SISTEMA DE SEGURIDAD MEDIANTE DISPOSITIVO DE INTERNET DE LAS COSAS PARA ALERTAS DE PELIGRO A PERSONAS, CONTROL Y MONITOREO DE EVENTOS CRIMINALES, Y MÉTODO GENERAL DE MONITOREO Y ATENCIÓN DE ACTIVIDADES SOSPECHOSAS

CAMPO DE LA INVENCIÓN

La invención en cuestión se ubica, en términos generales, en el ámbito del desarrollo de sistemas electrónicos inteligentes para seguridad personal. En particular, se refiere a invenciones implementadas por computador que se enfocan en la identificación de eventos sospechosos o criminales dirigidos a personas, y en el auxilio y asistencia para la protección de su integridad personal. Además, proporciona a los usuarios la posibilidad de generar alertas e información valiosa sobre ubicaciones geográficas de eventos, asistencia personal en salud, o personas criminales cercanas, notificando para que otras personas y la fuerza pública puedan brindar asistencia, gracias a la información concentrada en una plataforma tecnológica que les permita tomar decisiones oportunas.

ANTECEDENTES DE LA INVENCIÓN

Desde el inicio de la vida en comunidades se tienen referentes del interés y la dedicación de sus integrantes en la preservación de la vida, el cuidado de los componentes de su entorno y de sus bienes.

Una necesidad fundamental de todos los individuos que conforman cualquier sociedad es alcanzar un bienestar permanente derivado de estar y sentirse seguros, que va más allá de lograr la protección de los bienes materiales, pues cada persona busca garantizar su seguridad personal y la de su familia, lo cual abarca la preservación de la integridad física, emocional y psicológica.

En el artículo 8 de la Declaración de los Derechos del Hombre y del Ciudadano (1793), se define la seguridad como “la protección acordada por la sociedad a cada uno de sus miembros para la conservación de su persona, de sus derechos y de sus propiedades”. Así, cada Estado soberano ha tenido dentro de sus funciones la administración de cuatro campos fundamentales de protección de los ciudadanos: la salud, la educación, la seguridad y la justicia (Baracaldo Méndez, 2014).

Para buscar satisfacer la necesidad de seguridad antes mencionada, cada nación y a su vez cada ciudad o región que la conforma propone una legislación que plantea la creación de estrategias para velar por ella y funda instituciones que procuran realizar esa misión. No obstante, es de amplio conocimiento que, por más esfuerzos

que se hagan, los objetivos de protección de los ciudadanos no se logran cumplir cabalmente por parte de los gobiernos, sino que requieren del apoyo de entes privados.

En la República de Colombia, por ejemplo, se promulgó el Decreto 2137 de 1983 con el cual se empezó el reconocimiento de las diferentes formas de vigilancia, lo cual estimuló la conformación de empresas de seguridad privada.

En un contexto donde los índices de delincuencia mantienen una tendencia preocupante, la demanda de soluciones de seguridad personal aumenta constantemente. Las estadísticas muestran que ciertos grupos, especialmente las mujeres, son desproporcionadamente afectados por el secuestro y la violencia intrafamiliar.

Aún a pesar de la existencia de numerosas empresas activas con oferta de seguridad para el cuidado de objetos y propiedades, algunas de ellas ofrecen servicios para cuidar personas a través de escolta personal, lo cual eleva notablemente los costos por ser esquemas tradicionales poco asequibles e incluso inalcanzables para la mayoría de los ciudadanos.

En el año 2002, la Red de Apoyo y Solidaridad Ciudadana (RASCI) fue creada por el Gobierno Nacional con el propósito de enlazar los servicios de vigilancia y seguridad privada con la Policía Nacional, para prevenir y evitar la comisión de delitos. Desafortunadamente, un obstáculo consiste en la comunicación ineficiente entre los actores de la red, la cual está limitada a la mera interacción mediante grupos de mensajería instantánea, que no permite el cumplimiento cabal de los objetivos de la Red.

Aunque las empresas de seguridad privada, las redes de apoyo y solidaridad ciudadana y/o grupos comunitarios, entre otros, existen desde hace más de treinta años en el país, no existe una articulación sólida entre estos y la comunidad que los requiere, siendo entonces inasequibles e insuficientes en lo que respecta al cuidado de las personas.

Ahora bien, como alternativa de solución más eficaz, la apropiación tecnológica se ha extendido a todos los sectores del país incluso en las instituciones del Estado. Por ejemplo, la Policía Nacional de Colombia cuenta con una estrategia para consolidar la arquitectura empresarial como eje de cambio para la transformación digital institucional, la cual se centra en cuatro componentes: consolidación digital, innovación tecnológica, integridad humana y apropiación digital.

Consciente de los desafíos que se presentan en materia de la seguridad ciudadana y teniendo en cuenta los beneficios que brindan las TIC's para atender las problemáticas urbanas y rurales, la Policía Nacional de Colombia ha articulado proyectos con organizaciones internacionales, gubernamentales y locales, para el despliegue de la política de seguridad, defensa, convivencia ciudadana, garantías para la vida y la paz.

Entre las tecnologías utilizadas hasta el momento en el país se encuentran: la biometría dactilar, sistemas de reconocimiento facial, sistemas de reconocimiento de placas de automóviles, gestión de analítica avanzada, mecanismo de interacción ciudadana "APP123", enfoque restaurativo en centros de reclusión y modernización tecnológica del Equipo de Respuesta a Incidentes de Seguridad Informática de la Policía Nacional "CSIRT- PONAL".

La gestión de analítica avanzada tiene como fundamento modelos matemáticos, el procesamiento y análisis de la estadística delincuencial, data del servicio de policía, registros del sistema de medidas correctivas y las llamadas realizadas por los ciudadanos al 123; todo ello para obtener mejoras en la transcripción y el análisis de la información que reporta un ciudadano, además de categorizar el motivo para priorizar el despacho de apoyo y proyectar rutas óptimas de las patrullas cercanas. Con todo lo anterior se busca reducir los tiempos de respuesta al ciudadano y realizar la trazabilidad.

En el caso del aplicativo "APP123", la Policía la ha diseñado para fomentar la interacción ciudadana y cuenta con un botón de pánico que al ser activado genera un ticket directamente en los sistemas de seguimiento de la institución y es cerrado una vez el caso es atendido por funcionarios de la Policía.

Ya en el caso del sector de la seguridad privada, la modernización de servicios es notable pues también avanzan en materia tecnológica. Hoy día sus clientes cuentan con la posibilidad de acceder a: sistemas de vigilancia inteligente con cámaras de alta resolución, análisis de video y tecnología de reconocimiento facial para monitoreo y detección de actividades sospechosas en tiempo real; control de acceso biométrico para la seguridad de lugares críticos, basado en huellas dactilares, reconocimiento de retina y reconocimiento de voz; asistencia de inteligencia artificial para análisis predictivo, analítica de datos y la posibilidad de realizar estudios de prevención de riesgos especializados; drones de monitoreo para mejorar la capacidad de vigilancia y respuesta en terrenos de difícil acceso.

"Prosegur ContiGo" es el nombre que identifica a otra estrategia de seguridad privada la cual protege a una persona que se encuentra fuera de casa. Si la persona

se encuentra en peligro, debe activar un botón SOS en la App “Prosegur Smart” y recibirá ayuda de manera inmediata. La función cuenta atrás se puede activar en los recorridos que el usuario considere necesario para estar pendiente del regreso a casa. Son alarmas de un sistema completo anti-intrusión, anti-inhibición y anti-sabotaje. Está conectada a una central de monitoreo durante las 24 horas del día y ante una intrusión se activa un protocolo y avisa a la Policía.

“Esuclic” es el nombre de otra estrategia privada desarrollada como una iniciativa de la Administración Distrital y la Policía Metropolitana de Medellín en conjunto con la Empresa para la Seguridad y Soluciones Urbanas (ESU). Se trata de la entrega de botones de pánico con el fin de brindar seguridad a los negocios locales. Esta tecnología permite activar un sistema de llamado de alerta, que es enviado a las autoridades, para que estas puedan actuar rápidamente y llegar al lugar en el que se está efectuando el presunto robo. El botón “ESUCLIC” ofrece la opción de enviar una alerta al número de emergencias de la policía 123 o pueden enviar una alerta simultánea a múltiples contactos de emergencia. Permite crear una zona segura con varios usuarios de botones en la comunidad, para generar de esta manera un entorno de confianza. La zona segura busca un trabajo en conjunto para generar tranquilidad en los negocios y en la comunidad mediante botones inteligentes, aplicación móvil, múltiples notificaciones y alarmas comunitarias.

“112 Click” es el nombre que identifica a un proyecto de Wide Tech Development, que es una empresa tecnológica española creada en 2016 con sede en Santander, centrada básicamente en el diseño, desarrollo y comercialización de dispositivos IoT: sensores y localizadores GPS con conectividad para el envío y procesamiento de datos.

Los productos que manejan se engloban en sectores tan diversos como la seguridad personal, agricultura inteligente, seguridad vial y la restauración, donde se aplica la tecnología para lograr beneficios directos a particulares y empresas. “112 Click” está asociado a un dispositivo de alarma sumergible de cuello y a un dispositivo de alarma de muñeca.

“112 Click” es un pulsador de emergencia que, en casos de auxilio, requerimientos médicos o policiales, hace una llamada telefónica de manera automática al servicio de emergencias para recibir asistencia incluso cuando no se puede hablar. Efectúa aviso directamente a los servicios de emergencias oficiales sin intermediarios. Se puede usar como colgante, pulsera, llavero o como pulsador en lugares fijos del hogar, además llama y envía emails simultáneamente a los teléfonos que el usuario decida. Puede localizar a una persona extraviada cuando se supera una cierta distancia del domicilio.

Las tecnologías anteriores cuentan con una plataforma digital para el usuario, la cual posee un botón de pánico con diferentes funciones con el fin de generar tranquilidad y practicidad a las personas que adquieren este servicio. Manejan modelos de negocio por suscripción para vender un producto o servicio a los clientes por el que han de pagar de forma recurrente. Todos cuentan con un sistema de emergencias que efectúa aviso directamente a los servicios de emergencias como la Policía, médicos, seguridad privada propia, entre otros.

A pesar de los intentos por superar los numerosos problemas anteriormente identificados mediante las tecnologías existentes, persiste la necesidad urgente de contar con nuevas tecnologías eficaces, versátiles y seguras que realmente sean adecuadas para garantizar completamente la seguridad de los ciudadanos mediante tiempos de reacción mínimos. Esta circunstancia motivó la investigación y el desarrollo exitoso de la presente invención.

Esta invención soluciona la escasa articulación entre una alta demanda en materia de seguridad y/o cuidado personal y una oferta existente limitada desde hace ya muchos años, como lo que ofrecen las empresas de seguridad privada; además, soluciona la ineficiente interacción de las redes de apoyo y solidaridad ciudadana, y asociaciones comunitarias independientes.

La invención mejora la seguridad personal porque ofrece a los individuos una herramienta que les permite gestionar su seguridad personal con mayor control y eficacia al combinar una aplicación para dispositivos móviles con instrucciones implementadas por un procesador, con un dispositivo IoT físico para ofrecer una solución integral y accesible que responde a diversas situaciones de emergencia como: violencia intrafamiliar, robo, violencia general, acoso, extorsión y secuestro, riesgo en la vía, paquete abandonado, persona sospechosa, accidente de tránsito, o denuncia, asistencia de salud a personas que lo requieren. Dada la creciente necesidad de soluciones de seguridad personalizadas y de fácil acceso, esta invención surge como una propuesta tecnológicamente avanzada y socialmente necesaria.

Al considerar un análisis comparativo detallado entre la presente invención y otros productos del estado de la técnica, con la invención se alcanzan características únicas y ventajas competitivas como las siguientes:

Conectividad Independiente, pues a diferencia de muchos dispositivos de seguridad personal que requieren estar emparejados constantemente con un smartphone a través de Bluetooth, la invención incluye su propia conectividad 4G-5G-6G-7G. Esto

proporciona una gran ventaja, ya que permite la funcionalidad completa del dispositivo incluso si el smartphone está apagado, fuera de alcance o dañado, una situación común en casos de emergencia como robos o secuestros.

Alertas Silenciosas, pues mientras que algunos dispositivos ofrecen la opción de enviar alertas a contactos o autoridades, la invención permite enviar una alerta silenciosa mediante la presión de un botón, lo cual es vital en situaciones donde el usuario necesita mantener discreción para evitar agravar una situación de peligro.

Capacidades de localización mejoradas, pues el uso de tecnología de georreferencia como GPS avanzada en la invención asegura la precisión en la localización del usuario. Esto es superior a las aplicaciones que dependen únicamente del GPS del teléfono, que puede ser menos preciso o incluso inaccesible si el teléfono está apagado.

Funcionalidades Biométricas, pues por medio de lector de huella digital y de iris, distingue a la invención de la mayoría de los dispositivos convencionales. Estas tecnologías no solo mejoran la seguridad del dispositivo, sino que también facilitan la identificación rápida y precisa del usuario en situaciones críticas.

Todas las características antedichas aseguran que la invención no solo es una mejora técnica sobre las soluciones existentes sino también una herramienta crucial para mejorar de manera revolucionaria la seguridad en la sociedad moderna.

OBJETO DE LA INVENCIÓN

El objeto de la invención consiste en proporcionar un sistema y un método especializado en la seguridad de las personas para garantizar su integridad, que permita notificar a la fuerza pública y a otras personas cercanas de los eventos criminales que se alerten, todo ello para poder brindar ayuda a quienes puedan estar en riesgo de robo y/o ataque.

Otro objeto de la invención es proporcionar el sistema especializado en la seguridad de las personas mediante un dispositivo independiente, o como un accesorio que se interconecta con un dispositivo móvil.

Otro objeto de la invención es permitir a los usuarios alimentar y acceder a una base de datos de información, que les ayude en el rastreo de su seguridad personal, identificar eventos que estén sucediendo en tiempo real, u obtener estadísticas de las zonas con mayor problemática de seguridad.

Otro objetivo de la invención es contar con una aplicación con instrucciones ejecutadas por un procesador para dispositivos móviles interconectados con un hardware que sea capaz de registrar los eventos de un usuario que pide algún tipo de asistencia o ayuda.

Otro objeto de la invención es desarrollar una integración sinérgica de elementos de hardware y de instrucciones ejecutadas por un procesador, para contar con una herramienta que permita a los usuarios garantizar su asistencia en caso de alguna eventualidad que consideren esté atentando contra su vida, para generar las alertas necesarias y así recibir una atención pronta y oportuna, asegurando que los usuarios tengan la capacidad de alertar a las autoridades o a un equipo de respuesta que pueda atender la eventualidad en menos de tres minutos.

Otro objeto de la invención es proporcionar un sistema que logre la protección de las mujeres contra todo tipo de acoso, máxime la avalancha de denuncias que gracias a las redes sociales se han podido visibilizar. Al enfocarse en la seguridad de las mujeres, que son afectadas por ciertos tipos de violencia, la presente invención contribuye significativamente a la seguridad y empoderamiento femenino mediante la disponibilidad de botones de alerta: botón de prueba, botón de acoso sexual, botón de violencia intrafamiliar, botón de robo o atraco y botón de accidente.

Otro objeto de la invención es proporcionar una solución eficaz contra la desaparición involuntaria y contra la desaparición forzosa. La primera, como consecuencia de enfermedades neurológicas o psicológicas y la segunda, por rapto o secuestro.

Otro objeto de la invención es proporcionar un sistema que logre asistencia personal a turistas mediante guía turística y respaldo eficaz en materia de salud y seguridad para contar con apoyo inmediato e información veraz a través de la red del sistema. El usuario de la aplicación puede filtrar zonas turísticas seguras y tener información validada de las ofertas culturales, gastronómicas, de entretenimiento y atractivos relevantes de dichas zonas, también con acceso a promociones y descuentos de los comercios aliados y de promotores de eventos en las respectivas ciudades y zonas geográficas que visite.

Otro objeto de la invención es proporcionar una invención de impacto masivo que beneficie asociaciones como organismos gubernamentales, ONG’s y empresas privadas interesadas en mejorar la seguridad de sus miembros.

BREVE DESCRIPCIÓN DE LAS FIGURAS

La presente invención se entenderá de mejor manera con referencia a las figuras.

En las figuras que acompañan este documento se ilustra, a modo de ejemplo, una realización del sistema, los aparatos, y el método de la invención, pero sin limitar su alcance. En tales figuras, los códigos de referencia indican elementos idénticos o similares.

La figura 1 corresponde a la vista general del sistema con todos los subsistemas y dispositivos interconectados.

La figura 2 presenta a una vista superior e inferior del dispositivo de internet de las cosas IoT que forma parte del sistema de la invención y que emplean los usuarios para generar las alertas de peligro.

La figura 3 corresponde a una vista general del dispositivo de internet de las cosas que es independiente del dispositivo móvil que tiene la aplicación de instrucciones ejecutadas por un ordenador. En la figura se muestra la interconexión entre el dispositivo IoT y la aplicación de un celular inteligente o una tableta.

La figura 4 corresponde a las vistas laterales del dispositivo IoT que forma parte del sistema inventado. De izquierda a derecha está la vista lateral izquierda, en el medio la vista lateral derecha y al lado derecho la vista lateral derecha con separación lateral.

La figura 5 corresponde a una vista del dispositivo de internet de las cosas IoT que se integra con el dispositivo móvil que tiene la aplicación de instrucciones ejecutadas por un ordenador. Al lado izquierdo la aplicación a una tableta y al lado derecho a un celular inteligente.

La figura 6 corresponde a una vista en explosión del dispositivo IoT que forma parte del sistema inventado con los dispositivos de hardware que se interconectan interna y externamente.

La figura 7 presenta a una vista en explosión del dispositivo IoT con los dispositivos de hardware electrónicos que se interconectan internamente.

La figura 8 ilustra una toma de una de las pantallas de la plataforma de monitoreo del sistema de la invención.

La figura 9 presenta un diagrama general del método de funcionamiento del sistema de la invención.

La figura 10 presenta el diagrama detallado del método de funcionamiento del sistema de la invención.

LISTADO DE ELEMENTOS DE LA INVENCIÓN

El siguiente listado corresponde al conjunto de elementos que hacen parte de la presente invención. Al frente de cada elemento se indica el código de referencia incluido en el juego de figuras para su fácil identificación.

Sistema de seguridad mediante dispositivo de internet de las cosas para alertas de peligro a personas	1000
Servidor web de aplicación	1010
Servidor web de aplicación redundante	1011
Plataforma de monitoreo de alertas	1020
Servidor de base de datos para almacenamiento de información del sistema	1030
Servidor de base de datos de redundancia	1031
Red de intercomunicación	1040
Internet	1041
Dispositivo de comunicación inteligente del usuario de generación de alertas	1050
Dispositivo de comunicación inteligente de monitoreo de alarmas	1060
Estación de monitoreo de alertas	1061
Dron de monitoreo y asistencia	1070
Dispositivo de comunicación inteligente de la fuerza pública para monitoreo de alertas	1080
Dispositivo intercomunicador celular IoT	2000
Carcasa de cubrimiento inferior	2001
Batería	2002
Antena sistema georreferencia	2003
Sistema de georreferencia	2004
Sistema lector de tarjeta SIM	2005
Sistema de procesamiento	2006
Altavoz	2007
Contacto magnético	2008
Pulsador	2009
Sensor de efecto hall	2010
Resistencias	2011

Sistema amplificador	2012
Amplificador operacional	2013
Board	2014
Lector biométrico de huella	2015
Lector del iris	2016
Proyector holográfico	2017
Placa	2018
Puerto de entrada para tarjeta SIM	2019
Carcasa de cubrimiento superior	2020
Dispositivo IoT de generación de alertas de tipo conexión	3000
Conector USB del Dispositivo IoT de generación de alertas de tipo conexión	3010

BREVE DESCRIPCIÓN DE LA INVENCIÓN

La presente invención a la que se hace referencia consiste en una invención implementada por computador que corresponde a la integración entre una aplicación móvil de instrucciones ejecutadas por un procesador instalada en un dispositivo físico IoT de hardware que proporciona una herramienta robusta y discreta para la gestión de emergencias personales. La invención implementada por computador permite a los usuarios enviar alertas de emergencia a una central de respuesta notablemente rápida y a contactos personales, garantizando una reacción inmediata en situaciones críticas.

El dispositivo físico IoT de hardware que forma parte de la invención es un componente que funciona de manera autónoma o en conjunto con la aplicación móvil de instrucciones ejecutadas por un procesador, permitiendo a los usuarios enviar alertas incluso sin necesidad de acceso a su teléfono móvil. Este dispositivo está equipado con un botón de emergencia que al ser presionado por el propietario envía su ubicación de manera altamente precisa mediante diferentes tecnologías, una de ellas, la de georreferencia, por ejemplo, utilizando una conexión de datos móviles a través de diferentes tecnologías.

Este sistema en conjunto de hardware y la aplicación móvil de instrucciones ejecutadas por un procesador emplea comandos para identificar señales que emiten los usuarios del dispositivo de hardware, en lo que se podría clasificar como sistemas o aparatos de internet de las cosas (IOT). El sistema, junto con sus mecanismos interconectados, permite enviar y capturar señales de peligro que emiten los usuarios del dispositivo IoT. De esta forma, se identifica momentos o acciones de peligro, como asaltos, persecuciones, hostigamiento o cualquier evento

que atente contra la seguridad personal, que podría representar amenazas en ocasiones contra la integridad y la vida.

El sistema está integrado por una plataforma web, una central web de monitoreo y dos aplicaciones móviles que incorporan instrucciones ejecutadas por un procesador así: una aplicación que incorporan instrucciones ejecutadas por un procesador para usuarios y/o clientes, una aplicación que incorporan instrucciones ejecutadas por un procesador para la red de aliados y reacción, y un dispositivo intercomunicador celular IoT que hace y recibe llamadas en tiempo real al igual que emite alarmas silenciosas a la central de monitoreo.

Estos componentes facilitan la integración de personas de la comunidad, y les permite que se conecten con una red de apoyo solidario que les asistirá ante cualquier incidente, brindándoles una percepción de seguridad para que puedan disfrutar de sus entornos con tranquilidad y confianza al tener conexión e interacción 24/7, en tiempo real.

El sistema también realiza una trazabilidad completa de los eventos y envía señales a grupos de apoyo que puedan asistir a las personas que notifican algunos eventos sospechosos o criminales.

DESCRIPCIÓN DETALLADA DE LA INVENCIÓN

Esta divulgación corresponde a la explicación detallada de algunas de las modalidades de la invención y no implica la limitación del alcance de la invención definida en las reivindicaciones.

Para una comprensión más completa de la presente invención, ahora se hace referencia a la siguiente descripción de un modo ilustrativo y no limitativo de la misma, tomada en conjunto con los dibujos acompañantes en los cuales los números de referencia indican elementos idénticos o semejantes en los dibujos correspondientes.

Con el propósito de facilitar la comprensión de la invención, es necesario precisar los siguientes términos y expresiones a fin de interpretar las interacciones en el ecosistema:

La expresión *“grupo de reacción voluntaria y/o red de aliados y reacción”* hace referencia a la persona natural o jurídica (aliado de reacción) que voluntaria y solidariamente hace parte de este grupo, el cual está compuesto por redes de apoyo ciudadano, policía, fuerzas militares, organismos de socorro, taxistas, empresas de

seguridad, plataformas de transporte, vigilantes independientes, gestores de paz y convivencia ciudadana, empleados de establecimientos comerciales de la zona, lideres de reacción y los usuarios que utilizan el servicio, es decir, suscriptores.

La expresión *"líder de zona"* hace referencia al encargado o responsable de reaccionar entre 1 y 3 minutos a los llamados de alerta en su respectiva área asignada. Un área asignada dependiendo de su tamaño y densidad de número de usuarios y aliados disponibles a reaccionar puede tener uno o varios lideres de zona.

La expresión *"líder de servicio"* hace referencia a la persona que recibe las peticiones y asistencia y las clasifica según el tipo de alerta, se las delega o asigna al respectivo líder de zona y le hace el seguimiento hasta la conclusión y cierre del respectivo caso. Este líder de servicio puede tener varios lideres de zona a su cargo.

El término *"usuario y/o suscriptor"* hace referencia a una persona natural o jurídica, que accede a los servicios de la plataforma por medio de una suscripción mensual y/o anual personal e intransferible. Estos usuarios a través de una suscripción descargan la aplicación que incorpora instrucciones ejecutadas por ordenador en su dispositivo móvil celular.

El término *"plataforma"* hace referencia a la plataforma virtual compuesta por una aplicación que incorpora instrucciones ejecutadas por ordenador para usuarios y una aplicación que incorpora instrucciones ejecutadas por ordenador para la red de aliados y/o grupo de reacción voluntaria, ambas para dispositivos móviles en los sistemas operativos Android y iOS, y una central web por medio de la cual los aliados de reacción voluntaria y los suscriptores interactúan y acceden a los servicios adquiridos.

La expresión *"intercomunicador celular"* o *"botón de pánico"* hace referencia a un dispositivo móvil (hardware) con conectividad independiente a través de una tarjeta SIM cargada con plan de datos y minutos, el cual permite que su portador sea geolocalizado y georreferenciado (monitoreado) 24/7 de manera confidencial. Además, le permite al usuario suscriptor realizar y recibir llamadas, y enviar alertas silenciosas a la central.

El término *"suscripción"* hace referencia al servicio adquirido por un usuario, el cual lo convierte en suscriptor, por un determinado periodo de tiempo y por un valor establecido por ese periodo de tiempo.

La expresión *“círculo de vida”* hace referencia al número de personas que elige cada usuario como contacto de emergencia para ser notificados ante un incidente del mismo. Esta elección se realiza al momento de adquirir la suscripción y el número de contactos de emergencia varía de acuerdo con el tipo de suscripción adquirida por el usuario.

La expresión *“zona segura”* hace referencia a la delimitación por perímetro de un área en la cual se prioriza la seguridad de la comunidad que la habita o frecuenta, por medio de la designación de roles a cada uno de los actores de la misma, los cuales se ayudan y protegen entre sí de manera voluntaria. Comunidad integrada, seguridad manifiesta.

La expresión *“comunidades seguras”* hace referencia a la segmentación de comunidades que comparten afinidad de características, como género, gustos, vecindad, comercio, entretenimiento, entornos laborales, entre otros.

El término *“aliados”* hace referencia a una persona natural o jurídica que, de manera libre y solidaria, reacciona a voluntad a una petición de auxilio, socorro, ayuda y/ o apoyo solicitado por un usuario o suscriptor que hace parte de la comunidad.

La expresión *“datos personales”* hace referencia a toda información que permite identificar o hacer identificable a una persona natural.

El término *“titular”* corresponde a una persona natural cuyos datos personales son objeto de tratamiento.

El término *“tratamiento”* hace referencia a cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

La expresión *“suscriptor establecimiento”* hace referencia a una persona natural o jurídica que adquiera los servicios de la plataforma para su negocio o establecimiento de comercio, para beneficio propio o colectivo a sus clientes.

La expresión *“zona patrocinada”* hace referencia a la delimitación por perímetro de un área en la cual los usuarios que la habitan o frecuentan pueden descargar la aplicación de manera gratuita por medio de un código QR provisto por un patrocinador público o privado, mediante la obtención de una macro licencia de uso.

La expresión *“aliado comercial”* hace referencia a una persona natural o jurídica que ofrece, y comercializa sus productos y/o servicios a través de la plataforma, para que los mismos sean adquiridos por los suscriptores.

La expresión *“entornos seguros”* se define como el espacio determinado por ciertas características que lo delimitan haciéndolo diferente a otro. Cada entorno seguro se compone a su vez de *“zonas seguras”* que corresponde a la delimitación por perímetro de un área en la cual se prioriza la seguridad de la comunidad que la habita o frecuenta, por medio de la designación de roles a cada uno de los actores de esta, los cuales se ayudan y protegen entre sí de manera voluntaria. Estas *“zonas seguras”* pueden ser hoteles, sitios turísticos, centros comerciales, transporte, parques, entre otras.

Ahora bien, en términos generales, se listan y describen los componentes y funcionalidades principales del sistema de seguridad mediante dispositivo de internet de las cosas para alertas de peligro a personas (1000):

-Módulo de georreferencia. Puede emplear diferentes tecnologías como GPS, y este componente es crucial ya que permite la transmisión precisa de la ubicación geográfica del usuario en tiempo real. La capacidad de enviar coordenadas de latitud y longitud en intervalos regulares o al activarse mediante el botón central asegura que los servicios de emergencia puedan localizar rápidamente al usuario.

-Conexión de datos celular. Por medio de una tarjeta SIM y la conectividad (4G-5G-6G-7G), garantizan que el dispositivo pueda enviar alertas y ubicaciones a través de la red móvil o satelital, asegurando cobertura en amplias zonas geográficas.

-Procesamiento. Por medio de un procesador o microcontrolador, este componente dirige todas las operaciones internas del dispositivo, desde la gestión de la entrada de datos hasta la comunicación con la red celular y la ejecución de instrucciones que es capaz de procesar y que son emitidos por los usuarios.

-Componentes de comunicación y alerta. El dispositivo incluye un altavoz y un sistema de alerta silenciosa, que puede activarse sin generar ruido audible, informando discretamente a los agentes de respuesta sobre una emergencia.

-Reconocimiento biométrico. Mediante lector de huellas digitales y un lector de iris para mejorar la seguridad mediante la verificación biométrica del usuario.

-Interactividad. Se contempla la incorporación de un módulo holográfico para funcionalidades interactivas avanzadas.

-Energía. Equipado con una batería de 900 mAh, el dispositivo ofrece hasta dos días de autonomía, permitiendo a los usuarios permanecer protegidos sin preocuparse por la recarga continua.

-Instrucciones ejecutadas por un procesador de un celular inteligente o una tableta, A estas instrucciones se interconecta el dispositivo IoT funcionando como el complemento digital del dispositivo físico. Proporciona una interfaz usuario-centrada para la gestión de alertas y la comunicación con la red de respuesta a emergencias.

Subsistemas

De acuerdo con la **figura 1**, el sistema de seguridad mediante dispositivo de internet de las cosas para alertas de peligro a personas (1000) está conformado por un conjunto se subsistemas que son: un subsistema de almacenamiento y publicación de información de alertas en una plataforma de monitoreo web interconectada con un subsistema de generación y verificación de alertas, con un subsistema de monitoreo, con una red de intercomunicación (1040), y con internet (1041).

A continuación, se especifican los subsistemas que forman parte del sistema (1000), interconectados entre sí para lograr el efecto deseado de la invención integral aportando una funcionalidad específica:

Subsistema de almacenamiento y publicación de información de alertas

Este subsistema se encarga de la recepción de la información de alertas y la publicación de la información a través de la plataforma de monitoreo.

El subsistema incorpora los siguientes componentes: uno o varios servidores web de aplicación (1010) interconectados con uno o varios servidores web de aplicación redundante (1011); y ambos a su vez interconectados con la plataforma de monitoreo de alertas (1020); y con uno o varios servidores de base de datos para almacenamiento de información del sistema (1030) y también con servidores de base de datos de redundancia (1031) a través de una red de intercomunicación (1040) e internet (1041).

Subsistema de generación y verificación de alertas

Este subsistema es el encargado de generar y recibir las señales de alertas de las personas o usuarios de la plataforma, así como las que pueden generar personal civil o fuerzas militares desde sus dispositivos.

Este subsistema integra las siguientes partes: uno o varios dispositivos de comunicación inteligente del usuario de generación de alertas (1050); uno o varios dispositivos de comunicación inteligente de monitoreo de alarmas (1060); uno o varios drones de monitoreo y asistencia (1070); uno o varios dispositivos de comunicación inteligente de la fuerza pública para monitoreo de alertas (1080); uno o varios dispositivos intercomunicadores celular IoT (2000); y uno o varios dispositivos IoT de generación de alertas de tipo conexión (3000).

Subsistema de monitoreo

Este subsistema es el encargado de permitir identificar, rastrear y monitorear los eventos criminales notificados por los usuarios de la plataforma, para enviar notificaciones y alertas de ayuda a los grupos civiles y de fuerza pública para brindar apoyo a la víctima del evento. Este subsistema integra el siguiente componente mencionados anteriormente:

- Estación de monitoreo de alertas (1061)

Modalidades

Las modalidades preferidas que puede tener el sistema (1000) de acuerdo con una configuración e interconexión de componentes son los siguientes:

- Sistema donde el dispositivo intercomunicador celular IoT que forma parte de este, es un dispositivo independiente y se encuentra interconectado con la plataforma Web.

- Sistema donde el dispositivo intercomunicador celular IoT que forma parte de este, es una carcasa que se adapta al dispositivo donde está la plataforma Web de manera inalámbrica.

- Sistema donde el dispositivo intercomunicador celular IoT es una carcasa que se adapta al dispositivo donde está la plataforma Web a través de uno de sus puertos de manera física.

Descripción de elementos esenciales del sistema (1000)

A continuación, y en concordancia con las **figuras 1 a 7**, se realiza una descripción aún más específica de cada uno de los elementos esenciales que forman parte del sistema de seguridad mediante dispositivo de internet de las cosas para alertas de peligro a personas (1000):

Servidor web de aplicación

El servidor web de aplicación (1010) es una infraestructura de hardware que integra una plataforma con las instrucciones destinadas a ser ejecutadas por un ordenador. Este servidor facilita la interacción entre los usuarios finales y el código de la aplicación del lado del servidor, procesando las solicitudes de los usuarios. Su función principal es generar y proporcionar contenido dinámico, como resultados de transacciones, soporte para la toma de decisiones o análisis en tiempo real. Estos servidores pueden ser físicos o en servicios de computación en nube.

Servidor web de aplicación redundante

El servidor web de aplicación redundante (1011) presenta la misma definición del servidor web de aplicación (1010), pero su función es ser un soporte redundante de la aplicación para que esté disponible en caso de fallo del principal. Estos servidores pueden ser físicos o en servicios de computación en nube.

Plataforma de monitoreo de alertas

La plataforma de monitoreo de alertas (1020) es un conjunto de herramientas y tecnologías que promueven la interacción de los usuarios, la colaboración y la ejecución de tareas en línea. Además, estas herramientas gestionan toda la información que circula dentro del sistema de seguridad mediante dispositivo de internet de las cosas para alertas de peligro a personas (1000).

Servidor de base de datos para almacenamiento de información del sistema

El servidor de base de datos para almacenamiento de información (1030) de todo el sistema de seguridad mediante dispositivo de internet de las cosas para alertas de peligro a personas (1000), es un equipo con instrucciones ejecutadas por un procesador que proporciona servicios de base de datos a otros programas o computadoras, organizando, almacenando y gestionando toda la información mediante tablas, índices y registros de todo el sistema. Estos motores de bases de datos pueden tener soporte SQL, o NoSQL, o ser distribuidos con tecnología BlockChain para garantizar la integridad de la información.

Servidor de base de datos de redundancia

El servidor de base de datos de redundancia (1031) tiene la misma definición que el servidor de base de datos para almacenamiento de información del sistema

(1030) y sirve como soporte en caso de falla del principal para que continúe almacenando la información del sistema. Estos motores de bases de datos pueden tener soporte SQL, o NoSQL, o ser distribuidos con tecnología BlockChain para garantizar la integridad de la información.

Red de intercomunicación

La red de intercomunicación (1040) es un conjunto de dispositivos electrónicos de hardware con instrucciones ejecutadas por un procesador que están interconectados para compartir e intercambiar información, datos, archivos, recursos y servicios. Esta interconexión puede establecerse a través de medios físicos o inalámbricos.

En una de las modalidades de la invención, la red de interconexión puede ser internet o redes de área local (LAN), redes de área amplia (WAN), redes de área metropolitana (MAN), así como protocolos de conexión inalámbrica como WIFI.

Internet

Internet (1041) es una red de computadoras que se encuentran interconectadas a nivel mundial para compartir información. Se trata de una red de equipos de hardware con instrucciones ejecutadas por un procesador que se relacionan entre sí a través de la utilización de un protocolo de redes de comunicaciones.

Dispositivo de comunicación inteligente del usuario de generación de alertas

El dispositivo de comunicación inteligente del usuario de generación de alertas (1050) corresponde a al menos un celular inteligente o tableta del usuario, donde se encuentran instaladas las instrucciones ejecutadas por un procesador que se interconecta con la plataforma de monitoreo de alertas (1020) para enviar algún evento sospechoso al emplear el dispositivo intercomunicador celular IoT (2000).

El dispositivo de comunicación inteligente de monitoreo de alarmas (1060) Sistemas o teléfonos celulares inteligentes o tabletas de los líderes de zona, líderes de servicio, círculo vital o central que se interconecta con la plataforma de monitoreo de alertas (1020) para identificar algún evento sospechoso que registra el usuario o cliente, al emplear el dispositivo intercomunicador celular IoT (2000).

Estación de monitoreo de alertas

La estación de monitoreo de alertas (1061) corresponde a sistemas y aparatos de una central interconectados con la plataforma de monitoreo de alertas (1020) para identificar algún evento sospechoso que registra el usuario o cliente, al emplear el dispositivo intercomunicador celular IoT (2000).

Dron de monitoreo y asistencia

El dron de monitoreo y asistencia (1070) consiste en al menos un sistema de hardware e instrucciones ejecutadas por un procesador que actúa como aeronave no tripulada y que se puede controlar a distancia. Se utiliza en este sistema para tareas como vigilancia, filmación aérea, búsqueda y rescate, y reparto de mercaderías.

Los drones de monitoreo y asistencia (1070) envían la información de alerta a través de la red de intercomunicación (1040) e internet (1041) a los servidores web de aplicación (1010) y a los servidores web de aplicación redundante (1011) para registrarla en la plataforma de monitoreo de alertas (1020) gracias al almacenamiento en los servidores de base de datos para almacenamiento de información del sistema (1030) y los servidores de bases de datos de redundancia (1031).

Dispositivo de comunicación inteligente de la fuerza pública para monitoreo de alertas

Un dispositivo de comunicación inteligente de la fuerza pública para monitoreo de alertas (1080) consiste en al menos un sistema, teléfono celular inteligente o tableta de la fuerza pública que se interconecta con la plataforma de monitoreo de alertas (1020) para monitorear algún evento sospechoso que registra el usuario o cliente, al emplear el dispositivo intercomunicador celular IoT (2000).

Dispositivo intercomunicador celular IoT

Un dispositivo intercomunicador celular IoT (2000) es un sistema electrónico inteligente IoT (internet de las cosas). Es un objeto físico conectado a internet, con la capacidad de comunicarse con otros objetos IoT o sistemas mediante la transmisión de datos. Ejemplos de estos dispositivos pueden ser objetos cotidianos como bombillas de luz, dispositivos médicos, ropa y accesorios personales inteligentes, e incluso sistemas de ciudades inteligentes.

Estos sistemas electrónicos pueden combinar también las funciones de un teléfono móvil y una computadora en una sola unidad. El dispositivo IoT de la presente invención es configurado a partir de una tecnología con la capacidad de enviar las alertas que emiten los usuarios frente a alguna situación de peligro.

El dispositivo de hardware IoT de la presente invención es un sistema fundamental, diseñado para operar tanto de manera independiente como en conjunto con la aplicación que incorpora instrucciones ejecutadas por ordenador móvil.

El dispositivo intercomunicador celular IoT (2000) incorpora los siguientes componentes e interconexiones: carcasa metálica de cubrimiento inferior (2001) a la que se interconecta la board (2014) a la que se interconectan los siguientes dispositivos: la batería ion litio (2002); la antena sistema georreferencia (2003); el sistema de georreferencia (2004); el sistema lector de tarjeta SIM (2005); el sistema de procesamiento (2006); el altavoz (2007); el contacto magnético (2008); el pulsador (2009); el sensor de efecto hall (2010); las resistencias (2011); el sistema amplificador (2012); el amplificador operacional (2013); el lector biométrico de huella (2015); el lector del iris (2016); el proyector holográfico (2017); y la placa (2018); y el puerto de entrada para tarjeta SIM (2019). Todas las partes mencionadas protegidos por el cubrimiento de la carcasa de cubrimiento superior (2020) que encaja con la carcasa metálica de cubrimiento inferior (2001).

En una modalidad preferida, el dispositivo intercomunicador celular IoT (2000) es alimentado con una fuente de energía que brinda 5 voltios DC y suministra energía a todos los componentes.

Carcasa de cubrimiento inferior

La carcasa de cubrimiento inferior (2001) es preferiblemente un recubrimiento de naturaleza metálica a manera de tapa del dispositivo, al cual va interconectado el hardware interno del sistema, sus sistemas, dispositivos electrónicos y subcomponentes.

Batería

La batería (2002) es un dispositivo para almacenamiento de energía que suministra al sistema, como el hardware electrónico, para que pueda realizar su funcionamiento el dispositivo intercomunicador celular IoT (2000). En modalidades preferidas de la invención, la batería (2002) es ion litio.

Antena sistema georreferencia

Una antena sistema georreferencia (2003) es un componente utilizado en sistemas de posicionamiento global (GPS) y otros sistemas de navegación para recibir señales de satélites y determinar la ubicación precisa de un dispositivo o receptor en una ubicación geográfica de la Tierra

Sistema de georreferencia

El sistema de georreferencia (2004) implica la técnica de posicionamiento espacial de una entidad en una localización geográfica única y bien definida en un sistema de coordenadas y datum específicos. Se utiliza en sistemas de información geográfica (SIG) para determinar las ubicaciones de objetos

Sistema lector de tarjeta SIM

El sistema lector de tarjeta SIM (2005) es un sistema lector de tarjetas SIM (*Subscriber Identity Module*), correspondientes a una tarjeta inteligente removible utilizada en teléfonos móviles y módems, que contiene un chip que almacena de manera segura la clave de servicio del suscriptor, permitiendo la identificación en la red y el cambio de dispositivo.

Sistema de procesamiento

El sistema de procesamiento (2006) es un microcontrolador o microprocesador que interpreta y entiende las instrucciones de aplicaciones o programas informáticos que se ejecutan dentro de un sistema operativo.

Altavoz

Un altavoz (2007) es un dispositivo que convierte la corriente eléctrica en ondas sonoras. También conocido como parlante o bocina, el altavoz (2007) es un transductor eléctrico que transforma la energía eléctrica en una onda acústica. Su función es amplificar y reproducir el sonido de manera audible para los seres humanos.

Contacto magnético

El contacto magnético (2008) es un dispositivo capaz de detectar señales electromagnéticas y responder en consecuencia. Estos aparatos pueden

transformar las magnitudes físicas o químicas en magnitudes eléctricas y puede responder en consecuencia.

Pulsador

El pulsador (2009) es un elemento mecánico que emplea el usuario y que al presionarlo es capaz de notificar alguna alerta.

Sensor de efecto hall

El sensor de efecto Hall (2010) se basa en el efecto Hall para medir campos magnéticos o corrientes. Al aplicarse corriente a este sensor y acercarse a un campo magnético, genera un voltaje proporcional al producto de la fuerza del campo magnético y la corriente.

Resistencias

La resistencia eléctrica (2011) es un dispositivo convencional que se opone al paso de la corriente eléctrica a través de un material o sustancia.

Sistema amplificador

El sistema amplificador (2012) es un sistema que incorpora al menos un dispositivo circuito electrónico amplificador operacional (2013).

Amplificador operacional

El amplificador operacional (2013) es un circuito electrónico integrado activo diseñado para realizar con las señales eléctricas operaciones matemáticas como suma, resta, multiplicación, división, diferenciación, integración, etc. Los amplificadores operacionales (2013) pueden ser configurados de muchas maneras diferentes, como amplificadores inversores, no inversores, seguidores de voltaje, comparadores, sumadores, integradores, entre otros.

Board

La board (2014) es la tarjeta madre o principal de un aparato donde se interconectan los componentes y dispositivos electrónicos fundamentales de un sistema

Lector biométrico de huella

El lector biométrico de huella (2015) es el sistema de hardware e instrucciones ejecutadas por procesador que reconoce la huella dactilar de un humano y la diferencia del resto de personas.

Lector del iris

El lector de iris (2016) es el sistema de hardware e instrucciones ejecutadas por procesador que reconoce el iris del ojo de un humano y la diferencia del resto de personas.

Proyector holográfico

El proyector holográfico (2017) es el sistema de hardware e instrucciones ejecutadas por procesador que proyecta imágenes en medios como el aire o cualquier superficie.

Placa

La placa (2018) es la superficie donde se fijan e interconectan los dispositivos electrónicos. En modalidades preferidas, es una placa de naturaleza metálica.

Puerto de entrada para tarjeta SIM

El puerto de entrada para tarjeta SIM (2019) es una ranura de entrada donde se inserta la tarjeta SIM y queda interconectado con la board (2014) y la placa (2018).

Carcasa de cubrimiento superior

La carcasa de cubrimiento superior (2020) es una tapa, que en modalidades preferidas es metálica, empleada para cubrir el dispositivo intercomunicador celular IoT (2000) desde la parte superior.

El dispositivo intercomunicador celular IoT (2000) incorpora una carcasa de cubrimiento inferior (2001) que encaja con la carcasa de cubrimiento superior (2020), y en esta última se encuentra el orificio por el que sobresale el pulsador (2009) y el orificio de acceso para el puerto de entrada para tarjeta SIM (2019) en el que ingresa una tarjeta con acceso a datos móviles.

Dispositivo IoT de generación de alertas de tipo conexión

Un dispositivo IoT de generación de alertas de tipo conexión (3000) es una modalidad del dispositivo intercomunicador celular IoT (2000) que actúa como carcasa y se interconecta con un dispositivo móvil tal como un celular inteligente o una tableta, para que el usuario genere alertas sin portar un dispositivo extra.

Conector USB del dispositivo IoT de generación de alertas de tipo conexión

El conector USB del dispositivo IoT de generación de alertas de tipo conexión (3010) es un cable que permite interconectar el dispositivo IoT de generación de alertas de tipo conexión (3000) con el dispositivo móvil en donde está alojada la plataforma en el usuario.

Instrucciones ejecutadas por un procesador

Dentro de las características de las instrucciones ejecutadas por un procesador (aplicación móvil) se incluyen:

-Perfil de usuario seguro. Para usar la aplicación, los usuarios deben registrarse utilizando su documento de identificación, garantizando así la autenticidad y la seguridad de la cuenta.

-Certificados y tokens de seguridad. Cada sesión de usuario está protegida mediante certificados y tokens únicos que salvaguardan la comunicación y los datos personales dentro de la aplicación.

-Firewall y protecciones avanzadas. La infraestructura detrás de La presente invención está protegida con firewalls y sistemas avanzados de protección contra intrusiones, asegurando que los datos de los usuarios y las comunicaciones sean completamente seguros.

-Integración con servicios de emergencia. La aplicación permite la comunicación directa y eficiente con servicios de emergencia, utilizando datos de ubicación precisos y comunicación en tiempo real para optimizar los tiempos de respuesta.

-Gestión de Alertas. Los usuarios pueden enviar diferentes tipos de alertas desde el dispositivo IoT, que son clasificadas y gestionadas según su nivel de urgencia, asegurando una respuesta adecuada y escalada para cada situación.

En seguida se proporciona una explicación detallada de las interconexiones y funcionalidades del sistema (1000):

Interconexiones y funcionalidades

En una de las modalidades preferidas, como se muestra en la **figura 1**, el sistema de seguridad mediante dispositivo de internet de las cosas para alertas de peligro a personas (1000) muestra las siguientes partes, interconexiones y funcionalidades:

Uno o varios servidores web de aplicación (1010) en donde se aloja la plataforma de monitoreo de alertas (1020) que es la que gestiona toda información enviada por los dispositivos intercomunicadores celular IoT (2000), y la de los dispositivos IoT de generación de alertas de tipo conexión (3000).

Los servidores web de aplicación redundante (1010) interconectados con los servidores de base de datos para almacenamiento de información del sistema (1030).

Los servidores web de aplicación redundante (1011) interconectados con los servidores de base de datos de redundancia (1031) actúan como “espejo” de los servidores web de aplicación (1010) y de los servidores de base de datos para almacenamiento de información del sistema (1030) respectivamente, ya que se encargan de duplicar la información de la plataforma de monitoreo de alertas (1020) para garantizar total y continua disponibilidad de la información del sistema. La **figura 8** muestra una pantalla para visualizar el listado de alertas generadas por la plataforma de monitoreo de alertas (1020).

A través de la red de intercomunicación (1040) y de internet (1041), los servidores web de aplicación redundante (1011) exponen la plataforma de monitoreo de alertas (1020) para que pueda ser accedida mediante los dispositivos de comunicación inteligente del usuario de generación de alertas (1050) y de los dispositivos de comunicación inteligente de monitoreo de alarmas (1060).

Los dispositivos de comunicación inteligente del usuario de generación de alertas (1050), así como los dispositivos de comunicación inteligente de monitoreo de alarmas (1060) y también los dispositivos de comunicación inteligente de la fuerza pública para monitoreo de alertas (1080) son los encargados de accionar las alertas enviando a través de la red de intercomunicación (1040) y de internet (1041) a la plataforma de monitoreo de alertas (1020).

Los dispositivos intercomunicadores celular IoT (2000) son portados por las personas o usuarios del sistema, y son accionados para generar alertas que son recibidas por la interconexión con el dispositivo de comunicación inteligente del usuario de generación de alertas (1050).

En la **figura 2** se puede apreciar una vista superior e inferior del dispositivo intercomunicadores celular IoT (2000) en donde se aprecia el cubrimiento del dispositivo por medio de la carcasa de cubrimiento inferior (2001) y de la carcasa de cubrimiento superior (2020). En la **figura 3** se puede apreciar la interconexión del dispositivo intercomunicadores celular IoT (2000) con el dispositivo de comunicación inteligente del usuario de generación de alertas (1050), este último puede ser una tableta o teléfono inteligente.

En la **figura 3** se muestra otra modalidad del dispositivo intercomunicador celular IoT (2000) equivalente en funcionalidad y representado por el dispositivo IoT de generación de alertas de tipo conexión (3000) que se interconecta directamente a manera de protector del dispositivo de comunicación inteligente del usuario de generación de alertas (1050) y transmite información a la plataforma de monitoreo de alertas (1020).

La **figura 4** muestra las partes visibles del dispositivo intercomunicador celular IoT (2000) en el que se pueden apreciar la carcasa de cubrimiento inferior (2001) que encaja con la carcasa de cubrimiento superior (2020), y en esta última se visualiza el orificio por el que sobresale el pulsador (2009), y también está el orificio de acceso para el puerto de entrada para tarjeta SIM (2019).

La **figura 5** complementa la **figura 3** en el que se muestran los dos tipos de conexiones entre el dispositivo IoT de generación de alertas de tipo conexión (3000) y el dispositivo de comunicación inteligente del usuario de generación de alertas (1050), el de la izquierda muestra el inalámbrico a través de una tecnología de comunicación como Bluetooth, por ejemplo, y el de la derecha por conexión física por medio del conector USB del dispositivo IoT de generación de alertas de tipo conexión (3010).

Las **figuras 6 y 7** muestran las interconexiones de los elementos del dispositivo intercomunicador celular IoT (2000) en donde se puede apreciar:

Carcasa de cubrimiento inferior (2001) a la que se interconecta la board (2014) a la que se interconectan los siguientes dispositivos: la batería ion litio (2002); la antena sistema georreferencia (2003); el sistema de georreferencia (2004); el sistema lector de tarjeta SIM (2005); el sistema de procesamiento (2006); el altavoz (2007); el

contacto magnético (2008); el pulsador (2009); el sensor de efecto hall (2010); las resistencias (2011); el sistema amplificador (2012); el amplificador operacional (2013); el lector biométrico de huella (2015); el lector del iris (2016); el proyector holográfico (2017); la placa (2018); y el puerto de entrada para tarjeta SIM (2019); todos estos dispositivos protegidos por el cubrimiento de la carcasa de cubrimiento superior (2020) que encaja con la carcasa de cubrimiento inferior (2001).

Las estaciones de monitoreo de alertas (1061) se interconectan con los servidores web de aplicación (1010) y con los servidores web de aplicación redundante (1011) para acceder a la información de la plataforma de monitoreo de alertas (1020) y reaccionar en caso de alguna eventualidad reportada por los dispositivos de comunicación inteligente del usuario de generación de alertas (1050), o los dispositivos de comunicación inteligente de monitoreo de alarmas (1060), o los drones de monitoreo y asistencia (1070), o los dispositivos de comunicación inteligente de la fuerza pública para monitoreo de alertas (1080);

Los drones de monitoreo y asistencia (1070) son vehículos aéreos no tripulados que monitorean y permiten a través de una cámara detectar cualquier evento sospechoso para enviar la información de alerta a través de la red de intercomunicación (1040) e internet (1041) y registrarlo en la plataforma de monitoreo de alertas (1020).

Flujo base de funcionamiento

La plataforma de monitoreo de alertas (1020) siempre activa en los servidores web de aplicación (1010) y los servidores web de aplicación redundante (1011) es accedida a través de la red de intercomunicación (1040) y de internet (1041) por los dispositivos de comunicación inteligente del usuario de generación de alertas (1050) que portan los usuarios en su rutina del día a día.

Cuando el usuario detecte alguna eventualidad podrá accionarlos a través del dispositivo intercomunicador celular IoT (2000), o del dispositivo IoT de generación de alertas de tipo conexión (3000) y generar una alerta que se registra en la plataforma de monitoreo de alertas (1020) y almacenando información relevante en los servidores de bases de datos para almacenamiento de información del sistema (1030) y en los servidores de base de datos de redundancia (1031). Una vez la información está en la plataforma de monitoreo de alertas (1020) estará al alcance de las estaciones de monitoreo de alertas (1061) que generarán alertas y alarmas que llegarán a los dispositivos de comunicación inteligente de monitoreo de alarmas (1060) y a los dispositivos de comunicación inteligente de la fuerza pública para monitoreo de alertas (1080).

Gracias a los componentes del dispositivo intercomunicador celular IoT (2000) y del dispositivo IoT de generación de alertas de tipo conexión (3000) como el sistema de georreferencia (2004), la antena sistema georreferencia (2003), el puerto de entrada para tarjeta SIM (2019), en donde se ubica una tarjeta con acceso a redes de comunicación de datos móviles, es posible rastrear la ubicación exacta de la persona que realizó la alerta, y es fácil identificar grupos cercanos de personas y fuerza pública que pueda ir en su asistencia y apoyo.

Otra forma de registrar los eventos en la plataforma de monitoreo de alertas (1020) es a través de los drones de monitoreo y asistencia (1070) que estarán vigilando el espacio aéreo, o servirán de apoyo en caso de notar algún evento sospechoso, y gracias al apoyo que dan enviando señales de video en tiempo real que podrán verificar las estaciones de monitoreo de alertas (1061) y luego podrán registrar las alarmas de eventos asociados en dicha plataforma de monitoreo de alertas (1020).

En cualquiera de las formas de generación de alertas, por los usuarios con los dispositivos IoT, o por los vehículos aéreos no tripulados o por grupos de apoyo o la fuerza pública, la información será registrada en la plataforma de monitoreo de alertas (1020), será detectada por las estaciones de monitoreo de alertas (1061) y notificadas a los dispositivo de comunicación inteligente de monitoreo de alarmas (1060) y a los dispositivos de comunicación inteligente de la fuerza pública para monitoreo de alertas (1080) con el fin de que grupos de personas de apoyo civil y la fuerza pública puedan entrar a intervenir en ayuda de la persona que se está pudiendo ver afectada por el evento o el suceso sospechoso o criminal.

Todos los eventos detectados y la información asociada quedarán registrados en la plataforma de monitoreo de alertas (1020) para que sirva como referencia a otros usuarios de la aplicación de zonas o sectores que no son confiables para su tránsito.

Método general de funcionamiento

En términos generales y tal como puede verse en la **figura 9**, el método general de funcionamiento del sistema integrado de alta seguridad (1000) está conformado por las siguientes fases globales:

A. Monitorear alerta por medio de los elementos del subsistema de monitoreo;
B. Verificar existencia de alarma por medio de los elementos del subsistema de monitoreo. En caso de ser positivo pasa al paso C. En caso de ser negativo vuelve al paso A;

C. Notificar alerta por medio de los elementos del subsistema de generación y verificación de alertas;
D. Registrar evento por medio del subsistema de almacenamiento y publicación de información de alertas;
E. Asistir al usuario por medio del funcionamiento del subsistema de monitoreo; y
F. Registrar información por medio del subsistema de almacenamiento y publicación de información de alertas y volver al paso A.

Método detallado de funcionamiento

Como puede verse en la **figura 10**, el método general de funcionamiento del sistema integrado de alta seguridad está conformado por las siguientes fases detalladas adicionales:

G. Monitorear registro de alertas por medio de los servidores web de aplicación (1010); los servidores web de aplicación redundante (1011); y la plataforma de monitoreo de alertas (1020);
H. Verificar el registro de alarma en la plataforma de monitoreo de alertas (1020). En caso de que Sí se registre alarma pasa los pasos C, D, E y F. En caso de que NO se registre alarma vuelve al paso A. Las alarmas se generarían por medio de los dispositivos intercomunicador celular IoT (2000), los dispositivos IoT de generación de alertas de tipo conexión (3000), los dispositivos de comunicación inteligente del usuario de generación de alertas (1050), y los dispositivos de comunicación inteligente de monitoreo de alarmas (1060);
I. Notificar al líder de zona y pasar al punto H. La información almacenada en lo servidores de base de datos para almacenamiento de información del sistema (1030) y los servidores de base de datos de redundancia (1031) es publicada por medio de la plataforma de monitoreo de alertas (1020) a los dispositivos de comunicación inteligente de monitoreo de alarmas (1060) y dispositivos de comunicación inteligente de la fuerza pública para monitoreo de alertas (1080);
J. Notificar al líder de servicio y pasar al punto H. La información almacenada en los servidores de base de datos para almacenamiento de información del sistema (1030) y los servidores de base de datos de redundancia (1031) es publicada por medio de la plataforma de monitoreo de alertas (1020) a los dispositivos de comunicación inteligente de monitoreo de alarmas (1060) y dispositivos de comunicación inteligente de la fuerza pública para monitoreo de alertas (1080);
K. Notificar al círculo vital y pasar al punto H. La información almacenada en lo servidores de base de datos para almacenamiento de información del sistema (1030) y los servidores de base de datos de redundancia (1031) es publicada por medio de la plataforma de monitoreo de alertas (1020) a los dispositivos de

comunicación inteligente de monitoreo de alarmas (1060) y dispositivos de comunicación inteligente de la fuerza pública para monitoreo de alertas (1080);

L. Notificar a la central y pasar al punto G. Se almacena la información en los servidores de base de datos para almacenamiento de información del sistema (1030) y servidores de base de datos de redundancia (1031) y luego es accedida por la estación de monitoreo de alertas (1061);
M. Notificar a la red de apoyo y pasar al punto H. Por medio de la plataforma de monitoreo de alertas (1020) y del dispositivo de comunicación inteligente de monitoreo de alarmas (1060);
N. Registrar el evento en la plataforma de monitoreo. Se almacena la información en los servidores de base de datos para almacenamiento de información del sistema (1030) y servidores de base de datos de redundancia (1031);
O. Notificar a la fuerza pública. Por medio de la plataforma de monitoreo de alertas (1020) y del dispositivo de comunicación inteligente de la fuerza pública para monitoreo de alertas (1080);
P. Confirmar en la plataforma la asistencia al usuario. La plataforma de monitoreo de alertas (1020) registra la información ingresada por dispositivo de comunicación inteligente de monitoreo de alarmas (1060) y del dispositivo de comunicación inteligente de la fuerza pública para monitoreo de alertas (1080).
Q. Registrar la información del evento en la plataforma de monitoreo y volver al paso A. Se almacena la información en los servidores de base de datos para almacenamiento de información del sistema (1030) y servidores de base de datos de redundancia (1031).

Protocolos

La eficacia del funcionamiento del sistema de respuesta (1000) depende crucialmente de protocolos claramente definidos, que se activan automáticamente al recibir una alerta. Estos protocolos incluyen:

Verificación de la alarma. Inmediatamente después de recibir una alerta, se realiza una verificación para confirmar su autenticidad y evitar falsas alarmas. Esto se logra mediante una combinación de verificaciones automáticas y contacto directo con el usuario a la mayor brevedad posible.

Clasificación de la emergencia. Las alertas se clasifican según su tipo y severidad. Esto permite priorizar las respuestas y asignar los recursos más adecuados para cada situación específica.

Despliegue de Recursos. Dependiendo de la clasificación de la emergencia, se movilizan los recursos necesarios. Esto puede incluir el envío de agentes de

respuesta directa, la notificación a las autoridades locales, o la movilización de recursos médicos.

Monitoreo confidencial de recorridos

El sistema (1000) integra una función que monitorea de forma confidencial los recorridos de los usuarios 24 horas al día, los sietes días de la semana (24/7), a fin de brindarles acompañamiento y reacción inmediata ante cualquier incidente, de la siguiente manera:

Ingreso de datos esenciales. El usuario ingresa lugar de origen, lugar de destino, nombre del recorrido y descripción, o información en caso de emergencia. También ingresa el tiempo en el cual debe haber llegado a su destino y adicionalmente puede agregar paradas, con registro fotográfico o video y coordenadas GPS de donde fue la parada, junto con detalles y descripción.

Al momento de cumplirse el tiempo de finalización del recorrido, el usuario recibe una notificación para que confirme que llegó bien, así se cierra el recorrido y el registro queda guardado en BD para posterior.

Por el contrario, si el usuario no confirma que llegó bien a su destino, se disparan una serie de alarmas que hacen que el usuario recuerde confirmar; de no ser así, se dispara un protocolo de seguridad de la siguiente manera:

-Un minuto después de finalizado el tiempo de recorrido, se envía una notificación PUSH para que el usuario notifique que llegó bien.

-Dos minutos después de finalizado el tiempo de recorrido, se envía un comunicado por mensajería instantánea (por ejemplo, WhatsApp) indicando que debe reportar en la aplicación el estado o finalizar el viaje.

-Tres minutos después de finalizado el tiempo de recorrido, se envía un mensaje de texto informándole que debe reportar su estado o finalizar el viaje.

-Cuatro minutos después, se hace una llamada para recordarle que debe reportarse y finalizar el viaje, cerrando el acompañamiento.

-Cinco minutos después se dispara una alarma tal cual fuera un botón de alguno de los servicios y se inicia el protocolo, que incluye revisión de todo lo que el usuario haya reportado en su viaje: origen, destino, paradas, fotos, textos, etc.

Integración del invento con otros sistemas

La invención está integrada con los sistemas y servicios locales de emergencia, incluyendo policía, bomberos y servicios médicos. Esto permite una coordinación eficiente y una respuesta más rápida al compartir información crítica como la ubicación del usuario y la naturaleza de la emergencia.

También realiza la coordinación con los servicios de emergencia, dispone de un equipo de agentes de respuesta que pueden movilizarse directamente al lugar de la emergencia. Estos agentes están equipados con herramientas y formación específica para manejar situaciones diversas, desde asistencias médicas hasta intervenciones en casos de violencia.

El núcleo de recepción de alertas del sistema de emergencias es el centro de control, equipado con la tecnología más avanzada para la recepción y gestión de dichas alertas. Este centro opera 24 horas al día, los sietes días de la semana (24/7), con personal entrenado en la gestión de crisis y primeros auxilios psicológicos. La recepción de una alerta activa un protocolo de verificación rápida para determinar la naturaleza y gravedad de la emergencia.

La invención permite hacer de cada entorno un espacio seguro, para que quienes lo integren se sientan aliviados ante la incertidumbre de un evento adverso como un atraco, un accidente de tránsito, una emergencia médica o cualquier otra situación que ponga su vida en peligro, lo anterior a través de actores activos de la sociedad como lo son las redes de apoyo ciudadano, empresas de vigilancia, vigilantes independientes, organismos de socorro, policía, fuerzas militares, entre otros.

A través de la aplicación, haciendo uso de la tecnología, identifica en un perímetro de 500 metros a la redonda de donde ha sido activado un botón de alerta por una persona a través de la aplicación de usuarios, quien o quienes son los integrantes de esa red de aliados que le pueden asistir en menos de 3 minutos.

Aunque pueden reaccionar al llamado de alerta muchos aliados de las categorías descritas anteriormente, la aplicación que incorpora instrucciones ejecutadas por ordenador solo tomará los primeros que reaccionen a ese llamado así:

- Empresas de seguridad privada: Guardas cercanos a perímetro
- Líder de Reacción: Líder cercanos a perímetro
- Taxista: Conductores de servicio de taxi cercanos a perímetro
- Conductor de plataforma de transporte privado: Conductores cercanos a perímetro
- Comerciantes de la zona: personas cercanas a perímetro
- Vigilante independiente: Vigilantes Independientes cercanos a perímetro

- Entidades de socorro (Defensa Civil, Bomberos, Cruz Roja)
- Usuarios : Usuarios cercanos a perímetro

Estos aliados de reacción reciben a través de su aplicación, que incorpora instrucciones ejecutadas por ordenador, la confirmación para la atención inmediata del incidente, con el perfil de la persona que ha solicitado el servicio, al igual que los datos más relevantes de esa persona dependiendo el tipo de alerta emitida, siendo siempre estos datos de carácter confidencial y de uso exclusivo de los aliados de reacción en caso de urgencia vital.

Por ejemplo, si es una alerta por robo o atraco en la que la vida de quien solicitó el servicio está en peligro de perderse, la aplicación cuenta con los datos médicos necesarios para su atención inmediata. Igualmente, la aplicación cuenta con la información del usuario asociada a su círculo de vida, que son 3, 4, y hasta 5 personas que el usuario elige su contacto de emergencia para ser notificados ante un incidente.

A través de las dos aplicaciones que incorporan instrucciones ejecutadas por ordenador, tanto de usuarios como de reacción, la plataforma logra micro segmentar la oferta con la demanda sin aumentar los costos siempre con un pago justo al integrante de la red de aliados que la suple.

Esta solución evita el desgaste de la red de aliados al informar solo a los que pueden reaccionar, y así evita el pánico colectivo al informar solo a los que pueden ayudar, mejorando la percepción de seguridad de las ciudades.

Adicionalmente, esta solución tecnológica potencia en un 500% la eficacia y efectividad de la Policía Nacional y sus cuadrantes, al darles información fidedigna. Además, optimiza en un 500% el rendimiento de las centrales de emergencia, al permitir disminuir a milisegundos la perfilación de usuarios que actualmente les toma en promedio 10 minutos, y se debe tener presente que a la hora de un incidente un minuto es vital para salvar una vida.

Esta información surgió del proceso de perfilación y respuesta de las centrales de emergencia integradas en el número 123 de atención de emergencias en Colombia, lo cual evidencia que no puede haber una reacción debido a la perfilación antes de los 10 minutos, tiempo en el cual, el operador/receptor perfila al usuario que requiere el servicio y debe tramitar una vez hecha esta perfilación entre 3 a 5 minutos ubicar al líder del área de la policía para su respectiva reacción. Este proceso nos lleva a perfilar en milisegundos y al contactar en segundos a la red de aliados más próxima al usuario que requiere el apoyo. Esta optimización de tiempo e inclusión de la red de aliados en el área específica lleva realmente a potenciar en más del 500% la efectividad del cuadrante de la policía al ser apoyados por una tecnología prácticamente en tiempo real y una red de aliados y reacción comprometida.

La persona que, por ejemplo, oprima cualquiera de las alertas, recibe un mensaje a al dispositivo móvil celular inteligente o tableta, también recibe la llamada de la plataforma, y recibe llamadas personalizadas de acuerdo con el guion establecido, informándole que recibirá asistencia personalizada en menos de 3 minutos.

Si el caso es violencia intrafamiliar o acoso sexual, el líder de reacción se comunica al cuadrante de la policía; un líder de reacción inicia su acompañamiento presencial cercano a la mujer denunciante únicamente cuando llegue la policía al sitio; igualmente se recibe el acompañamiento por parte de los usuarios cercanos de acuerdo con el perímetro establecido (esto determina cuantas personas deben llegar al sitio a prestar asistencia). Con el líder de reacción nuestro, la mujer define si denuncia oficialmente a través de los canales institucionales.

Si el caso es robo o atraco, la persona que oprima este botón de alerta en la aplicación que incorpora instrucciones ejecutadas por ordenador, recibe un mensaje al celular móvil inteligente, recibe la llamada de la plataforma Web y recibe una llamada personalizada de acuerdo con el guion establecido, informándole que recibirá asistencia personalizada en menos de 3 minutos.

Se dirige a ese llamado al líder de reacción, al igual que el equipo de reacción de la red de apoyo más cercana (taxista, conductor de plataforma de transporte, etc.). Si la persona ha sido drogada o víctima de sustancias psicoactivas, el protocolo a seguir indica el llamado de una ambulancia, ponerse en contacto con su círculo vital, y jamás desamparar al usuario victima hasta que sus familiares estén presentes y se hagan cargo.

Si el caso es accidente de tránsito, la persona que oprima este botón de alerta en la aplicación que incorpora instrucciones ejecutadas por ordenador, recibe llamada automática o de operador, reacción a cargo del líder de reacción asignado y de 3 integrantes de la red de aliados de reacción.

Cuando el usuario oprima este botón indicando un accidente, la central de operaciones lanza una llamada automática al usuario que reportó indicándole que en cuestión de minutos recibirá acompañamiento por parte de un líder de reacción, y ese líder de reacción es quien define si se le notifica al círculo vital de la persona accidentada, si requiere llamar al tránsito y de acuerdo con la gravedad si requiere una ambulancia.

Si el caso es extorsión, la persona que oprima este botón de alerta en la aplicación, debe detallar la extorsión y adjuntar las fotos y videos si los tiene. Esto se les notifica a las fuerzas militares.

Si es secuestro se aplica el protocolo anterior de extorsión, y adicional se crea un candado virtual donde se le estará reportando dicho desplazamiento y ubicación del usuario a los cuadrantes de las autoridades que están en el desplazamiento de este.

Además, integra una función de candado virtual, que permite delimitar una zona en la cual a los usuarios presentes en dicha zona les llegue la información del delincuente o sospechoso, la información del infractor y/o su descripción para que vayan dando información por donde va pasando para así mismo ir informando a la autoridad respectiva para su abordaje y seguimiento. Esta función sirve tanto para reportar atracadores o como un infractor de tránsito que se da a la fuga o a un extorsionista o secuestrador.

Para todo proceso existe un formulario virtual para el líder que atiende el caso, que le permite tomar foto, hacer un video, para llevar un historial del caso, su desenlace y posterior cierre, observaciones, esto con el objetivo que exista una trazabilidad de cada caso. Al final, se envía el formulario o encuesta al cliente a través de la aplicación que incorpora instrucciones ejecutadas por ordenador, que nos permite optimizar el proceso.

Función cuenta regresiva: aquellos usuarios y adicionalmente los agentes de la red de aliados que reaccionen ante la solicitud de asistencia y socorro por parte de un usuario reportando un incidente, a los que reaccionen en el rango de 1 a 1.000 metros (1 km), la aplicación según su distancia establece un tiempo máximo de reportarse en el sitio del incidente, para lo cual genera a quienes reaccionan un conteo regresivo generándoles sentido de urgencia y tiempo concedido para desplazarse hasta el sitio del incidente.

Otros requerimientos

Un componente crucial para la efectividad del sistema de respuesta a emergencias es la capacitación continua del personal involucrado en la gestión y respuesta a las alertas. Esto incluye:

Formación en primeros auxilios y manejo de crisis. Todo el personal, desde operadores del centro de control hasta agentes de campo, recibe formación regular en primeros auxilios, manejo de crisis y técnicas de comunicación efectiva.

Simulacros y pruebas de sistema. Se realizan simulacros regulares para asegurar que todos los sistemas y protocolos funcionen correctamente en caso de una emergencia real. Esto también ayuda a identificar áreas de mejora en la respuesta

a incidentes.

Feedback y mejora continua. La retroalimentación de los usuarios y el análisis de la respuesta a cada incidente son fundamentales para el mejoramiento continuo del sistema, el cual utiliza esta información para ajustar protocolos y entrenamientos, garantizando una adaptación constante a nuevas necesidades y tecnologías.

Características de la opción streaming

El streaming de video es una tecnología que se utiliza para enviar video y audio a través de internet en tiempo real. Se realiza transmisión en vivo y gráficamente puede ir en cada alerta de la siguiente manera:

- No urgente
- Urgente
- Transmitir en vivo (icono de una cámara).

Así queda la trazabilidad y registro de qué tipo de transmisión es, y así mismo se puede activar el protocolo de reacción dependiendo el tipo de alerta.

Tener presente que debe estar la opción en la función acompáñame también.

Descripción:

- Al oprimir el botón, como en alertas, permite al usuario iniciar una transmisión, solo si la integridad está en inminente riesgo.

- Al oprimir transmitir en vivo, de inmediato se pueda acceder a la cámara del dispositivo celular e iniciar a transmitir a la central y al líder de zona más cercano y a los usuarios que estén en un perímetro de 500 m (el rango de cobertura administrable).

- La central o el líder de zona seleccionado definen según la gravedad del incidente o tipo de alerta activar el protocolo de reacción. En la central se debe producir una alerta ruidosa al igual que al líder de zona más cercano, y a los usuarios y aliados que estén en el perímetro establecido de cobertura, una notificación para que le hagan seguimiento y reaccionen dependiendo la instrucción de la central según sea el caso.

- Esa grabación se guarda en un canal privado, por ejemplo, de YouTube como prueba legal.

- Una vez concluida la transmisión se debe cerrar el incidente con los respectivos reportes.

- Estas grabaciones quedan como evidencia en caso tal de una denuncia legal formal ante la entidad competente.

Beneficios de la función:

- Sirve de material probatorio.

- Sirve de disuasión para los acosadores, sospechosos, etc.

- Sirve como acompañamiento a las mujeres en sus desplazamientos en solitario.

- Tener presente la opción que la central y el líder de zona, puedan tener varias transmisiones en vivo al mismo tiempo, y se pueden encolar o ver como una video llamada grupal.

- Esta función sirve de base para la transmisión en vivo (igual forma) para los drones.

Protocolo de reacción según gravedad del incidente:

- La central y el líder de zona deben tener la capacidad de definir el protocolo de reacción según la gravedad del incidente o tipo de alerta activada.

- En caso de activación del protocolo de reacción, se debe generar una alerta sonora en la central y en el dispositivo del líder de zona más cercano.

- Los usuarios y aliados dentro del perímetro de cobertura deben recibir notificaciones para que puedan seguir y reaccionar según las instrucciones de la central.

Almacenamiento de la grabación en un canal privado:

- Durante la transmisión en vivo, se debe almacenar la grabación en un canal privado, por ejemplo, de YouTube como evidencia.

- Al concluir la transmisión en vivo, se debe cerrar el incidente y generar los reportes correspondientes.

- Las grabaciones almacenadas deben estar disponibles como evidencia en caso de denuncia legal formal ante la entidad competente.

Criterios de aceptación:

- El mensaje de confirmación al iniciar la transmisión debe ser claro y comprensible para el usuario.

- La transmisión en vivo debe comenzar inmediatamente después de confirmar la acción.

- Al pulsar el botón de inicio de transmisión, se muestra un mensaje de advertencia sobre la importancia de la acción.

- Se debe requerir confirmación por parte del usuario antes de iniciar la transmisión en tiempo real.

- Solo se permite la activación de la transmisión en situaciones de emergencia real.

Transmisión a la central y usuarios cercanos:

- Al iniciar la transmisión, se accede automáticamente a la cámara del dispositivo móvil.

- La transmisión se envía a la central y al líder de zona más cercano.

- Los usuarios dentro de un radio de 500 metros del emisor también reciben la transmisión.

- La central y el líder de zona pueden seleccionar el protocolo de reacción según la gravedad del incidente.

Notificaciones efectivas:

- Las notificaciones a la central, líder de zona y usuarios cercanos deben entregarse de manera rápida y confiable.

- La central y el líder de zona reciben una alerta audible al recibir la transmisión en tiempo real.

- Los usuarios dentro del radio de cobertura reciben notificaciones para seguir la situación y actuar según las instrucciones de la central.

Flexibilidad en el protocolo de reacción:

- Las notificaciones a los usuarios deben incluir instrucciones claras y precisas sobre cómo actuar.

Almacenamiento seguro de grabaciones:

- Las grabaciones almacenadas en el canal privado deben ser accesibles solo para usuarios autorizados.

- La grabación debe estar disponible como evidencia en caso de una denuncia legal formal ante la entidad competente.

- Los reportes generados al concluir la transmisión deben contener toda la información relevante del incidente.

Beneficios de la función:

- La función sirve como material probatorio en situaciones de emergencia.

- Actúa como disuasión para acosadores y posibles agresores.

- Brinda acompañamiento a mujeres en sus desplazamientos en solitario, proporcionando una sensación de seguridad.

Capacidad de múltiples transmisiones simultáneas:

- Tanto la central como el líder de zona pueden gestionar varias transmisiones en vivo al mismo tiempo.

- Las transmisiones pueden ser encoladas o visualizadas como una video llamada grupal para una gestión eficiente.

Escalabilidad y simultaneidad de transmisiones:

- La aplicación debe ser capaz de manejar varias transmisiones en vivo simultáneamente.

- La función de transmisión en vivo debe ser escalable para soportar futuras implementaciones, como la transmisión desde drones.

- Se deben considerar los requisitos técnicos y de infraestructura para integrar la transmisión desde drones de manera eficiente y segura.

- Con sus características únicas y tecnología avanzada, este producto no solo atrae a individuos preocupados por su seguridad personal, sino que también ofrece oportunidades para colaboraciones con agencias de seguridad pública, proveedores de servicios de emergencia, empresas que quieran garantizar la seguridad de sus colaboradores y compañías de seguros.

A partir de los valores de los parámetros definidos y por medio de las instrucciones ejecutadas por un ordenador, e interacción entre software y hardware en las diferentes configuraciones elegidas se puede realizar el seguimiento y trazabilidad de alertas de situaciones de peligro de los usuarios para dar la atención oportuna y atender cualquier eventualidad mencionada.

Efectos técnicos

La presente invención está fundamentada en la combinación única de tecnología avanzada, integración de sistemas, hardware, aplicaciones con instrucciones ejecutadas por un ordenador, y funcionalidades específicamente diseñadas para ofrecer una solución de seguridad personal eficaz y accesible.

La presente invención presenta los siguientes efectos técnicos que sin duda son inesperados y sorprendentes, incorporando una serie de innovaciones tecnológicas que no solo mejoran la funcionalidad del producto, sino que también lo diferencian respecto a otras soluciones, tal como se mencionan a continuación:

- Se distingue no solo por su tecnología avanzada, sino también por su enfoque holístico y adaptado a las necesidades específicas de seguridad personal.

- Integra tecnologías de georreferenciación y de comunicaciones (4G, 5G, 6G, 7G), en un dispositivo intercomunicador celular IoT portátil y discreto, junto con la capacidad de realizar verificaciones biométricas.

- Es un sistema completo que integra dispositivos de seguridad personal.

- Esta combinación de hardware avanzado, instrucciones implementadas por un procesador y una interfaz intuitiva para el usuario ofrece una solución única en

el mercado, proporcionando no solo seguridad sino también paz mental a sus usuarios.

- Incluye características de identificación biométrica y hologramas por medio del uso del dispositivo intercomunicador celular IoT para garantizar la seguridad personal.

- La posibilidad de emplear diferentes modalidades del dispositivo intercomunicador celular IoT como independiente de un celular inteligente o tableta, así como también el de estar conectado como una carcasa de manera inalámbrica o alámbrica que amplía las funcionalidades de los dispositivos mencionados.

- Botón de emergencia físico con alerta silenciosa a diferencia de las aplicaciones que incorporan instrucciones ejecutadas por un ordenador para móviles comunes que dependen de la interacción con un smartphone, la presente invención ofrece un dispositivo físico con un botón dedicado que permite enviar alertas de emergencia. La funcionalidad de alerta silenciosa, que activa una señal de auxilio sin emitir ruido, es crucial para situaciones donde el usuario necesita pedir ayuda sin alertar a un agresor cercano.

- Integración de conectividad independiente a diferencia de otros dispositivos de seguridad dependen de la conectividad Bluetooth o Wi-Fi a través de smartphones, la presente invención utiliza su propia conexión de alguna de las tecnologías móviles como 4G-5G-6G-7G. Esto asegura que el dispositivo pueda funcionar y enviar alertas incluso si el smartphone del usuario no está disponible o fuera de servicio.

- Verificación biométrica: la inclusión de tecnologías de verificación biométrica, como el lector de huellas dactilares y el lector de iris, agrega una capa adicional de seguridad, permitiendo la verificación de la identidad del usuario de manera rápida y segura antes de enviar una alerta de peligro. Esto es particularmente útil para evitar falsas alarmas y asegurar que los recursos de emergencia se movilicen de manera adecuada.

- Módulo holográfico: el desarrollo de un módulo holográfico para el dispositivo intercomunicador celular IoT, introduce una dimensión completamente nueva en la interacción usuario-dispositivo en situaciones de emergencia, posiblemente permitiendo visualizaciones de hologramas en tiempo real o instrucciones interactivas, que le pueden salvar la vida o evitar algún incidente.

- Diseño ergonómico y fácil de usar: ha sido diseñado pensando en la usabilidad. El sistema ha sido diseñado para que sea fácilmente accesible y puede ser activado intuitivamente en situaciones de estrés, a diferencia de otros sistemas que pueden requerir múltiples pasos para enviar una alerta. También en diferentes modalidades el dispositivo podría ser externo al celular inteligente o tableta; o también acoplarse y actuar como carcasa del celular o tableta para cargar un solo dispositivo ofreciendo la misma funcionalidad.

- Independencia de la tecnología del smartphone: eso es crucial para usuarios en regiones con baja penetración de smartphones avanzados o para individuos que prefieren no depender completamente de sus teléfonos móviles para su seguridad.

- Tecnología de dispositivo independiente y conectado: el dispositivo intercomunicador celular IoT de la presente invención opera tanto de manera independiente como sincronizada con la aplicación móvil avanzada que integra instrucciones ejecutadas por un procesador, lo que permite una versatilidad y accesibilidad sin precedentes en situaciones de emergencia.

- Mecanismo de alerta silenciosa: la capacidad de enviar alertas silenciosas con solo presionar un botón, sin necesidad de desbloquear o manipular un smartphone, es una característica distintiva que mejora la discreción y la rapidez de la respuesta en situaciones potencialmente peligrosas

- Integración completa de servicios: La integración entre el dispositivo intercomunicador celular IoT, la aplicación y el centro de respuesta no tiene paralelo en términos de eficiencia operativa y capacidad de respuesta. Esta integración permite un flujo de información más rápido y seguro, esencial en situaciones de emergencia.

- Protección de datos y privacidad: La presente invención ha sido diseñado con un fuerte enfoque en la protección de la privacidad y la seguridad de los datos, utilizando encriptación avanzada y protocolos seguros que cumplen con las normativas sobre protección de datos.

- Transparencia y consentimiento: Los términos y condiciones del uso de La presente invención son claros y transparentes, asegurando que los usuarios estén plenamente informados sobre cómo se manejan sus datos y cómo funciona el dispositivo

- Incorporaciones tecnológicas: La propuesta de incorporación de tecnologías de identificación biométrica y proyección holográfica supera las capacidades de los dispositivos de seguridad personal conocidos hasta el momento.

- Comunidades seguras integralmente, ya que conecta una red de aliados con actores activos de la sociedad como lo son las empresas de seguridad, redes de apoyo ciudadano, policía, fuerzas militares, organismos de socorro, taxistas, vigilantes independientes y ciudadanos ángeles, previniendo y planificando acciones de éxito que le permite a los usuarios contar con una red de reacción capaz, eficaz, voluntaria, decidida, prudente y solidaria.

- Seguridad y tranquilidad: El dispositivo intercomunicador celular IoT brinda la tranquilidad de poder localizar a personas en tiempo real a través de la aplicación, lo que es especialmente útil en situaciones de emergencia o para el cuidado de niños, personas mayores o mascotas.

- Ubicación precisa: Con una precisión de 5-10 metros, el dispositivo intercomunicador celular IoT garantiza una ubicación exacta, lo que facilita la localización rápida y efectiva de personas en cualquier momento.

- Alertas personalizadas: La capacidad de recibir alertas personalizadas a través de la aplicación permite estar al tanto de la ubicación y situación de la persona rastreada, lo que brinda una capa adicional de seguridad y control.

- Funcionalidad SOS: dispositivo intercomunicador celular IoT permite a la persona rastreada enviar una señal de emergencia con su ubicación precisa, lo que es crucial en situaciones de peligro o emergencia.

- Diseño compacto y resistente: Con un diseño compacto y resistente al agua (IP67), el dispositivo intercomunicador celular IoT es versátil y duradero, lo que lo hace ideal para su uso en diversas situaciones y entornos.

- Fácil de usar: La plataforma web es intuitiva y amigable facilita la visualización de la ubicación del dispositivo, la configuración de alertas y el monitoreo en tiempo real, lo que brinda una experiencia de uso sencilla y eficiente.

- El dispositivo intercomunicador celular IoT está avalado por la CRC (Comisión de Regulación de Comunicaciones) en cuanto a que cumple con las reglas técnicas y estándares de calidad establecidos. Esto se debe a que el dispositivo intercomunicador celular IoT ofrece características y funcionalidades que

cumplen con los requisitos técnicos y de calidad exigidos por las autoridades regulatorias colombianas.

- En términos técnicos, dispositivo intercomunicador celular IoT ha sido diseñado y fabricado siguiendo normas y especificaciones que garantizan su correcto funcionamiento y precisión en la localización de personas. Además, al contar con funciones como la precisión de 5-10 metros, resistencia al agua IP67, botón de SOS, y una aplicación intuitiva, demuestra su capacidad para cumplir con los estándares de calidad y seguridad establecidos por la CRC.

- La certificación de la CRC respalda que el dispositivo intercomunicador celular IoT cumple con los requisitos técnicos y normativas vigentes, asegurando a los usuarios que están adquiriendo un dispositivo confiable, seguro y que cumple con los estándares de calidad necesarios para su correcto funcionamiento y uso en la localización de personas.

- El dispositivo intercomunicador celular IoT, no interrumpe con la señal de marcapasos y otros dispositivos que operan en diferentes frecuencias. Esta característica es fundamental en la seguridad y el uso adecuado del dispositivo, ya que garantiza que no haya interferencias con otros dispositivos médicos o tecnológicos que funcionen en frecuencias distintas, asegurando así la integridad y el correcto funcionamiento de estos equipos.

La aplicación práctica de la presente invención también genera beneficios sociales significativos, como se menciona a continuación:

- Mejora en la respuesta a emergencias: ya que está diseñada para optimizar la eficiencia de los servicios de emergencia. Con la transmisión instantánea de la ubicación geográfica mediante sistemas de posicionamiento global como GPS, los detalles del incidente a través de redes de comunicación (4G, 5G, 6G y 7G), y de esta manera los tiempos de respuesta se reducen significativamente, lo que puede ser decisivo en situaciones de vida o muerte.

- Accesibilidad y facilidad de uso: ya que el dispositivo intercomunicador celular IoT y la aplicación con instrucciones ejecutadas por un ordenador están diseñados para ser extremadamente fáciles de usar, garantizando que personas de todas las edades y habilidades tecnológicas puedan beneficiarse de su protección. Esto es especialmente importante en comunidades vulnerables o para individuos que pueden estar en mayor riesgo de violencia.

- Promoción de la seguridad personal: ya que no solo proporciona una herramienta de seguridad personal, sino que también actúa como un disuasivo contra el crimen. Su presencia puede disuadir a los potenciales agresores y aumentar la confianza y la sensación de seguridad de los usuarios.

- Dispositivo de seguimiento para bicicletas, el cual una vez instalado permite su ubicación a la redonda en un perímetro determinado, logrando mayor efectividad por la integración existente de la comunidad de personas vinculada al presente sistema, entre las interacciones de los usuarios y las de reacción o de la red de aliados.

- Dispositivo de seguimiento para mascotas, el cual permite a través de la red de apoyo y la comunidad de personas vinculada al presente sistema, ubicar de manera eficiente la mascota que lo lleve consigo.

- Drones: a través de una plataforma de lanzamiento denominada dron puertos, ubicadas en las azoteas de los edificios altos, integrar a los drones con el intercomunicador de dispositivos celulares y en la zonas seguras establecidas ubicados dichos dron puertos , una vez el usuario oprima una alerta silenciosa dirige el dron en dicha zona segura a que transmita lo que usuario está viviendo en un término de distancia de 1 minuto, transmitiendo vía streaming a la central para que esta pueda coordinar a través de la identificación del delincuente y/o victimario activar el protocolo de reacción para que dicho infractor sea capturado por las autoridades, ya que la plataforma emitirá en un perímetro determinando el video y las características del infractor para que por medio de la red de usuarios ir reportando al cuadrante de la policía más cercano para su respectiva captura .

- Holograma: A través de un dispositivo el cual está sujeto a la pretina, cinturón o correa de un usuario (persona) proyecta un holograma similar a la imagen de un guarda de seguridad armado el cual simula compañía e interacción con el usuario; así le dará la impresión al delincuente de que esta persona no está sola sino en compañía de alguien que lo puede defender.

- Streaming: El streaming de video es una tecnología que se utiliza para enviar video y audio a través de internet en tiempo real, permitiendo así que el usuario pueda ver y escuchar el contenido sin necesidad de descargarlo por completo. El streaming permite la transmisión continua de videos y audios sin almacenarlos previamente en el dispositivo del usuario.

Frente a lo anterior, la presente invención no solo ofrece una solución de seguridad, sino también una herramienta de empoderamiento para individuos en riesgo, proporcionándoles una manera de pedir ayuda de forma rápida, eficaz y discreta.

Además, el producto se alinea con las tendencias tecnológicas actuales que favorecen dispositivos interconectados y sistemas de respuesta rápida integrando avanzadas capacidades de geolocalización y comunicación, junto con futuras implementaciones como reconocimiento biométrico (lector de huella e iris) y módulos holográficos.

En resumen, la presente invención ofrece una serie de características innovadoras que no solo mejoran la seguridad personal de los usuarios, sino que también presentan claras ventajas sobre los productos existentes en términos de tecnología, usabilidad y aplicabilidad social. Este análisis demuestra la superioridad y la justificación de la invención, asegurando su lugar como una solución pionera en el campo de la seguridad personal.

Ejemplos

A continuación, se realizará la descripción de los experimentos y pruebas de campo realizadas con una modalidad preferida de la invención. Estas son pruebas técnicas hechas sobre el dispositivo intercomunicador celular IoT (2000).

El dispositivo ha atravesado diferentes pruebas para poder certificar que funciona correctamente y puede emitir y recibir llamadas sobre la frecuencia de telefonía móvil que se encuentra en Colombia actualmente. El cuadro 1 presenta las bandas que funcionan actualmente en Colombia.

Cuadro 1. Frecuencias y bandas empleadas en Colombia

Cobertura	Bandas y Frecuencias
2G	B2 (1900), B5 (850)
3G	B2 (1900), B5 (850)
4G	B2 (1900), B4 (1700/2100), B7 (2600)
5G	No

Considerando lo anterior, el dispositivo intercomunicador celular IoT (2000) que forma parte del sistema (1000) ha pasado por pruebas de laboratorio de la Comisión Federal de Comunicaciones (FCC), demostrando su buen funcionamiento y pasando las pruebas en diferentes bandas de operación, incluyendo las que actualmente funcionan en Colombia y en un operador reconocido. En el cuadro 2 se presentan los resultados de estas pruebas.

Cuadro 2. Resultados de pruebas en diferentes bandas de operación – Relación pico promedio

Banda	Ancho de banda (MHz)	Canal UL	Tamaño RB	Posición RB	Modulación	Resultado (dB)	Límite alto (dB)	Veredicto
Banda 12	1,4	23095	1	#0	QPSK	5,54	13	Aprobado
Banda 12	1,4	23095	1	#0	QAM16	6,30	13	Aprobado
Banda 12	3	23095	1	#0	QPSK	5,85	13	Aprobado
Banda 12	3	23095	1	#0	QAM16	6,95	13	Aprobado
Banda 12	5	23095	1	#0	QPSK	6,30	13	Aprobado
Banda 12	5	23095	1	#0	QAM16	6,40	13	Aprobado
Banda 12	10	23095	1	#0	QPSK	5,59	13	Aprobado
Banda 12	10	23095	1	#0	QAM16	6,68	13	Aprobado
Banda 2	1,4	18900	1	#0	QPSK	5,23	13	Aprobado
Banda 2	1,4	18900	1	#0	QAM16	5,64	13	Aprobado
Banda 2	3	18900	1	#0	QPSK	5,49	13	Aprobado
Banda 2	3	18900	1	#0	QAM16	6,23	13	Aprobado
Banda 2	5	18900	1	#0	QPSK	5,89	13	Aprobado
Banda 2	5	18900	1	#0	QAM16	6,12	13	Aprobado
Banda 2	10	18900	1	#0	QPSK	5,41	13	Aprobado
Banda 2	10	18900	1	#0	QAM16	6,27	13	Aprobado
Banda 2	15	18900	1	#0	QPSK	5,00	13	Aprobado
Banda 2	15	18900	1	#0	QAM16	5,92	13	Aprobado
Banda 2	20	18900	1	#0	QPSK	4,77	13	Aprobado
Banda 2	20	18900	1	#0	QAM16	5,42	13	Aprobado
Banda 5	1,4	20525	1	#0	QPSK	5,35	13	Aprobado
Banda 5	1,4	20525	1	#0	QAM16	5,72	13	Aprobado
Banda 5	3	20525	1	#0	QPSK	5,66	13	Aprobado
Banda 5	3	20525	1	#0	QAM16	6,29	13	Aprobado
Banda 5	5	20525	1	#0	QPSK	5,61	13	Aprobado
Banda 5	5	20525	1	#0	QAM16	6,09	13	Aprobado
Banda 5	10	20525	1	#0	QPSK	4,94	13	Aprobado
Banda 5	10	20525	1	#0	QAM16	5,67	13	Aprobado

De lo anterior se demuestra que el dispositivo (2000) puede recibir y transmitir llamadas y mensajes SMS en las bandas de funcionamiento actuales, las mismas que utilizan los celulares modernos, y puede transmitir una comunicación en poco tiempo, aproximadamente entre 3 y 5 segundos.

La mayoría de los dispositivos se han probado con más de 400 horas de funcionamiento y un total de más de 1000 horas cada uno, verificando el enlace con el sistema de telecomunicaciones a través de una tarjeta SIM. Estos dispositivos pueden realizar y recibir llamadas, enviar y recibir SMS, y transmitir datos a través de la red celular. Esto permite enviar más información a través de este medio y

generar una ubicación (GPS) con mayor precisión de los usuarios que tienen el dispositivo intercomunicador celular IoT a la mano.

El dispositivo intercomunicador celular IoT (2000), al enviar datos a través de la red celular, permite que los servidores reciban esta información y la procesen de manera rápida y optimizada, permitiendo reaccionar y tomar decisiones en el momento de asistir a un usuario que se encuentra en una situación de peligro o presencia una situación peligrosa.

Con el ecosistema del sistema, que integra la APP, el dispositivo intercomunicador celular IoT junto con el procesamiento de información en la nube potenciado y logrado por el uso de plataformas de servicios y computación en nube, se logra una alta disponibilidad en el control del flujo de decisiones algorítmicas. Esto permite proteger y dar respuesta lo antes posible, o casi de inmediato, a los usuarios en los diferentes sectores de protección.

El compromiso con la innovación tecnológica permite a la presente invención mejorar continuamente su capacidad de respuesta. La integración de tecnologías emergentes como la inteligencia artificial y el análisis de datos masivos optimiza la toma de decisiones y la eficiencia operativa.

* * * * *