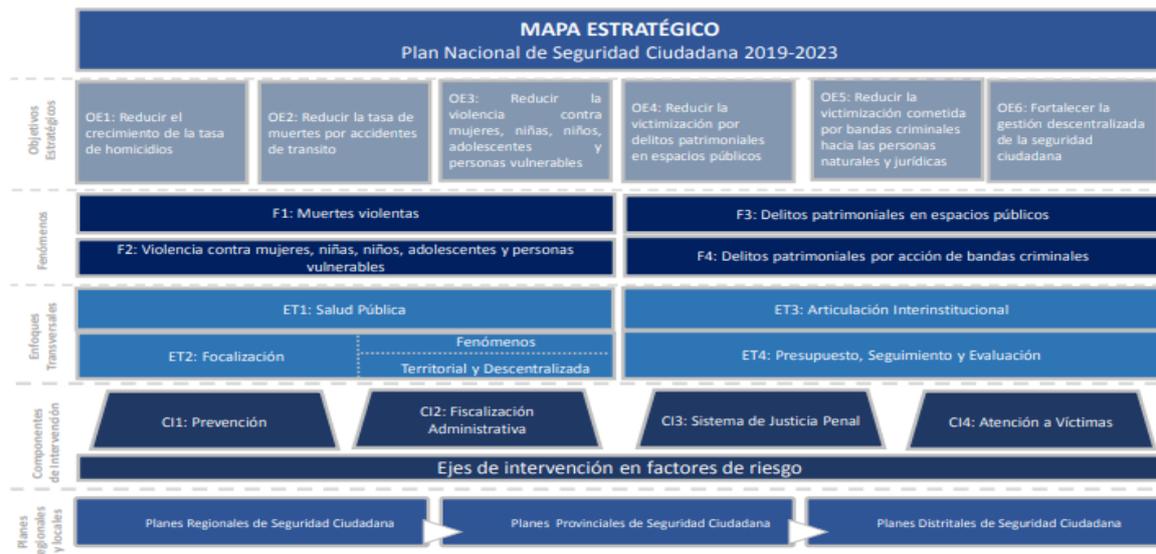


Figura 3. Mapa Estratégico PNSC 2019 - 2023<sup>3</sup>

Como componente de prevención del delito, están contempladas las siguientes acciones estratégicas que tienen que ver con las Tecnologías de la Información que a continuación se detallan y darán sustento a la investigación propuesta:

- Incrementar el número de comisarias que cuenten con óptima conectividad a internet
- Incrementar la cantidad de usuarios que hacen uso de aplicativos móviles para la prevención del delito
- Implementar Tecnologías de la información y comunicaciones para el monitoreo de los patrullajes policiales e integrarlo en comisarías mediante el Sistema Informático de Programación y Vigilancia de Patrullaje Policial
- Realizar campañas de difusión ciudadana vía internet para la prevención de victimización por delitos patrimoniales.
- Realizar intervenciones en flagrancia delictiva.

### 3.2. Objetivo 2: Estudiar y analizar los diferentes tipos de dispositivos wearables, así como los protocolos de comunicación utilizados.

#### 3.2.1 Wearables inteligentes

Los biosensores se pueden definir como dispositivos o componentes de un dispositivo, que monitorean y cuantifican datos físicos y químicos ambientales, que luego se emiten como

<sup>3</sup> Elaboración: Ministerio del Interior

una señal eléctrica. Los dispositivos portátiles inteligentes incorporan uno o varios biosensores en las prendas u otros elementos que se llevan en el cuerpo.

Los avances recientes en las tecnologías electrónicas se han aprovechado en el campo de la biometría (la medición de características biológicas) para permitir la producción de dispositivos cada vez más pequeños y potentes. Algunos dispositivos portátiles discretos ahora pueden monitorear continuamente variables que incluyen signos vitales como la frecuencia cardíaca (FC), que se encuentran entre los afectados por la reacción de lucha y huida, por lo tanto, indican que el usuario ha percibido una amenaza ambiental. Los dispositivos inteligentes que incluyen bandas, relojes y artículos de fitness y equipos médicos ahora pueden acumular una gran cantidad de datos importantes sobre el estado de sus usuarios (Rodríguez-Rodríguez I. a.-V.-I.-A., 2018) y compartirlos conectando los dispositivos a sistemas como Bluetooth, ZigBee o comunicaciones de campo cercano (NFC). Estos elementos portátiles y la variedad de datos fisiológicos que pueden capturar (El-Gayar, 2020), por lo tanto, puede proporcionar una imagen útil y compartible de la condición física del usuario, que es de obvio beneficio en el contexto de los sobrevivientes de la violencia.

Otra opción que se puede utilizar para controlar el estado fisiológico de las personas vulnerables es el teléfono inteligente, un elemento que ahora utiliza un gran número de personas. La incorporación de sensores de acelerómetro, podómetros, giroscopios y dispositivos de monitorización similares en este elemento de uso diario también puede recopilar grandes cantidades de datos cuantificables sobre la actividad física (Case, 2015). Aunque estos sensores en particular son generalmente utilizados por usuarios recreativos, otros sensores pueden estar dirigidos a grupos específicos. Los sensores que ofrecen una mayor precisión son de interés para el trabajo investigativo.

### **3.2.2 Reconocimiento de emociones**

Las emociones humanas se expresan en una amplia variedad de formas: desde la expresión facial hasta el tono vocal, el tono y el volumen, la forma de andar, los gestos, la elección de palabras, etc. Estos medios visibles o audibles para expresar emociones van acompañados de señales fisiológicas fácilmente perceptibles, que pueden ser, por ejemplo, un aumento de la frecuencia cardíaca (FC), la conductancia de la piel (CS) o la temperatura corporal. A diferencia de los enumerados anteriormente, estos cambios fisiológicos, que no

están asociados con la emoción, no están (o lo están sólo en raras ocasiones) bajo control consciente; de ahí que sea virtualmente imposible prevenir o disfrazar los bioseñales.

El reconocimiento de emociones es un área relativamente nueva dentro de la informática, aunque la investigación sobre la caracterización de las emociones ha estado en curso durante aproximadamente dos décadas (Picard, 2010). Se enfoca en la interpretación de la emoción humana y la investigación y producción de procesamiento de datos para crear software que monitorea y se adapta al cambio afectivo en los usuarios con el fin de ofrecer un mejor reconocimiento y satisfacción de sus necesidades. El software “consciente de los afectos” tiene potencial para su uso en una extensa gama de aplicaciones, como la atención médica, el e-learning y la recreación, así como la propia ingeniería de software (Landowska, 2013), (Wrobel, 2013). Se puede recopilar información afectiva de varios canales, entre los que se encuentran los de audio / video (Zeng, 2008), dispositivos de entrada estándar (Kolakowska, 2013), las respuestas fisiológicas (Rattanyu, 2010) y las expresiones faciales (Szwoch, 2014) han recibido atención reciente.

### **3.2.3 Tele monitorización pasiva**

La tele monitorización se refiere a la práctica de recopilar continuamente datos de supervivientes de violencia para determinar su situación y ubicación precisa. Los avances en biometría y tecnologías de IoT permiten el monitoreo 24 horas al día, los 7 días a la semana de personas vulnerables; por lo tanto, los datos biométricos vitales se pueden recopilar y utilizar para detectar situaciones peligrosas. Todo esto se puede lograr mediante el uso de un teléfono inteligente. El potencial de los datos recopilados es extremadamente alto. En este sentido, el trabajo de (Islam, 2018) muestra cómo los sensores pueden captar adecuadamente, a través de la combinación de sensores, el movimiento de la vida diaria, que es un gran indicador de la libertad y las capacidades prácticas de una persona.

Existen varias soluciones para medir las variables físicas del usuario, entre las cuales las Smartbands muestran un potencial considerable (Wu, 2018). Diferentes fabricantes están comercializando modelos fiables y a precios razonables que no solo controlan una lista cada vez mayor de variables, como la temperatura corporal, la presión arterial y las tasas de transpiración, sino que también mejoran rápidamente la duración de la batería y la conectividad.

### 3.2.4 Variables a monitorizar para detectar una situación de agresión

Los datos sobre las emociones humanas pueden obtenerse de una variedad de cambios fisiológicos; por lo tanto, estos también pueden aprovecharse para activar una alarma en caso de que un sobreviviente de violencia sea amenazado. Las señales relacionadas con el corazón incluyen cambios en la frecuencia cardíaca y el pulso, temperatura corporal, actividad eléctrica respiratoria y muscular, SC (también conocida como actividad electrodérmica (EDA) y respuesta galvánica de la piel (GSR)) y la actividad eléctrica del cerebro, todos los cuales pueden medirse por sensores comúnmente disponibles.

La Figura 4 presenta estas variables y los dispositivos que miden cada una.

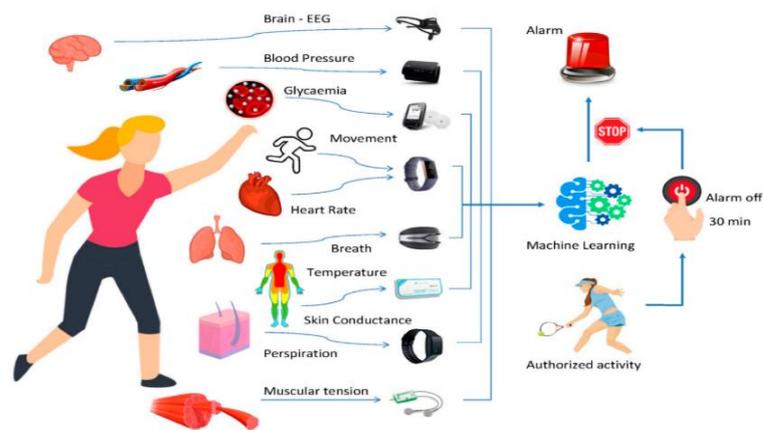


Figura 4. Sistema de alarma autónomo para sobrevivientes de violencia basado en Monitoreo Pasivo<sup>4</sup>

### 3.2.5 Movimientos abruptos

Los cambios físicos anormales causados por la amenaza o la ocurrencia de violencia física, varios estudios han investigado el movimiento y la velocidad acelerados. Los hallazgos de Ye et al. (Ye, 2018) demuestran que la actividad del usuario de un dispositivo de monitoreo que usa acelerómetros para extraer y filtrar patrones de movimiento puede indicar que la violencia está ocurriendo o es probable que ocurra.

Los acelerómetros hacen referencia a la medición de la aceleración de un cuerpo en dos o tres dimensiones. Estas herramientas han demostrado ser confiables con respecto a los datos que presentan, menos agobiantes para los individuos, versátiles y menos costosas en

<sup>4</sup> Fuente: (Rodríguez-Rodríguez, I., Rodríguez, J. V., Elizondo-Moreno, A., & Heras-González, P. (2020). An autonomous alarm system for personal safety assurance of intimate partner violence survivors based on passive continuous monitoring through biosensors. *Symmetry*, 12(3), 460.)

comparación con otros métodos de criterio de la energía de la actividad física como la calorimetría directa o indirecta. (Ndahimana, 2017).

Un estudio más reciente y extenso de Elbasiony (Elbasiony, Reda and Gomaa, Walid, 2019) investigó si los comportamientos humanos normales se pueden describir mediante el uso de movimientos registrados únicamente, una posibilidad también explorada por los teléfonos inteligentes en los que están incrustados acelerómetros (Nakano, 2017), (Alruban, 2019).

Los wearables diseñados para monitorear características específicas también suelen tener un acelerómetro.

### **3.2.6 Respiración**

El estrés agudo permite que los sobrevivientes respiren más rápido y más profundamente en un intento por absorber mayores cantidades de oxígeno, que es requerido por los músculos para generar la energía necesaria para huir o luchar. Durante esta respuesta, primero el tórax y luego el diafragma suben y bajan y se pueden capturar las señales dadas por la respiración tanto del tórax como del diafragma. Los datos relacionados con la rapidez y la profundidad de la respiración son útiles para evaluar la salud, el estado, la emoción y el estado de respuesta. Uno de estos dispositivos ha sido probado en el contexto de la investigación del comportamiento (Cai, 2018).

Los sensores de respiración han traído un cambio significativo a los diagnósticos médicos al permitir la detección y el monitoreo no invasivos de una variedad de parámetros de salud y también tienen potencial uso en el monitoreo de personas vulnerables a la pareja u otras formas de violencia.

### **3.2.7 Actividad del corazón**

Ocurrido un asalto, se requiere que el cuerpo lleve oxígeno y nutrientes a los músculos para permitir la lucha o la huida. Para que esto sea posible, tanto la frecuencia cardíaca como la fuerza de los latidos deben aumentar. Este cambio en la actividad cardíaca se puede medir mediante electrocardiograma (ECG), que requiere la colocación de electrodos en varios puntos del cuerpo del sujeto, una técnica que se utiliza con frecuencia para detectar la presencia de una enfermedad.

Otra señal fisiológica relacionada con el afecto es la frecuencia cardíaca. La excitación aumenta la variabilidad y la FC está determinada por dos ramas del sistema nervioso

autónomo, juntas o independientemente, a saber, la simpática (que la aumenta) y la parasimpática (que la disminuye) (Berntson, 1991).

La gran mayoría de los wearables actuales incorporan un monitor de recursos humanos. Además, muchas Smartbands permiten la monitorización no invasiva de la frecuencia del pulso, así como la fotopleletismografía (monitorización óptica de la frecuencia cardíaca). La diferencia entre el ECG y la fotopleletismografía es que el primero detecta actividad eléctrica, mientras que el segundo arroja una luz penetrante sobre la piel para examinar el flujo sanguíneo subyacente.

### **3.2.8 Presión sanguínea**

El estrés agudo también hace que el cuerpo segregue un mayor volumen de hormonas del estrés, lo que está asociado con el aumento de la presión arterial. La profesión médica ha sido consciente de esta conexión durante varias décadas (Sherwood, 1990).

Los dispositivos disponibles para controlar la presión arterial en la actualidad son considerablemente más sofisticados que sus predecesores, siendo más baratos, más precisos y más pequeños y, por lo tanto, más fáciles de llevar o usar. Varios investigadores han investigado la posibilidad de usar Bluetooth para conectar monitores de presión arterial portátiles a teléfonos inteligentes (Singh, 2016) y el consenso es que hacerlo daría resultados satisfactorios.

### **3.2.8 Glicemia**

La amenaza de agresión también se puede detectar en sujetos sanos mediante cambios en la glucemia. Se han identificado asociaciones entre las concentraciones de glucosa, los cambios de comportamiento característicos del estrés y las variables sanguíneas presentes en la hiperglucemia de estrés (a saber, concentraciones plasmáticas de glucosa, lactato, insulina, glucagón, cortisol, epinefrina y norepinefrina). Además, existe una fuerte correspondencia entre el estrés y las concentraciones de glucosa y lactato en el cuerpo, ya que estas últimas aumentan de forma pronunciada y detectable en presencia de riesgo (Rand, 2002).

### **3.2.9 La temperatura**

La temperatura corporal de una persona también proporciona datos valiosos sobre su estado de salud. Los datos obtenidos pueden indicar cambios de humor y estado afectivo; sin embargo, es esencial tener en cuenta el contexto y las condiciones, como en qué parte del

cuerpo se toma la medición, la hora del día y si, y en qué medida, la persona ha estado activa recientemente. La desventaja de usar la temperatura como una indicación de estrés es que cambia relativamente lentamente; por lo tanto, puede haber un retraso en el seguimiento de los cambios emocionales. El trabajo realizado en e-Health, específicamente en pediatría, se ha investigado la utilidad de la monitorización continua de la temperatura (Sampson, 2019).

### **3.2.10 La transpiración**

Los sobrevivientes de violencia responden a la amenaza sudando o transpirando, lo que puede considerarse el sistema de ajuste natural del cuerpo. La evaporación de la transpiración permite que el cuerpo se enfríe cuando está en peligro de sobrecalentamiento y, en consecuencia, un aumento del sudor asegura que podamos luchar o huir sin sufrir agotamiento por calor.

Los investigadores han investigado tanto el flujo de sudor como la presencia de anomalías; sin embargo, a pesar de estudios prometedores (Sim, 2018), ninguna solución de monitorización continua de la transpiración ha avanzado más allá de la etapa de prototipo.

### **3.2.11 Conductancia de la piel**

La conductancia de la piel (SC) mide la conductancia eléctrica de la piel, mediante la fijación de electrodos a la piel del sujeto por ejemplo. Como el grado de conductancia está determinado por el sistema nervioso, se puede detectar una asociación entre el estado de excitación y el SC. Por lo tanto, las señales SC se utilizan a menudo en pruebas de polígrafo (detector de mentiras) y se utilizan a menudo para medir la excitación, con la que se asocia (Brouwer, Anne-Marie and Van Wouwe, Nelleke and Muhl, Christian and Van Erp, Jan BF and Toet, Alexander, 2013), con niveles bajos de SC que indican niveles bajos de excitación.

Se encuentra disponible una amplia gama de dispositivos sensores que incorporan un monitor SC, muchos de ellos a un costo relativamente bajo.

### **3.2.12 Actividad cerebral**

El estrés puede provocar cambios en la actividad eléctrica del cerebro, que pueden detectarse mediante un electroencefalograma. Se ubican electrodos en varios lugares del cuero cabelludo del sujeto para registrar las señales eléctricas. Aunque esta técnica proporciona datos importantes, la desventaja es que el engorroso equipo requerido la convierte en una experiencia intrusiva para los pacientes (Byrom, 2018).

### **3.2.13 Tensión muscular**

Otro componente de la respuesta de lucha o huida ante situaciones amenazantes es la tensión muscular. Los usuarios experimentan tensión, que puede manifestarse como temblores o comportamientos como espasmos, parpadeo u otros movimientos del cuerpo para los que aún no se ha encontrado una explicación médica. La actividad eléctrica muscular tiene lugar durante el proceso cíclico de contracción y relajación de los músculos y puede registrarse mediante electromiografía (EMG).

Los seres humanos no pueden controlar las contracciones menores de los músculos faciales que hacen que las emociones sean visibles para los demás, un electromiograma facial podría ser útil en el reconocimiento de emociones. Sin embargo, es un proceso muy invasivo, ya que los electrodos deben colocarse en la cara del sujeto, lo que a la mayoría de la gente le resulta desagradable y, por lo tanto, el procedimiento tiene poco valor práctico.

### **3.2.14 Voz, sonido ambiental**

Muchos investigadores han indicado que la voz es un aspecto clave del reconocimiento de emociones (Wioleta, 2013) y se han implementado ciertas soluciones de detección y monitoreo vocal, como lo indica la Referencia (Sumathy, 2019). Otro elemento que puede contener información importante es el sonido ambiental, que permite la inferencia de tensión, miedo o emociones similares en la voz del sujeto. Se encuentra disponible una gama de dispositivos inteligentes que incorporan micrófonos para monitoreo de voz y el uso de unidades de control ambiental (ECU), más conocidas como "altavoces inteligentes" o "asistentes virtuales", se ha generalizado cada vez más con la comercialización de equipos habilitados para IA como "Alexa" de Amazon, "Siri Homepod" de Apple y "Google Home" de Google. Todos estos no solo son valiosos para el cuidado de los discapacitados y los ancianos, sino también para la vigilancia (Hoy, 2018). Dado que el objetivo de la presente tesis es diseñar un sistema de monitoreo portátil para sobrevivientes de la violencia, sin embargo, un teléfono inteligente con un micrófono también es adecuado para este propósito.

### **3.2.15 Variables biológicas adicionales**

Elemento de la respuesta fisiológica de lucha o huida es la dilatación de las pupilas, que aumenta la cantidad de luz disponible para el cuerpo para permitir la acción necesaria ante la amenaza (Guyon I. a., 2003). Además, la respuesta desencadena una disminución de la actividad del sistema digestivo para desviar energía a las tareas que requiere la pura

supervivencia. En consecuencia, la salivación disminuye, dando lugar a una sensación de sequedad en la boca. Otros efectos secundarios comunes pueden incluir náuseas, diarrea y sensación de pesadez en el estómago.

Las emociones se pueden reconocer a partir de una variedad de señales, incluidas las expresiones faciales, el tono y el timbre de la voz, el paso y los gestos. Monitorear estos eventos fisiológicos producirá datos objetivos valiosos con el propósito de reconocer las emociones.

### **3.2.16 Parámetros de medición**

Se pueden registrar numerosas señales biológicas identificadas con el estado del sobreviviente, es aceptable determinar que, bajo ciertas condiciones, un subconjunto ideal de factores puede ser suficiente para identificar una agresión. Las características deben expresarse como datos de series de tiempo, sobre la base de que la cantidad de ocasiones auténticas consideradas es significativa.

Las técnicas de selección de características en series de tiempo normalmente se pueden caracterizar en enfoques de filtro y envoltura. El enfoque de filtro utiliza solo la información para elegir qué características deben conservarse. Por otra parte, el enfoque de envoltura envuelve la búsqueda de variables en torno a una técnica de aprendizaje y utiliza su rendimiento para elegir las características (Rodríguez-Rodríguez I. a.-V.-I.-A., 2018).

La selección de características en series de tiempo no es lo mismo que la selección de características en información estática típica (Guyon I. y., 2003).

### **3.2.17 Dispositivos de activación de la alerta**

Los dispositivos de activación de alertas pueden ser fundamentales para la detección precoz de un posible problema de seguridad. Por lo que se analizan las señales biológicas de un individuo que pueden ser supervisados desde dispositivos corporales, de acuerdo al estado actual de la tecnología wearables y determinar de forma precoz cuando debe ejecutar una señal de alerta en caso de sufrir un incidente que afecta a la seguridad personal de un individuo. Por otro lado, se compararon los diferentes tipos de wearables que existen actualmente. Analizando las características de cada dispositivo, teniendo en cuenta sus ventajas y desventajas.

Gracias a este estudio se pudo escoger los parámetros de medición más convenientes para la plataforma, así como el tipo de wearable que mejor se ajusta a la plataforma.

Los datos recopilados por los biosensores portátiles se pueden almacenar y procesar para activar de forma autónoma una alarma cuando el usuario está en peligro, en lugar de pedirle que lo haga el mismo. Para permitir una solución de este tipo, se deben recopilar datos sobre todos los aspectos posibles de la vida del sujeto para que se pueda caracterizar su estado y aprender de él, y los cambios en él puedan activar la alarma. Este tipo de solución se encuentra en el área de rápido desarrollo del reconocimiento de emociones (Fabiano, 2019).

Cuando una persona es sometida, su cuerpo muestra lo que se conoce como la respuesta de “lucha o huida” o estrés agudo, es decir, los cambios fisiológicos provocados por un miedo físico o mental extremo. El cuerpo está inundado de hormonas diseñadas para dotarlo de los medios para combatir la amenaza o huir de ella (Goldstein, 2010).

La tecnología de biosensores puede realizar un monitoreo en tiempo real de las señales biológicas como un medio para proteger a las personas contra la violencia.

### **3.3. Objetivo 3: Estudiar y analizar los diferentes sistemas de monitorización basados en seguridad personal, que mejor se adapten al proyecto.**

#### **3.3.1 Sistemas de monitorización y control**

Los sistemas tecnológicos que prestan servicio de monitoreo y control de la seguridad personal, presentan una serie de investigaciones en los diversos tipos de sistema por ello es importante conocer los sistemas actuales, para poder comparar estos sistemas con la nueva plataforma a implementar. Así poder obtener características que la plataforma desarrollada destaque de otras similares a esta.

#### **3.3.2 Sistemas de activación autónoma**

Un sistema de seguimiento pasivo continuo utiliza biosensores adheridos al superviviente y aplica técnicas de aprendizaje automático para inferir si se está produciendo una situación anormal relacionada con la violencia de género, activando en este caso una alerta. La monitorización del sistema supervisa una gran cantidad de señales biológicas de acuerdo con el estado actual de la tecnología de wearables y dispositivos biomédicos. La solución de vigilancia basada en biosensores se puede desconectar manualmente durante 30/60/90 min

(bajo demanda) para evitar falsos positivos cuando una persona, por ejemplo, está practicando deporte o realizando otras actividades inofensivas que podrían activar incorrectamente la alarma (Rodríguez-Rodríguez I. a.-V.-M.-G., 2020).

El diseño de un enfoque basado en relojes inteligentes, utiliza un modelo de aprendizaje profundo, para reconocer gestos específicos del usuario que podrían dar como resultado la notificación de situaciones peligrosas y alertar a las autoridades para solicitar ayuda (Kasnesis, 2019).

La mayoría de los dispositivos de llamada de emergencia de tipo botón de pánico también requieren presionar un botón para comunicarse con los servicios de emergencia. El requisito de la intervención activa de la víctima reduce la efectividad del servicio para garantizar la seguridad personal. Para resolver este inconveniente, se utiliza un dispositivo portátil inteligente, en forma de una pulsera, para detectar e identificar automáticamente un atentado a la integridad física. La pulsera inteligente utiliza una multitud de sensores y aprendizaje automático para detectar un atentado en contra del usuario al momento que ocurre y luego procede a contactar a los servicios de emergencia. La detección automática de agresiones físicas utilizando la pulsera de joyería inteligente. Puede diferenciar entre movimientos regulares y luchas relacionadas con los atacantes, automatizando así el problema de pedir ayuda durante un atentado sorpresa. Este dispositivo será muy beneficioso para las víctimas potenciales de agresión física o para los usuarios de edad avanzada (Patel, 2018).

### **3.3.3 Sistemas de activación manual**

Un sistema portátil se asemeja a un reloj normal con un botón. Cuando se activa, el sistema rastrea la ubicación de la persona mediante el sensor del Sistema de posicionamiento global (GPS) y envía un correo electrónico de emergencia a la persona que puede ayudarla o salvarla. El sistema también incorpora una alarma de gritos que utiliza un reloj en tiempo real para pedir ayuda. La principal ventaja de este sistema es que el usuario no necesita un teléfono inteligente a diferencia de otras aplicaciones. El uso de componentes sofisticados asegura la precisión del sistema y lo hace confiable (Kannan, 2020).

Los teléfonos tienen muchas capacidades y no se limitan solo a llamadas y mensajes de texto. Se puede utilizar convirtiéndolo en un dispositivo de seguridad de emergencia cuando los usuarios se encuentran en una situación potencialmente insegura y peligrosa. El proceso de obtención de ayuda permite que los usuarios notifiquen rápidamente a las personas sobre

una situación de emergencia con solo presionar un botón. My Guardian, es una aplicación de seguridad personal desarrollada para teléfonos inteligentes, que tiene como objetivo ayudar a que los usuarios notifiquen a un conjunto de contactos predefinidos cuando se sientan en una situación insegura o simplemente estén nerviosos por viajar solos. Con solo presionar un botón. Además de eso, los usuarios pueden activar el timbre de alarma y compartir su ubicación actual con amigos o contactos predefinidos a través del móvil(teléfono) del usuario (Azman, 2018).

### **3.3.4 Sistemas de activación autónoma - manual**

El usuario puede activar la banda manualmente presionando el botón de activación. Además, cuenta con un sistema de autoactivación mediante un sensor de micrófono si el usuario está imposibilitado de poder activarlo manualmente. Al activarse, se puede rastrear la ubicación de la banda sin el uso de un módulo GPS separado. Una aplicación de desarrollo propio permanece conectada a la banda, en la que se puede acceder a la ubicación, el historial, los detalles del contacto y los datos de audio y video almacenados al iniciar sesión. La banda garantiza la seguridad de las mujeres durante cualquier situación insegura. Con la ayuda del módulo de micrófono y el GPS incorporado, la voz y la ubicación de la víctima se envían a sus contactos cercanos a través de la aplicación. Con la información recibida, pueden informar a la comisaría cercana para tomar alguna acción (Chaudhari, 2020).

La mayoría de las realizaciones de invención son para un dispositivo de seguridad pública que se usa y puede recopilar varios tipos de información de los estímulos, ya sea del entorno o, si se usa, también del cuerpo donde lleva el dispositivo. El dispositivo está en comunicación constante con al menos un servidor remoto. En ciertas realizaciones, el dispositivo puede enviar datos para ser procesados por un dispositivo informático remoto al detectar una situación de combate y transmitir una señal de emergencia (United States Patente n° US20200168074A1, 2020).

Un dispositivo de seguridad de respuesta y notificación rápida para las mujeres se asemeja a una banda inteligente, con varios sensores integrados dentro de la banda. Cuando se lleva la pulsera o el reloj, Si se enfrenta a algún tipo de acoso o si sienten que algo está en peligro, se puede presionar el botón ubicado en el reloj, cuando se cae, se envía la información diversa como ubicación, postura corporal, frecuencia del pulso y alerta por SMS a los números predefinidos utilizando GSM a través de Raspberry Pi. Cuando se presiona el botón,

los sensores recopilan la información del usuario y luego la información se envía al número predefinido junto con la llamada. Este sistema ayudará a acelerar el seguimiento de la seguridad de las mujeres mediante el mecanismo de seguimiento GPS. Se enviarán SMS a los números preprogramados. El proyecto garantiza la seguridad de las mujeres al proporcionar detección automática de problemas, amenazas y enviar mensajes de ayuda y la posición de la víctima a los familiares y la comisaría cercana utilizando Internet of Things (Nagamma, 2019).

Un sistema de seguridad personal incluye un módulo de detección de alertas para recibir, en un dispositivo, una entrada que indica un evento de alerta; y un módulo de comunicación para transmitir información sobre el evento de alerta a un servicio en la nube; y difundir información de red inalámbrica de un entorno inalámbrico alrededor del dispositivo, obtenida por el dispositivo, a una pluralidad de dispositivos en el entorno inalámbrico. La respuesta oportuna a una llamada de emergencia es fundamental. Cuando se realiza una llamada de emergencia, generalmente se enruta a un centro de llamadas u otra agencia central. A partir de ahí, se evalúa el contenido de la llamada y se asignan los equipos de respuesta adecuados y se los dirige al lugar de la emergencia. La calidad del servicio prestado por los equipos de respuesta varía mucho de una región a otra y de un país a otro (United States Patente nº US Patent 10,349,227, 2019).

### **3.3.5 Sistemas de seguridad personal en el mercado**

A continuación, se presenta una tabla comparativa de los diversos dispositivos de seguridad personal que ofrece el mercado y que forman parte de algunas soluciones que las compañías como: GetHomeSafe, Amazon, Silent Beacon, Ora y Stanley ofrecen a sus potenciales clientes, interesados en adquirir un sistema de seguridad personal.

En la tabla 4, se presenta una relación de los dispositivos de seguridad personal del mercado y sus características más resaltantes que se podrían utilizar para hacer uso del sistema de monitoreo y control.

Compañía	Dispositivo	características													Costos			
		Monitoreo del movimiento físico	Batería de larga duración	Grabador de audio y/o video	Bluetooth	Rastreo ID MAC de los enrutadores WIFI	Protección con pin	Altavoz integrado	Rastreo GPS	Rastreo satelital	Tarjeta SIM	Envío de alerta a los números de contacto predefinido	Alerta de llamadas telefónicas automáticas	Función de geovalla	Canal de comunicación alternativo al móvil	Equipo	Servicio	
<b>GetHome Safe</b> <a href="https://www.gethomesafe.com/">https://www.gethomesafe.com/</a>	Botón de pánico						X			X								Cuenta corporativa mensual Servicio estándar \$3.50 x usuario Servicio Premium \$4.50 x usuario
	Mandown y sin movimiento	X	X		X							X					Requiere ser consultado a la Cía.	Requiere ser consultado a la Cía.
<b>Amazon</b> <a href="https://www.amazon.com/Best-Personal-Safety-Devices/s?k">https://www.amazon.com/Best-Personal-Safety-Devices/s?k</a>	Invisawear Smart Jewelry - Collar de oro		X		X					X							\$ 149.00	-
	Alphahom Care Go		X		X					X							\$ 40.90	-

=Best+Personal+Safety+Devices	Smart Alarma personal																
	Dispositivo de seguridad personal portátil SEAM Lotus			X				X	X			X	X			\$ 39.99	-
	Mini localizador GPS en tiempo real modelo Tracki 2020					X			X		X			X		\$ 25.88	cuota mensual de \$ 19.95 o \$ 9.95 para planes de largo plazo
	PRIMET RACKING Rastreador GPS personal	X							X		X					\$ 49.97	Cuota mensual de \$ 25.00 o \$ 20.00 durante 6 meses por monitoreo.
	ACR ResQLink 400 - Baliza de localización personal GPS							X	X	X						\$ 299.95	-
	Mensajero GPS								X	X		X				\$ 99.99	-

	satelital Spot 3																	
	Rastreador GPS personal, Mini dispositivo de rastreo GPS portátil TK1000		X						X		X				X		\$ 38.98	-
	Rastreador de ubicación GPS GeoZilla		X						X		X	X			X		\$ 69.00	Planes de servicio asequibles a partir de \$ 12.99 al mes
	YEPZON Smart Tracker 4G LTE		X		X		X		X						X		\$ 69.00	Planes de servicio a partir de \$ 12.99 al mes
	Prime Tracker Personal GPS Tracker - Mini, portátil, seguimiento en tiempo real - 4G LTE		X						X		X						\$ 29.97	\$ 25 / mes, o \$ 20 / mes durante 6 meses x monitoreo

	Orbit Protect: dispositivo de seguridad portátil con botón de emergencia		X						X							\$ 29.99	-
Swissphone <a href="https://www.swissphone.com/applications/personal-safety/">https://www.swissphone.com/applications/personal-safety/</a>	RES.Q Alerta híbrida		X		X				X							Requiere ser consultado a la Cía.	Requiere ser consultado a la Cía.
	Botón SOS La llamada de emergencia inteligente		X						X				X		Requiere ser consultado a la Cía.	Requiere ser consultado a la Cía.	
	SOS-Beacon de larga duración Tecnología IoT		X						X						Requiere ser consultado a la Cía.	Requiere ser consultado a la Cía.	
	Aplicación SOS-Mobile						X					X	X		Requiere ser consultado a la Cía.	Requiere ser consultado a la Cía.	

<b>Silent beacon</b> <a href="https://silentbeacon.com/">https://silentbeacon.com/</a>	Sistema de alerta personal Silent Beacon								X					X	X			\$ 99.99	-
<b>Oraforyo u</b> <a href="https://www.oraforyo.com/">https://www.oraforyo.com/</a>	Sistema de alarma de seguridad personal ORA		X						X					X	X			\$ 182.00	-
<b>Stanley Security</b> <a href="https://www.stanleysolutions.com/GUARD">https://www.stanleysolutions.com/GUARD</a>	Guardia Stanley	X		X					X					X				Requiere ser consultado a la Cía.	Requiere ser consultado a la Cía.

Tabla 4. Comparativa de los dispositivos de seguridad personal en el mercado

**3.4. Objetivo 4: Seleccionar los mecanismos de reconocimiento de la agresión física del usuario en base al análisis de los diferentes tipos de dispositivos wearables que porta el usuario, las distintas técnicas de captación de la información, los medios utilizados para recoger dicha información y almacenarla en una plataforma.**

#### **3.4.1 Posibles arquitecturas y tecnologías utilizadas en la plataforma a desarrollar**

Las posibles arquitecturas y tecnologías utilizadas en el sistema a implementar. En primera instancia se hizo una descripción de cada arquitectura y tecnología. En base a lo estudiado se tomó decisiones para llevar a cabo la mejor implementación posible para la nueva plataforma.

Las arquitecturas estudiadas son la arquitectura dirigida a eventos y el estilo arquitectónico rest, el cual se fundamenta en el protocolo de transferencia de hipertexto (HTTP). Por otro lado, se presentarán las tecnologías Bluetooth, Bluetooth Low Energy, Gatt, NFC, Android, SQLITE, JAVA, Jersey y MySQL.

#### **3.4.2 Arquitectura**

##### *3.4.2.1 Arquitectura dirigida a eventos*

La arquitectura dirigida a eventos es un patrón que promueve la creación, detección y reacción de eventos. Cuando ocurre algo notable dentro del sistema, se difunde a todas las partes que estén suscritas. Los suscritos evaluarán el hecho y pueden tomar o no medidas ejecutando rutinas a partir de lo acontecido (Michelson, Event-driven architecture overview, 2006).

Dentro de las características de la arquitectura basada en eventos se encuentra la comunicación de difusión, los sistemas participantes transmiten eventos a cualquier interesado más de un participante escucha el evento y los procesa. Por otro lado, los eventos deben publicarse a medida que ocurren, estos no se deben almacenar para ser procesados después. Además, los sistemas con esta arquitectura deben ser asíncronos, si estos envían el evento no se debe esperar que los receptores lo procesen. Por lo general los eventos tienen una forma de jerarquía y categorías para que los receptores puedan procesarlos con mayor facilidad (Hohpe, 2006).

### 3.4.3 Eventos

Un evento es un acontecimiento notable que ocurre dentro o fuera del sistema. Puede significar un problema, una oportunidad o un cambio de estado. Los eventos tienen algunas propiedades como el ID de especificación del evento, el tipo de evento, el nombre del evento, la fecha de ocurrencia, número de ocurrencias y el objeto creador del evento (Michelson, Event-driven architecture overview, 2006).

#### 3.4.3.1 Generador de evento

Es el componente que crea el evento, puede ser un sensor, proceso de negocio o servicio. Existirá un procesador de eventos que evaluará la generación de un nuevo evento notable.

#### 3.4.3.2 Canales de evento

Es una conexión entre los componentes que transporta eventos de una forma estándar entre los generadores de los eventos y los suscriptores posteriores.

En la **figura 5** se observa el flujo del procesamiento de un evento donde se aprecia la generación del evento, pasando por el canal al procesador de eventos, además de cómo es procesado para una posterior suscripción en el mismo.

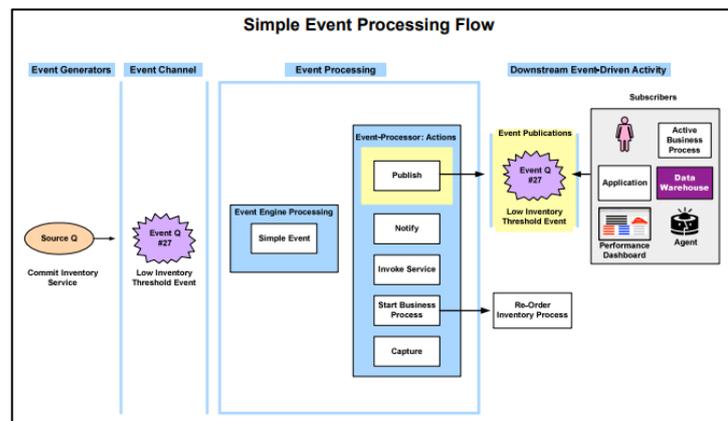


Figura 5. Flujo para el Procesamiento de un Evento<sup>5</sup>

### 3.4.4 Estilo arquitectónico REST.

Es un estilo arquitectónico web basado en estándares utilizando como base el protocolo HTTP, lo cual aceptará todas operaciones HTTP y estas son: PUT, GET, POST, DELETE. obteniendo accesos para poder eliminar, crear, actualizar y obtener un recurso. Cada servicio

<sup>5</sup> Fuente: Event-driven architecture overview, Michelson, 2006.

está identificado por una URI eliminando así algún tipo de ambigüedad. Puede soportar diferentes extensiones de entrada como XML o JSON (Eden, 2006).

Se hace mención del estilo arquitectónico REST en el año 2000 en una tesis doctoral escrita por Roy Fielding (Tanaka Terukina, 2016). Él cual definió el término REST para generar la idea de que los elementos de las aplicaciones en red estaban intercambiando sus estados utilizando protocolos a través de la red (Severance, 2015).

Después de 19 años REST se sigue utilizando como guía para comprender cómo está diseñada la WWW. Sin embargo, REST también se ha convertido en una palabra de moda en la industria: se confunde con la noción general de usar HTTP (Fielding R. T., 2017).

En la **figura 6** se observa la arquitectura del estilo arquitectónico rest donde existen varios clientes como un ordenador o un móvil. Los cuales hacen una petición http a un servicio web. Esta petición lleva un cuerpo en formato Xml o Json.

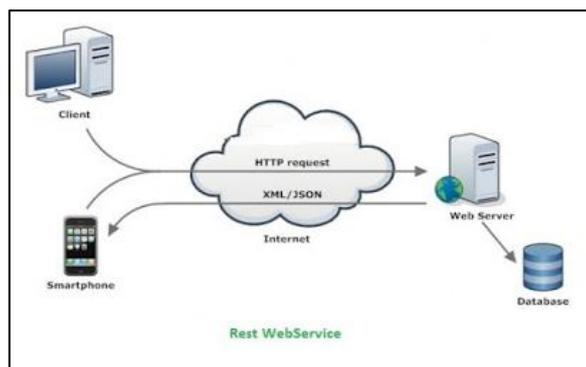


Figura 6. Arquitectura REST<sup>6</sup>

### Protocolo HTTP:

El protocolo de transferencia de hipertexto (HTTP) se encuentra en el nivel de aplicaciones del modelo OSI, sirve para tener información distribuida y compartida, su tarea principal es la transferencia de hipertexto en la red, ha sido utilizada en la WWW desde el año 1990 (Fielding R. a.-L., 1999).

### Verbos HTTP:

<sup>6</sup> Fuente: <http://dsanchezzz.blogspot.com/2015/10/rest.html>

**GET:** A través del método GET se puede recuperar cualquier información en forma de entidad, la cual se identifica con el URI de la solicitud (Fielding R. a.-L., 1999).

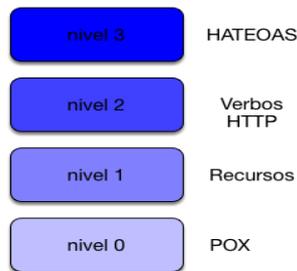
**POST:** A través del método POST se le solicita al servidor que registre una nueva entidad del recurso que se mandó en la solicitud identificada por el URI (Fielding R. a.-L., 1999).

**PUT:** A través del método PUT se solicita que la entidad mandada en la solicitud sea modificada si esta se encuentra existente como recurso (Fielding R. a.-L., 1999).

**DELETE:** A través del método DELETE se solicita la eliminación de una entidad proporcionando el identificador de esta (Fielding R. a.-L., 1999).

### Niveles de la Arquitectura REST:

En la **figura 7** se pueden observar los cuatro niveles de la arquitectura REST.



*Figura 7. Niveles de la Arquitectura REST<sup>7</sup>*

En el **nivel 0** se encuentran a una arquitectura basada en XML utilizando los métodos POST de HTTP la transferencia de mensajes se hace a través del formato XML (Caules, 2018).

En el **nivel 1** aparece un nuevo concepto llamado recurso, realizado operaciones básicas como insertar, borrar, actualizar y buscar a través de peticiones sencillas HTTP, el formato más utilizado es JSON (Caules, 2018).

En el **nivel 2** ya se comienzan a utilizar los verbos HTTP utilizados para cada operación (Caules, 2018).

En el **nivel 3** se pueden encontrar recursos relacionados entre ellos a través de conectores por ejemplo si se solicita la lista de empleados pueden incluir los turnos realizados (Caules, 2018).

---

<sup>7</sup> Fuente: <https://www.arquitecturajava.com/arquitecturas-rest-y-sus-niveles/>

### **3.4.4 Tecnologías usadas en el proyecto**

#### *3.4.4.1 Bluetooth*

Bluetooth es una tecnología de comunicación con un gran crecimiento y de bajo costo, en 2001 tuvo un pronóstico de 200 millones de dispositivos electrónicos con el incorporado. El objetivo de utilizar Bluetooth es evitar la conectividad de dispositivos electrónicos a través de cables físicos. Convirtiendo esta conectividad en algo simple e intuitivo. Sin embargo, para conseguir estas ventajas se requiere de una complejidad en su implementación. La primera versión de Bluetooth fue lanzada en el año 1999, sin embargo, ya se venía trabajando en ella 5 años atrás. Realizando estudios de cómo se podrían comunicar los dispositivos electrónicos sin la necesidad de utilizar un cable físico (Bray, 2001).

Bluetooth cuenta con ventajas con respecto a otras tecnologías de conectividad y paso de información, como que todos los dispositivos hablan el mismo idioma puede ser un ordenador o una impresora, mientras que con un infrarrojo no se puede hacer, además que el canal de comunicación está abierto y no requiere la intervención del usuario cada vez que se quiere enviar un paquete (Castellano, 2012).

A través Bluetooth se puede hacer una transmisión de datos entre diferentes dispositivos que estén en corto alcance mediante un enlace de radio frecuencia la cual trabaja a banda 2.4 GHz y los dispositivos tienen una dirección única de 48 bits basado en el estándar IEEE 802.15.1. Es una especificación industrial y estándar para WPAN (red de área personal). El contralor Bluetooth este compuesto de varios niveles: nivel de radiofrecuencia, nivel de banda base y nivel de gestión de enlace. El nivel de radiofrecuencia facilita la consecución de la calidad de la señal entre los dispositivos y la compatibilidad entre transceptores. El nivel de banda base es el encargado de controlar las operaciones sobre los datos detectando y corrigiendo errores. El nivel de gestión de enlace es el encargado de establecer y finalizar las conexiones entre dispositivos (Castellano, 2012).

#### *3.4.4.2 Bluetooth Low Energy*

La versión 4.0 de Bluetooth es un nuevo avance en la tecnología para reducir los costes en batería y corregir errores de seguridad. Esta versión está enfocada a reducir el consumo de la batería, por lo cual se necesita que la trasmisión de datos también sea baja. Es muy factible utilizarlo en dispositivos donde la autonomía juega un papel importante o donde no se cuentan con los recursos de hardware necesario para mantener un Bluetooth de versiones

anteriores. En los dispositivos como los wearables, domótica o dispositivos médicos viene muy bien utilizarlos (Avila, 2017). Para dispositivos wearables si bien la tasa de datos es más baja todavía se puede satisfacer las necesidades de estos dispositivos. Además de tener menor consumo de energía permitirá que la autonomía sea mayor y el tamaño de la batería pueda ser mucho menor (Zhang, 2014) .

En la **figura 8** se observa la arquitectura de un dispositivo wearable el cual cuenta con un chip de BLE para conectarse a través de un servicio Gatt a un móvil.

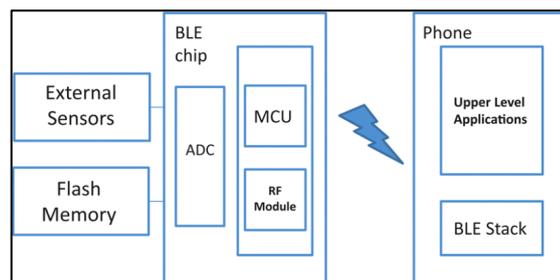


Figura 8. *Arquitectura de un Dispositivo Wearable con BLE<sup>8</sup>*

Bluetooth Low Energy se basa en una pila de protocolos nuevas para hacer la comunicación de los enlaces más rápida y simple. tiene un rango de comunicación más amplio, un consumo de energía mucho menor y una velocidad de datos más baja que otras versiones de Bluetooth. Además, define dos roles de dispositivo en la conexión, un esclavo y un maestro. Cuando se transmiten los datos, los esclavos están en modo de suspensión por defecto (permitiéndolo ahorrar batería) y se activan periódicamente para consultar si existen paquetes nuevos provenientes del maestro (Zhang, 2014).

#### 3.4.4.3 NFC

NFC (Near Field Communication) es una tecnología de comunicación de proximidad inalámbrica que permite transferir datos a una distancia de hasta 10 cm. La principal ventaja de NFC sobre otras tecnologías de comunicación inalámbrica es la simplicidad: las transacciones se inician automáticamente, simplemente tocando un lector, otro dispositivo NFC o un transpondedor compatible con NFC. La tecnología NFC brinda funcionalidad adicional a un dispositivo móvil, como usarlo como una tarjeta de crédito sin

<sup>8</sup> Fuente: <https://ieeexplore.ieee.org/abstract/document/7038922>

contacto o como un boleto de autobús sin contacto. Las conexiones Bluetooth y WiFi se pueden establecer simplemente tocando un transpondedor (Collins, 2007).

La combinación de una tecnología de comunicación inalámbrica con aplicaciones puede generar posibles problemas de privacidad y riesgos de seguridad. Los ataques contra un dispositivo NFC se pueden realizar en cualquier lugar y es posible que la víctima no los note, ya que la comunicación en sí es sin contacto. Además, el beneficio obtenido al hacerse cargo de un dispositivo NFC es alto. Los atacantes podrían abusar de la funcionalidad de pago o utilizar el dispositivo para llamadas de voz o tráfico de datos (Kfir, 2005). Por lo tanto, la integración de tecnología y aplicaciones debe ir de la mano para proteger el dispositivo y el consumidor.

#### *3.4.4.4 Gatt*

Gatt es un protocolo de datos que permite establecer el tipo de información que se transmite a través de los paquetes de Bluetooth. El Gatt se basa en el Protocolo de atributos ATT el cual utiliza la menor cantidad de bytes posibles, define la forma en que dos dispositivos Bluetooth incorporado envían y reciben mensajes de una forma estándar. se puede usar con Bluetooth Low Battery como transporte, Los atributos Gatt definen una estructura de datos jerárquica que está expuesta a dispositivos Bluetooth conectados. Gatt cuenta con perfiles que describen una funcionalidad específica y un comportamiento basado en esta funcionalidad, los cuales están compuestos de uno o más servicios. Los servicios son colecciones de características y relaciones con otros servicios que encapsulan el comportamiento de parte de un dispositivo. Una característica se representa por un identificador único (UUID) las cuales son un conjunto de propiedades que indican las operaciones que admite esta característica. (SIG, 2019).

Hay dos roles en Gatt un cliente y un servidor, los cuales funcionan a través de tres procedimientos: procedimiento de descubrimiento, procedimientos iniciados por el servidor y procedimiento iniciado por el cliente para la lectura, escritura, notificaciones e indicaciones. El servidor almacena los datos transportados a través del ATT y acepta solicitudes, comandos y confirmaciones del cliente. Además de enviar indicaciones y notificaciones de forma asincrónica al cliente cuando ocurren eventos específicos en el servidor. Por último, especifica el formato de los datos contenidos en el servidor (SIG, 2019).

En la **figura 9** se observan la jerarquía de las capas de cómo están compuestos el Gatt.

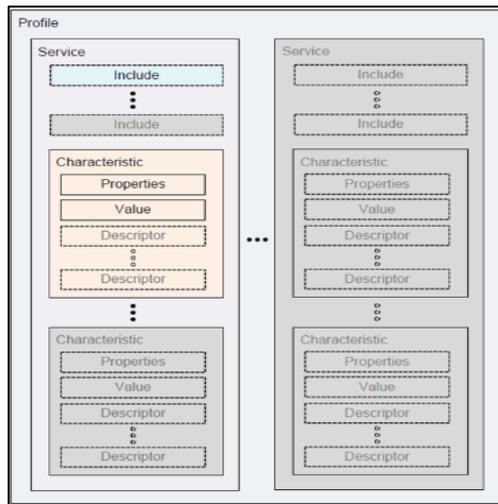


Figura 9. Jerarquía de Perfiles GATT<sup>9</sup>

### 3.5 Objetivo 5 Determinar las herramientas para el diseño y modelado; así como la arquitectura del sistema para el desarrollo de la plataforma de este proyecto.

#### 3.5.1 Android

En el diseño de aplicaciones móviles se optó por el sistema Android por ser uno de los más utilizados.

##### 3.5.1.1 Arquitectura Android

Android presenta una arquitectura basada en 4 niveles, todas las capas están basadas en software libre (Girones, 2013):

#### Kernel Linux

Está formado por el sistema operativo Linux 2.6, se encarga de la gestión de drivers, manejo de memoria, protocolos. Capa más cercana al hardware.

#### Librerías nativas y RunTime de Android

- **Librerías nativas:** Son librerías a bajo nivel en C y C++, como SQLite un ligero motor de base de datos, disponible para todas las aplicaciones, librerías para 3D como OpenGL, Media Framework para reproducción y grabación de video en diferentes formatos.

<sup>9</sup> Fuente: <https://www.bluetooth.com/specifications/specs/>

- **Runtime de Android:** Basado en el concepto de máquina virtual de Java, dada las limitaciones de Hardware se creó la máquina virtual Darvik.

## Entorno de aplicación

Proporciona una plataforma de desarrollo y consta de clases y servicios que permiten la funcionalidad básica y la programación de aplicaciones de los teléfonos móviles. Tenemos, entre otros: Activity Manager, Windows Manager, views, notification manager, package manager, content provider, telephony manager, resource manager, location manager.

## Aplicaciones

Son las aplicaciones básicas que incluye el teléfono como cámara, envío de mensajes, correo electrónico, calendario, explorador de internet, estas pueden ser utilizadas por aplicaciones externas.

En la **figura 10** se observan los cuatros niveles de la arquitectura de Android en cada nivel se muestra los sub componentes que están incorporados a estos. Organizados por nivel de interacción con el usuario.

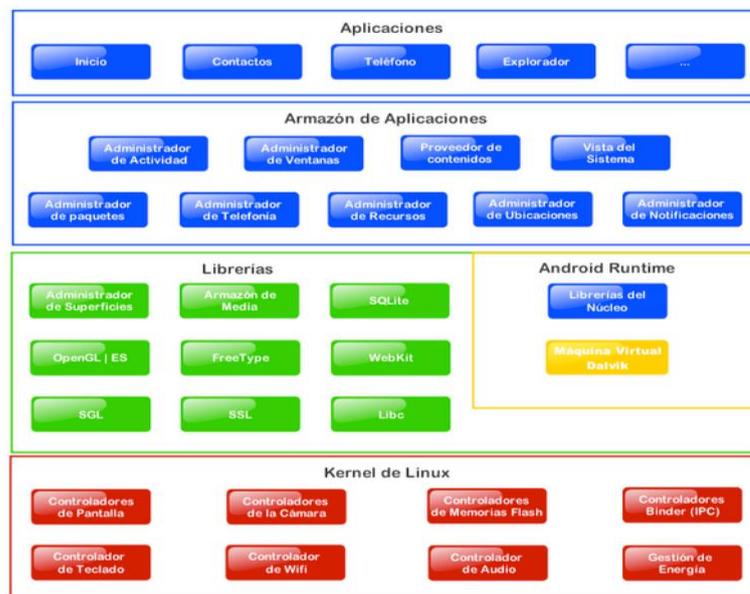


Figura 10. Arquitectura del Sistema Operativo Android<sup>10</sup>

<sup>10</sup> Fuente: El gran libro de Android. Alfaomega.

### 3.5.1.2 Arquitectura de una Aplicación en Android

Varios son los elementos claves que toda aplicación en Android debe tener. En estos se encuentran: vistas, Layout, actividades, servicios, intención, receptor de anuncios, proveedores de contenido (Blanco, 2009).

- **Vistas (View):** son los elementos que componen la interfaz de usuario de una aplicación, todas las vistas van a ser objetos que hereden de la clase View, sin embargo. Lo habitual va a ser definir las vistas utilizando un fichero XML.
- **Layout:** es un conjunto de vistas agrupadas de una determinada forma. Se pueden tener diferentes formas de layouts para organizar las vistas. Estos heredan de la clase View. Lo habitual va a ser definirlos utilizando un fichero XML.
- **Actividad (Activity):** son las pantallas de visualización, su función principal es la creación del interfaz de usuario. En una aplicación puede necesitar de varias actividades, estas serán independientes entre sí. Contendrá objetos View.
- **Servicios (Service):** Es un proceso que se ejecuta en segundo plano, sin necesidad de una interacción con el usuario. Existen dos tipos de servicios en Android los locales y los remotos.
- **Receptor de anuncios (Broadcast receiver):** recibe y reacciona ante anuncios de tipo broadcast, ejemplos batería baja, llamada entrante, las aplicaciones también puede lanzar un anuncio broadcast.
- **Proveedores de contenido (Content Provider):** se utiliza para la compartición de información entre aplicaciones, con esto podemos acceder a datos de otras aplicaciones.
- **Intención (intent):** Es la voluntad de realizar una acción; Se utiliza siempre que desee ejecutar una función, un servicio, enviar un mensaje o interactuar con un servicio. Los componentes invocados pueden ser internos o externos a la aplicación.
- **Archivo Manifest:** es un archivo con formato XML obligatorio y único para todas las aplicaciones Android cuyo objetivo es tener información de la aplicación como nombre, icono, versión, requisitos, estructura de la aplicación.

## **3.5.2 Gestores de Bases de Datos**

### **3.5.2.1 SQLITE**

SQLite es un gestor de base de datos que implementa un motor de base de datos SQL autónomo, sin servidor. El código para SQLite está en el dominio público y, por lo tanto, es de uso gratuito para cualquier propósito, comercial o privado. SQLite es la base de datos más implementada en el mundo con más aplicaciones de las que podemos contar, incluidos grandes proyectos (SQLite, 2019).

SQLite tiene un motor de base de datos SQL incorporado. A diferencia de la mayoría de las otras bases de datos SQL, SQLite no tiene un proceso de servidor separado. SQLite lee y escribe directamente en archivos de disco ordinarios. Una completa base de datos SQL con múltiples tablas, índices, disparadores y vistas, está contenida en un solo archivo de disco. El formato de archivo de la base de datos es multiplataforma: puede copiar libremente una base de datos entre sistemas de 32 y 64 bits. Estas características hacen de SQLite una opción popular como formato de archivo de aplicación. Además de ser una biblioteca compacta. Con todas las funciones habilitadas. El proyecto SQLite se inició en el año 2000. Se pretende dar mantenimiento a SQLite hasta el año 2050 (SQLite, 2019).

Android incorpora herramientas necesarias para la creación y gestión de bases de datos SQLite, y entre ellas una API para llevar a cabo de manera sencilla todas las tareas necesarias.

### **3.5.2.2 MySQL**

MySQL es un gestor de base de datos de código abierto más popular del mercado. Gracias a su rendimiento probado, a su fiabilidad y a su facilidad de uso, MySQL se ha convertido en la base de datos líder elegida para las aplicaciones basadas en web y utilizada por propiedades web de perfil alto, como Facebook, Twitter, YouTube entre otras (Oracle, mysql, 2019).

MySQL es un sistema de gestión de base de datos relacionales, extremadamente expandido y popular en los servidores de internet. Su éxito viene por un lado de su facilidad de implementación y por otro de su carácter original. Una comunidad muy grande le da soporte. Funciona en un gran número de plataformas como AIX, Unix, Windows, Solaris,

Mac OS. Además de accesible desde muchos lenguajes de programación como C, C++, C#, Java, PHP, Python siendo PHP el más utilizado (Oracle, mysql, 2019).

MySQL utiliza varias versiones de motores:

**MyISAM:** motor por defecto. Es el más fácil de usar y de instalar.

**InnoDB:** desarrollado por InnoDB. Gestiona transacciones, bloqueos a nivel de filas, claves foráneas, triggers, vistas.

### 3.5.3 JAVA

Java es un lenguaje de programación creado por Sun Microsystems, empresa que posteriormente fue comprada por Oracle) para poder funcionar en distintos tipos de procesadores. Su sintaxis es muy parecida a la de C o C++, e incorpora como propias algunas características que en otros lenguajes son extensiones: gestión de hilos, ejecución remota, etc. (Barnes, 2007).

El código Java, una vez compilado, puede llevarse sin modificación alguna sobre cualquier máquina, y ejecutarlo. Esto se debe a que el código se ejecuta sobre una máquina virtual, la Java Virtual Machine, que se encarga de interpretar el código (archivos compilados .class) y convertirlo a código particular de la CPU que se esté utilizando (siempre que se soporte dicha máquina virtual). Java es un lenguaje orientado a objetos (OO) (Barnes, 2007).

Java es un lenguaje fuertemente tipado y estricto. La sintaxis se verifica al momento de la compilación. Lo que permite reducir los errores y los problemas de incompatibilidad entre versiones. Por otro lado, se encarga totalmente de la gestión de los punteros y el programa no tiene manera de acceder a estos, lo que evita la sobreescritura accidental de los datos que se encuentran en memoria (Barnes, 2007).

Java permite desarrollar aplicaciones que ponen en marcha la ejecución simultánea de varios hilos. Esto permite efectuar simultáneamente varias tareas, con el fin de aumentar la velocidad de las aplicaciones (Barnes, 2007).

### 3.5.4 JERSEY

Jersey es un conjunto de librerías que permite el desarrollo de servicios web RESTful en Java para implementar la exposición de los datos en una variedad de tipos de medios de representación como XML o JSON. La última versión estable es la 2.28. Por otro lado,

abstrae los detalles de bajo nivel de la comunicación cliente-servidor haciendo el desarrollo de la aplicación más sencillo. Para simplificar el desarrollo de los servicios web RESTful y sus clientes en Java, se ha diseñado una API JAX-RS estándar y portátil. El marco de los Servicios Web RESTful de Jersey es de código abierto (Oracle, Jersey, 2019).

El marco de Jersey es la Implementación de Referencia JAX-RS. Jersey proporciona su propia API que amplía el kit de herramientas JAX-RS con funciones y utilidades adicionales para simplificar aún más el servicio RESTful y el desarrollo del cliente. Jersey también expone numerosos API de extensión para que los desarrolladores puedan extender Jersey para que se adapte mejor a sus necesidades. Utilizando Jersey, el propio marco de trabajo asignará internamente un servlet que se encargará de analizar las peticiones HTTP entrantes y seleccionar las clases y métodos adecuados para responder a dicha petición (Oracle, Jersey, 2019).

JAX-RS es un soporte REST para las aplicaciones y servicios web a través del estándar JSR-311. Esta especificación se aplica al API de Java para Servicios Web que sean RESTful. JAX-RS utiliza anotaciones, que sirven de soporte para utilizar esta tecnología, para definir la parte que tiene que ver con el estilo REST dentro de las clases Java programadas en las aplicaciones.

### **3.6 Objetivo 6: Seleccionar los dispositivos wearables, la tecnología de comunicación y dispositivos móviles más adecuados al proyecto, en base a los datos que pueden proporcionar en el envío de la alerta.**

#### **3.6.1 Los dispositivos wearables**

Los wearables generalmente recopilan algún tipo de información del usuario o del entorno a través de sensores de seguimiento e incorporan uno o más métodos de sincronización a través de diversas tecnologías inalámbricas. Van desde sensores muy especializados que miden un único parámetro hasta multisensores muy complejos con un potente procesamiento interno. La peculiaridad aquí es que cuanto más simple es el dispositivo, menos energía consume y más dura la batería interna. Esta energía puede provenir de la carga de la red (enchufado para que no se pueda usar como un dispositivo portátil durante el tiempo de carga) o de fuentes externas dinámicas (movimiento, vibración, rotación, por lo que produce poca energía), solar (vestibles integrados en la ropa, también aptos para interiores), termoeléctrica (directa a la

piel, alta eficiencia), piezoeléctrica (usa energía extra del movimiento, ineficiente) o electricidad inalámbrica. Considerar al elegir los dispositivos wearables el alto nivel de configuración. La mayoría de los dispositivos wearables son configurables, permitiendo al usuario la parametrización casi total del dispositivo eligiendo qué funcionalidades se quiere activar y cómo se desea que se midan y presenten los datos.

### **3.6.2 Wearables para monitorear la seguridad personal**

Los wearables (artículos vestibles) podrían ser considerados como ropa inteligente o computadoras portables (Dunne, 2004). Estos dispositivos han tenido un crecimiento considerable en la última década, están presentes en la vida diaria de muchas personas, sus aplicaciones más importantes son el seguimiento diario de la actividad física, la evaluación fisiológica y la evaluación médica. (Guo, 11) Existen muchos wearables para el monitoreo diario de los usuarios y dentro de los más destacados se encuentran: relojes, pulseras, anillos, Hearables, ropa inteligente, etc. Los cuales tienen sus diferencias respecto a costos, usabilidad y fiabilidad. Estos wearables tendrán algunos de estos sensores incorporados: pulsómetro, acelerómetro, podómetro o giroscopio, además tendrán algún tipo de conectividad Bluetooth o WiFi. (de la Cal, 2018).

Estudios realizados por Henriksen y Mikalsen en 2018 identificó 423 wearables únicos, distribuidos entre 132 marcas diferentes. Casi la mitad de las marcas (47.0%, 62/132) tenían solo un dispositivo. Además, el 75.0% (99/132) de las marcas tenía tres o menos dispositivos, y el 83.3% (110/132) tenía cinco o menos dispositivos. Las marcas se originaron en 23 países diferentes, pero los Estados Unidos (43,2%, 57/132) y China (16,7%, 22/132, China continental; 19,0%, 25/132, incluido Taiwán) representaron el mayor número de origen de marca. Cada país restante representó entre el 0,8% (1/132) y el 5,3% (7/132) de las marcas. (Henriksen, 2018).

A continuación, se estudian los diferentes wearables utilizados para el seguimiento diario personal de la actividad física.

### **3.6.3 Relojes (Smart Watch)**

Puede ser considerado como un mini computador, este tiene numerosas funciones más allá de solo mostrar la hora. (Chuah, 2016), es un dispositivo de muñeca que, en su mayoría, actúa como una extensión de un teléfono móvil. (Henriksen, 2018) Pueden recibir

notificaciones, GPS, Manejo de redes sociales, control de la salud, seguimiento de la actividad física entre otras.

El usuario puede interactuar con el reloj utilizando pantallas táctiles, botones analógicos o entradas de voz. Dentro de los más conocidos están Apple Watch y Samsung Gear (Richardson S, 2018).

En la **Figura 11** se muestra la versión Apple Watch Series 7.



*Figura 11. Apple Watch Series 7<sup>11</sup>*

### **3.6.4 Pulseras (Smart Bands)**

Normalmente se usan en la muñeca, son dispositivos más dedicados al seguimiento de la actividad física. Suele ser más barato que un Smart Watch debido a que el hardware es menos costoso y a menudo tiene menos sensores. Debido a esto, generalmente también tiene una mejor duración de la batería y una interfaz limitada para mostrar los resultados del seguimiento. (Henriksen, 2018)

Las pulseras suelen tener una visualización mínima. La mayoría de los dispositivos requieren una App en un móvil para ver el seguimiento de la actividad física y de las estadísticas. Algunas también incorporan capacidades de notificación y entrenamiento cuando se combina con un teléfono inteligente. Algunos miden la frecuencia cardíaca y otros parámetros fisiológicos. Dentro de las más conocidas se encuentran Fitbit y Misfits (Richardson S, 2018).

En la **Figura 12** se muestra la versión de Fitbit Charge 5.

---

<sup>11</sup> Fuente: <https://www.apple.com/es/shop/buy-watch>



Figura 12. Fitbit Charge 5<sup>12</sup>

### 3.6.5 Anillos (Smart Ring)

Dentro de sus aplicaciones se pueden encontrar el envío de notificaciones o contestar llamadas. Se pueden recibir las alertas de las redes sociales, manipular la cámara del celular, seguimiento de la actividad física entre otras. Es evidente el avance en el desarrollo de wearables invisibles e inmersos lo que ayuda a tener mediciones más confiables (Lobelo, 2016). Dentro de los anillos más conocidos encontramos Motiv, Oura, NFC.

En la **Figura 13** se muestra el anillo Motiv.



Figura 13. Anillo Motiv<sup>13</sup>

### 3.6.6 Hearables

Son dispositivos de audio portátiles inteligentes que hacen más que permitir la comunicación por voz o la reproducción de música. Existen múltiples aplicaciones relacionadas con la salud para Hearables. En el caso de BeHear, es la amplificación auditiva. Otras funcionalidades es que pueden controlar la frecuencia cardíaca, la presión arterial, el nivel de oxígeno y la actividad física (Goldin, 2018).

En la **Figura 14** se muestra los audífonos BeHear.



Figura 14. Audífonos BeHear<sup>14</sup>

---

<sup>12</sup> Fuente: <https://www.fitbit.com/global/latam/products/trackers/charge5>

<sup>13</sup> Fuente: <https://www.mymotiv.com/>

<sup>14</sup> Fuente: <https://www.wearandhear.com/es/>

### 3.6.7 Ropa inteligente (Smart Clothes)

Para su elaboración se utilizan telas inteligentes y textiles interactivos, con sensores que permiten detectar y comunicar cambios en el individuo. Permitiendo por ejemplo la vigilancia de la salud, protección y seguridad, y seguimiento de la actividad física. (Lymberis, 2008) La ropa inteligente tiene varias ventajas, se puede destacar la eliminación de la colocación de sensores por un profesional ofreciendo un entorno natural. Además, proporciona una mayor precisión por tener una Interfaz más cercana al cuerpo. Los sensores están encerrados en las capas de tejido (por ejemplo, fibra óptica) (Lymberis, 2008).

En la **Figura 15** se muestra la ropa inteligente Athos.



Figura 15. Smart Clothes Athos<sup>15</sup>

En la tabla 5, se presenta una relación de los dispositivos wearables y sus características más resaltantes que se podrían utilizar para hacer uso en el sistema de monitoreo y control.

Dispositivo	Fabricante	Características medidas	Formas de conexión	Sitio web
 Spire Stone	Salud de la aguja	Respiración, frecuencia del pulso, actividad, pasos, calorías, estrés	Bluetooth	<a href="https://www.amazon.es/Spire-Stone-Stress-Activity-Tracker/dp/B00TH3SQOI?th=1">https://www.amazon.es/Spire-Stone-Stress-Activity-Tracker/dp/B00TH3SQOI?th=1</a>
 Mi Smart Band 6	Xiaomi	Sueño, PAI, Frecuencia cardiaca, actividad, análisis del sueño, peso, estrés y SPO <sub>2</sub>	Bluetooth	<a href="https://www.xataka.com/analisis/xiaomi-mi-smart-band-6-analisis-caracteristicas-precio-especificaciones">https://www.xataka.com/analisis/xiaomi-mi-smart-band-6-analisis-caracteristicas-precio-especificaciones</a>

<sup>15</sup> Fuente: <https://www.liveathos.com/>

 Fitbit Charge 4	Fitbit	Frecuencia cardíaca, actividad, análisis del sueño	Bluetooth	<a href="https://www.fitbit.com/global/es/home">https://www.fitbit.com/global/es/home</a>
 Omron Evolv	Omron	Presión arterial	Bluetooth	<a href="https://www.omron-healthcare.com/eu">https://www.omron-healthcare.com/eu</a>
 Freestyle Libre	Abbott	Glicemia	NFC	<a href="https://www.freestyle.abbot.com/us-en/home.html">https://www.freestyle.abbot.com/us-en/home.html</a>
 Temp Traq	Temp Traq	La temperatura corporal	Bluetooth	<a href="https://www.temptraq.com/">https://www.temptraq.com/</a>
 Empatica E4	Empatica	Temperatura, conductancia de la piel, pulso de volumen sanguíneo, actividad	Bluetooth	<a href="https://www.empatica.com/en-int/research/e4/">https://www.empatica.com/en-int/research/e4/</a>
 Microsoft Band 2	Microsoft	Temperatura, conductancia de la piel, frecuencia cardíaca, actividad, luz ambiental	Bluetooth	<a href="https://www.amazon.com/-/es/Microsoft-MU5-00002-Band-mediano-Negro/dp/B0163COWP2">https://www.amazon.com/-/es/Microsoft-MU5-00002-Band-mediano-Negro/dp/B0163COWP2</a>
 My Signals	My Signals	Sonido, temperatura, sensor EMG, frecuencia del pulso, respiración, conductancia cutánea, presión arterial, glucemia	Wi-Fi, Bluetooth	<a href="http://www.my-signals.com/">http://www.my-signals.com/</a>

 MindWare Mobile2	NeuroSky	Electroencefalograma	Bluetooth	<a href="https://store.neurosky.com/pages/mindwave/">https://store.neurosky.com/pages/mindwave/</a>
 Emotiv Insight	Emotiv	Electroencefalograma, Actividad	Bluetooth	<a href="https://www.emotiv.com/insight/">https://www.emotiv.com/insight/</a>
 Shimmer 3	Shimmer Sensing	Sensor EMG, respiración, actividad, temperatura, presión, fuerza	Bluetooth	<a href="http://www.shimmersensing.com/products/shimmer3-development-kit">http://www.shimmersensing.com/products/shimmer3-development-kit</a>
 Biometrics	Biometrics Ltd	Sensor EMG, electrogoniómetro, torsiómetro, actividad	Wi-Fi, Bluetooth	<a href="https://www.biometricsltd.com/">https://www.biometricsltd.com/</a>

Tabla 5. Wearables para monitorear los sobrevivientes de violencia

## TECNOLOGÍAS EMPLEADAS

Las tecnologías utilizadas en los artículos vestibles portátiles wearables se enmarcan principalmente de acuerdo con su propósito y funcionalidad. En primer lugar, deben tener buenas capacidades inalámbricas, ya sea Bluetooth (BLE para bajo consumo de energía), WiFi, NFC u otros estándares e incluso protocolos propietarios.

A las redes creadas por estos dispositivos se les denomina WBAN (Wireless Body Área Network, red inalámbrica en el área corporal) o WSN (Wireless Sensor Network, red inalámbrica de sensores).

Además, deben presentar la información relevante de forma correcta y clara en pantallas LED, u otro similar. Para dispositivos HUD (Head-Up Display) como cascos de realidad virtual o gafas inteligentes, estas pantallas son mucho más complejas, por lo que encarecen el producto.

Asimismo, de acuerdo con su propósito y la cantidad de datos a almacenar, deben tener suficiente capacidad de memoria y métodos apropiados para leer, actualizar y recuperar datos. Un caso típico son las tarjetas SD o microSD o alguna otra memoria interna.

### **3.7 Objetivo 7: Realizar pruebas unitarias del sistema para evaluar el buen funcionamiento, conforme a los requisitos establecidos.**

La plataforma de monitoreo y control de la seguridad personal durante el proceso de desarrollo se ha seguido en base a las etapas de ingeniería del software. Para ello, se realizó un análisis de los requisitos de la plataforma, describiendo cada caso de uso, por otro lado, se verifico previo análisis la plataforma, seleccionando cuales son los parámetros de medición más adecuados, además los dispositivos que se seleccionaran para esta medición. También se realizó un modelo conceptual indicando las entidades que influyen en el sistema. Por último, se realizó una explicación del sistema de seguridad personal, indicando el funcionamiento del algoritmo.

Por otro lado, se realizó el diseño de la arquitectura que más se adecuada para la plataforma con el respectivo modelado de datos. Luego se muestra cómo se implementó la plataforma, explicando cada una de las capas y las partes de la arquitectura principal, dividiéndola en cinco secciones: requisitos, análisis, diseño, implementación y pruebas. Siguiendo los pasos del ciclo de vida del software.

#### **3.7.1 Especificaciones técnicas para el despliegue de la plataforma.**

A continuación, se describen las máquinas para el despliegue tanto del nivel de persistencia como el de captura de datos.

##### *3.7.1.1 Máquina virtual del servicio Rest*

La máquina virtual cuenta con las siguientes características:

- **Sistema operativo:** Windows 10
- **Disco duro:** 1 tera byte
- **Memoria RAM instalada:** 8 gb

Los servicios instalados son:

- **Servicio de base de datos:**

- **Java:**
- **Tomcat:**
- **Jersey:**

#### 3.7.1.2 *Dispositivo móvil*

El dispositivo móvil donde se ejecutó la aplicación cuenta con las siguientes características:

- **Marca del dispositivo:** Samsung Galaxy A32.
- **Numero de modelo:** SM-A325M
- **Sistema operativo:** versión android 12
- **Permisos de internet:** Si.
- **Permisos de Bluetooth:** Si.

#### 3.7.1.3 *Ordenador de desarrollo*

El ordenador donde se desarrolló el servicio rest y la aplicación móvil tiene las siguientes características:

- **Procesador:** Intel Core I7.
- **Memoria RAM instalada:** 8 GB.
- **Sistema operativo:** Windows 10 de 64 bits.
- **Disco duro:** 1 tera byte.
- **Versión de Java:** 1.8.0.2

### 3.7.2 **Descripción de la plataforma**

El propósito principal de la plataforma es reducir la violencia pública, brindando seguridad y protección a través de las intervenciones en el momento del evento, reduciendo así los temores y miedo del usuario en el delito.

Esta plataforma cuenta con un sistema de seguimiento pasivo continuo que hace uso de biosensores adheridos al usuario y técnicas de reconocimiento de voz mediante un sensor de micrófono, para determinar si se está produciendo una situación anormal relacionada con la violencia. Además, cuenta con un botón de pánico de activación manual para el envío de la alerta.

La estructura de monitorización del sistema supervisa las señales biológicas de acuerdo con el estado actual de la tecnología de wearables. La solución de monitoreo y control se puede desconectar manualmente durante un tiempo (bajo demanda) para evitar falsos positivos cuando un usuario, por ejemplo, está practicando algún deporte o realizando otras actividades que podrían activar incorrectamente la alarma.

Cuando se activa, el sistema rastrea la ubicación del usuario mediante el sensor del Sistema de posicionamiento global (GPS) y envía un correo electrónico de emergencia a la

persona que puede ayudarlo o salvarlo. El uso de componentes sofisticados asegura la precisión del sistema y lo hace confiable.

El sistema propuesto estará disponible las 24 horas del día, los 7 días de la semana, para ayudar a evitar situaciones desafortunadas. La aplicación puede acceder a la ubicación, el historial, los detalles de contacto y los datos de audio y fotografía almacenados previamente al iniciar sesión.

Las interfaces de usuario de la plataforma deben ser lo más intuitivas posibles, además de tratar de reducir el número de clics necesarios para llevar a cabo las distintas acciones o actividades.

Por último, dado el carácter investigador de la plataforma propuesta se propone la elaboración de distintos estudios científicos que permitan determinar las distintas formas de monitorear y controlar la seguridad personal de los usuarios.

### **3.7.3 Requerimientos de la plataforma**

El sistema cuenta con los siguientes diagramas de casos de uso del sistema, agrupados en: gestión de contactos, gestión del aprendizaje automático, gestión del modo cuenta atrás, gestión del modo supervisión, gestión de alertas y gestión del administrador, donde el actor participante será el encargado de enviar la alerta, contacto es quien recibe la alerta, temporizador y dispositivo son los encargados de enviar la alerta, grabar el audio del entorno, obtener información del entorno y tomar fotos, asistente de biosensor y audio son los encargados de activar la alerta y administrador encargado de enviar las actualizaciones de la aplicación instalada.

En la **figura 16** se muestra el diagrama general de casos de uso.

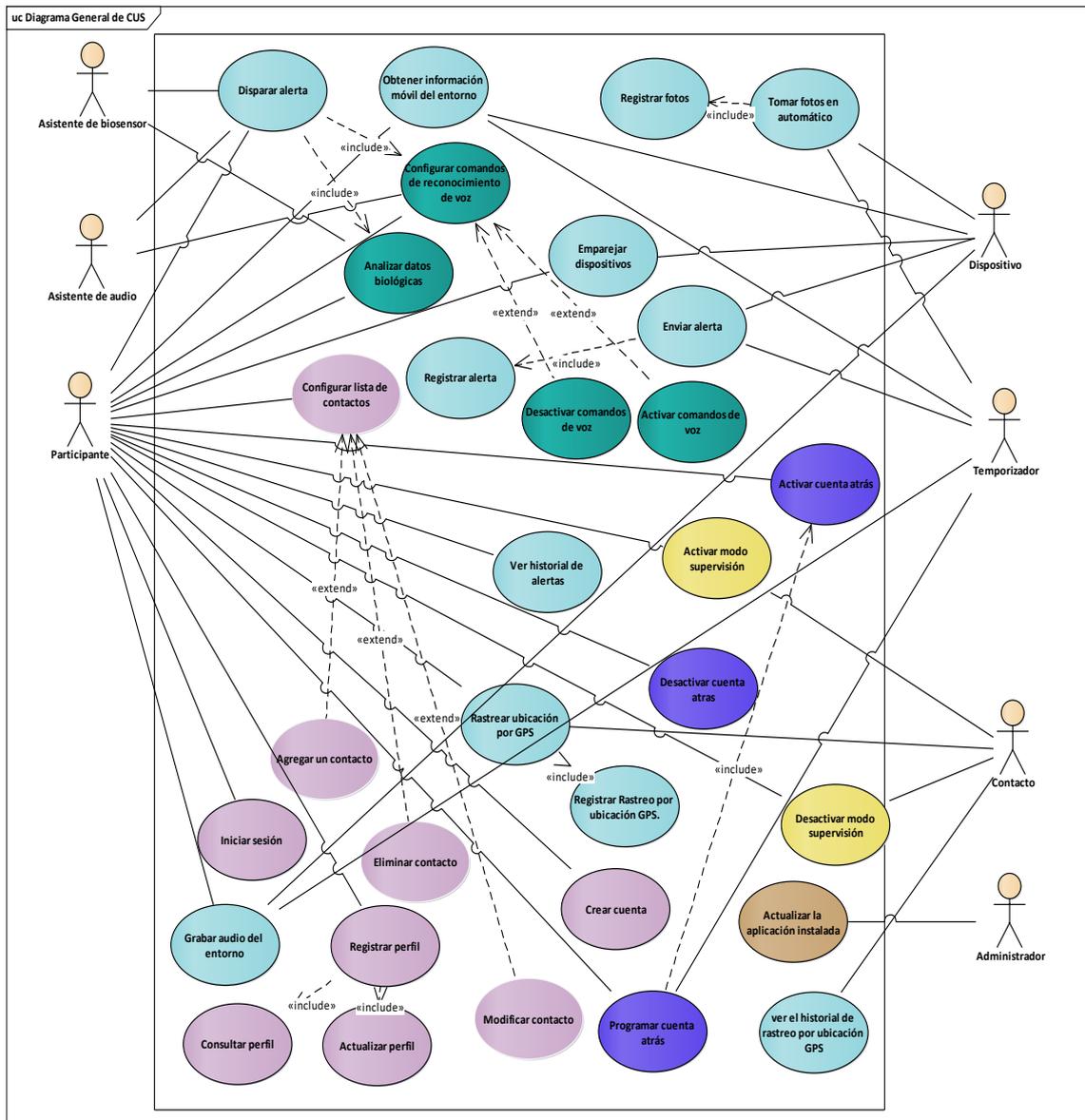


Figura 16. Diagrama General de Casos de Uso

En la **figura 17** se muestra el diagrama de casos de uso de gestión de contactos.

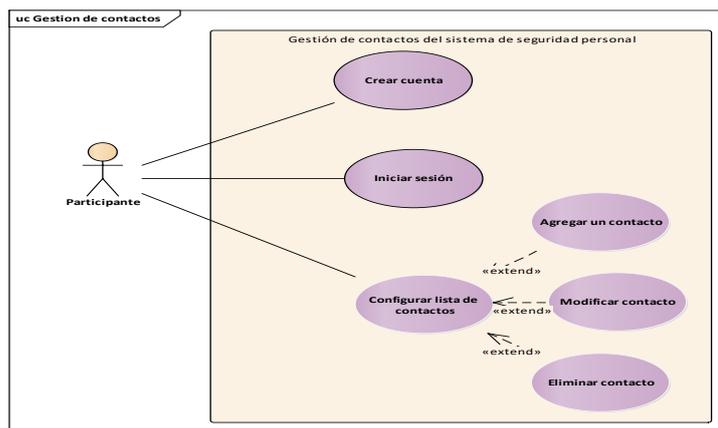


Figura 17. Gestión de Contactos

En la **tabla 6** se muestra la especificación del caso de uso crear cuenta.

<b>RF- SMC-001</b>	Crear cuenta	
<b>Actores</b>	Participante	
<b>Descripción</b>	Permite a los usuarios participantes registrarse en el sistema.	
<b>Precondición</b>	Se haya cargado la pantalla inicial del sistema. Se haya seleccionado el botón registrarse.	
<b>Secuencia</b>	<b>Paso</b>	<b>Acción</b>
<b>Normal</b>	S1	El participante ingresa el email y su contraseña para crear su cuenta.
	S2	El participante presiona el botón siguiente
	S3	El participante ingresa sus datos.
	S4	El participante presiona el botón siguiente
	S5	El sistema valida los datos ingresados
	S6	El sistema mostrará la pantalla principal con las opciones del menú respectivas.
<b>Postcondición</b>	Queda habilitada la pantalla principal del sistema, para su posterior uso.	
<b>Excepciones</b>	<b>Paso</b>	<b>Acción</b>
	E1	El participante solo podrá usar el correo y contraseña para crear una sola cuenta
	E2	El sistema despliega un mensaje de error, dando a conocer que la información ingresada ya existe.
<b>Rendimiento</b>	<b>Paso</b>	<b>Cota de tiempo</b>

	S5	3 segundos
	S6	5 segundos
<b>Frecuencia esperada</b>	10/día	
<b>Importancia</b>	Alta	
<b>Comentarios</b>	<comentarios adicionales>	

Tabla 6. Crear cuenta

En la **tabla 7** se muestra la especificación del caso de uso iniciar sesión.

<b>RF- SMC-002</b>	<b>Iniciar sesión</b>	
<b>Actores</b>	Participante	
<b>Descripción</b>	Permite a los usuarios participantes iniciar sesión para ingresar al sistema de acuerdo a su perfil.	
<b>Precondición</b>	Se haya cargado la pantalla inicial del sistema. Se haya registrado el participante. Se haya ingresado el usuario con su password correspondiente.	
<b>Secuencia Normal</b>	<b>Paso</b>	<b>Acción</b>
	S1	El participante ingresa el email y su contraseña en la pantalla principal. Presiona el botón iniciar sesión
	S2	El sistema valida los datos ingresados
	S3	El sistema carga la pantalla de acuerdo al perfil y habilita las opciones correspondientes
	S4	Si el participante no recuerda la información de acceso al sistema, deberá seleccionar el botón olvido contraseña.
	S5	El sistema solicitará el ingreso de la dirección de correo electrónico y selecciona el botón de envío.
	S6	El sistema verifica la información y envía los datos del usuario a la dirección correo electrónico.
<b>Postcondición</b>	Habilitadas las opciones de ingreso al sistema de acuerdo al perfil de acceso.	
<b>Excepciones</b>	<b>Paso</b>	<b>Acción</b>
	E1	Los datos del perfil sólo deben ingresarse al momento que se crea la cuenta del usuario participante.

	E2	El sistema despliega un mensaje de error, dando a conocer que la información ingresada de usuario no existe.
<b>Rendimiento</b>	<b>Paso</b>	<b>Cota de tiempo</b>
	S2	3 segundos
	S3	5 segundos
	S6	5 segundos
<b>Frecuencia esperada</b>	10 /dia	
<b>Importancia</b>	Alta	
<b>Comentarios</b>	<comentarios adicionales>	

Tabla 7. Iniciar Sesión

En la **tabla 8** se muestra la especificación del caso de uso configurar lista de contactos

<b>RF- SMC-003</b>	Configurar lista de contactos	
<b>Actores</b>	Participante	
<b>Descripción</b>	Permite al usuario participante gestionar la lista de contactos agregando, modificando o eliminando los contactos en el sistema.	
<b>Precondición</b>	Ingresado a la pantalla de contactos del sistema con éxito.	
<b>ESCENARIO 1: Agregar contacto</b>		
<b>Secuencia Normal</b>	<b>Paso</b>	<b>Acción</b>
	S1.1	El participante ingresa a la pantalla de contactos
	S1.2	El sistema carga la pantalla mostrando la lista de contactos existentes
	S1.3	El participante presiona el botón agregar
	S1.4	El sistema habilita una pantalla con los campos correspondientes para ingresar los datos del contacto
	S1.5	El participante ingresa los datos del contacto en la aplicación como: nombre, email, y número de celular. Presiona el botón para guardar datos
	S1.6	El sistema actualiza la información ingresada en la base de datos y actualiza la pantalla de la lista de contactos.
<b>ESCENARIO 2: Modificar contacto</b>		
<b>Secuencia Normal</b>	S2.1	El participante ingresa a la pantalla de contactos

	S2.2	El sistema carga la pantalla mostrando la lista de los contactos
	S2.3	El participante busca el contacto deseado y lo selecciona
	S2.4	El sistema cargará la pantalla con los datos del contacto seleccionado para modificar la información
	S2.5	El participante modifica los datos necesarios correspondientes en la aplicación y luego pulsa el botón grabar.
	S2.6	El sistema actualiza la información modificada en la base de datos y se actualiza la pantalla
<b>ESCENARIO 3: Eliminar contacto</b>		
<b>Secuencia Normal</b>	S3.1	El participante ingresa a la pantalla de contactos
	S3.2	El sistema carga la pantalla mostrando la lista de contactos.
	S3.3	El participante buscará el contacto deseado y lo selecciona
	S3.4	El participante selecciona el botón eliminar contacto y el sistema elimina el contacto y actualiza la base de datos y la pantalla.
<b>Postcondición</b>	Operaciones realizadas correspondiente al configurar la lista de contactos.	
<b>Excepciones</b>	<b>Paso</b>	<b>Acción</b>
	E1	Si el participante no selecciona un registro para modificar o eliminar, el sistema mostrará un mensaje en pantalla.
	E2	Mensaje: debe seleccionar un contacto.
<b>Rendimiento</b>	<b>Paso</b>	<b>Cota de tiempo</b>
	S1.2	2 segundos
	S2.2	2 segundos
	S3.2	2 segundos
<b>Frecuencia esperada</b>	1 /día	
<b>Importancia</b>	Alta	
<b>Comentarios</b>	<comentarios adicionales>	

Tabla 8. Configurar lista de contactos

En la **figura 18** se muestra el diagrama de casos de uso de gestión del aprendizaje automático.

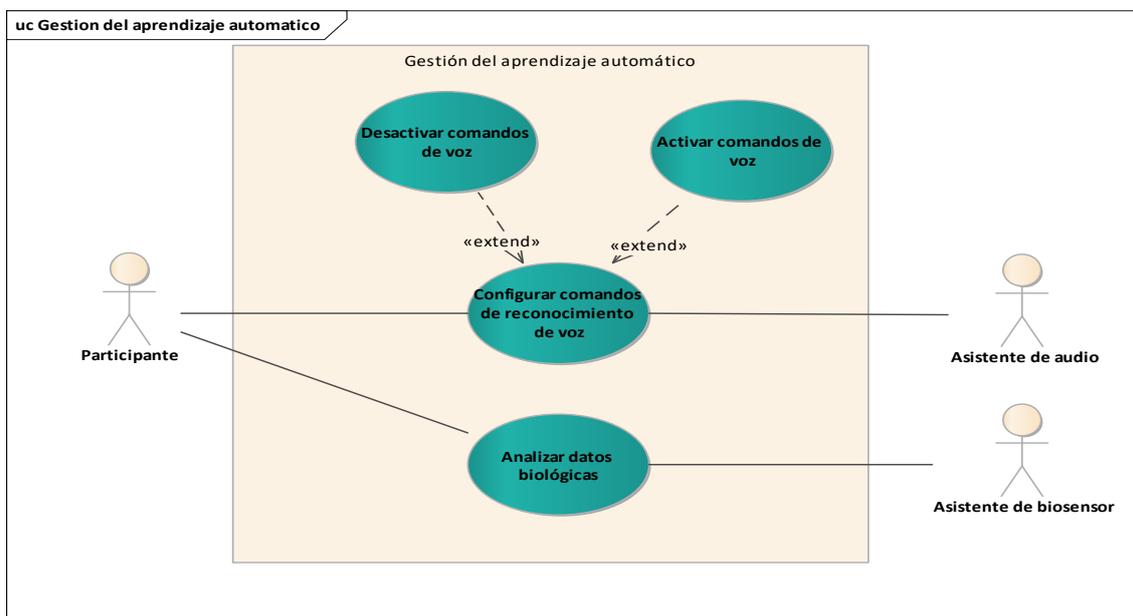


Figura 18. Gestión del Aprendizaje Automático

En la **tabla 9** se muestra la especificación del caso de uso configurar comandos de reconocimiento de voz.

<b>RF- SMC-004</b>	Configurar comandos de reconocimiento de voz	
<b>Actores</b>	Participante, asistente de audio	
<b>Descripción</b>	Permite al participante configurar y almacenar los comandos de reconocimiento de voz	
<b>Precondición</b>	Se haya ingresado con éxito a la pantalla de alerta por reconocimiento por voz.	
<b>ESCENARIO 1: Configuración de los comandos de voz</b>		
<b>Secuencia Normal</b>	<b>Paso</b>	<b>Acción</b>
	S1.1	El participante crea los audios de los comandos de voz que el asistente de audio reconocerá antes de disparar la alerta.
	S1.2	El asistente de audio cifra los comandos de voz y los almacena en la base de datos como parte del perfil de autenticación del participante.
	S1.3	El sistema despliega un mensaje en pantalla. Mensaje: audios de voz almacenados exitosamente.

	S1.4	El asistente captura los audios de los comandos de voz del usuario y analiza el patrón de expresión según lo almacenado.
<b>ESCENARIO 2: Activar por comandos de voz</b>		
<b>Secuencia Normal</b>	S2.1	Cada vez que el participante con autenticación de voz emite un comando, su voz se compara con los audios almacenados en la base de datos.
	S2.2	Si el comando de voz del participante coincide con alguno de los audios almacenados en la base de datos del sistema
	S2.3	El asistente de audio dispara la alerta a modo de activación por comandos de voz.
<b>ESCENARIO 3: Desactivar por comandos de voz</b>		
	S3.1	Si el disparo de la alerta es a consecuencia de un falso positivo
	S3.2	El participante dentro del rango programado de tiempo de activación de cuenta atrás, podrá desactiva la alerta con otro comando de voz
	S3.3	El asistente de audio emite un mensaje de voz
	S3.4	Mensaje: disparo de alerta desactivado
<b>Postcondición</b>	Operaciones realizadas correspondiente al análisis de comandos de reconocimiento de voz	
<b>Excepciones</b>	<b>Paso</b>	<b>Acción</b>
	E1	Si el comando voz del participante no coincide con los audios almacenados en la base de datos del sistema
	E2	El asistente de audio no dispara la alerta
	E3	El sistema dispara la alerta a través de otro medio de activación
<b>Rendimiento</b>	<b>Paso</b>	<b>Cota de tiempo</b>
	S1.3	2 segundos
<b>Frecuencia esperada</b>	10 /mes	
<b>Importancia</b>	Alta	
<b>Comentarios</b>	<comentarios adicionales>	

Tabla 9. Configurar comandos de reconocimiento de voz

En la **tabla 10** se muestra la especificación del caso de uso Analizar datos biológicos.

<b>RF- SMC-005</b>	Analizar datos biológicos	
<b>Actores</b>	Participante, asistente de biosensor	
<b>Descripción</b>	En todo momento el asistente de biosensor deberá estar monitoreando los signos vitales del participante, obtenido del dispositivo wearable los siguientes datos: frecuencia cardiaca, la temperatura corporal y el oxígeno en la sangre, para inferir si se está produciendo una acción anormal relacionada con la violencia.	
<b>Precondición</b>	El participante deberá llevar consigo una pulsera wearable que permita emitir los signos vitales de forma continua desde los sensores al dispositivo móvil.	
<b>Secuencia</b>	<b>Paso</b>	<b>Acción</b>
<b>Normal</b>	S1	El dispositivo móvil recibe y analiza las señales biológicas del participante, de acuerdo a la tecnología de la pulsera wearable y a los parámetros establecidos.
	S2	Si los signos vitales están fuera del rango establecido, el asistente del biosensor emite y envía la señal de alerta.
	S3	El sistema almacena los signos vitales del participante en la base de datos
<b>Postcondición</b>	Operación realizada correspondiente al análisis de datos biológicos.	
<b>Excepciones</b>	<b>Paso</b>	<b>Acción</b>
	E1	Si los signos vitales de los participantes están dentro de lo permitido no se ejecuta ninguna señal de alerta
	E2	La aplicación podrá ser ejecutarse en cualquier momento incluso cuando el usuario no tenga la aplicación en primer plano.
<b>Rendimiento</b>	<b>Paso</b>	<b>Cota de tiempo</b>
	S1	5 segundos
	S2	2 segundos
<b>Frecuencia esperada</b>	10 /día	
<b>Importancia</b>	Alta	
<b>Comentarios</b>	<comentarios adicionales>	

Tabla 10. Analizar Datos Biológicos

En la **figura 19** se muestra el diagrama de casos de uso de gestión del modo cuenta atrás.

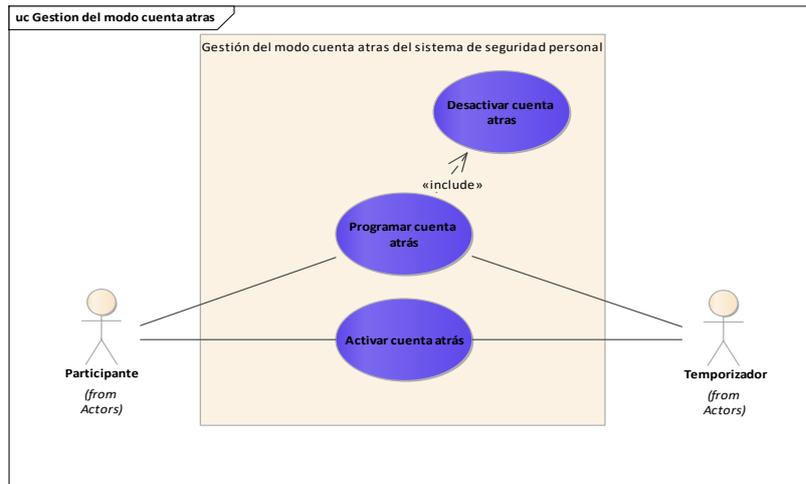


Figura 19. Gestión del modo cuenta atrás

En la **tabla 11** se muestra la especificación del caso de uso programar cuenta atrás.

<b>RF- SMC-006</b>	Programar cuenta atrás	
<b>Actores</b>	Participante, Temporizador	
<b>Descripción</b>	Permite al usuario participante programar el tiempo de duración de la cuenta atrás después de haberse ejecutado la alerta, evitando de esta manera los falsos positivos.	
<b>Precondición</b>	Se haya ingresado con éxito a la pantalla de cuenta atrás.	
<b>Secuencia</b>  <b>Normal</b>	<b>Paso</b>	<b>Acción</b>
	S1	El participante elige la opción programar cuenta atrás.
	S2	El sistema muestra una pantalla con las opciones del tiempo de duración de la cuenta atrás.
	S3	El participante selecciona el tiempo de duración de la cuenta atrás.
	S4	El participante guarda los cambios deseados
	S5	El sistema muestra un mensaje de conformidad
<b>Postcondición</b>	El sistema quedará preparado para la activación y desactivación de la cuenta atrás.	
<b>Excepciones</b>	<b>Paso</b>	<b>Acción</b>
	E1	Si el participante no ha programado la cuenta atrás, el temporizador no entrará en funcionamiento y el sistema no enviará ninguna alerta.

	E2	El participante a tras de esta pantalla, podrá desactivar la cuenta atrás.
<b>Rendimiento</b>	<b>Paso</b>	<b>Cota de tiempo</b>
	S2	2 segundos
<b>Frecuencia esperada</b>	10 /día	
<b>Importancia</b>	Alta	
<b>Comentarios</b>	<comentarios adicionales>	

Tabla 11. Programar cuenta atrás

En la **tabla 12** se muestra la especificación del caso de uso activar cuenta atrás.

<b>RF- SMC-007</b>	Activar cuenta atrás	
<b>Actores</b>	Participante, Temporizador	
<b>Descripción</b>	Permite al sistema activa la cuenta atrás, a partir del disparado de la señal de alerta por parte del participante.	
<b>Precondición</b>	Disparo de la señal de alerta	
<b>Secuencia Normal</b>	<b>Paso</b>	<b>Acción</b>
	S1	El sistema dispara la señal de alerta al presionarse un botón del dispositivo NFC, del dispositivo móvil, emitir un sonido el participante o a través de las señales biológicas del cuerpo que emiten los sensores del dispositivo wearable.
	S2	Al disparo de la señal de alerta, el temporizador contará en regresiva el tiempo programado en la configuración de la cuenta atrás, antes de que se envíe la alerta.
	S3	Transcurrido el tiempo programado, el sistema envía la alerta.
<b>Postcondición</b>	La cuenta atrás quedará activa, después de haberse disparado la alerta.	
<b>Excepciones</b>	<b>Paso</b>	<b>Acción</b>
	E1	Si el participante no ha programado la cuenta atrás, esta no se activará después de haberse disparado la alerta.
<b>Rendimiento</b>	<b>Paso</b>	<b>Cota de tiempo</b>
	S3	2 segundos
<b>Frecuencia esperada</b>	10 /día	
<b>Importancia</b>	Alta	

<b>Comentarios</b>	<comentarios adicionales>
--------------------	---------------------------

Tabla 12. Activar cuenta atrás

En la **tabla 13** se muestra la especificación del caso de uso desactivar cuenta atrás.

<b>RF- SMC-008</b>	Desactivar cuenta atrás	
<b>Actores</b>	Participante	
<b>Descripción</b>	Permite al participante desactivar la cuenta atrás por un periodo de tiempo programado para que no interfiera en situaciones no amenazantes como un falso positivo. El participante también podrá desactivar la cuenta atrás después de haberse disparado la alerta	
<b>Precondición</b>	Se haya ingresado con éxito a la pantalla de cuenta atrás.	
<b>Secuencia</b>  <b>Normal</b>	<b>Paso</b>	<b>Acción</b>
	S1	El participante ingresa exitosamente a la pantalla de cuenta atrás
	S2	Si la cuenta atrás sólo se encuentra programada, el participante podrá desactivarla para evitar falsos positivos, debiendo guardar los cambios.
	S3	El sistema despliega un mensaje en pantalla
	S4	Mensaje: cuenta atrás desactivada
	S5	Si la cuenta atrás ya ha sido activada después del disparo de la alerta, el participante a través de la pantalla de configuración podrá desactivarla.
	S6	El sistema despliega un mensaje en la pantalla
	S7	Mensaje: cuenta atrás desactivada
<b>Postcondición</b>	El sistema quedará desactivado y no podrán darse el envío de alertas.	
<b>Excepciones</b>	<b>Paso</b>	<b>Acción</b>
	E1	Si la cuenta atrás no ha sido desactiva y la alerta ya ha sido enviada
	E2	El participante a través del sistema podrá enviar un mensaje a sus contactos indicando que el envío de la alerta se trata de un falso positivo.
<b>Rendimiento</b>	<b>Paso</b>	<b>Cota de tiempo</b>
	S1	2 segundos

	S2	2 segundos
	S5	2 segundos
<b>Frecuencia esperada</b>	15 /mes	
<b>Importancia</b>	Alta	
<b>Comentarios</b>	<comentarios adicionales>	

Tabla 13. Desactivar cuenta atrás

En la **figura 20** se muestra el diagrama de casos de uso de gestión del modo supervisión de la actividad.

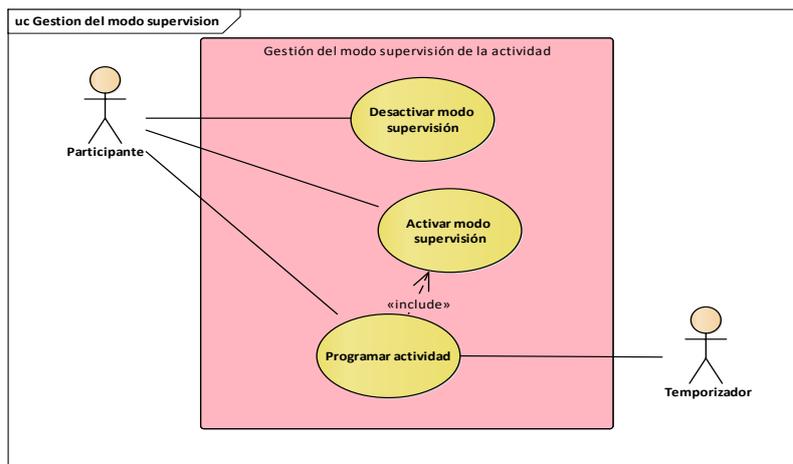


Figura 20. Gestión del modo supervisión

En la **tabla 14** se muestra la especificación del caso de uso activar modo supervisión de la actividad.

<b>RF- SMC-009</b>	Activar modo supervisión de la actividad	
<b>Actores</b>	Participante, Temporizador, contacto	
<b>Descripción</b>	Permite al participante activar el modo supervisión de una actividad, por parte de los contactos seleccionados.	
<b>Precondición</b>	Se haya ingresado con éxito a la pantalla de modo supervisión.	
<b>Secuencia Normal</b>	S1	El participante deberá definir la nueva actividad, el tiempo, el destino y los contactos
	S2	El participante podrá agregarlo a favoritos la nueva actividad creada, para las próximas definiciones de actividades del mismo tipo.
	S3	La supervisión o monitoreo de los contactos empezará a partir de que el usuario participante selecciona el botón iniciar monitoreo.

	S4	El sistema enviará la alerta con los datos de ubicación y estado de la batería al participante, según la programación de la cuenta atrás.
<b>Postcondición</b>	El modo supervisión quedará activo para dar inicio al monitoreo del participante por parte de los contactos.	
<b>Excepciones</b>	<b>Paso</b>	<b>Acción</b>
	E1	El participante podrá seleccionar el botón de pánico y el sistema enviará la alerta a los contactos de manera inmediata, no considerando la programación de la cuenta atrás.
<b>Rendimiento</b>	<b>Paso</b>	<b>Cota de tiempo</b>
	S1	2 segundos
<b>Frecuencia esperada</b>	10 /mes	
<b>Importancia</b>	Alta	
<b>Comentarios</b>	<comentarios adicionales>	

Tabla 14. Activar modo supervisión

En la **tabla 15** se muestra la especificación del caso de uso desactivar modo supervisión.

<b>RF- SMC-010</b>	Desactivar modo supervisión	
<b>Actores</b>	Participante	
<b>Descripción</b>	Permite al participante desactivar el modo supervisión de una actividad.	
<b>Precondición</b>	Se haya ingresado con éxito a la pantalla de modo supervisión.	
<b>Secuencia Normal</b>	<b>Paso</b>	<b>Acción</b>
	S.1	El participante podrá desactivar el modo supervisión de una actividad
	S.2	El sistema mostrará en pantalla el mensaje
	S.3	Mensaje: Modo supervisión de la actividad se encuentra desactivado
<b>Postcondición</b>	Los contactos no podrán supervisar al participante, hasta que el modo supervisión quede activado.	
<b>Excepciones</b>	<b>Paso</b>	<b>Acción</b>
	E1	Si el modo supervisión de una actividad no se encuentra desactivado, los contactos podrán seguir monitoreando al participante.

Rendimiento	Paso	Cota de tiempo
	S.1	2 segundos
	S.2	2 segundos
Frecuencia esperada	10 /mes	
Importancia	Alta	
Comentarios	<comentarios adicionales>	

Tabla 15. Desactivar modo supervisión

En la **figura 21** se muestra el diagrama de casos de uso de gestión de alertas.

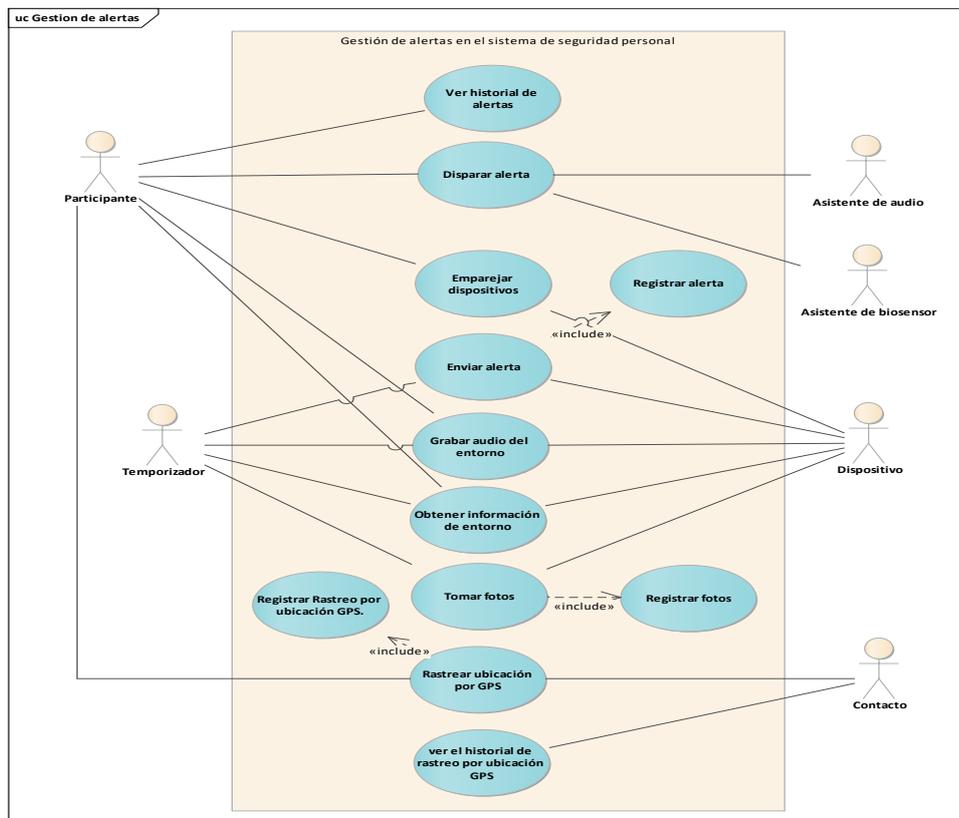


Figura 21. Gestión de alertas

En la **tabla 16** se muestra la especificación del caso de uso efectuar alerta.

<b>RF- SMC-011</b>	Efectuar alerta
<b>Actores</b>	Participante, asistente de audio, asistente de biosensor
<b>Descripción</b>	Permite al usuario participante efectuar la alerta ya sea de forma manual (presionando un botón del dispositivo / agitando el teléfono móvil) o automática, según los parámetros establecidos.
<b>Precondición</b>	El participante presione el botón de alerta, emita un sonido de voz o algún signo vital fuera de lo normal.

<b>Secuencia</b>	<b>Paso</b>	<b>Acción</b>
<b>Normal</b>	S1	El participante presiona el botón de alerta, emite algún audio de voz o algún signo vital fuera de lo normal.
	S2	Si el participante presiona el botón de alerta del dispositivo móvil o del dispositivo NFC, el sistema efectúa la alerta.
	S3	Si el participante emite algún audio de voz de acorde con las palabras de audio ya establecidas en el sistema, el sistema efectúa la alerta
	S4	Si el participante a través del sistema emite algún signo vital fuera de lo normal, el sistema efectúa la alerta.
<b>Postcondición</b>	El sistema quedará activo para dar inicio a la activación de la cuenta atrás por parte del temporizador, para luego enviar la alerta.	
<b>Excepciones</b>	<b>Paso</b>	<b>Acción</b>
	E1	Si el participante no presiona ningún botón de alerta, emite un sonido de voz diferente a las palabras establecidas o los signos vitales que se emiten están dentro de lo normal
	E2	El sistema no efectúa ninguna alerta
<b>Rendimiento</b>	<b>Paso</b>	<b>Cota de tiempo</b>
	S2	2 segundos
	S3	2 segundos
	S4	2 segundos
<b>Frecuencia esperada</b>	15 /mes	
<b>Importancia</b>	Alta	
<b>Comentarios</b>	<comentarios adicionales>	

Tabla 16. Efectuar alerta

En la **tabla 17** se muestra la especificación del caso de uso enviar alerta.

<b>RF- SMC-012</b>	Enviar alerta
<b>Actores</b>	Temporizador, Dispositivo

<b>Descripción</b>	<p>Permite al dispositivo móvil enviar la alerta a los contactos, después de haber sido disparada y transcurrido el tiempo de cuenta atrás.</p> <p>El envío de la alerta irá acompañado de los siguientes datos: identidad, estado de la batería, coordenadas de latitud y longitud obtenidas por GPS, la dirección a través de un enlace de google Maps, las direcciones MAC Bluetooth del entorno operativo y fotos del atacante generadas a partir de la manipulación del teléfono móvil.</p>	
<b>Precondición</b>	Se haya efectuado la alerta y activado la cuenta atrás.	
<b>Secuencia</b>	<b>Paso</b>	<b>Acción</b>
<b>Normal</b>	S1	Si en el sistema se haya agotado el tiempo programado de activación de la cuenta atrás, el dispositivo envía la alerta a los contactos.
	S2	El dispositivo registra la alerta como un archivo log de los eventos ocurridos.
<b>Postcondición</b>	El sistema activará una función de llamada de manera automática para hacer que los teléfonos de los contactos suenen al momento de la recepción de la alerta.	
<b>Excepciones</b>	<b>Paso</b>	<b>Acción</b>
	E1	Si dispositivos móviles están en modo silencio, el sistema sonará al momento de la recepción de la alerta.
	E2	El sistema no podrá enviar la alerta a los contactos si el modo cuenta atrás se encuentra desactivado.
<b>Rendimiento</b>	<b>Paso</b>	<b>Cota de tiempo</b>
	S1	2 segundos
	S2	3 segundos
<b>Frecuencia esperada</b>	15 /mes	
<b>Importancia</b>	Alta	
<b>Comentarios</b>	<comentarios adicionales>	

Tabla 17. *Enviar alerta*

En la **tabla 18** se muestra la especificación del caso de uso grabar audio del entorno.

<b>RF- SMC-013</b>	Grabar audio del entorno
<b>Actores</b>	Participante, Temporizador, dispositivo
<b>Descripción</b>	Permite al dispositivo móvil, grabar el audio del entorno generado a partir del envío de la alerta a los contactos.

<b>Precondición</b>	Envío de la alerta a los contactos.	
<b>Secuencia</b>  <b>Normal</b>	<b>Paso</b>	<b>Acción</b>
	S1	Si el dispositivo envía la alerta satisfactoriamente a los contactos, el dispositivo inicia la grabación de audio según el tiempo programado por el temporizador.
	S2	El sistema almacena el audio en la base de datos.
	S3	El participante podrá descargar el audio como un archivo mp3, el cual servirá de evidencia para las investigaciones pertinentes.
<b>Postcondición</b>	En el sistema quedarán grabados los archivos de audio.	
<b>Excepciones</b>	<b>Paso</b>	<b>Acción</b>
	E1	Si la alerta no ha sido enviada satisfactoriamente, el dispositivo no iniciará la grabación de audio.
<b>Rendimiento</b>	<b>Paso</b>	<b>Cota de tiempo</b>
	S1	10 segundos
<b>Frecuencia esperada</b>	15 /mes	
<b>Importancia</b>	Alta	
<b>Comentarios</b>	<comentarios adicionales>	

Tabla 18. Grabar audio del entorno

En la **tabla 19** se muestra la especificación del caso de uso obtener información del entorno.

<b>RF- SMC-014</b>	Obtener información del entorno	
<b>Actores</b>	Participante, Temporizador, dispositivo	
<b>Descripción</b>	<p>Permite al dispositivo móvil del participante obtener datos de los dispositivos móviles de su entorno operativo, después de haber sido enviada la alerta.</p> <p>El rastreo de contactos es directo, utilizando redes de proximidad Bluetooth. Esta aplicación utiliza la fuerza de la señal recibida RSSI para medir la proximidad entre dos teléfonos inteligentes.</p>	
<b>Precondición</b>	El dispositivo del usuario participante deberá tener activado el servicio Bluetooth.	
<b>Secuencia</b>  <b>Normal</b>	<b>Paso</b>	<b>Acción</b>
	S1	El dispositivo móvil del participante hace un rastreo de todos los teléfonos móviles más cercanos, dentro de un determinado rango de tiempo.

	S2	El sistema almacena en la base de datos la dirección Bluetooth, el código IMEI, la intensidad de la señal, número de serie y dirección MAC de wifi de los teléfonos móviles de los contactos más cercanos.
<b>Postcondición</b>	El sistema quedará activo para dar inicio a la generación de archivos csv de los datos obtenidos del entorno del participante.	
<b>Excepciones</b>	<b>Paso</b>	<b>Acción</b>
	E1	Si en el dispositivo del participante el servicio Bluetooth no se encuentra activo, no podrá obtener la información de los contactos del entorno más cercano.
<b>Rendimiento</b>	<b>Paso</b>	<b>Cota de tiempo</b>
	S1	10 segundos
	S2	5 segundos
<b>Frecuencia esperada</b>	20 /mes	
<b>Importancia</b>	Alta	
<b>Comentarios</b>	<comentarios adicionales>	

Tabla 19. Obtener información del entorno

En la **tabla 20** se muestra la especificación del caso de uso tomar foto.

<b>RF- SMC-015</b>	Tomar foto	
<b>Actores</b>	Temporizador, dispositivo	
<b>Descripción</b>	Permite al dispositivo móvil del participante tomar fotos de manera automática al momento que el agresor trata de apagar el dispositivo o manipular el patrón de ingreso.	
<b>Precondición</b>	El dispositivo haya enviado la alerta a los contactos	
<b>Secuencia</b> <b>Normal</b>	<b>Paso</b>	<b>Acción</b>
	S1	Si en el dispositivo móvil se mantiene presionado el botón de apagado de manera permanente.
	S2	Automáticamente el dispositivo tiene un máximo de 10 segundos para la toma de las fotos correspondientes.
	S3	Si en el dispositivo móvil se manipula el patrón de ingreso de manera permanente.
	S4	Automáticamente el dispositivo tiene un máximo de 10 segundos para la toma de las fotos correspondientes.
<b>Postcondición</b>	El sistema almacenará en la base de datos las fotos tomadas a partir de los eventos generados.	

<b>Excepciones</b>	<b>Paso</b>	<b>Acción</b>
	E1	Si en el dispositivo móvil no se ha presionado el botón de apagado o manipulado el patrón de ingreso de manera permanente.
	E2	El dispositivo no tomará ninguna foto del usuario agresor.
<b>Rendimiento</b>	<b>Paso</b>	<b>Cota de tiempo</b>
	S1	10 segundos
	S3	10 segundos
<b>Frecuencia esperada</b>	15 /mes	
<b>Importancia</b>	Alta	
<b>Comentarios</b>	<comentarios adicionales>	

Tabla 20. Tomar foto

En la **tabla 21** se muestra la especificación del caso de uso rastreo de ubicación por GPS.

<b>RF- SMC-016</b>	<b>Rastreo de ubicación por GPS</b>	
<b>Actores</b>	Participante, contacto	
<b>Descripción</b>	Los contactos autorizados después de haber recibido la alerta del participante podrán hacer el seguimiento, visualizando en pantalla los datos de la ubicación actual, porcentaje de la batería, el mapa de ubicación de google según fecha y hora cada cierto tiempo.	
<b>Precondición</b>	El dispositivo del participante haya enviado la alerta a los contactos autorizados.	
<b>Secuencia</b>  <b>Normal</b>	<b>Paso</b>	<b>Acción</b>
	S1	El contacto autorizado haya recibido la alerta del participante (llamada telefónica, email, mensaje de texto) de forma automática.
	S2	El sistema muestra en pantalla los datos de la ubicación actual del participante
	S3	El sistema muestra en pantalla los datos del porcentaje de batería actual del participante
	S4	El sistema muestra en pantalla la ubicación actual del participante en el mapa de google.

	S5	El contacto autorizado podrá a través del sistema ir actualizando los datos del participante cada cierto tiempo, determinando el recorrido que está haciendo a partir del envío de la alerta.
	S5	El sistema almacena en la base de datos el registro del historial del rastreo por ubicación GPS del participante.
	S6	El sistema genera un archivo csv del rastreo por ubicación GPS, por cada participante
<b>Postcondición</b>	El sistema quedará activo para obtener la información generada del rastreo por ubicación GPS de cada participante.	
<b>Excepciones</b>	<b>Paso</b>	<b>Acción</b>
	E1	Si el contacto autorizado no recibe ninguna alerta, entonces el contacto no podrá realizar ningún rastreo por GPS de algún participante.
	E2	Mensaje: rastreos inválidos, verifique por favor
<b>Rendimiento</b>	<b>Paso</b>	<b>Cota de tiempo</b>
	S2	5 segundos
	S3	5 segundos
	S4	5 segundos
	S5	5 segundos
<b>Frecuencia esperada</b>	15 /mes	
<b>Importancia</b>	Alta	
<b>Comentarios</b>	<comentarios adicionales>	

Tabla 21. Rastreo de ubicación por GPS

En la **tabla 22** se muestra la especificación del caso de uso ver historial de alertas.

<b>RF- SMC-017</b>	Ver historial de alertas	
<b>Actores</b>	Participante	
<b>Descripción</b>	El usuario participante a través del sistema podrá visualizar el historial de las alertas enviadas.	
<b>Precondición</b>	Las alertas hayan sido enviadas a través del dispositivo móvil	
<b>Secuencia</b> <b>Normal</b>	<b>Paso</b>	<b>Acción</b>
	S1	El participante seleccione en pantalla historial de alertas y podrá visualizar todas alertas emitidas según fecha y hora.

	S2	El participante a través del sistema podrá generar un archivo csv a partir de las alertas emitas.
	S3	El sistema desplegará un mensaje en pantalla del historial de alertas generado.
<b>Postcondición</b>	El sistema quedará activo para dar inicio a la visualización del historial de alertas en el momento deseado.	
<b>Excepciones</b>	<b>Paso</b>	<b>Acción</b>
	E1	Si el historial de alertas ha sido eliminado, entonces el sistema mostrará un mensaje.
	E2	Mensaje: el historial de alertas no se puede visualizar por no tener registros guardados.
<b>Rendimiento</b>	<b>Paso</b>	<b>Cota de tiempo</b>
	S1	5 segundos
	S2	5 segundos
<b>Frecuencia esperada</b>	5 /día	
<b>Importancia</b>	Alta	
<b>Comentarios</b>	<comentarios adicionales>	

Tabla 22. Ver historial de alertas

En la **tabla 23** se muestra la especificación del caso de uso ver historial de rastreo por ubicación GPS.

<b>RF- SMC-018</b>	<b>Ver historial de rastreo por ubicación GPS</b>	
<b>Actores</b>	Contacto autorizado	
<b>Descripción</b>	El contacto autorizado a través del sistema podrá visualizar el historial del rastreo por ubicación GPS del participante.	
<b>Precondición</b>	El sistema haya enviado la alerta los contactos autorizados.	
<b>Secuencia</b> <b>Normal</b>	<b>Paso</b>	<b>Acción</b>
	S1	El contacto a través del enlace que le llega por email o mensaje SMS podrá cargar la pantalla de visualización de datos.
	S2	El contacto autorizado selecciona en pantalla el historial de rastreo por GPS y podrá visualizar los datos y mapa del rastreo por ubicación GPS del participante según fecha y hora.
<b>Postcondición</b>	El sistema quedará activo para dar inicio a la visualización del historial de rastreo por ubicación GPS en el momento deseado.	

<b>Excepciones</b>	<b>Paso</b>	<b>Acción</b>
	E1	Si el historial de rastreo por ubicación GPS ha sido eliminado, entonces el sistema mostrará un mensaje.
	E2	Mensaje: el historial de rastreo por ubicación no se puede visualizar por no tener registros guardados.
<b>Rendimiento</b>	<b>Paso</b>	<b>Cota de tiempo</b>
	S2	5 segundos
<b>Frecuencia esperada</b>	5 /día	
<b>Importancia</b>	Alta	
<b>Comentarios</b>	<comentarios adicionales>	

Tabla 23. Ver historial de rastreo por ubicación GPS

En la **tabla 24** se muestra la especificación del caso de uso emparejar dispositivos.

<b>RF- SMC-019</b>	Emparejar dispositivos	
<b>Actores</b>	Participante, dispositivo	
<b>Descripción</b>	Con el fin de conectar el dispositivo wearable o un dispositivo NFC a la plataforma se crea una interfaz donde aparecerá una lista de los dispositivos disponibles, mostrando el nombre del dispositivo y la MAC, se permitirá seleccionar el que se desee emparejar, mostrando un mensaje de conexión realizada con éxito.	
<b>Precondición</b>	El sistema mostrará una interfaz con los dispositivos disponibles, permitiendo al usuario seleccionar el que se desee emparejar.	
<b>Secuencia Normal</b>	<b>Paso</b>	<b>Acción</b>
	S1	El participante deberá visualizar en pantalla la lista de los dispositivos disponibles, mostrando el nombre y la MAC.
	S2	El sistema deberá permitir al participante seleccionar el dispositivo que desea emparejar
	S3	El sistema desplegará un mensaje en pantalla de conexión realizada con éxito.
	S4	Una vez conectado ya se podrá realizar la recepción de los datos del dispositivo y poder hacer las operaciones pertinentes.
<b>Postcondición</b>	El sistema quedará activo para dar inicio al emparejado de los dispositivos en el momento deseado.	

<b>Excepciones</b>	<b>Paso</b>	<b>Acción</b>
	E1	Si el dispositivo pierde la conexión se deberá mostrar un mensaje de alerta informando el problema.
	E2	Mensaje: el dispositivo no se encuentra conectado, revisar conexión.
<b>Rendimiento</b>	<b>Paso</b>	<b>Cota de tiempo</b>
	S1	5 segundos
	S2	5 segundos
<b>Frecuencia esperada</b>	5 /día	
<b>Importancia</b>	Alta	
<b>Comentarios</b>	<comentarios adicionales>	

Tabla 24. Emparejar dispositivos

En la **figura 22** se muestra el diagrama de casos de uso de gestión del administrador del sistema.

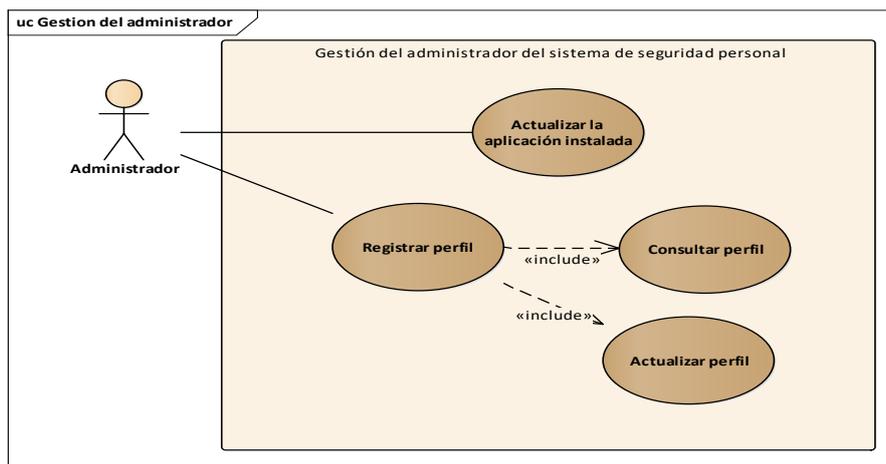


Figura 22. Gestión del administrador

En la **tabla 25** se muestra la especificación del caso de uso actualizar la aplicación instalada.

<b>RF- SMC-020</b>	Actualizar la aplicación instalada	
<b>Actores</b>	Administrador	
<b>Descripción</b>	Permite al administrador actualizar la aplicación instalada en base a mejoras.	
<b>Precondición</b>	El Administrador haya cargado los archivos fuentes del sistema.	
<b>Secuencia</b>	<b>Paso</b>	<b>Acción</b>

<b>Normal</b>	S1	El administrador realiza los cambios correspondientes a la mejora del sistema.
	S2	El administrador compila el sistema y guarda los cambios como una nueva versión.
	S3	El administrador a través del sistema comunica los cambios a los usuarios participantes, para su actualización correspondiente.
	S4	El sistema muestra un mensaje indicando que la aplicación ha sido actualizada.
<b>Postcondición</b>	El sistema quedará operativo con la nueva versión instalada del sistema.	
<b>Excepciones</b>	<b>Paso</b>	<b>Acción</b>
	E1	Si el participante no actualiza la nueva versión, la aplicación no hará uso de las nuevas mejoras.
<b>Rendimiento</b>	<b>Paso</b>	<b>Cota de tiempo</b>
	S3	5 segundos
	S4	2 segundos
<b>Frecuencia esperada</b>	1 /mes	
<b>Importancia</b>	Alta	
<b>Comentarios</b>	<comentarios adicionales>	

Tabla 25. Actualizar aplicación instalada

En la **tabla 26** se muestra la especificación del caso de uso registrar perfil.

<b>RF- SMC-021</b>	Registrar perfil	
<b>Actores</b>	Participante, contacto	
<b>Descripción</b>	Permite al participante registrar su nombre, apellido, número telefónico, fecha de nacimiento, país y género como parte de su perfil.	
<b>Precondición</b>	Se haya ingresado a la pantalla perfil del usuario con éxito.	
<b>Secuencia Normal</b>	<b>Paso</b>	<b>Acción</b>
	S1	Al momento del registro del usuario el sistema carga la pantalla perfil para el ingreso de datos
	S2	El participante ingresa sus nombres, apellidos, número telefónico, fecha de nacimiento y género presiona el botón ingresar.

	S3	El sistema almacena la información ingresada y actualiza la pantalla.
<b>Postcondición</b>	Operación realizada correspondiente al perfil del usuario	
<b>Excepciones</b>	<b>Paso</b>	<b>Acción</b>
	E1	Los datos del perfil sólo deben ingresarse al momento que se crea la cuenta del usuario participante.
<b>Rendimiento</b>	<b>Paso</b>	<b>Cota de tiempo</b>
	S3	2 segundos
<b>Frecuencia esperada</b>	5 /mes	
<b>Importancia</b>	Alta	
<b>Comentarios</b>	<comentarios adicionales>	

Tabla 26. Registrar perfil

En la **tabla 27** se muestra la especificación del caso de uso consultar perfil.

<b>RF- SMC-022</b>	Consultar perfil	
<b>Actores</b>	Participante, contacto	
<b>Descripción</b>	Permite al usuario participante consultar los datos de su perfil	
<b>Precondición</b>	Se haya ingresado a la pantalla configuración del sistema con éxito.	
<b>Secuencia Normal</b>	<b>Paso</b>	<b>Acción</b>
	S1	El participante selecciona la pantalla con los datos del perfil existente
	S2	El sistema carga una pantalla con los respectivos datos del perfil seleccionado.
<b>Postcondición</b>	Operación realizada correspondiente a perfiles del usuario	
<b>Excepciones</b>	<b>Paso</b>	<b>Acción</b>
	E2	El participante en la pantalla de consulta del detalle del perfil, sólo podrá consultar sus datos correspondientes.
<b>Rendimiento</b>	<b>Paso</b>	<b>Cota de tiempo</b>
	S2	2 segundos
<b>Frecuencia esperada</b>	5 /mes	
<b>Importancia</b>	Alta	
<b>Comentarios</b>	<comentarios adicionales>	

Tabla 27. Consultar perfil

En la **tabla 28** se muestra la especificación del caso de uso actualizar perfil

<b>RF- SMC-023</b>	Actualizar perfil	
<b>Actores</b>	Participante, contacto	
<b>Descripción</b>	Permite al participante actualizar su perfil registrado.	
<b>Precondición</b>	Se haya ingresado a la pantalla configuración del sistema con éxito y se visualice el perfil que se desee actualizar.	
<b>Secuencia Normal</b>	S1	El participante selecciona en pantalla la opción configuración
	S2	El sistema carga la pantalla con los datos del usuario
	S3	El participante modifica los datos necesarios correspondientes al perfil y presiona el botón grabar.
	S4	El sistema actualiza la información modificada y se refresca la pantalla
<b>Postcondición</b>	Operación realizada, correspondiente al perfil del usuario.	
<b>Excepciones</b>	<b>Paso</b>	<b>Acción</b>
	E1	Si el participante no ha seleccionado un registro del perfil para modificar, el sistema desplegará un mensaje.
	E2	El sistema no permitirá modificar ningún perfil.
	E3	Mensaje: seleccionar registro del perfil.
<b>Rendimiento</b>	<b>Paso</b>	<b>Cota de tiempo</b>
	S2	3 segundos
	S4	2 segundos
	S6	2 segundos
<b>Frecuencia esperada</b>	5 /mes	
<b>Importancia</b>	Alta	
<b>Comentarios</b>	<comentarios adicionales>	

*Tabla 28. Actualizar perfil*

Los requisitos no funcionales de la plataforma son los siguientes:

- ✓ Las respuestas de la aplicación deben ser en tiempo real con restricciones de tiempo mínimas para que el usuario tenga una monitorización de su actividad en cualquier momento.

- ✓ La aplicación móvil debe funcionar sin internet, cuando exista nuevamente conectividad se enviará los datos para actualizar el clúster si la aplicación está configurada de esta forma.
- ✓ La aplicación siempre debe estar en funcionamiento 24/7 al ser una supervisión continua.
- ✓ La aplicación debe funcionar con varios wearables para no restringirlo a un solo dispositivo.
- ✓ La aplicación se debe basar en la guía de diseño para aplicaciones móviles.

### **3.8 Objetivo 8: Preparar un piloto del sistema con voluntarios, para evaluar el grado de aceptación del sistema.**

#### **3.8.1 Análisis del sistema**

##### **3.8.1.1 Selección de los parámetros para medir la actividad física**

Para la selección de los parámetros de medición se partió de la tabla 4 la cual indica por cada medida su costo, practicidad, y utilización.

Se descartan el monitoreo de la temperatura, la transpiración y la conductancia en la piel, debido a que no son muy prácticos al momento de utilizarlos cotidianamente, por tanto, no se podrá hacer una motorización constante del usuario.

Los parámetros seleccionados para medir la actividad física en la plataforma serán los acelerómetros, la frecuencia cardíaca y el monitoreo de la respiración. Estos sensores se encuentran en varios dispositivos disponibles en el mercado como los wearable. Los dispositivos que cuentan con estos parámetros de medidas tienen un costo accesible, además de ser muy prácticos por lo tanto se pueden utilizar de uso cotidiano. A través de estos parámetros de medición se puede medir el movimiento en un espacio tridimensional, la frecuencia cardíaca y la frecuencia de la respiración, necesarios para el funcionamiento de la plataforma.

Además de estos parámetros de medición se utilizará un sensor que mida los niveles de oxígeno en la sangre, para obtener información de la fatiga y que el sistema sea capaz de enviar notificaciones cuando vea anomalías en este parámetro.

En consecuencia, los parámetros de medición serán:

- Acelerómetros.

- Frecuencia cardiaca (Pulsómetro).
- Frecuencia respiratoria (niveles de oxígeno en la sangre).
- SPO2 (niveles de oxígeno en la sangre).

### 3.8.2 Selección del wearables para la implementación

Para la selección del wearable de la implementación se realizó un estudio de diferentes tipos de dispositivos corporales o wearables. Como resultado del estudio se ha elaborado la tabla 5 en la que se encuentra la información de los wearables analizados, así como sus características y forma de conexión.

Se seleccionó como dispositivo wearable las pulseras de actividad, las cuales tienen un costo más accesible comparado con los demás dispositivos. Por otro lado, tiene una mayor autonomía de batería. Las pulseras cuentan con una mayor documentación para desarrollar aplicaciones con base a esta. Las pulseras seleccionadas fueron Fitbit Charge 4 y Mi Smart Band 6.

Mi Smart Band 6, se selecciona por ser la pulsera con mayor autonomía y con un costo muy inferior con respecto a Fitbit Charge 4 que tiene la misma autonomía. Cuenta con los parámetros de medición necesarios para que la aplicación funcione los cuales son: acelerómetros y pulsómetros. En la **figura 23** se muestra Mi Smart Band 6.



*Figura 23. Mi Smart Band 6*

### 3.8.3 Modelo conceptual del sistema

En la **figura 24** se observa el modelo conceptual representado por un diagrama de clases.



	<ul style="list-style-type: none"> <li>✓ ale_hora</li> <li>✓ ale_Id</li> <li>✓ ale_latitud</li> <li>✓ ale_longitud</li> <li>✓ ale_mac_bluetooth</li> </ul>	<p>atrás</p> <ul style="list-style-type: none"> <li>✓ uno a uno con la clase participante</li> </ul>
Audio	<ul style="list-style-type: none"> <li>✓ aud_cmdvoz</li> <li>✓ aud_Id</li> </ul>	<ul style="list-style-type: none"> <li>✓ uno a muchos con la clase participante</li> </ul>
Contacto	<ul style="list-style-type: none"> <li>✓ con_apellidos</li> <li>✓ con_direccion</li> <li>✓ con_dni</li> <li>✓ con_email</li> <li>✓ con_fecha</li> <li>✓ con_nombres</li> <li>✓ con_num_celular</li> <li>✓ con_sexo</li> </ul>	<ul style="list-style-type: none"> <li>✓ cero a muchos con la clase rastreo GPS</li> <li>✓ uno a uno con la clase perfil</li> <li>✓ uno a muchos con la clase alerta</li> <li>✓ uno a uno con la clase participante</li> <li>✓ hereda de la clase usuario</li> </ul>
Cuenta atrás	<ul style="list-style-type: none"> <li>✓ cat_estado</li> <li>✓ cat_Id</li> <li>✓ cat_tiempo</li> </ul>	<ul style="list-style-type: none"> <li>✓ uno a muchos con la clase alerta</li> <li>✓ uno a uno con la clase participante</li> <li>✓ uno a uno con la clase estado</li> </ul>
Dispositivo	<ul style="list-style-type: none"> <li>✓ dip_descripcion</li> <li>✓ dip_Id</li> <li>✓ dip_imei</li> <li>✓ dip_marca</li> <li>✓ dip_modelo</li> <li>✓ dip_serie</li> </ul>	<ul style="list-style-type: none"> <li>✓ cero a muchos con la clase foto</li> <li>✓ uno a muchos con la clase info_entorno</li> <li>✓ uno a uno con la clase participante</li> </ul>
Foto	<ul style="list-style-type: none"> <li>✓ fot_codigo</li> <li>✓ fot_descripcion</li> </ul>	<ul style="list-style-type: none"> <li>✓ uno a uno con la clase dispositivo</li> </ul>
Info_entorno	<ul style="list-style-type: none"> <li>✓ ent_audio</li> <li>✓ ent_direc_bluetooth</li> <li>✓ ent_fotos</li> <li>✓ ent_imei</li> <li>✓ ent_intens_senal</li> <li>✓ ent_mac_wifi</li> <li>✓ ent_serie</li> </ul>	<ul style="list-style-type: none"> <li>✓ uno a uno con la clase dispositivo</li> </ul>
Parámetro biológico	<ul style="list-style-type: none"> <li>✓ pbi_descripcion</li> <li>✓ pbi_nombre</li> <li>✓ pbi_valor_final</li> <li>✓ pbi_valor_inicial</li> </ul>	<ul style="list-style-type: none"> <li>✓ uno a muchos con la clase participante</li> </ul>
Parámetro de audio	<ul style="list-style-type: none"> <li>✓ pau_cmdvoz</li> <li>✓ pau_descripcion</li> <li>✓ pau_Id</li> </ul>	<ul style="list-style-type: none"> <li>✓ uno a muchos con la clase participante</li> </ul>
Participante	<ul style="list-style-type: none"> <li>✓ par_apellidos</li> <li>✓ par_direccion</li> </ul>	<ul style="list-style-type: none"> <li>✓ hereda de la clase usuario</li> <li>✓ uno a uno con la clase perfil</li> </ul>

	<ul style="list-style-type: none"> <li>✓ par_dni</li> <li>✓ par_email</li> <li>✓ par_fechnac</li> <li>✓ par_nombres</li> <li>✓ par_num_celular</li> <li>✓ par_sexo</li> </ul>	<ul style="list-style-type: none"> <li>✓ uno a muchos con la clase signos vitales</li> <li>✓ uno a muchos con la clase contacto</li> <li>✓ uno a muchos con la clase dispositivo</li> <li>✓ cero a muchos con la clase alerta</li> <li>✓ cero a muchos con la clase supervisión</li> <li>✓ uno a muchos con la clase parámetros biológicos</li> <li>✓ cero a muchos con la clase cuenta atrás</li> <li>✓ uno a muchos con la clase parámetro de audio</li> </ul>
Perfil	<ul style="list-style-type: none"> <li>✓ per_descripcion</li> <li>✓ per_nombre</li> </ul>	<ul style="list-style-type: none"> <li>✓ uno a muchos con la clase administrador</li> <li>✓ cero a muchos con la clase contacto</li> <li>✓ cero a muchos con la clase participante</li> </ul>
Rastreo GPS	<ul style="list-style-type: none"> <li>✓ ras_fecha_hora</li> <li>✓ ras_map_ubicacion</li> <li>✓ ras_porc_bateria</li> <li>✓ ras_ubic_actual</li> </ul>	<ul style="list-style-type: none"> <li>✓ uno a muchos con la clase contacto</li> </ul>
Signos vitales	<ul style="list-style-type: none"> <li>✓ siv_nombre</li> <li>✓ siv_valor_inicial</li> <li>✓ siv_valor_final</li> </ul>	<ul style="list-style-type: none"> <li>✓ uno a uno con la clase participante</li> </ul>
Supervisión	<ul style="list-style-type: none"> <li>✓ sup_nombre</li> <li>✓ sup_estado</li> </ul>	<ul style="list-style-type: none"> <li>✓ uno a uno con la clase participante</li> </ul>
Usuario	<ul style="list-style-type: none"> <li>✓ sup_nombre</li> <li>✓ usu_password</li> </ul>	<ul style="list-style-type: none"> <li>✓ superclase de las clases participante, contacto y administrador</li> </ul>

Tabla 29. Descripción de las clases de la plataforma

### 3.8.4 Diseño de la plataforma

#### 3.8.4.1 Arquitectura principal del sistema

En la **figura 25** se observa la arquitectura principal del sistema, mostrando los respectivos niveles y componentes.

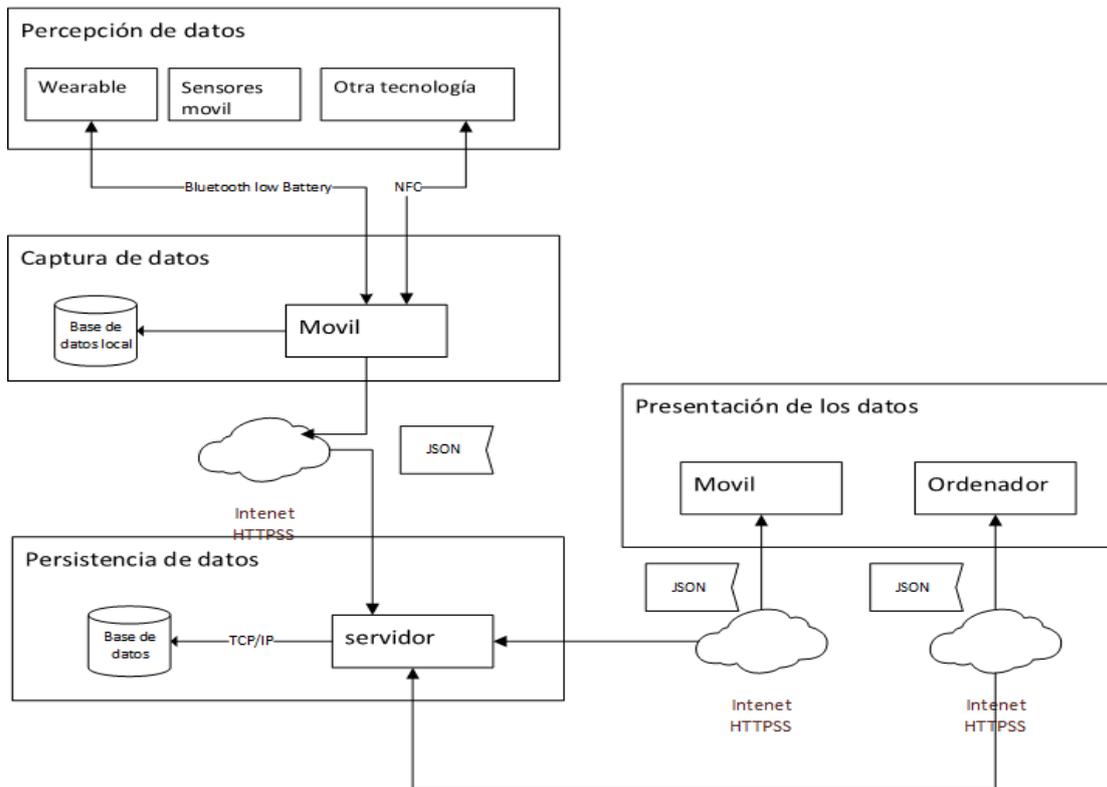


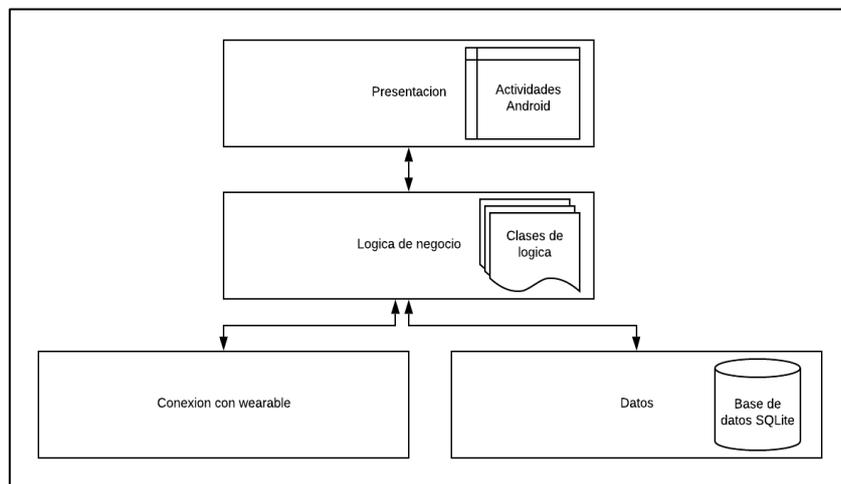
Figura 25. Arquitectura principal de la plataforma

La arquitectura principal de la plataforma está dividida en cuatro niveles:

- ✓ **Percepción de datos:** El primer nivel es el de percepción de datos donde se encuentra un dispositivo vestible wearable, los sensores del dispositivo móvil y otra tecnología como NFC. Con este nivel se pretende recibir los datos fisiológicos del usuario a través de los sensores incorporados a este y el disparo de la alerta a través de botón de pánico con tecnología NFC.
- ✓ **Captura de datos:** Con este nivel se pretende capturar los datos para ser enviados a un servidor externo además de almacenarlos localmente. En este nivel se encuentra un dispositivo móvil el cual se conecta al primer nivel a través del protocolo Bluetooth Low Battery. Luego de esta conexión se utilizará una arquitectura basada en eventos donde se recibirán los cambios en los servicios Gatt, como lecturas, escrituras, estados de conexión, cambios en el descriptor. Todos estos eventos son enviados a una cola donde se van publicando para que la aplicación se suscriba al que le interese. Luego estos datos son enviados al siguiente nivel y almacenados internamente en una base de datos local.

- ✓ **Persistencia de datos:** La persistencia de los datos se almacenan en un servidor externo, para el envío de la información se hace a través de internet mediante el protocolo HTTPS mandando como cuerpo un objeto JSON, ya que se utilizará el estilo arquitectónico REST, este servidor tendrá una conexión a una base de datos a través de la TCP/IP. En este nivel de persistencia además de almacenar la información, se hará los procesamientos correspondientes a esta.
- ✓ **Presentación de datos:** La presentación de los datos se hace a través de los navegadores de un ordenador o a través de un móvil. Para recibir la información se hace una petición al servicio a través del protocolo HTTPS. Con este nivel los datos almacenados en el nivel de persistencia de datos podrán ser visualizados.

En la **figura 26** se observa la arquitectura por capas de la aplicación móvil anteriormente mencionada.



*Figura 26. Arquitectura por capas de la aplicación móvil*

La aplicación móvil tendrá una arquitectura de cuatro capas, una primera capa de datos la cual se encargará de la manipulación de los datos. Una segunda capa que maneja los eventos de conexión con la pulsera y está representada en la **figura 27**. Una tercera capa de lógica de negocio donde se realizarán los cálculos y procesamientos pertinentes con los datos. Por último, se tendrá la capa de presentación donde será visualizada toda la información de la aplicación.

### 3.8.5 Diseño de interfaces gráficas de la plataforma

#### Principios de diseño

En la medida de lo posible se diseñaron interfaces que fueran amigables para el usuario con respecto a colores y estilos. Además, se intentó realizar diseños donde el número de clics fuera reducido lo mayor posible. También que las interfaces fueran intuitivas, para que el usuario pueda utilizar la plataforma y navegar en ella sin problemas, ni tener que utilizar ningún manual.

A continuación, se presenta los prototipos de las interfaces graficas de la aplicación móvil.

### **Registrarse e iniciar Sesión**

Después de instalada la aplicación se cargará una interfaz con dos botones, con el primero se creará el usuario si todavía no tiene ninguno registrado y con el segundo se iniciará sesión.

En la **figura 27** se observa el prototipo de la interfaz iniciar sesión.



*Figura 27. prototipo de la interfaz Iniciar sesión*

### **Crear cuenta**

En la **figura 28** se observa el prototipo crear cuenta.



*Figura 28. Prototipo crear cuenta*

En la **figura 29** se observa el prototipo crear cuenta registrando teléfono.



Figura 29. Prototipo crear cuenta registrando teléfono

En la **figura 30** se observa el prototipo crear cuenta validando teléfono.



Figura 30. Prototipo crear cuenta validando teléfono

## Configurar lista de contactos

En la **figura 31** se observa el prototipo configurar lista de contactos.



Figura 31. Prototipo configurar lista de contactos

En la **figura 32** se observa el prototipo importar contactos existentes



*Figura 32. Prototipo importar contactos existentes*

En la **figura 33** se observa el prototipo registrar contacto nuevo.



*Figura 33. Prototipo registrar contacto nuevo*

En la **figura 34** se observa el prototipo seleccionar contacto existente a editar.



*Figura 34. Prototipo para seleccionar contacto existente a editar*

En la **figura 35** se observa el prototipo editar contacto existente.



Figura 35. Prototipo para editar contacto existente

### Configurar comandos de reconocimiento de voz

En la **figura 36** se observa el prototipo configurar los comandos de voz.



Figura 36. Prototipo para configurar los comandos de voz

### Programar cuenta atrás

En la **figura 37** se observa el prototipo programar cuenta atrás



Figura 37. Prototipo para programar cuenta atrás.

## Programar supervisión de la actividad

En la **figura 38** se observa el prototipo programar actividad



Figura 38. Prototipo para programar supervisión de actividad

En la **figura 39** se observa el prototipo registrar nueva actividad



Figura 39. Prototipo para registrar nueva actividad

En la **figura 40** se observa el prototipo para iniciar supervisión de actividad



Figura 40. Prototipo para iniciar supervisión de actividad

En la **figura 41** se observa el prototipo para rastrear ubicación por GPS

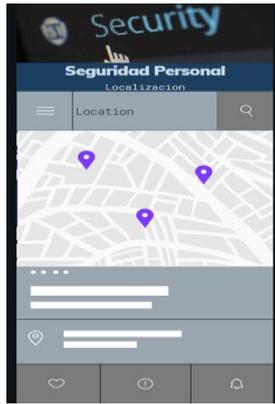


Figura 41. Prototipo para rastrear ubicación GPS de la actividad

En la **figura 42** se observa el prototipo para finalizar supervisión de actividad



Figura 42. Prototipo para finalizar supervisión de actividad

En la **figura 43** se observa el prototipo para activar el botón de pánico



Figura 43. Prototipo para activar el botón de pánico

En la **figura 44** se observa el prototipo para enviar alerta de pánico



Figura 44. Prototipo para enviar alerta de pánico

En la **figura 45** se observa el prototipo para cancelar alerta de pánico



Figura 45. Prototipo para cancelar alerta de pánico

## Menú Principal

En la **figura 46** se observa el prototipo del menú principal de la aplicación.



Figura 46. Prototipo para mostrar el menú principal

## Registrar perfil

En la **figura 47** se observa el prototipo registrar perfil.

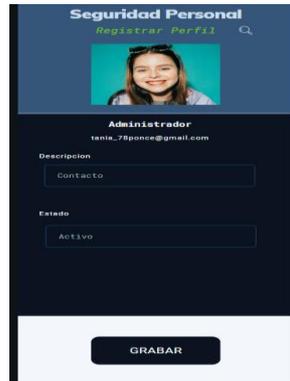


Figura 47. Prototipo de registrar perfil

## Emparejar dispositivos

En la **figura 48** se observa el prototipo emparejar dispositivos.



Figura 48. Prototipo de emparejar dispositivos

## Historial de alertas

En la **figura 49** se observa el prototipo historial de alertas.

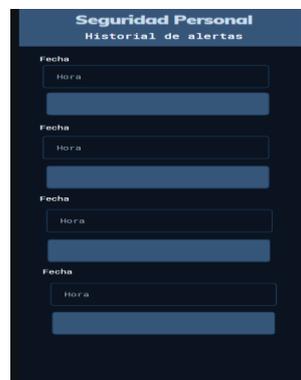


Figura 49. Prototipo de historial de alertas

## Configuraciones del sistema

En la **figura 50** se observa el prototipo ajustes avanzados.



*Figura 50. Prototipo de ajustes avanzados*

En la **figura 51** se observa el prototipo información adicional.



*Figura 51. Información adicional*

### 3.8.6 Modelo relacional de la base de datos

A partir del modelo conceptual del sistema se han identificado los conceptos, sus propiedades y la relación entre los distintos conceptos. Esto nos facilita determinar la información que tiene que almacenarse persistentemente en el sistema mediante un diagrama entidad-relación.

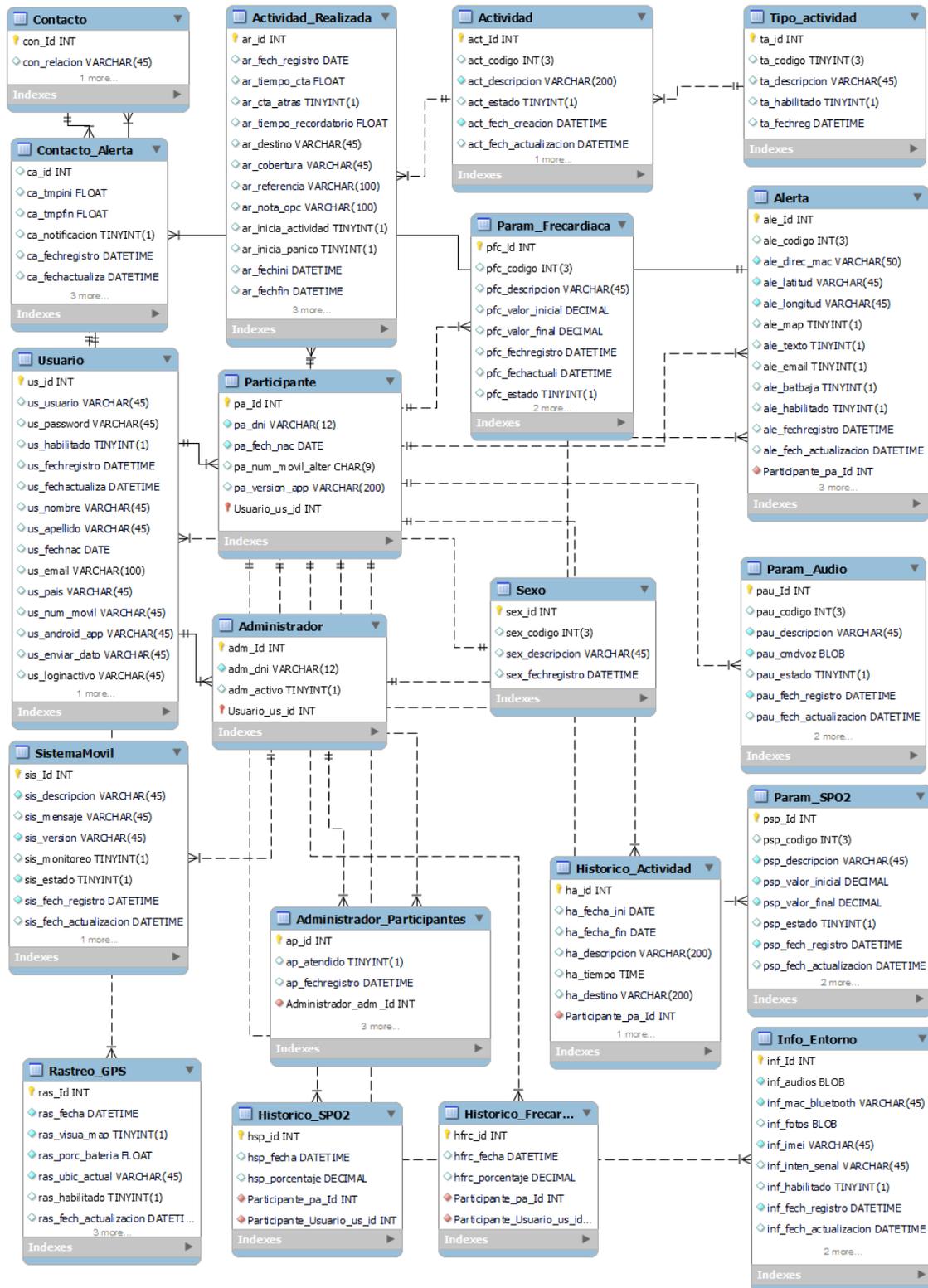


Figura 52. Modelo relacional de Base de Datos

En la figura 52 se puede observar el modelo relacional diseñado para la plataforma, se parte de la tabla participante la cual tiene los siguientes atributos: identificador, usuario,

password, habilitado, nombre, apellido, DNI, país, email, fecha de nacimiento, sexo, número de móvil, estado, versión app, fecha registro y fecha actualización.

Existen once tablas relacionadas a la tabla Participante las cuales son: Actividad, Param\_Audio, Param\_Estres, Param\_SPO2, Rastreo\_GPS, Perfil, Contacto, Alerta, Info\_Entorno, Historico\_SPO2, Historico\_Frecardiaca. Esto es con el fin de separar la información que está directamente relacionada con la tabla Participante. La llave primaria de cada tabla corresponde a la llave primaria de la tabla Participante.

La tabla participante, se registrarán todos los usuarios que quieran utilizar la aplicación para fines de monitorizar y controlar su seguridad personal.

La tabla Contacto, se almacena la información de los contactos que recibirán los mensajes de alerta, cuando el participante dispare la alerta.

La tabla Param\_Audio, registra los parámetros de audio configurados por el participante, que hará que se dispare la alerta en caso se emita un sonido ya pre configurado.

La tabla Tipo\_actividad, se registra los tipos de actividades que van a ser supervisadas por uno o más contactos.

La tabla Actividad, se registra la actividad que va a ser supervisada por uno o más contactos a solicitud del participante.

La tabla Perfil, registra el perfil al que pertenece un usuario.

La tabla Alerta, se almacena la información que el participante y el sistema envía a sus Contactos, para su posterior rastreo.

Las tablas Param\_Audio, Param\_FreCardiaca y Param\_SPO2, registran los parámetros biológicos normales registrados por el participante, que hará que se dispare la alerta en caso los parámetros reales emitidos por el dispositivo wearables del Participante estén fuera de dichos parámetros

La tabla Administrador, almacena la información del Usuario Administrador del sistema móvil y del participante.

La tabla SistemaMovil, registra cada una de las actualizaciones, versiones y estado de la aplicación móvil.

La tabla Info\_Entorno, registra la información del entorno del participante, a través del dispositivo móvil, después de haberse disparado la alerta.

Por otro lado, la tabla Contacto tiene relación de uno a muchos con la tabla Rastreo\_GPS, que almacena la información del rastreo que hacen los contactos a los participantes, una vez recibido el mensaje de alerta.

Todas las tablas de la plataforma cuentan con tres atributos comunes como lo son fecha registro, fecha de actualización y habilitado, con el fin de no eliminar registros si no actualizarlos.

### 3.8.7 Implementación

#### 3.8.7.1 Implementación a nivel de persistencia de datos

El nivel de persistencia se ha implementado con dos componentes, una base de datos hecha en MySQL y un servicio web REST implementado en java con librerías de Jersey contenido en un contenedor de Servlet en un servidor web basado en Tomcat 10.0.

En la **figura 53**, se observa el diagrama de despliegue del nivel de persistencia de datos.



Figura 53. Despliegue del nivel de persistencia de datos

A continuación, se detalla la implementación de los dos componentes del nivel de persistencia de datos:

#### 3.8.7.1 Base de datos en MySQL

Para la creación de la base de datos se utilizó el motor de base de datos MySQL con el IDE de desarrollo Workbench en su versión 8.0 CE <https://www.mysql.com/products/workbench/>. Workbench crea un script de la base de datos a partir de un modelo relacional, este script crea tanto el esquema como las tablas con sus restricciones y relaciones.

Luego de la generación y ejecución del esquema de la base de datos se procedió a poblar las siguientes tablas con los datos correspondientes:

- **Sexo:** Masculino, Femenino.
- **Param\_audio:** Colaborar, Problema.
- **Param\_SPO2:** Grave 90% a menos, Preocupante 91% a 94%, Normal 95% a 100%.
- **Param\_frecardiaca:** Normal 60 a 100, Taquicardia más 100, Bradicardia menos de 60 latidos x minuto.
- **Param\_estres:** Reposo 0 a 25, Bajo 26 a 50, Medio 51 a 75, Alto 76 a 100.
- **Tipo\_actividad:** Visitar lugares, viaje, trabajando solo, otros.

La base de datos cumple con todas las especificaciones del sistema, se encuentra normalizada la mayor parte posible. Además, se crearon índices para mejorar las consultas en las tablas de actividades realizadas e histórico de actividad física. Las cuáles serán las que tendrán el mayor número de registros.

Con respecto a las conexiones a la base de datos se hizo un nuevo usuario diferente a root para la conexión desde el servicio rest. Con el fin de limitar este usuario a funciones de DML (Lenguaje de manipulación de datos). Y evitar que con este se puedan crear, actualizar o eliminar las tablas.

### 3.8.7.2 Servicio Web REST con Jersey en Java

Para la creación del servicio Restful se utilizó como lenguaje de programación Java y las librerías Jersey para la elaboración de las peticiones http. Jersey simplificó el proceso de desarrollo del servicio web, y así optimizar los tiempos de desarrollo.

El servicio web se encarga de recoger la información que captura el móvil del dispositivo wearable, y si tiene permiso del usuario, lo almacena en la base de datos que se encuentra en la nube.

El servicio cuenta con seis paquetes para la separación de cada capa de la arquitectura.

En la **figura 54**, se observa el diagrama de paquetes del servicio Rest

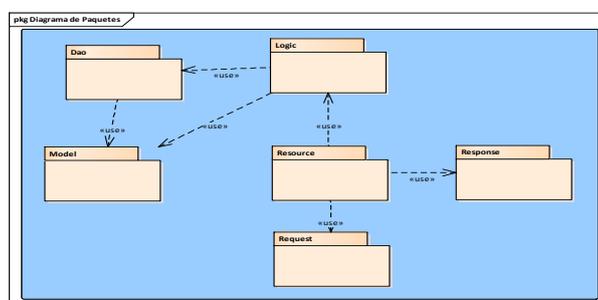


Figura 54. Diagrama de paquetes del servicio Rest

A continuación, se describe cada uno de los paquetes del servicio Rest:

### 3.8.7.3 Paquete model

En este paquete se definieron todas las clases que hacen referencia a las tablas de la base de datos, con el fin de hacer un mapeo de los datos de la tabla a un objeto en memoria con el cual se pueda trabajar.

En la **figura 55**, se observa las clases del paquete model

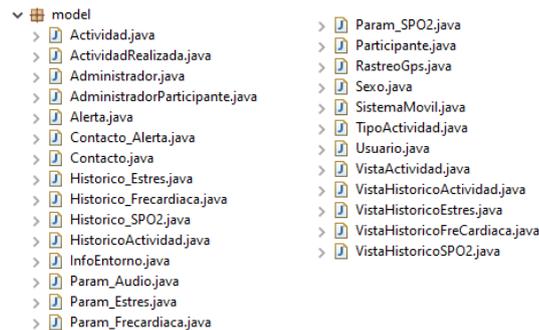


Figura 55. Clases del paquete model.

### 3.8.7.4 Paquete DAO (Data Acces object).

En este paquete se definieron las clases en las cuales se realizarán los procesos de inserción, actualizado, eliminación y consulta de las tablas. Para esto se necesitó un jar para la conexión con MySQL. El jar utilizado fue mysql-connector-java-5.1.3.6.

Se creó una clase para manipular la conexión con MySQL llamada ConexionBD la cual obtiene el driver de conexión jdbc y crea una nueva conexión a partir de unas credenciales recibidas por parámetro. Esta clase permite recibir un comando de manipulación de datos para ser ejecutado en la base de datos.

Todas las clases pertenecientes a este paquete heredan de la clase abstracta Dao. Dao cuenta con métodos abstractos para la inserción, actualización y consulta de una entidad específica. Cada clase modelo tendrá su respectiva clase Dao.

En la **figura 56** se observan las clases del paquete dao.

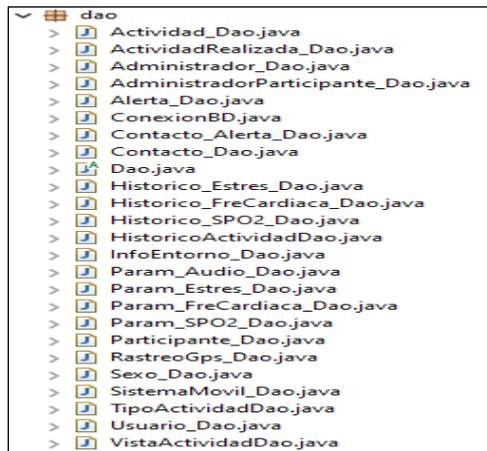


Figura 56. Clases del paquete dao.

### 3.8.7.5 Paquete logic.

En este paquete se definieron las clases en las cuales se realiza la lógica del sistema, todas estas clases heredan de la clase Logic. La clase Logic recibe el contexto de la aplicación, para obtener las credenciales de conexión. Con las credenciales de conexión se crea una instancia de la clase ConexionBD la cual es pasada a todos los Daos que se encuentren llamados. En el archivo de configuración se encuentran las credenciales. En la **figura 57** se observa el archivo de configuración del proyecto del servicio rest. En él se pueden observar los parámetros de conexión a la base de datos, como nombre de la base de datos, contraseña, usuario y url de conexión.

```

<context-param>
  <description>Nombre de base de datos</description>
  <param-name>dbName</param-name>
  <param-value>dbName</param-value>
</context-param>

<context-param>
  <description>Password base de datos</description>
  <param-name>password</param-name>
  <param-value>password</param-value>
</context-param>

<context-param>
  <description>Usuario base de datos</description>
  <param-name>userName</param-name>
  <param-value>userName</param-value>
</context-param>

<context-param>
  <description>Url base de datos</description>
  <param-name>url</param-name>
  <param-value>url</param-value>
</context-param>

```

Figura 57. Parámetros de configuración de la base de datos en web.xml.

En la **figura 58** se observa las clases del paquete logic.

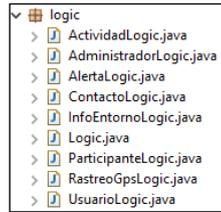


Figura 58. Clases del paquete logic.

### 3.8.7.6 Paquete request.

En este paquete se definieron las clases para las solicitudes que se van hacer al servicio, todas estas clases heredan de la clase Solicitud. La cual cuenta con una instancia de la clase Credencial la que maneja el userName y la contraseña del usuario que está haciendo la solicitud. En la **figura 59** se presentan las clases del paquete request encardado de las solicitudes del servicio.

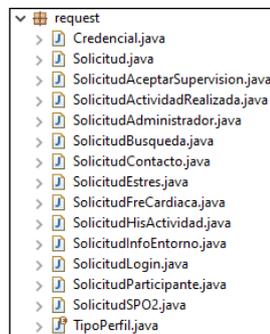


Figura 59. Clases del paquete request.

### 3.8.7.6 Paquete response.

En este paquete se definieron las clases para las respuestas del servicio. Todas las clases tienen los atributos públicos para que al momento de hacer la serialización a Json no se presenten problemas de accesibilidad. En todos los métodos del servicio siempre se va a retornar un objeto de la clase Repuesta, el cual tendrá un mensaje, un tipo de respuesta: error o éxito y un objeto con la información de la respuesta, por ejemplo, la información de un participante.

En la **figura 60** se presentan las clases del paquete response, el cual es el encargado de las respuestas del servicio.

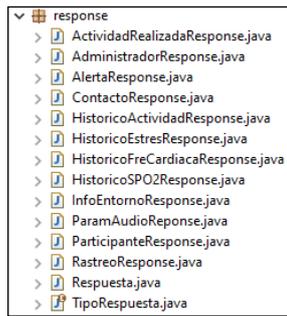


Figura 60. Clases del paquete response.

### 3.8.7.7 Paquete resource.

En este paquete se definieron las clases para la capa de presentación del servicio, en estas clases serán utilizadas las librerías correspondientes a jersey para la creación del servicio. En la definición de los métodos hay que colocar las etiquetas del path, media-type y tipo de verbo http: post, delete, get, put. Por otro lado, hay que colocar una etiqueta de la ruta principal. En la **figura 61** se muestran las librerías necesarias para el funcionamiento de Jersey.

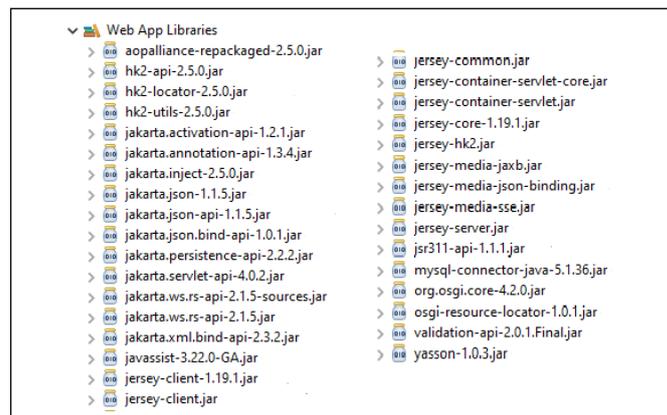


Figura 61. jar para utilizar Jersey.

Por otro lado, se debe configurar el archivo xml para que sepa cual paquete utilizar para el servicio, en el caso de este proyecto será el paquete resource.

En la **figura 62** se muestra la configuración del archivo xml, hay que definir el servlet de Jersey (ServletContaint). Además, se define el paquete donde están las clases del servicio (resource). Se establece el tipo respuesta que será JSON y la ruta de los servicios /rest/\*.

```

<display-name>MyPersonalSafetyRest</display-name>
<servlet>
<servlet-name>Servicio REST de Jersey</servlet-name>
<servlet-class>org.glassfish.jersey.servlet.ServletContainer</servlet-class>

<init-param>
<param-name>jersey.config.server.provider.packages</param-name>
<param-value>resource</param-value>
</init-param>

<init-param>
<param-name>com.sun.jersey.api.json.POJOMappingFeature</param-name>
<param-value>true</param-value>
</init-param>

<load-on-startup>1</load-on-startup>
</servlet>
<servlet-mapping>
<servlet-name>Servicio REST de Jersey</servlet-name>
<url-pattern>/rest/*</url-pattern>
</servlet-mapping>

```

Figura 62. configuración de Jersey en el web.xml.

En la **figura 63** se observan las clases del paquete resource.

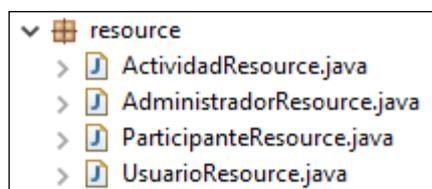


Figura 63. Clases del paquete resource.

### 3.8.8 Implementación a nivel de captura de datos

La implementación del nivel de captura de datos se realizó en un sistema operativo Android. Creando una aplicación móvil, la cual utiliza las librerías de conexión a una base de datos SQLite.

En la **figura 64** se observa el diagrama de despliegue del nivel de captura de datos.

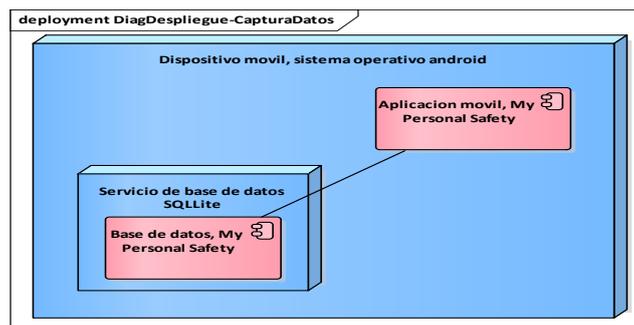


Figura 64. diagrama de despliegue del nivel de captura de datos.

A continuación, se detalla la implementación de los dos componentes del nivel de captura de datos:

#### 3.8.8.1 Implementación de la Base de datos en Móvil con SQLite

La información del participante se necesitó almacenar en el mismo dispositivo móvil debido a que la plataforma puede funcionar sin la necesidad de estar conectado a internet y no consumir el servicio rest.

Para la creación de la base datos se debe extender en Android una clase llamada SQLiteOpenHelper la cual cuenta con un constructor, donde se define un contexto donde estará la base de datos, un nombre y una versión para esta.

En la implantación se creó la clase ConexionBD que hereda de la super clase SQLiteOpenHelper. Para esto se debe crear el constructor anteriormente mencionado. En la **figura 65** se observa el constructor de la clase que hereda de SQLiteOpenHelper. Recibe como parámetros de entrada el contexto de la aplicación, el nombre de la base de datos, un cursor y la nueva versión de la base de datos. Todos estos parámetros son enviados a la super clase.

```
public ConexionBD(Context context, String name, SQLiteDatabase.CursorFactory factory, int version) {  
    super(context, name, factory, version);  
    this.setContext(context);  
    this.setName(name);  
    this.setFactory(factory);  
    this.setVersion(version);  
}
```

*Figura 65. constructor para generar la conexión con SQLite.*

Para la creación y actualización de las tablas en la base de datos se deben implementar dos métodos que son heredados de la clase padre, los cuales son: onCreate(SQLiteDatabase db) y onUpgrade(SQLiteDatabase db, int versionAntigua, int versionNueva). En el método onCreate se hace la creación de las tablas del sistema, para esto se crearon variables estáticas de texto donde se almacena la estructura de la tabla. En la **figura 66** se muestra el método onCreate el cual recibe como parámetro un objeto SQLiteDatabase, el cual representa la base de datos en donde se van a crear las tablas. Para ejecutar los DDL (Lenguaje de definición de datos) se utiliza el método execSQL el cual ejecuta el comando de la variable tipo cadena que tiene la estructura de la tabla.

```

@Override
public void onCreate(SQLiteDatabase db) {
    db.execSQL(Actividad_Dao.CREAR_TABLA);
    db.execSQL(ActividadRelizada_Dao.CREAR_TABLA);
    db.execSQL(Administrador_Dao.CREAR_TABLA);
    db.execSQL(AdministradorParticipante_Dao.CREAR_TABLA);
    db.execSQL(Alerta_Dao.CREAR_TABLA);
    db.execSQL(Contacto_Alerta_Dao.CREAR_TABLA);
    db.execSQL(Contacto_Dao.CREAR_TABLA);
    db.execSQL(Dispositivo_Dao.CREAR_TABLA);
    db.execSQL(Historico_Estres_Dao.CREAR_TABLA);
    db.execSQL(Historico_FreCardiaca_Dao.CREAR_TABLA);
    db.execSQL(Historico_SP02_Dao.CREAR_TABLA);
    db.execSQL(HistoricoActividadDao.CREAR_TABLA);
    db.execSQL(InfoEntorno_Dao.CREAR_TABLA);
    db.execSQL(Param_Audio_Dao.CREAR_TABLA);
    db.execSQL(Param_Estres_Dao.CREAR_TABLA);
    db.execSQL(Param_FreCardiaca_Dao.CREAR_TABLA);
    db.execSQL(Param_SP02_Dao.CREAR_TABLA);
    db.execSQL(Participante_Dao.CREAR_TABLA);
    db.execSQL(RastreoGps_Dao.CREAR_TABLA);
    db.execSQL(Sexo_Dao.CREAR_TABLA);
    db.execSQL(TipoActividadDao.CREAR_TABLA);
    db.execSQL(Usuario_Dao.CREAR_TABLA); }

```

Figura 66. método para crear las tablas en SQLite.

En el método onUpgrade se actualizan las estructuras de las tablas por si hubo un cambio. Primero se eliminan las tablas creadas y luego se llama al método onCreate para volver a crearlas con la nueva estructura. Para que este método puede ser llamado se debe pasar una nueva versión de la base de datos. En la variable versionNueva.

En la **figura 67** se observa como a través del objeto SQLiteDatabase es eliminada la tabla, además del llamado del onCreate al final del método.

```

@Override
public void onUpgrade(SQLiteDatabase db, int versionAntigua, int versionNueva) {
    db.execSQL("DROP TABLE IF EXISTS "+Actividad_Dao.TABLA);
    db.execSQL("DROP TABLE IF EXISTS "+ActividadRelizada_Dao.TABLA);
    db.execSQL("DROP TABLE IF EXISTS "+Administrador_Dao.TABLA);
    db.execSQL("DROP TABLE IF EXISTS "+AdministradorParticipante_Dao.TABLA);
    db.execSQL("DROP TABLE IF EXISTS "+Alerta_Dao.TABLA);
    db.execSQL("DROP TABLE IF EXISTS "+Contacto_Alerta_Dao.TABLA);
    db.execSQL("DROP TABLE IF EXISTS "+Contacto_Dao.TABLA);
    db.execSQL("DROP TABLE IF EXISTS "+Dispositivo_Dao.TABLA);
    db.execSQL("DROP TABLE IF EXISTS "+Historico_Estres_Dao.TABLA);
    db.execSQL("DROP TABLE IF EXISTS "+Historico_FreCardiaca_Dao.TABLA);
    db.execSQL("DROP TABLE IF EXISTS "+Historico_SP02_Dao.TABLA);
    db.execSQL("DROP TABLE IF EXISTS "+HistoricoActividadDao.TABLA);
    db.execSQL("DROP TABLE IF EXISTS "+InfoEntorno_Dao.TABLA);
    db.execSQL("DROP TABLE IF EXISTS "+Param_Audio_Dao.TABLA);
    db.execSQL("DROP TABLE IF EXISTS "+Param_Estres_Dao.TABLA);
    db.execSQL("DROP TABLE IF EXISTS "+Param_FreCardiaca_Dao.TABLA);
    db.execSQL("DROP TABLE IF EXISTS "+Param_SP02_Dao.TABLA);
    db.execSQL("DROP TABLE IF EXISTS "+Participante_Dao.TABLA);
    db.execSQL("DROP TABLE IF EXISTS "+RastreoGps_Dao.TABLA);
    db.execSQL("DROP TABLE IF EXISTS "+Sexo_Dao.TABLA);
    db.execSQL("DROP TABLE IF EXISTS "+TipoActividadDao.TABLA);
    db.execSQL("DROP TABLE IF EXISTS "+ Usuario_Dao.TABLA);
    onCreate(db); }

```

Figura 67. método para actualizar las estructuras de las tablas.

Las variables estáticas se crearon en cada acceso a dato, en la **figura 68** se muestra un ejemplo de una variable para la creación de una tabla. El nombre de la tabla se encuentra una variable llamada TABLA, además se cuentan los campos de la tabla separadas en cada

variable para que sea más fácil la inserción y actualización de registros, por último, se tiene la variable `CREAR_TABLA` donde se crea la estructura de dicha tabla.

```
public static final String TABLA="Participante";
public static final String CAMPO_ID="pa_id";
public static final String CAMPO_DNI="pa_dni";
public static final String CAMPO_FECHNAC="pa_fech_nac";
public static final String CAMPO_APPANDROID="pa_version_app";

public static final String CREAR_TABLA = " CREATE TABLE " + TABLA + " (" +CAMPO_ID+" INTEGER PRIMARY KEY, "
    CAMPO_DNI+" TEXT,"+CAMPO_FECHNAC+" TEXT,"+CAMPO_APPANDROID+"TEXT)";
```

Figura 68. variables para la creación de una tabla en *SQLite*.

Para insertar los registros de configuración, estados o tipos se registran la primera vez que se crean las tablas. Se hace una validación previa, para saber si existen o no los registro. Las tablas donde se insertan datos son:

- **Sexo:** Masculino, Femenino.
- **Param\_audio:** Colaborar, Problema.
- **Param\_SPO2:** Grave 90% a menos, Preocupante 91% a 94%, Normal 95% a 100%.
- **Param\_frecardiaca:** Normal 60 a 100, Taquicardia más 100, Bradicardia menos de 60 latidos x minuto.
- **Param\_estres:** Reposo 0 a 25, Bajo 26 a 50, Medio 51 a 75, Alto 76 a 100.
- **Tipo\_actividad:** Visitar sitio, viaje, trabajando solo, otros.

En la **figura 69** se observa cuáles son los registros iniciales para que la plataforma funcione correctamente. Cada método tendrá los registros de una forma manual de las tablas anteriormente mencionadas.

```
Sexo_Dao.insertartodo();
Param_Audio_Dao.insertartodo();
Param_SPO2_Dao.insertartodo();
Param_Frecardiaca_Dao.insertartodo();
Param_Estres_Dao.insertartodo();
TipoActividadDao.insertartodo();
```

Figura 69. insertar valores por defecto en tablas básicas.

### 3.8.8.2 Implementación de la Aplicación Android

La aplicación fue desarrollada en Android y cuenta con 7 paquetes para llevar a cabo las capas de la arquitectura. En la **figura 70** se observa el diagrama de paquetes y sus relaciones.

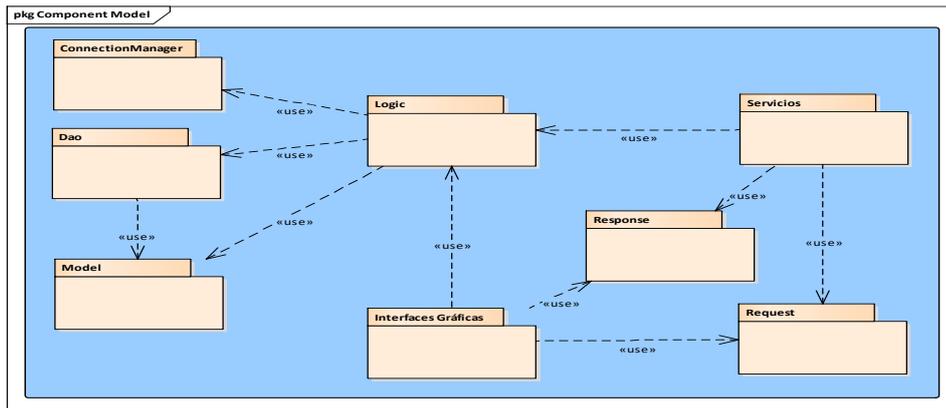


Figura 70. diagrama de paquetes de la aplicación móvil.

A continuación, se describe cada paquete de la aplicación:

### Paquete connectionManager

En este paquete se desarrolló todo lo relacionado a las comunicaciones con los dispositivos wearables. En el paquete existen tres interfaces para su implementación dependiendo de la pulsera.

La interfaz IBand tiene los métodos de emparejar, leer la actividad física, leer niveles de oxígeno en la sangre, escanear y leer el ritmo cardiaco. La interfaz IBandAction contiene los métodos para manejar los eventos que ocurren con la pulsera, por ejemplo, un cambio de estado, una recepción de actividad física o una recepción del valor del ritmo cardiaco. La interfaz IConnection contiene los métodos necesarios para abrir o cerrar una conexión con un dispositivo en este caso Bluetooth. En dado caso se requiera agregar una nueva pulsera al sistema se deben implementar estas interfaces con su respectiva comunicación.

Además de las interfaces existen dos clases que tiene atributos constantes estáticos para tener configurados los servicios y características Gatt de cada dispositivo, los cuales son ConsLeotec y ConstMiBand3. Estas constantes varían dependiendo de cada servicio, por tanto, se tendrá una clase por cada pulsera que se quiera implementar en la aplicación.

La clase LeotectConnection y MiBand3DeviceConnection son las implementaciones de la interfaz IConnection, mientras que las clases MiBand3 y Leotec son la implementación de la interfaz IBand. Por último, la clase Util contiene métodos necesarios para el funcionamiento del api, como encriptaciones y suma de vectores de bytes. En la **figura 71** se presentan las clases del paquete ConnectionManager.

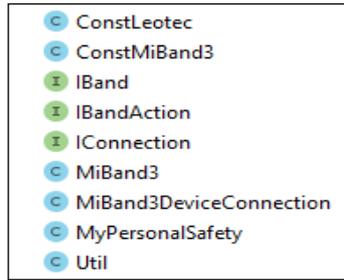


Figura 71. clases del paquete ConnectionManager.

### Paquete clienteRest

El paquete clienteRest contiene la clase para la conexión al servicio rest desde la aplicación móvil. En esta clase se envían todas las peticiones de los diferentes verbos, tiene variables estáticas que define la URL de cada servicio.

Tiene un método principal llamado consumirMetodos que recibe como parámetros la url, el Json de envío y el verbo de la petición Http. Este método crea una instancia de la clase HttpURLConnection que es la encargada de hacer peticiones http en Android. En la **figura 72** se observa la única clase del paquete clienteRest.



Figura 72. clases del paquete clienteRest.

### Paquete model

En este paquete se definieron todas las clases que hacen referencia a las tablas de la base de datos en SQLite, con el fin de hacer un mapeo de los datos de la tabla a un objeto en memoria con el cual se pueda trabajar. A diferencia del modelo del servicio rest en este paquete se añade una nueva clase llamada dispositivo la cual manipula los dispositivos conectados.

En la **figura 73** se observa las clases del paquete model.



Figura 73. clases del paquete model.

## Paquete dao

En este paquete se definieron las clases en las cuales se realizarán los procesos de inserción, actualizado, eliminación y consulta de las tablas. Para esto se necesitó realizar una conexión con SQLite a través de la implementación de la clase: SQLiteOpenHelper.

Se creó una clase para manipular la conexión con SQLite llamada ConexionBD la cual gestiona todo lo relacionado a la creación y actualización de la estructura de la base de datos. Todas las clases pertenecientes a este paquete heredan de la clase abstracta Dao. Dao cuenta con métodos abstractos para la inserción, actualización y consulta de una entidad específica. Cada clase modelo tendrá su respectiva clase Dao. A diferencia del paquete Dao del servicio Rest este cuenta con una clase llamada Dispositivo para el manejo de los dispositivos emparejados en la aplicación móvil.

En la **figura 74** se observan las clases del paquete dao de la aplicación móvil.



Figura 74. clases del paquete dao.

### Paquete logic

En este paquete se definieron las clases en las cuales se realiza la lógica de la aplicación, todas estas clases heredan de la clase Logic. La clase Logic recibe el un objeto de tipo ConexionBD, con el cual se puede realizar todos procesos transaccionales del aplicativo.

En la **figura 75** se observan las clases del paquete logic.

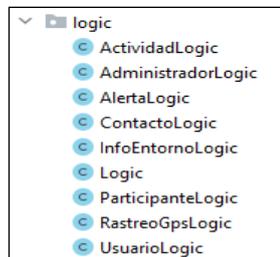


Figura 75. clases del paquete logic.

### Paquete request

En este paquete se definieron las clases para las solicitudes que se van a enviar por la clase ClienteRest, todas estas clases heredan de la clase Solicitud. La cual cuenta con una instancia de la clase Credencial la que maneja el usuario y la contraseña del usuario que está haciendo la solicitud, la estructura de estas clases son idénticas a las del servicio. Para convertir estas clases a una cadena JSON se utilizó la librería Gson. En la **figura 76** se observan las clases del paquete request.



Figura 76. clases del paquete request.

## Paquete response

En este paquete se definieron las clases para las respuestas del servicio. Todas las clases tienen los atributos públicos para que al momento de hacer la serialización de Json al objeto del tipo deseado no se presenten problemas de accesibilidad. En todos los métodos del servicio siempre se va a retornar un objeto de la clase Respuesta, el cual tendrá un mensaje, un tipo de respuesta: error o éxito y un objeto con la información de la respuesta, por ejemplo, la información de un participante. Estas serán las respuestas de todos los métodos del servicio Rest que se consumen en la clase ClienteRest. En la **figura 77** se muestran las clases del paquete response.

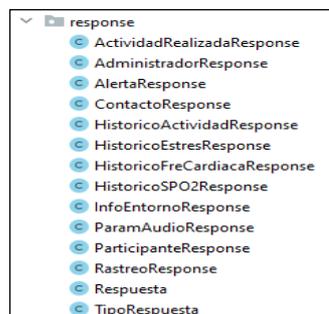


Figura 77. clases del paquete response

## Paquete de interfaces gráficas.

El paquete de interfaces gráficas cuenta con todas las actividades, fragmentos, menús, listas y adaptadores que fueron desarrollados en la plataforma. Todas las actividades heredan de una super clase la cuenta con un objeto conexión de base de datos el cual es pasado como parámetro a las clases del paquete logic. Cada Actividad desarrollada cuenta con su respectivo archivo xml para el diseño e interacción con el usuario.

Las actividades desarrolladas son:

- Login

- Crear perfil
- Editar perfil participante.
- Editar perfil administrador.
- Aceptar supervisión.
- Emparejar dispositivo.
- Home participante.
- Home administrador.

Los fragmentos desarrollados:

- Fragmento histórico de spo2.
- Fragmento histórico actividad.
- Fragmento del perfil de usuario.

Los menús desarrollados:

- Menú participante.
- Menú administrador.

Los adaptadores desarrollados:

- Lista de solicitudes de administradores.
- Lista de históricos de actividad.
- Lista de históricos de parámetros de salud.
- Lista de solicitudes por aceptar.

En la **figura 78** se observa el funcionamiento de las actividades en Android. Cada actividad o fragmento cuenta con un layout el cual es un archivo XML con todos los componentes con el usuario interactúa.

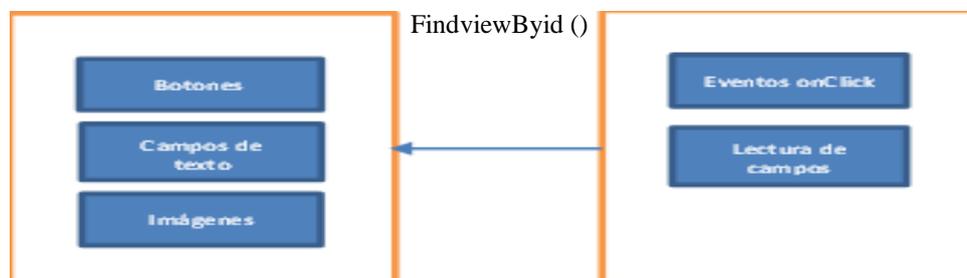


Figura 78. funcionamiento de actividades y fragmentos

## Paquete de servicios

Se crearon tres servicios que se ejecutan en segundo plano, cada servicio cuenta con un timer que se ejecuta en un cierto tiempo dependiendo de cada requerimiento. Todos los servicios heredan de la clase ServicioBase la cuenta con la conexión a la base de datos. Esta clase hereda de la clase Service la cual se encuentra en el paquete aplicaciones de Android. Además, de la conexión a la base de datos SQLite la clase ServicioBase sobrescribe el método onBind retornado null, este método debe ser sobrescrito para el buen funcionamiento de los servicios.

### **Servicio de monitorización de la actividad**

Se configuro para que el timer se ejecute una vez iniciada la actividad por parte del participante, comparando la lectura anterior menos la lectura obtenida, si la diferencia es igual a cero quiere decir que se ha activado la alerta en el último minuto.

En dicho caso si la diferencia es positiva quiere decir que la alerta todavía no se ha iniciado, la aplicación también enviará al participante un mensaje indicando que el contador de tiempo ha sido activado y podrá desactivarlo si así lo desea. Por último, si la diferencia de las lecturas da igual a cero se crea un histórico de la actividad y se envía la alerta a los contactos predefinidos.

Estos históricos se crean tanto en la aplicación móvil como en el servicio rest si la persona tiene configurado que sus datos tienen respaldo en un servidor externo.

### **Servicio de ejecutar actividad por tiempo**

El timer configurado en este servicio dependerá de la configuración de la actividad a realizar, por ejemplo, si la actividad es recorrer treinta minutos, el timer se ejecutará treinta minutos después de haber colocado a inicializar la actividad.

Cuando se ejecuta el método del timer se valida el tiempo asignado a la actividad con el tiempo transcurrido. Una vez transcurrido el tiempo previamente configurado se manda una notificación de alerta a los contactos configurados. También podrá desactivar la actividad antes de haber concluido para evitar los falsos positivos, además, el participante podrá activar el botón de pánico después de haber iniciado la actividad en caso se presenten problemas. Si el participante tiene configurado que sus datos tienen respaldo, la actividad realizada se manda al servicio junto con el valor obtenido.

### Servicio de notificaciones a aplicación.

El servicio de notificaciones consiste en enviar mensajes de alerta para que los contactos previamente configurados puedan ayudar al participante, el timer se ejecuta cada día, tomando un mensaje de la lista de mensajes que provienen de la activación de alerta por el tiempo transcurrido de la actividad, la activación del botón de pánico, los parámetros de salud y los parámetros de voz del participante, permitiendo configurar los mensajes presentados dependiendo de las características de cada persona.

### 3.8.9 Implementación a nivel de percepción de datos

La implementación del nivel de percepción de datos se realizó la conexión gatt entre la aplicación móvil y el dispositivo con la que se obtiene las mediciones fisiológicas del participante. Es el complemento al paquete ConnectionManager anteriormente mencionado en la implementación de la aplicación móvil.

En la **figura 79** se observa el diagrama de despliegue del nivel de percepción de datos. Cabe resaltar que en este proyecto no se modifica el firmware del dispositivo wearable, se trabaja con el del fabricante, solo se realiza una conexión a los servicios Gatt de la pulsera.

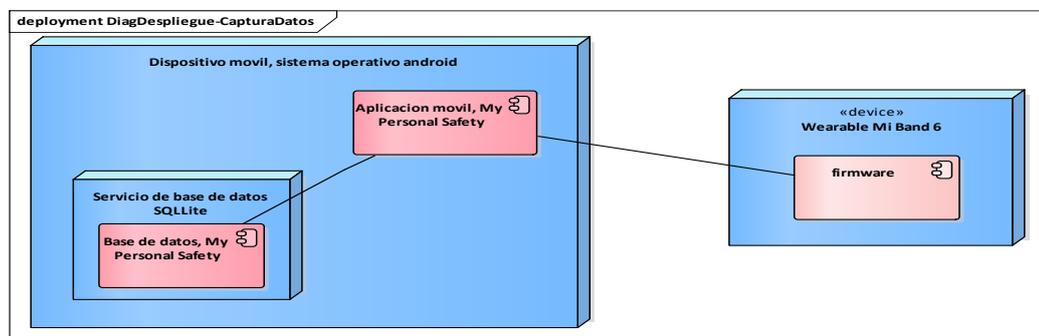


Figura 79. despliegue del nivel de percepción de datos

Dentro de la implementación de la aplicación móvil se tiene una conexión Bluetooth basada en eventos para recibir las notificaciones de los eventos del servicio Gatt.

En la **figura 80** se observa la arquitectura basada en eventos del servicio Gatt. Los eventos que se podrán controlar son: un cambio de estado de la conexión (conectado, desconectado), un cambio de lectura de la característica, un cambio de escritura en una característica. Todos estos eventos llegan a una cola donde son publicados para que una aplicación se suscriba a este.

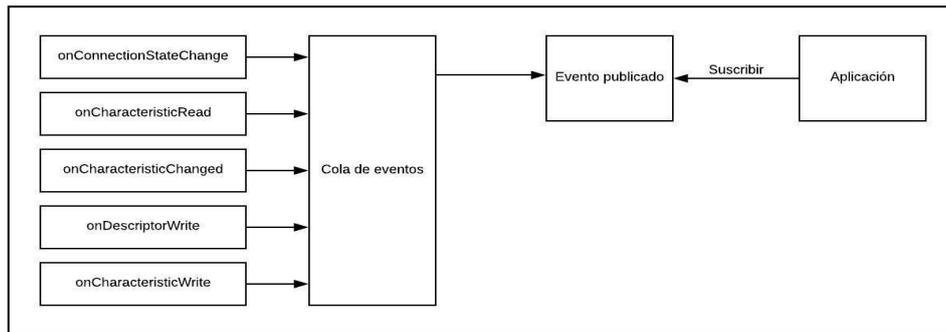


Figura 80. conexión Bluetooth con la pulsera.

A continuación, se detalla la implementación de las conexiones con los wearables Xiaomi mi band 6.

### 3.8.10 Conectividad con los diferentes wearables.

#### Gatt en Android

Android proporciona una API pública para manejar los perfiles GATT de Bluetooth Low Battery, la cual permite la comunicación con dispositivos con sistema operativo Android. Está disponible a partir de la versión 4.3 (Jelly Bean). Esta API permite descubrir dispositivos, consultar servicios y transmitir información. Para comenzar con la implementación se debe otorgar permisos a la aplicación para realizar cualquier comunicación utilizando Bluetooth, además de comprobar si el dispositivo donde se ejecuta la aplicación es compatible con BLE. Luego de otorgar los permisos y verificar si es compatible se procede a consultar los dispositivos que se encuentran cercanos a través del Bluetooth Adapter. Una vez encontrados se puede conectarse al servidor GATT y se obtendrá un objeto de tipo BluetoothGatt con el cual se podrá utilizar para realizar las operaciones como un cliente GATT. Para recibir los eventos del servidor GATT se utiliza el objeto BluetoothGattCallback el cual devuelve el estado de la conexión, así como cualquier otra operación, como el resultado de la escritura o lectura, por ejemplo. Para terminar, se debe cerrar la conexión de la aplicación con el servicio GATT (Developers, 2019).

#### 3.8.11 Implementación con Xioami Mi Band 6

Mi Band 6 es una pulsera desarrollada por Xiaomi, la cual tiene varios sensores que miden la actividad física. Cuenta con acelerómetro, pulsómetro y en su aplicación comercial puede obtener SPO2. Dentro de la Autonomía es una de las mejores pulseras con una duración de 20 días aproximadamente. Además, el precio promedio es de 30 euros siendo más económica comparada con una pulsera Fitbit o Samsung.

Esta pulsera funciona con BLE y cuenta con una seguridad propia para poder establecer una comunicación persistente sino esta se desconecta al paso de 30 segundos. Primero hay que configurar la notificación de autorización la cual es la característica x009 del servicio xfee1, enviando el comando x01 x00 + la clave a cifrar. Luego hay que solicitar una clave aleatoria al dispositivo escribiendo el comando x02 x00 a la característica. Esta devolverá la clave aleatoria en los últimos 16 bytes. La clave aleatoria se encripta utilizando el algoritmo de cifrado AES y se envía nuevamente a la pulsera escribiendo a la misma característica el comando x03 x00 + la clave cifrada. Una vez conectada ya se puede enviar y leer información del dispositivo. Para la implementación se realizaron varios métodos como el envío de notificaciones a la pulsera. La cual es la característica x2A46 del servicio x1811, el comando a escribir es: en el primer byte va el tipo de notificación, en el segundo byte va el tipo de alerta y en los bytes siguientes va el mensaje (Ojha, 2018).

En la **figura 81** se muestra cómo se debe encontrar el dispositivo Bluetooth y obtenerlo en el objeto BluetoothDevice, la búsqueda se realiza a través de la MAC de la pulsera. Se debe obtener primero el BluetoothAdapter a través del contexto de la aplicación.

```
@Override
public BluetoothDevice getDevice() { return device; }

@SuppressLint("MissingPermission")
@Override
public void disconnect()
{
    if(myGatBand == null)
    {
        return;
    }

    myGatBand.close();
}
```

*Figura 81. obteniendo el dispositivo a través de la MAC.*

Se debe obtener el Gatt del dispositivo y además se le debe pasar la clase que gestionara la comunicación con él, para este caso la clase se llama MiBand6DeviceConnection la cual debe extender de la clase BluetoothGattCallback esta clase contiene los métodos de escritura, lectura, detectar cambios en la conexión y detectar cambios en las características.

En la **figura 82** se observa cómo se realiza la conexión del dispositivo mi band 3 a través de los servicios Gatt con el método connectGatt pasándole como parámetros el contexto y la clase para el call back MiBand6DeviceConnection.

```

myGatBand = device.connectGatt(myContext, autoConnect: false,

if (myGatBand == null)
{
    raiseOnErrorNotification("GATT no encontrado.");
    this.connected = false;
    return connected;
}

if(!myGatBand.connect())
{
    raiseOnErrorNotification("No se pudo conectar al GATT.");
    this.connected = false;
    return connected;
}

```

Figura 82. conexión a los servicios gatt de un dispositivo.

Si la comunicación se realizó con éxito se podrá detectar el cambio con el método `onConnectionStateChange`.

En la **figura 83** se observa el método `onConnectionStateChange` de mi band 6 el cual cuando detecta una conexión debe hacer un proceso de autorización mencionado anteriormente.

```

@Override
public void onConnectionStateChange(BluetoothGatt gatt, int status, int newState) {

    switch (newState) {
        case BluetoothProfile.STATE_CONNECTED:

            myGatBand = gatt;
            myGatBand.discoverServices();

            myHandler.postDelayed(new Runnable() {
                @Override
                public void run() { AuthBand(); }
            }, delayMillis: 3000);
            raiseOnNotification("Conectando...");
            break;
        default:
            gatt.close();
            raiseOnDisconnect();
            connected = false;
            break;
    }
}

```

Figura 83. método que detecta un cambio en la conexión con la gatt del dispositivo.

Para detectar los cambios de las características se sobre escribe el método `onCharacteristicChanged`, todos los cambios de características llegaran a este método y en la tercera de posición del value siempre ira si se realizó con éxito el cambio, si la característica es de autorización se realiza los métodos de autorización, envío de claves cifradas y conexión realizada con éxito.

Para el método de escribir se parametrizo tanto los servicios, las características y en el comando a enviar.

En la **figura 84** se muestra el método `writeDate` el cual recibe como parámetro un UUID del servicio y un UUID de la característica, además de un array de bytes que se escribirán en la característica. Primero se obtiene el servicio y la característica, si ambos existen se llama al método `writeCharacteristic`.

```
public void writeData(UUID service, UUID Characteristics, byte[] data) {
    if (!connected || myGatBand == null) {
        raiseOnErrorNotification("Dispositivo no conectado.");
        return;
    }

    BluetoothGattService myGatService = myGatBand.getService(service);
    if (myGatService != null) {
        BluetoothGattCharacteristic myGatChar
            = myGatService.getCharacteristic(Characteristics);
        if (myGatChar != null) {
            myGatChar.setValue(data);
            myGatBand.writeCharacteristic(myGatChar);
        }
    }
}
```

Figura 84. *método que permite escribir en cualquier servicio y característica un array de bytes.*

Un ejemplo de escribir en una característica es el método de enviar una notificación. En la **figura 85** se observa cuáles son los UUID mandados y el mensaje que se desea mandar recibido por parámetro.

```
@Override
public void sendNotification(String message)
{
    byte notif= ConstMiBand6.llamada;
    byte alert= ConstMiBand6.alert1;
    byte [] parametros=new byte[]{notif,alert};
    byte [] bytes = message.getBytes(StandardCharsets.US_ASCII);
    byte [] mensaje= Util.unitBytes(parametros,bytes);

    connection.writeData(ConstMiBand6.UUID_SERVICE_1811, ConstMiBand6.UUID_CHARACTERISTIC_2A46,
        mensaje);
}
```

Figura 85. *método para enviar una notificación a la pulsera Mi band 6.*

### 3.8.12 Resultados de la implementación.

La mayoría de los requisitos funcionales y no funcionales fueron desarrollados con todas las especificaciones que se mencionaban en los casos de uso. El único faltante fue la activación de la alerta a través de los parámetros de voz, el cual no pudo ser implementado por los tiempos de la planeación y por qué abarca más desarrollo e investigación en el tema.

Se cumplieron las especificaciones de diseño, con la única diferencia que el menú fue colocado como iconos en la parte superior central.

Se realizaron pruebas tanto de la aplicación móvil como del api desarrollado. Obteniendo respuestas favorables para todos los casos de uso.

A continuación, se describen las pruebas de cada uso en la aplicación móvil, así como las dificultades presentadas en el desarrollo.

### **Inicio de Sesión y registro de usuario**

Cuando es la primera vez aparece la interfaz para iniciar sesión, ya que todavía no tiene una sesión activa en la aplicación. Esta interfaz cumple con todas las especificaciones del diseño de la parte de análisis.

En la **figura 86** se observa la interfaz de inicio de sesión.



*Figura 86. iniciar sesión del participante.*

### **Registrar participante.**

Una vez validado, la aplicación redirige a página principal para crear la cuenta del participante.

En la **figura 87** se observa la interfaz de registrar participante.



*Figura 87. registrar participante.*

## Empareja dispositivo.

En el símbolo de Bluetooth del menú abre la función para emparejar algún dispositivo. Esta interfaz cumple con todas especificaciones del diseño inicial. Se debe presionar el botón buscar para que aparezcan todos los posibles dispositivos conectados. Una vez que encuentra el dispositivo se podrá emparejar el dispositivo y este aparecerá en la parte superior cuando se empareja con éxito. En la prueba se selecciona el dispositivo Mi Band 6 para emparejarlo en la aplicación.

Esta interfaz a veces presenta algunos problemas por parte de la librería de conexión con el Bluetooth, debido a que no aparecen algunas veces los dispositivos cercanos. En este caso se debe volver a buscar los dispositivos para que la lista se vuelva a refrescar.

En la **figura 88** se observa la interfaz de emparejar dispositivos.



Figura 88. emparejar dispositivos.

### 3.8.13 Resultados del servicio rest.

Todos los casos de uso fueron realizados en el servicio. Para las pruebas del servicio Restful se utilizó la aplicación Postman. La cabecera de todas las peticiones que se hicieron al servicio contaba con el valor Content-type igual a application/json. Se hicieron pruebas unitarias en cada método del servicio, comprobando que la información sea íntegra y sea almacenada correctamente en la plataforma.

### 3.8.14 Casos de prueba realizados en la plataforma.

En esta sección se describen los casos de prueba realizados en la plataforma, indicando la prueba realizada, el actor que la ejecuta, el estado de cumplimiento y una observación.

## Funcionalidad iniciar sesión

<b>Caso de prueba</b>	<b>Actor</b>	<b>Estado</b>	<b>Observación</b>
¿Se puede iniciar correctamente la sesión?	Participante	Cumplido	
¿Se puede iniciar correctamente la sesión?	Supervisor	No cumplido	La aplicación no ha contemplado el actor Supervisor.
¿Se puede iniciar correctamente la sesión?	Administrador	Cumplido	

Tabla 30. Descripción de la funcionalidad al iniciar sesión.

### **Funcionalidad crear usuario**

<b>Caso de prueba</b>	<b>Actor</b>	<b>Estado</b>	<b>Observación</b>
¿Se puede crear un usuario?	Participante	Cumplido	
¿Se puede crear un usuario?	Administrador	Cumplido	
¿Se valida la existencia de un usuario con el userName proporcionado?	Participante	Cumplido	
¿Se valida la existencia de un usuario con el userName proporcionado?	Administrador	Cumplido	
¿Se valida que la contraseñas y repetir contraseña sean iguales?	Participante	Cumplido	
¿Se valida que la contraseñas y repetir contraseña sean iguales?	Administrador	Cumplido	

Tabla 31. Descripción de la funcionalidad al crear usuario.

### **Funcionalidad ver perfil**

<b>Caso de prueba</b>	<b>Actor</b>	<b>Estado</b>	<b>Observación</b>
¿El participante puede ver su perfil?	Participante	Cumplido	
¿El participante puede ver el histórico de la actividad?	Participante	Cumplido	
¿El participante puede ver el histórico de los parámetros fisiológicos?	Participante	No cumplido	La interfaz gráfica existe, pero no tiene datos para mostrar.

Tabla 32. Descripción de la funcionalidad ver perfil.

### **Funcionalidad editar usuario.**

<b>Caso de prueba</b>	<b>Actor</b>	<b>Estado</b>	<b>Observación</b>
¿El participante puede editar sus datos?	Participante	Cumplido	
¿El participante puede editar parámetros fisiológicos?	Participante	Cumplido	
¿El participante puede crear lista de contactos?	Participante	Cumplido	
¿El participante puede gestionar el modo cuenta atrás?	Participante	Cumplido	
¿El participante puede gestionar el modo supervisión de la actividad?	Participante	Cumplido	
¿El participante puede disparar la alerta?	Participante	Cumplido	
¿El participante puede obtener	Participante	Cumplido	

información del entorno?			
¿El participante puede rastrear la ubicación por GPS?	Participante	Cumplido	
¿El contacto puede rastrear la ubicación por GPS?	Contacto	Cumplido	

Tabla 33. Descripción de la funcionalidad editar usuario.

### Funcionalidad emparejar dispositivo

Caso de prueba	Actor	Estado	Observación
¿Se puede emparejar un dispositivo wearable?	Participante	Cumplido	
¿La lista de dispositivos disponibles se elimina el que está ya emparejado?	Participante	No Cumplido	Se utiliza la librería de Bluetooth de Android no permite cambiar el listado.

Tabla 34. Descripción de la funcionalidad emparejar dispositivo.

### Funcionalidad de los servicios de monitorización

Caso de prueba	Actor	Estado	Observación
¿En todo momento se monitoriza la actividad?	Participante	Cumplido	
¿En todo momento se monitoriza la actividad?	Contacto	Cumplido	
¿Los datos de la actividad son actualizados en la interfaz?	Participante	Cumplido	

Tabla 35. Descripción de los servicios de monitorización.

### Funcionalidad de supervisión

<b>Caso de prueba</b>	<b>Actor</b>	<b>Estado</b>	<b>Observación</b>
¿El supervisor puede buscar participantes?	Supervisor	Cumplido	
¿El participante puede ver la lista de solicitudes que tiene pendientes por aceptar?	Participante	Cumplido	
¿El supervisor puede ver los participantes y sus datos de actividad?	Supervisor	Cumplido	
¿La interfaz del listado de participantes supervisados se actualiza cuando detecta un cambio?	Supervisor	No cumplido	Se debe refrescar la interfaz manualmente.
¿El participante puede eliminar una supervisión?	Participante	No cumplido	Una vez aceptada no puede cancelar la supervisión, no se especificó este requerimiento.
¿El supervisor puede eliminar una supervisión?	Supervisor	No cumplido	Una vez aceptada no puede cancelar la supervisión, no se especificó este requerimiento.

*Tabla 36. Descripción de la funcionalidad en la supervisión*

#### **IV.DISCUSIÓN**

Esta parte interpreta los resultados del uso de la aplicación móvil implementada con el fin de evaluar el logro de los objetivos.

El objetivo de este proyecto fue desarrollar una plataforma que permita monitorizar de forma continua la seguridad personal, mediante la utilización de dispositivos wearables en la ciudad de Bagua; que se encuentra apoyado en los objetivos específicos que fueron analizados en la parte de los resultados.

En el primer objetivo específico hemos obtenido información tanto en lo cuantitativo como cualitativo para comprender a profundidad sobre la seguridad personal y de qué manera juega un papel significativo los dispositivos wearables en el proceso de automatización de la seguridad personal para definir luego la metodología a utilizar para el desarrollo de software.

En el segundo objetivo específico se realizó el estudio y análisis de los diferentes tipos de dispositivos wearables, así como los protocolos de comunicación utilizados por lo que se observó las ventajas y desventajas de los dispositivos wearables que existen en el mercado para desarrollar el sistema de monitoreo y control para la seguridad personal especificando una ponderación para ello (baja: 1, media: 2, alta: 3) y además se elaboró un cuadro de puntuación para las ventajas en donde se obtuvo como resultado elegir la pulsera de salud y actividad Mi Smart Band 6 con una puntuación de 9. Se utilizó dispositivos móviles con sistema operativo Android y en cuanto al principal aporte al trabajo de investigación sobre las alertas o notificaciones se pueden realizar para todo tipo de dispositivo a donde se enviarán las coordenadas de ubicación del usuario.

En el tercer objetivo específico se estudió y analizó los diferentes sistemas de monitorización basados en seguridad personal, que mejor se adapten al proyecto por lo que el aplicativo contará con tres funcionalidades principales de “Crear alerta”, “Grabar recorrido”, “Ver mapa” y tendrá un menú desplegable en donde encontraremos la opción de “Mi perfil”, “Mi contacto”, “Cerrar sesión”. Este sistema de motorización para la seguridad personal al momento de activarse la funcionalidad “Crear la alerta” obteniendo las coordenadas de la ubicación y lo envía rápidamente por mensaje de texto. Con respecto a la funcionalidad de “Grabar recorrido” obtiene las coordenadas de la ubicación y lo guarda en una base de datos. Con respecto a la funcionalidad “Ver mapa” carga una lista de las ubicaciones guardadas, al seleccionar el registro lo pinta en el mapa.

En el quinto objetivo específico se determinó las herramientas para el diseño y modelado; así como la arquitectura del sistema para el desarrollo de la plataforma de este proyecto para ello los artefactos utilizados analizados incluyen diagramas de casos de uso, descripciones de casos de uso, diagramas de secuencia, diagramas de robustez o colaboración, diagramas de despliegue, modelos de clase, modelos lógicos, modelos físicos, modelos de arquitectura y prototipos de aplicaciones móviles.

Considerando los objetivos siguientes se elaboró el prototipo para luego evaluar el grado de aceptación del sistema.

Con el análisis del sistema que permite monitorizar de forma continua la seguridad personal, con el uso de dispositivos wearables, se puede afirmar que la plataforma en mención permite monitorizar de forma continua la seguridad personal, sincronizando con los dispositivos móviles para poder acudir a la brevedad en la ayuda del usuario, con la información que se obtiene de los dispositivos wearables será de mucha utilidad para el posterior análisis permitiendo tomar decisiones eficientes y acertadas en base a información sólida.

Las características más representativas, ventajosas y destacadas del sistema propuesto son:

- Los atributos o características del sistema propuesto han sido analizados por expertos de los cuales se han obtenido resultados favorables hacia el sistema propuesto.
- El sistema propuesto ha sido validado a través de su aplicación al análisis de indicadores, del cual se obtuvo resultados positivos que garantizan que el sistema propuesto cumple con el objetivo la seguridad personal.

#### **4.1 Análisis del Despliegue del sistema de monitoreo y control para la seguridad personal utilizando dispositivos wearables propuesto.**

De los resultados obtenidos en el despliegue del sistema de monitoreo y control para la seguridad personal utilizando dispositivos wearables, se puede observar una reducción del tiempo para generar y analizar respuestas a las alertas, así como también el número de personas involucradas en el proceso de análisis de indicadores, lo cual indica que dicho proceso en la seguridad personal tuvo una mejora significativa.

#### **4.2 Análisis de la validación del sistema de monitoreo y control para la seguridad personal utilizando dispositivos wearables propuesto**

Según la tabla de resultados obtenidos de la evaluación por expertos de los atributos del sistema propuesto, expuestos en el anexo, se puede apreciar claramente que el sistema propuesto resulta mucho más ventajoso en cada uno de sus atributos:

**Conformidad del sistema:** aprobado en todos los procesos presentados.

**Amigabilidad del Sistema:** aprobado en gran parte los procesos presentados.

**Tiempo de respuesta a un incidente:** aprobado en la mayoría de los procesos presentados.

Dando un ponderado a cada criterio para un proyecto de este tipo se encontró que en su mayoría los atributos son favorables.

Tabla 37. Relevancia Final de cada atributo del sistema de monitoreo y control para la seguridad personal utilizando dispositivos wearables propuesta.

	<b>Puntaje Final</b>	<b>Ponderación acorde al proyecto</b>	<b>Relevancia final</b>
Conformidad del sistema	13,97	2,0	27,94
Amigabilidad del sistema	13,60	2,0	27,20
Respuesta a un incidente	14,37	3,0	43,11

*Tabla 37. Relevancia Final de cada atributo del sistema de monitoreo y control para la seguridad personal*

Análisis de los resultados obtenidos de la evaluación de los indicadores del sistema de monitoreo y control para la seguridad personal utilizando dispositivos wearables propuesto, en comparación con los resultados obtenidos sin el análisis minucioso de expertos con respecto al sistema de monitoreo y control para la seguridad personal utilizando dispositivos wearables. En la tabla de Resultados que muestran los datos obtenidos con el uso del sistema de monitoreo y control para la seguridad personal utilizando dispositivos wearables propuesto, con el análisis de los indicadores se puede determinar a través de la comparación, si los resultados indican que el sistema produce una elevación del rendimiento de respuesta, determinan que los resultados antes y después son significativamente diferentes.

En este proyecto no fue necesario el uso de cálculos estadísticos muy sofisticados como para demostrar de manera categórica si existe una mejora.

Los resultados obtenidos durante con la implementación del sistema de monitoreo y control de seguridad personal con dispositivos wearables son bastante claros, la tabla y figura a continuación muestran a través de los resultados de la evaluación de los indicadores que si existe mejora significativa con la propuesta.

Tabla 38. Promedio Final de cada indicador de la toma de decisiones con el sistema de monitoreo y control para la seguridad personal utilizando dispositivos wearables propuesto comparando la opinión antes del análisis de verificación del sistema por el experto y opinión después del análisis de verificación del sistema por el experto.

Indicadores	Unidad de Medida	Promedio	
		Opinión antes del análisis de verificación del sistema por el experto	Opinión después del análisis de verificación del sistema por el experto
<b>Granularidad de los datos reportados en la alerta</b>	Porcentaje	15	50,5
<b>Tiempo de espera de respuesta del sistema</b>	minutos	10,05	2,5

Tabla 38. Opinión antes del análisis de verificación del sistema por el experto y opinión después del análisis de verificación del sistema por el experto.

Figura 89. Promedio de los indicadores del análisis, opinión antes del análisis de verificación del sistema por el experto propuesto versus Opinión después del análisis de verificación del sistema por el experto.

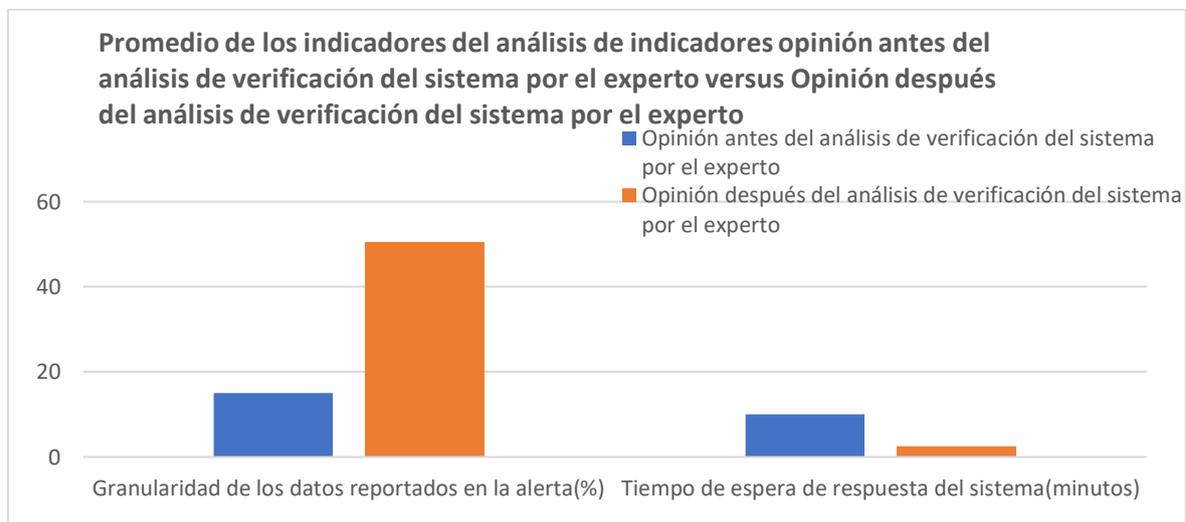


Figura 89. Promedio de los indicadores del análisis de opinión

En consecuencia, se confirma la hipótesis, “El desarrollo de un sistema con dispositivos wearables permitirá realizar el monitoreo y control de la seguridad personal con una eficiencia aceptable mayor al 50%”. Por lo que el sistema emitirá alerta basada en GPS, permitiendo reducir el tiempo de respuesta para acudir a la persona que sufrió un ataque por robo u otro tipo de violencia delictiva.

## V.CONCLUSIONES

1. De acuerdo al primer objetivo específico “Determinar las fuentes de información tanto cuantitativas como cualitativas que permitan profundizar en el estudio de la seguridad personal”. Inicialmente, hemos obtenido información tanto cuantitativas como cualitativas para comprender a profundidad sobre la seguridad personal y de qué manera juega un papel significativo los dispositivos wearables en el proceso de automatización de la seguridad personal. En lo cuantitativo se han analizado el tiempo de respuesta, obtención de datos obtenidos del usuario el tiempo de procesamiento de información obtenida. En lo cualitativo se observó la efectividad de los datos obtenidos por los dispositivos wearables diversos.
2. Continuando con el segundo objetivo específico “Estudiar y analizar los diferentes tipos de dispositivos wearables, así como los protocolos de comunicación utilizados”. Permitieron elegir al dispositivo wearables con las prestaciones convenientes acorde al trabajo de investigación.
3. Continuando con el tercer objetivo específico “Estudiar y analizar los diferentes sistemas de monitorización basados en seguridad personal, que mejor se adapten al proyecto”. Permitted analizar los sistemas de monitorización de seguridad personal existentes o trabajos de investigación similares realizados hasta la fecha para poder elegir y adaptar en función del objetivo del proyecto.
4. Cuarto objetivo específico, Seleccionar los mecanismos de reconocimiento de la agresión física del usuario en base al análisis de los diferentes tipos de dispositivos wearables que porta el usuario, las distintas técnicas de captación de la información, los medios utilizados para recoger dicha información y almacenarla en una plataforma. Se seleccionó como dispositivo wearable las pulseras de actividad, la cual tiene un costo más accesible comparado con los demás dispositivos, Mi Smart Band 6 es una pulsera con mayor autonomía y con un costo muy inferior con respecto a Empatica E4 que tiene la misma autonomía, pero más costosa. Mi Smart Band 6 cuenta con los parámetros de medición necesarios para que la aplicación funcione los cuales son: acelerómetros y pulsómetros. permiten detectar el pánico del usuario y es de fácil sincronización con los dispositivos móviles.
5. Quinto objetivo específico es determinar las herramientas para el diseño y modelado; así como la arquitectura del sistema para el desarrollo de la plataforma de este proyecto. Se utilizó en el diseño de aplicaciones móviles el sistema Android por ser uno de los más utilizados. Además de que Android presenta una arquitectura basada en 4 niveles, todas las capas están basadas en software libre (Girones, 2013)

6. Determinar los dispositivos wearables más adecuados al proyecto, en base a los datos que puede proporcionar durante la agresión física. Se seleccionó como dispositivo wearable las pulseras de actividad Mi Smart Band 6 por ser la pulsera con mayor autonomía y con un costo muy inferior con respecto a otros similares. Mi Smart Band 6 cuenta con los parámetros de medición necesarios para que la aplicación funcione como son: acelerómetros y pulsómetros.

7. Realizar pruebas unitarias del sistema para evaluar el buen funcionamiento, conforme a los requisitos establecidos.

Las pruebas iniciales utilizando la pulsera de actividad Xiaomi Mi Smart Band 6 demuestran que la nueva plataforma cubre los objetivos que se han propuesto, y proporciona la utilidad que se esperaba.

8. Preparar un piloto del sistema con voluntarios, para evaluar el grado de aceptación del sistema.

La arquitectura realizada cumple con todas las especificaciones del sistema, ya que la plataforma puede funcionar con o sin internet. Además de utilizar protocolos seguros y de bajo coste como el caso de BLE.

Las pruebas del desarrollo se hicieron probando cada requerimiento y su buen funcionamiento, no se logró realizar pruebas con voluntario, sin embargo, las pruebas desarrolladas en laboratorio abarcaron la mayoría de los requerimientos planteados en la aplicación, solo faltó evaluar la activación de la alerta según los parámetros de audio, el cual no se pudo realizar por falta de tiempo de implementación.

No se logró comparar los datos obtenidos en la aplicación con respecto a dispositivos médicos para analizar la confiabilidad de estos resultados.

## **VI. RECOMENDACIONES**

Se recomienda que el sistema de monitorización basados en seguridad personal para personas que sufrieron algún acto delictivo, puede ser replicado para otras localidades del país siempre en cuanto exista cobertura adecuada de internet.

Desarrollar una plataforma web donde un administrador pueda monitorear a los usuarios que han enviado la señal de alerta, sincronizando con los dispositivos móviles para poder acudir con certeza y a la brevedad en su ayuda.

La elaboración de estrategias de seguridad personal requiere una evaluación objetiva de las diversas situaciones de riesgo, así como la identificación y análisis del grado de vulnerabilidad del entorno y por ende del desarrollo de contingencias.

## VII.REFERENCIAS BIBLIOGRAFICAS

- Alruban, A. a. (2019). Physical activity recognition by utilising smartphone sensor signals. *8th International Conference on Pattern Recognition Applications and Methods* (págs. 342-351). SciTePress.
- Avila, L. a. (2017). Revisión estado del Arte de la tecnología Bluetooth. *Revista Investigación y Desarrollo en TIC*.
- Azman, F. a. (2018). My guardian: A personal safety mobile application. *2018 IEEE Conference on Open Systems (ICOS)* (págs. 37-41). IEEE.
- Barnes, D. J. (2007). *Programación orientada a objetos con Java*. Pearson Educación.
- Berntson, G. G. (1991). Autonomic determinism: the modes of autonomic control, the doctrine of autonomic space, and the laws of autonomic constraint. *Psychological review*, 98, 459.
- Blanco, P. a. (2009). Metodología de desarrollo ágil para sistemas móviles. Introducción al desarrollo con Android y el iPhone. *Dr. en Ing. Sist. Telemáticos*, 1--30.
- Bray, J. a. (2001). *Bluetooth 1.1: connect without cables*. New Jersey: Pearson Education.
- Brouwer, Anne-Marie and Van Wouwe, Nelleke and Muhl, Christian and Van Erp, Jan BF and Toet, Alexander. (2013). Perceiving blocks of emotional pictures and sounds: effects on physiological variables. *Frontiers in human neuroscience*, 7, 295.
- Byrom, B. a. (2018). Brain monitoring devices in neuroscience clinical research: the potential of remote monitoring using sensors, wearables, and mobile devices. *Clinical Pharmacology & Therapeutics*, 104, 59-71.
- Cai, R. a. (2018). Correlation analyses between personality traits and personal behaviors under specific emotion states using physiological data from wearable devices. *2018 IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing, 16th Intl Conf on Pervasive Intelligence and Computing, 4th Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech)* (págs. 46-53). IEEE.
- Case, M. A. (2015). Accuracy of smartphone applications and wearable devices for tracking physical activity data. *Jama*, 313, 625-626.
- Castellano, A. R. (2012). Bluetooth: Introducción a su funcionamiento. *Univ. Pontif. Comillas, Madrid*, 1--16.
- Caules, C. Á. (22 de 03 de 2018). *arquitecturajava*. Obtenido de Arquitectura rest y sus niveles: <https://www.arquitecturajava.com/arquitecturas-rest-y-sus-niveles/>
- Chaudhari, A. a. (2020). Women's safety band using IoT. *Proceedings of International Conference on Wireless Communication* (págs. 493-501). Springer.
- Chaudhari, Archana and Patel, Jahnvi and Savla, Krishi and Shetty, Akshitha and Shah, Vrushika. (2020). Women's safety band using IoT. *Proceedings of International Conference on Wireless Communication* (págs. 493--501). Springer.

- Chaudhari, Archana and Patel, Jahnvi and Savla, Krishi and Shetty, Akshitha and Shah, Vrushika. (2020). Women's safety band using IoT. *Proceedings of International Conference on Wireless Communication* (págs. 493-501). Springer.
- Chinchilla, Laura and Vorndran, Doreen. (2018). Seguridad ciudadana en America Latina y el Caribe. *Desafios e innovacion en gestion y politicas publicas en los ultimos, 10*.
- Chuah, S. H.-W. (2016). Wearable technologies: The role of usefulness and visibility in smartwatch adoption. *Computers in Human Behavior, 276--284*.
- Collins, J. (10 de 2007). *ABI Research Insight: No OTA, No NFC*. Obtenido de <http://www.abiresearch.com>: <http://www.abiresearch.com>
- Cornish, Derek Blaikie y Clarke, Ronald V. (2003). Oportunidades, precipitadores y decisiones criminales: una respuesta a la crítica de Wortley de la prevención del delito situacional. *Estudios de prevención del delito, 41-96*.
- de la Cal, E. a. (2018). Plataforma para el estudio de caídas y desvanecimientos en grupos de personas mayores. *Cognitive Area Networks, 17*.
- Developers, A. (2019). *Android Developers*. Obtenido de Bluetooth low energy overview: <https://developer.android.com/guide/topics/connectivity/bluetooth-le#java>
- Dunne, L. (2004). The design of wearable technology: addressing the human-device interface through functional apparel design.
- Eden, A. H. (2006). Abstraction classes in software design. *IEE Proceedings-Software, 163-182*.
- Elbasiony, Reda and Gomaa, Walid. (2019). A survey on human activity recognition based on temporal signals of portable inertial sensors. *International Conference on Advanced Machine Learning Technologies and Applications* (págs. 734-745). Springer.
- El-Gayar, O. F. (2020). Wearables, artificial intelligence, and the future of healthcare. En *AI and Big Data's Potential for Disruptive Innovation* (págs. 104--129). IGI Global.
- Fabiano, D. a. (2019). Emotion recognition using fused physiological signals. *2019 8th International Conference on Affective Computing and Intelligent Interaction (ACII)* (págs. 42-48). IEEE.
- Fielding, R. a.-L. (1999). Hypertext transfer protocol--HTTP/1.1.
- Fielding, R. T. (2017). Reflections on the REST architectural style and principled design of the modern web architecture (impact paper award). *Proceedings of the 2017 11th Joint Meeting on Foundations of Software Engineering, 4-14*.
- Girones, J. T. (2013). *El gran libro de Android*. Alfaomega.
- Goldin, A. (2018). Hearing Hearables and Hearing Health. *GSMA*.
- Goldstein, D. S. (2010). Adrenal responses to stress. *Cellular and molecular neurobiology, 30, 1433-1440*.
- Guo, L. a. (11). Knitted wearable stretch sensor for breathing monitoring application. En *Ambience'11, Boraas, Sweden, 2011*.

- Guyon, I. a. (2003). An introduction to variable and feature selection. *Journal of machine learning research*, 1157-1182.
- Guyon, I. y. (2003). Una introducción a la selección de características y variables. *Journal of machine learning research*, 1157-1182.
- Henriksen, A. a. (2018). Using Fitness Trackers and Smartwatches to Measure Physical Activity in Research: Analysis of Consumer Wrist-Worn Wearables. *Journal of medical Internet research*.
- Hohpe, G. (2006). Programming without a call stack--event-driven architectures. *Objekt Spektrum*.
- Hoy, M. B. (2018). Alexa, Siri, Cortana, and more: an introduction to voice assistants. *Medical reference services quarterly*, 37, 81-88.
- inei. (Abril de 2020). Obtenido de Inei.gob.pe:  
[https://www.inei.gob.pe/media/MenuRecursivo/boletines/informe\\_seguridad\\_ciudadana\\_1.pdf](https://www.inei.gob.pe/media/MenuRecursivo/boletines/informe_seguridad_ciudadana_1.pdf)
- Islam, M. N. (2018). SAFeBanD: A wearable device for the safety of women in Bangladesh. *Proceedings of the 16th International Conference on Advances in Mobile Computing and Multimedia*, (págs. 76-83).
- Just, M. a. (2019). Personal Safety App Effectiveness. *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*, (págs. 1-6).
- Kamalraj, R and Madhan, ES and Ghanya, K and Bhargavi, V. (2020). Enhance Safety and Security System for Children in School Campus by using Wearable Sensors. *2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC)* (págs. 986--990). IEEE.
- Kannan, M. R. (2020). IoT-Based Women Security System. En *Inventive Communication and Computational Technologies* (págs. 1369-1378). Springer.
- Kannan, Megalingam Rajesh and Jyothsna, K and Aparna, TS and Anjali, T and Meera, M and Amrutha, SD. (2020). IoT-Based Women Security System. En *Inventive Communication and Computational Technologies* (págs. 1369--1378). Springer.
- Kasnesis, P. a. (2019). Gesture-based incident reporting through smart watches. *2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)* (págs. 249-254). IEEE.
- Kfir, Z. a. (2005). Picking virtual pockets using relay attacks on contactless smartcard. *First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05)* (págs. 47-58). IEEE.
- Kolakowska, A. (2013). A review of emotion recognition methods based on keystroke dynamics and mouse movements. *2013 6th international conference on human system interactions (HSI)* (págs. 548-555). IEEE.
- Kulkarni, R. (2021). Near Field Communication (NFC) Technology and Its Application. *Techno-Societal 2020*, 745-751.
- Landowska, A. (2013). Affect-awareness framework for intelligent tutoring systems. *2013 6th International Conference on Human System Interactions (HSI)* (págs. 540-547). IEEE.

- Levy, Sharon and Xiong, Wenhan and Belding, Elizabeth and Wang, William Yang. (2020). SafeRoute: Learning to Navigate Streets Safely in an Urban Environment. *ACM Transactions on Intelligent Systems and Technology (TIST)*, 1--17.
- Lewis Jr, R. P. (2020). *Estados Unidos Patente n° US Patent App. 16/200,610*.
- Lewis Jr, R. P. (2020). *United States Patente n° US20200168074A1*.
- Lobelo, F. a. (2016). The wild wild west: A framework to integrate mhealth software applications and wearables to support physical activity assessment, counseling and interventions for cardiovascular disease risk reduction. *Progress in cardiovascular diseases*, 584--594.
- Lymberis, A. a. (2008). Smart fabrics and interactive textile enabling wearable personal applications: R\&D state of the art and future challenges. En *Engineering in Medicine and Biology Society, 2008. EMBS 2008. 30th Annual International Conference of the IEEE* (págs. 5270-5273).
- Madhuri, Madhuri and Gill, Asif Qumer and Khan, Habib Ullah. (2020). IoT-enabled smart child safety digital system architecture. *2020 IEEE 14th International Conference on Semantic Computing (ICSC)* (págs. 166--169). IEEE.
- Maxwell, L and Sanders, A and Skues, J and Wise, L. (2020). A content analysis of personal safety apps: are they keeping us safe or making us more vulnerable? *Violence against women*, 233--248.
- Melendez, O. a. (2020). *Estados Unidos Patente n° US Patent 10,681,201*.
- Michelson, B. M. (2006). Event-driven architecture overview. *Patricia Seybold Group*, 2, 10-1571.
- Michelson, B. M. (2006). Event-driven architecture overview. *Patricia Seybold Group*, 10--1571.
- Mishra, Vinay and Shivankar, Nilesh and Gadpayle, Sanam and Shinde, Sandip and Khan, Mohd Amaan and Zunke, Sonali. (2020). Women's Safety System by Voice Recognition. *2020 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS)* (págs. 1--5). IEEE.
- Mukhopadhyay, Subhas Chandra. (2014). Wearable sensors for human activity monitoring: A review. *IEEE sensors journal*, 15, 1321-1330.
- Nagamma, H. a. (2019). IoT Based Smart Security Gadget for Women's Safety. *2019 1st International Conference on Advances in Information Technology (ICAIT)* (págs. 348-352). IEEE.
- Nakano, K. a. (2017). Effect of dynamic feature for human activity recognition using smartphone sensors. *2017 IEEE 8th International Conference on Awareness Science and Technology (iCAST)* (págs. 539-543). IEEE.
- Ndahimana, D. a.-K. (2017). Measurement methods for physical activity and energy expenditure: a review. *Clinical nutrition research*, 68-80.
- Ojha, Y. (11 de 2018). *medium*. Obtenido de I hacked MiBand 3, and here is how I did it. Part I: <https://medium.com/@yogeshojha/i-hacked-xiaomi-miband-3-and-here-is-how-i-did-it-43d68c272391>
- Oracle, C. (26 de 06 de 2019). *Jersey*. Obtenido de <https://jersey.github.io/>

- Oracle, C. (25 de 06 de 2019). *mysql*. Obtenido de <https://www.mysql.com/>
- Patel, J. a. (2018). Smart bracelets: Towards automating personal safety using wearable smart jewelry. *2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC)* (págs. 1-2). IEEE.
- Picard, R. W. (2010). Affective computing: from laughter to IEEE. *IEEE Transactions on Affective Computing, 1*, 11-17.
- Programa de las Naciones Unidas para el Desarrollo. (15 de abril de 2014). *pnud*. Obtenido de <https://www1.undp.org/content/undp/es/home/librarypage/crisis-prevention-and-recovery/IssueBriefCitizenSecurity.html>
- Rand, J. S. (2002). Acute stress hyperglycemia in cats is associated with struggling and increased concentrations of lactate and norepinephrine. *Journal of veterinary internal medicine, 16*, 123-132.
- Rattanyu, K. a. (2010). Emotion monitoring from physiological signals for service robots in the living space. En *ICCAS 2010* (págs. 580-583). IEEE.
- Richardson S, M. D. (01 de 03 de 2018). *Left to their own devices? Privacy implications of wearable technology in Canadian workplaces*. Obtenido de <http://www.sscqueens.org/publications/left-to-their-own-devices>
- Rodriguez-Rodriguez, I. a.-V.-I.-A. (2018). Variables to be monitored via biomedical sensors for complete type 1 diabetes mellitus management: an extension of the “on-board” concept. *Journal of diabetes research, 2018*.
- Rodriguez-Rodriguez, I. a.-V.-M.-G. (2020). An Autonomous Alarm System for Personal Safety Assurance of Intimate Partner Violence Survivors Based on Passive Continuous Monitoring through Biosensors. *Symmetry, 12*, 460.
- Rodriguez-Rodriguez, Ignacio and Rodriguez, Jose-Victor and Elizondo-Moreno, Aranzazu and Heras-Gonzalez, Purificacion. (2020). An Autonomous Alarm System for Personal Safety Assurance of Intimate Partner Violence Survivors Based on Passive Continuous Monitoring through Biosensors. *Symmetry*, 460.
- Sampson, M. a. (2019). Feasibility of continuous temperature monitoring in pediatric immunocompromised patients: A pilot study. *Pediatric blood & cancer, 66*, e27723.
- Saxena, P. a. (2019). *United States Patente n° US Patent 10,349,227*.
- Severance, C. (2015). Roy T. Fielding: Understanding the REST style. *Computer IEEE, 7-9*.
- Sherwood, A. a. (1990). Hemodynamics of blood pressure responses during active and passive coping. *Psychophysiology, 27*, 656-668.
- SIG, B. (2019). *Bluetooth*. Obtenido de Especificaciones GATT: <https://www.bluetooth.com/specifications/gatt/generic-attributes-overview/>
- Sim, J. K.-H. (2018). Wearable sweat rate sensors for human thermal comfort monitoring. *Scientific reports, 8*, 1-11.
- Singh, M. a. (2016). Performance and evaluation of smartphone based wireless blood pressure monitoring system using Bluetooth. *IEEE Sensors Journal, 16*, 8322-8328.

- SQLite, m. C. (25 de 06 de 2019). *SQLite*. Obtenido de <https://www.sqlite.org/index.html>
- Sumathy, B. a. (2019). Virtual Friendly Device for Women Security. *Journal of Physics: Conference Series* (pág. 012042). IOP Publishing.
- Szwoch, M. (2014). On facial expressions and emotions RGB-D database. *International Conference: Beyond Databases, Architectures and Structures* (págs. 384-394). Springer.
- Tanaka Terukina, R. (2016). Sistema de gestión de fuerza de ventas web y móvil, utilizando el estilo arquitectónico Rest, metodología Scrum y la geolocalización. *Universidad Nacional Mayor de San Marcos*.
- Villa-Mar, K. (Abril de 2020). *Líderes para la gestión en seguridad ciudadana y justicia*. Obtenido de Publications.iadb.org: <https://publications.iadb.org/es/lideres-para-la-gestion-en-seguridad-ciudadana-y-justicia>
- Wioleta, S. (2013). Using physiological signals for emotion recognition. *2013 6th International Conference on Human System Interactions (HSI)* (págs. 556-561). IEEE.
- Wrobel, M. R. (2013). Emotions in the software development process. *2013 6th International Conference on Human System Interactions (HSI)* (págs. 518-523). IEEE.
- Wu, J. a. (2018). Sensor fusion for recognition of activities of daily living. *Sensors*, 18, 4029.
- Ye, L. a. (2018). Physical violence detection with movement sensors. *International Conference on Machine Learning and Intelligent Communications* (págs. 190-197). Springer.
- Zeng, Z. a. (2008). A survey of affect recognition methods: Audio, visual, and spontaneous expressions. *IEEE transactions on pattern analysis and machine intelligence*, 31, 39-58.
- Zhang, T. a. (2014). Bluetooth low energy for wearable sensor-based healthcare systems. *IEEE Healthcare Innovation Conference (HIC)*, 251--254.

## ANEXO N° 01

### ENCUESTA PARA EVALUAR EL SISTEMA DE MONITOREO Y CONTROL PARA LA SEGURIDAD PERSONAL CON DISPOSITIVOS WEARABLES

Con antelación a la aplicación de la encuesta sobre los atributos del sistema de monitoreo y control para la seguridad personal propuesto, se mostró la propuesta y se expuso las fases (actividades, peculiaridades y componentes) a 5 expertos sobre el desarrollo de la aplicación, considerando para ello la experticia en campos que cada uno tiene, relacionados a desarrollo de software y Proyectos similares, para que puedan validar como expertos como tal.

#### PREGUNTAS

Su puntuación puede ser de 0 a 20.

- a) **Conformidad del sistema propuesto:** evalúe las etapas planteadas del sistema propuesto con respecto al nivel de conformidad.

Ítem	Valor
1	Evalué la adaptación del sistema en la etapa de Comodidad de uso del entorno.
2	Evalué la adaptación del sistema en la etapa de Recopilación de los datos.
3	Evalué la adaptación del sistema en la etapa de Pre procesamiento de datos
4	Evalué la adaptación del sistema en la etapa de Tiempo de ejecución de alerta.
5	Evalué la adaptación del sistema en la etapa de Evaluación de resultados.
6	Evalué la adaptación del sistema en la etapa de transmisión de resultados.

Tabla 39. Formato de encuesta al atributo conformidad del sistema.

- b) **Amigabilidad:** evalúe las fases planteadas del sistema propuesto con respecto al nivel de amigabilidad.

Ítem	Valor
1	Evalué la amigabilidad en la etapa de Entendimiento del entorno
2	Evalué la amigabilidad en la etapa de Adquisición de los datos.
3	Evalué la amigabilidad en la etapa de Pre procesamiento de datos.
4	Evalué la amigabilidad en la etapa de Modelamiento.

5	Evalué la amigabilidad en la etapa de Evaluación de resultados.
6	Evalué la amigabilidad en la etapa de Transmisión de resultados.

Tabla 40. Formato de encuesta al atributo amigabilidad del sistema.

- c) **Tiempo de respuesta a un incidente:** evalué las fases planteadas del sistema propuesto con respecto al tiempo de desarrollo, se debe considerar el mayor puntaje a las fases del sistema que generan un menor tiempo de desarrollo.

	<b>Ítem</b>	<b>Valor</b>
1	Evalué el tiempo de desarrollo en la etapa de Entendimiento del entorno.	
2	Evalué el tiempo de desarrollo en la etapa de Adquisición de los datos.	
3	Evalué el tiempo de desarrollo en la etapa de Pre procesamiento de datos.	
4	Evalué el tiempo de desarrollo en la etapa de Modelamiento.	
5	Evalué el tiempo de desarrollo en la etapa de Evaluación de resultados.	
6	Evalué el tiempo de desarrollo en la etapa de transmisión de resultados.	

Tabla 41. Formato de encuesta al atributo tiempo de respuesta a un incidente.

**ANEXO N° 02**  
**RESULTADOS DE LA ENCUESTA PARA EVALUAR EL SISTEMA PROPUESTO**  
**RESUMEN DE RESULTADOS DE LAS ENCUESTAS EFECTUADAS**

<b>ATRIBUTOS DEL SISTEMA</b>	<b>EXPERTOS</b>				
	<b>E1</b>	<b>E2</b>	<b>E3</b>	<b>E4</b>	<b>E5</b>
<b>1. Conformidad</b>					
1. Entendimiento del entorno	14	13	11	14	13
2. Adquisición de los datos	14	14	14	14	13
3. Pre procesamiento de datos	13	13	13	14	14
4. Modelamiento	14	14	14	15	15
5. Evaluación de resultados	15	15	14	15	14
6. Difusión de resultados	16	15	14	13	15
<b>PROMEDIO POR EXPERTO:</b>	<b>14,33</b>	<b>14,00</b>	<b>13,33</b>	<b>14,17</b>	<b>14,00</b>
<b>PROMEDIO TOTAL DE EXPERTOS:</b>	<b>13,97</b>				

Tabla 42. Resultado de encuestas de evaluación del sistema en conformidad.

<b>ATRIBUTOS DEL SISTEMA</b>	<b>EXPERTOS</b>				
	<b>E1</b>	<b>E2</b>	<b>E3</b>	<b>E4</b>	<b>E5</b>
<b>2. Amigabilidad</b>					

1.Entendimiento del entorno	15	13	12	15	14
2.Adquisición de los datos	13	14	15	14	14
3.Pre procesamiento de datos	12	13	13	13	13
4.Modelamiento	14	13	13	14	14
5.Evaluación de resultados	12	14	14	14	14
6.Difusión de resultados	14	13	13	15	14
<b>PROMEDIO POR EXPERTO:</b>	<b>13,33</b>	<b>13,33</b>	<b>13,33</b>	<b>14,17</b>	<b>13,83</b>
<b>PROMEDIO TOTAL DE EXPERTOS:</b>	<b>13,60</b>				

Tabla 43. Resultado de encuestas de evaluación del sistema en amigabilidad.

ATRIBUTOS DEL SISTEMA	EXPERTOS				
<b>3. Tiempo de respuesta</b>	<b>E1</b>	<b>E2</b>	<b>E3</b>	<b>E4</b>	<b>E5</b>
1.Entendimiento del entorno	14	17	16	16	15
2.Adquisición de los datos	14	14	14	13	13
3.Pre procesamiento de datos	14	14	14	13	13
4.Modelamiento	15	15	14	16	14
5.Evaluación de resultados	14	14	13	15	14
6.Difusión de resultados	15	15	14	15	14
<b>PROMEDIO POR EXPERTO:</b>	<b>14,33</b>	<b>14,83</b>	<b>14,17</b>	<b>14,67</b>	<b>13,83</b>
<b>PROMEDIO TOTAL DE EXPERTOS:</b>	<b>14,37</b>				

Tabla 44. Resultado de encuestas de evaluación del sistema en tiempo de respuesta a un incidente

### ANEXO N° 03

#### HERRAMIENTAS Y TECNOLOGÍAS UTILIZADAS.

La siguiente tabla resume las herramientas y tecnologías utilizadas durante el desarrollo del proyecto. El propósito de uso se revela para cada herramienta.

Herramienta	Propósito	URL de fabricante.
mRemoteNG	Cliente SSH para la gestión del servidor.	<a href="https://mremoteng.org/download">https://mremoteng.org/download</a>
WinSCP	Cliente FTP para envío de archivos al servidor.	<a href="https://winscp.net/eng/download.php">https://winscp.net/eng/download.php</a>
Eclipse IDE 2022-06	Creación del servicio Rest.	<a href="https://www.eclipse.org/downloads/">https://www.eclipse.org/downloads/</a>
Post Man	Desarrollo de pruebas del servicio.	<a href="https://www.postman.com/">https://www.postman.com/</a>
Android Studio	Creación de la aplicación móvil.	<a href="https://developer.android.com/studio">https://developer.android.com/studio</a>

GitHub	Repositorio y control de versiones.	<a href="https://github.com/">https://github.com/</a>
Tortoise SVN	Cliente para controlar el repositorio SVN.	<a href="https://tortoisesvn.net/">https://tortoisesvn.net/</a>
Notepad++	Editor ligero para la edición de textos	<a href="https://notepad-plus-plus.org/downloads/v8.4.2/">https://notepad-plus-plus.org/downloads/v8.4.2/</a>
MySQL Workbench 8.0 CE	Gestión y diseño de la base de datos	<a href="https://dev.mysql.com/downloads/installer/">https://dev.mysql.com/downloads/installer/</a>
Microsoft Word 2019	Redacción de la tesis.	<a href="https://products.office.com/es-es/word">https://products.office.com/es-es/word</a>
Enterprise Architect	Creación de diagramas para la tesis.	<a href="https://sparxsystems.com/products/ea/">https://sparxsystems.com/products/ea/</a>
Marvel	Creación de prototipos de las interfaces.	<a href="https://marvelapp.com/">https://marvelapp.com/</a>
Mendeley	Organización de las referencias de la tesis.	<a href="https://www.mendeley.com/">https://www.mendeley.com/</a>

Tabla 45. Herramientas y tecnologías utilizadas