

UNIVERSIDAD LATINA DE COSTA RICA

**FACULTA DE INGENIERÍAS Y TECNOLOGÍAS DE LA INFORMACIÓN
Y COMUNICACIÓN TIC's**

ESCUELA DE INGENIERÍA ELÉCTRICA Y MECÁNICA

LICENCIATURA EN INGENIERIA ELECTRÓNICA

**Trabajo Final de Graduación para optar por el título de Licenciatura de
Ingeniería Electrónica con énfasis en Telecomunicaciones**

**Sistema de Rastreo y Alerta de Apertura No Autorizada de
Contenedores Marítimos**

Autor:

Luis Alberto Ramírez Jiménez

Heredia, Costa Rica

Enero 2023



TRIBUNAL EXAMINADOR

Este proyecto titulado: Sistema de Rastreo y Alerta de Apertura No Autorizada de Contenedores Marítimos, por el estudiante: Luis Alberto Ramírez Jiménez, fue aprobada por el Tribunal Examinador de la carrera de Ingeniería Electrónica de la Universidad Latina de Costa Rica, Sede Heredia, como requisito para optar por el grado de Licenciatura en Ingeniería Electrónica con énfasis en Telecomunicaciones:

Ing. Christopher Ryan Russell Clark

Tutor

Ing. Ángel Alejo Quirós García

Lector

Ing. Freed Castillo Moya

Representante

Carta de aprobación del filólogo

Cartago, 26 de enero de 2023

Los suscritos, Elena Redondo Camacho, mayor, casada, filóloga, incorporada a la Asociación Costarricense de Filólogos con el número de carné 0247, portadora de la cédula de identidad número 3-0447-0799 y, Daniel González Monge, mayor, casado, filólogo, incorporado a la Asociación Costarricense de Filólogos con el número de carné 0245, portador de la cédula de identidad número 1-1345-0416, ambos vecinos de Quebradilla de Cartago, revisamos el trabajo final de graduación que se titula: *Sistema de Rastreo y Alerta de Apertura No Autorizada de*

Contenedores Marítimos, sustentado por Luis Alberto Ramírez Jiménez.

Hacemos constar que se corrigieron aspectos de ortografía, redacción, estilo y otros vicios del lenguaje que se pudieron trasladar al texto. A pesar de esto, la originalidad y la validez del contenido son responsabilidad directa de la persona autora.

Esperamos que nuestra participación satisfaga los requerimientos de la Universidad Latina de Costa Rica.

**X ANA ELENA
REDONDO
CAMACHO
(FIRMA)**

Firmado digitalmente por
ANA ELENA REDONDO
CAMACHO (FIRMA)
Fecha: 2023.01.26
14:53:22 -06'00'

Elena Redondo Camacho
Filóloga - Carné ACFIL n.º 0247

**X DANIEL ALBERTO
GONZALEZ
MONGE (FIRMA)**

Firmado digitalmente por
DANIEL ALBERTO
GONZALEZ MONGE (FIRMA)
Fecha: 2023 01 26 14:55:11

Daniel González Monge
Filólogo - Carné ACFIL n.º 0245

Declaración Jurada

Yo, Luis Alberto Ramírez Jiménez estudiante de la Universidad Latina de Costa Rica, declaro bajo la fe de juramento y consciente de las responsabilidades penales de este acto, que soy el Autor Intelectual del Proyecto de Graduación , titulado:

Sistema de Rastreo y Alerta de Apertura No Autorizada de Contenedores Marítimos

Por lo que libero a la Universidad de cualquier responsabilidad en caso de que mi declaración sea falsa.

Firmo en Cartago, 9 de enero de 2023



Luis Alberto Ramírez Jiménez

Licencia De Distriibución No Exclusiva (carta de la persona autora para uso didáctico)

Universidad Latina de Costa Rica

Yo (Nosotros): Luis Alberto Ramírez Jiménez

De la Carrera / Programa: Ingeniería en Electrónica

Modalidad de TFG: Proyecto de Graduación

Titulado: Sistema de Rastreo y Alerta de Apertura No Autorizada de Contenedores Marítimos

Al firmar y enviar esta licencia, usted, el autor (es) y/o propietario (en adelante el "**AUTOR**"), declara lo siguiente: **PRIMERO:** Ser titular de todos los derechos patrimoniales de autor, o contar con todas las autorizaciones pertinentes de los titulares de los derechos patrimoniales de autor, en su caso, necesarias para la cesión del trabajo original del presente TFG (en adelante la "**OBRA**"). **SEGUNDO:** El **AUTOR** autoriza y cede a favor de la **UNIVERSIDAD U LATINA S.R.L.** con cédula jurídica número 3-102-177510 (en adelante la "**UNIVERSIDAD**"), quien adquiere la totalidad de los derechos patrimoniales de la **OBRA** necesarios para usar y reusar, publicar y republicar y modificar o alterar la **OBRA** con el propósito de divulgar de manera digital, de forma perpetua en la comunidad universitaria. **TERCERO:** El **AUTOR** acepta que la cesión se realiza a título gratuito, por lo que la **UNIVERSIDAD** no deberá abonar al autor retribución económica y/o patrimonial de ninguna especie. **CUARTO:** El **AUTOR** garantiza la originalidad de la **OBRA**, así como el hecho de que goza de la libre disponibilidad de los derechos que cede. En caso de impugnación de los derechos autorales o reclamaciones instadas por terceros relacionadas con el contenido o la autoría de la **OBRA**, la responsabilidad que pudiera derivarse será exclusivamente de cargo del **AUTOR** y este garantiza mantener indemne a la **UNIVERSIDAD** ante cualquier reclamo de algún tercero. **QUINTO:** El **AUTOR** se compromete a guardar confidencialidad sobre los alcances de la presente cesión, incluyendo todos aquellos temas que sean de orden meramente institucional o de organización interna de la **UNIVERSIDAD**. **SEXTO:** La presente autorización y cesión se regirá por las leyes de la República de Costa Rica. Todas las controversias, diferencias, disputas o reclamos que pudieran derivarse de la presente cesión y la materia a la que este se refiere, su ejecución, incumplimiento, liquidación, interpretación o validez, se resolverán por medio de los Tribunales de Justicia de la República de Costa Rica, a cuyas normas se someten el **AUTOR** y la **UNIVERSIDAD**, en forma voluntaria e incondicional. **SÉPTIMO:** El **AUTOR** acepta que la **UNIVERSIDAD**, no se hace responsable del uso, reproducciones, venta y distribuciones de todo tipo de fotografías, audios, imágenes, grabaciones, o cualquier otro tipo de

presentación relacionado con la **OBRA**, y el **AUTOR**, está consciente de que no recibirá ningún tipo de compensación económica por parte de la **UNIVERSIDAD**, por lo que el **AUTOR** haya realizado antes de la firma de la presente autorización y cesión. **OCTAVO:** El **AUTOR** concede a **UNIVERSIDAD**, el derecho no exclusivo de reproducción, traducción y/o distribuir su envío (incluyendo el resumen) en todo el mundo en formato impreso y electrónico y en cualquier medio, incluyendo, pero no limitado a audio o video. El **AUTOR** acepta que **UNIVERSIDAD** puede, sin cambiar el contenido, traducir la **OBRA** a cualquier lenguaje, medio o formato con fines de conservación. **NOVENO:** El **AUTOR** acepta que **UNIVERSIDAD** puede conservar más de una copia de este envío de la **OBRA** por fines de seguridad, respaldo y preservación. El **AUTOR** declara que el envío de la **OBRA** es su trabajo original y que tiene el derecho a otorgar los derechos contenidos en esta licencia. **DÉCIMO:** El **AUTOR** manifiesta que la **OBRA** y/o trabajo original no infringe derechos de autor de cualquier persona. Si el envío de la **OBRA** contiene material del que no posee los derechos de autor, el **AUTOR** declara que ha obtenido el permiso irrestricto del propietario de los derechos de autor para otorgar a **UNIVERSIDAD** los derechos requeridos por esta licencia, y que dicho material de propiedad de terceros está claramente identificado y reconocido dentro del texto o contenido de la presentación. Asimismo, el **AUTOR** autoriza a que en caso de que no sea posible, en algunos casos la **UNIVERSIDAD** utiliza la **OBRA** sin incluir algunos o todos los derechos morales de autor de esta. **SI AL ENVÍO DE LA OBRA SE BASA EN UN TRABAJO QUE HA SIDO PATROCINADO O APOYADO POR UNA AGENCIA U ORGANIZACIÓN QUE NO SEA UNIVERSIDAD U LATINA, S.R.L., EL AUTOR DECLARA QUE HA CUMPLIDO CUALQUIER DERECHO DE REVISIÓN U OTRAS OBLIGACIONES REQUERIDAS POR DICHO CONTRATO O ACUERDO.** La presente autorización se extiende el día 9 de enero de 2023 a las 16:44

1 Firma del estudiante(s):



I. Resumen

El presente trabajo es una investigación aplicada que plantea una solución al problema de que, a pesar de que la tecnología requerida está disponible, no se desarrolló un producto de bajo costo que permita dar seguimiento a contenedores marítimos, que los haga visibles en todo momento y permita informar en tiempo real de eventos que hagan sospechar sobre una posible contaminación con drogas del contenedor durante su traslado, desde el punto donde se carga hasta el momento en que se embarca.

La metodología usada para el desarrollo del presente proyecto combina investigación documental, empírica, experimental y tecnológica, cuyos resultados se utilizan en beneficio de la sociedad.

Durante el desarrollo del proyecto se formula la propuesta de un sistema de rastreo satelital para contenedores marítimos, combinando el Internet de las cosas (IoT) con tecnologías de geolocalización satelital y redes móviles terrestres, utilizando plataformas de desarrollo disponibles.

Del desarrollo del proyecto se confirma que la tecnología necesaria para la creación del producto propuesto está disponible y es asequible, incluso más asequible de lo que se esperaba cuando se formuló el problema.

II. Índice general

I. Resumen.....	I
II. Índice general	II
III. Índice de tablas.....	V
IV. Índice de figuras.....	VI
Capítulo I.....	1
1 Problema y propósito	1
1.1 Síntomas	1
1.2 Causas	1
1.3 Pronóstico.....	3
1.4 Control al pronóstico.....	3
1.5 Formulación del problema	3
1.6 Sistematización del problema.....	4
1.7 Objetivo general	7
1.8 Objetivos específicos.....	7
1.9 Estado actual de la investigación.....	7
1.10 Metodológica	15
Capítulo II.....	18
2 Marco teórico	18
2.1 Marco situacional.....	18
2.2 Marco conceptual	30

2.3	Sistemas globales de navegación por satélite (GNSS)	32
2.4	Internet de las cosas (IoT)	45
2.4.1	Sensores	50
2.4.2	Microcontroladores.....	52
2.4.3	Firmware	56
2.4.4	Conectividad	57
2.4.5	Baterías.....	60
2.4.6	Plataforma IoT.....	62
2.5	Automated Vehicle Location	63
2.6	Hipótesis.....	64
2.7	Limitaciones.....	64
2.8	Alcances.....	64
Capítulo III.....		65
3	Propuesta.....	65
3.1	Plataforma IoT.....	67
3.2	Selección de la plataforma	70
3.3	Diseño de hardware.....	72
3.3.1	Primera prueba experimental	72
3.3.2	Segunda prueba experimental	73
3.3.3	Análisis de resultados de las pruebas	75
3.3.4	Selección de hardware.....	76
3.3.5	Diseño de la carcasa de protección y soporte.....	95

3.3.6 Firmware del dispositivo IoT.....	99
3.4 Análisis de costos.....	105
Conclusiones	107
Recomendaciones	107
Referencias.....	109
Bibliografía citada:	109
Bibliografía consultada.....	118
Glosario.....	120
Anexos	121

III. Índice de tablas

Tabla 1. Análisis de Afinidad de las Soluciones Comerciales al Problema	12
Tabla 2. Resultados de Mediciones importantes	73
Tabla 3. Respuesta a la consulta de estado de Wetrack	74
Tabla 4. Resultados obtenidos en la Prueba	75
Tabla 5. Criterios de Búsqueda de Componentes	78
Tabla 6. Estimación de la Cantidad de datos de la Trama.....	92
Tabla 7. Cálculo de corriente Individual por módulo	94
Tabla 8. Resumen de costos Escenario 3	106

IV. Índice de figuras

Figura 1. Método de contaminación llamado gancho ciego	26
Figura 2. Diagrama de una jaula de Faraday.....	31
Figura 3. Comparativa de sistemas globales de navegación por satélite.....	32
Figura 4. Planteamiento Geométrico de trilateración.....	35
Figura 5. Patrón de Radiación Ideal para una Antena GNSS	41
Figura 6. Diagrama general de constitución de un receptor GNSS (Antena)....	42
Figura 7. Diagrama general de constitución de un receptor GNSS (Sección RF)	43
Figura 8. Diagrama general de constitución de un receptor GNSS (Sección de Procesamiento)	45
Figura 9. diagrama de bloques de un microcontrolador esp32	55
Figura 10. Sistema de Rastreo y Alerta de Apertura No Autorizada de Contenedores Marítimos	66
Figura 11. Concox, Wetrack	73
Figura 12. Dimensiones del PCB de la Tarjeta de Desarrollo Elegida	83
Figura 13. Tarjeta de Desarrollo Elegida	85
Figura 14. Fuentes de reactivación del cpu	88
Figura 15. Sección de la configuración del multiplexor de GPIO	89
Figura 16. Características eléctricas de los GPIO	90
Figura 17. Especificaciones del fotoresistor PDV-P9203.....	91
Figura 18. Divisor de Tensión	91

Figura 19. Tiempos de actividad de los Diferentes Módulos.....	95
Figura 20. Fotografías de las Principales Mediciones	97
Figura 21. Diseño Propuesto para la Carcasa Plástica	98
Figura 22. Diagrama de flujo del firmware Propuesto.....	99
Figura 23. Coordenadas de la ULatina	102
Figura 24. Tiempo Unix para el Ejemplo.....	102
Figura 25. Geolocalización Según los Datos Enviados a la plataforma	103

Capítulo I

1 Problema y propósito

1.1 Síntomas

- ❖ Se emplean sistemas de seguridad inadecuados o anticuados intentando prevenir que los contenedores marítimos se vulneren.
- ❖ Los grupos de delincuencia organizada aprovechan las vulnerabilidades del sistema logístico de exportación de productos por la vía marítima para introducir drogas entre los contenedores de exportación.
- ❖ Cuando se da un decomiso de drogas dentro de un contenedor, ya sea en el país de origen o en el país de destino, el dueño del contenido del contenedor, el exportador, se ve afectado seriamente: su producto se confisca y somete a revisión, proceso que puede dañarlo. Además, aún si el producto no sufrió daños durante la contaminación o el proceso de exportación, es probable que pierda su posibilidad de venta por haber perdido calidad o inocuidad, lo que genera al exportador grandes pérdidas económicas, ya que ningún seguro ofrece protección para este tipo de eventos (O. Abrahams, comunicación personal, 26 de diciembre de 2022).

1.2 Causas

- ❖ En Costa Rica, cuando se da un decomiso de drogas en contenedores de exportación, la empresa naviera y la compañía transportista sufren poca afectación, por este motivo, les importa poco que un contenedor suyo sea contaminado con drogas. Su principal interés es mantener los costos bajos para competir en el mercado por lo que evitan incurrir en gastos innecesarios

para su operación (K. Chinchilla, comunicación personal, octubre de 2021; J. C. Bonilla, comunicación personal, 4 de noviembre de 2022).

- ❖ Para la mayoría de los exportadores, un costo de exportación adicional de un monto mayor que \$100 por cada contenedor se considera inviable para la mayoría de los casos. Las soluciones que tienen un precio menor que \$100 son poco seguras e inútiles para resolver el problema (A. Flores, comunicación personal, 11 de noviembre de 2022).
- ❖ Debido a que las empresas navieras no se interesan por el seguimiento de contenedores, cualquier costo adicional que mejore la seguridad de las mercancías corre por cuenta del exportador, lo que aumenta sus costos.
- ❖ En el ámbito mundial solamente el 3.6 % de los contenedores marítimos se rastrean mediante IoT, pues el rastreo convencional de contenedores que se basa en los registros de arribo y partida de los buques suele ser suficiente para fines logísticos. En tierra, los contenedores se rastrean con fines logísticos mediante el rastreo de los camiones que los transportan, sin embargo, es común que el chofer del camión esté involucrado cuando se da un evento de contaminación durante el traslado hasta el puerto. Históricamente, el seguimiento de contenedores mediante IoT no ha tenido demanda suficiente para justificar el costo adicional (Bartlett, 2022).
- ❖ Los problemas de contaminación de contenedores con drogas están circunscritos a unos pocos países.
- ❖ El mercado de rastreo de contenedores marítimos es poco interesante para los fabricantes de dispositivos de rastreo debido a su baja demanda y a que las soluciones existentes en el mercado, incluso cuando no son del todo seguras, son suficientes para los requerimientos de la mayoría de sus clientes (A. Ko, comunicación personal, 13 de junio de 2022; L. Leig, comunicación

personal, 18 de octubre de 2022; G. Deng, comunicación personal, 18 de agosto de 2022).

- ❖ El costo promedio de las pocas soluciones existentes en el mercado diseñadas especialmente para el seguimiento de contenedores tiene los inconvenientes de que: su precio unitario ronda los \$350 (C. Drelevich, comunicación personal, 19 de diciembre de 2022). Estos equipos no pueden recuperarse si no se implementa una logística compleja y costosa, sus antenas quedan fuera del contenedor y son susceptibles de ser violentadas.

1.3 Pronóstico

Debido al poco interés por el rastreo de contenedores en el ámbito mundial, no parece que en el corto o mediano plazo se vaya a desarrollar una solución IoT que tenga las características necesarias para fungir como herramienta que prevenga la contaminación de contenedores marítimos con drogas.

1.4 Control al pronóstico

Debido a la gran cantidad de tiempo que es necesaria para obtener estadísticas sobre este problema y la gran cantidad de variables que inciden en este, no es posible controlar el pronóstico. Los fabricantes consultados indicaron que los productos que tienen actualmente satisfacen las necesidades del mercado.

1.5 Formulación del problema

Es necesario poner a disposición de los exportadores costarricenses y las autoridades de control de drogas una solución especializada y de bajo costo, para dar seguimiento a los contenedores marítimos a lo largo de toda la cadena de abasto, que permitan tener pleno control de sus movimientos y eventos, funcionando como un sistema de seguridad integral y no solo como un sistema de apoyo logístico.

Los sistemas tecnológicos de seguridad existentes en el mercado no pueden dar seguimiento a los contenedores marítimos de exportación durante todo su trayecto, hasta que se cargan en el buque o lo permiten, pero son vulnerables de ser removidos, violentados o engañados y a un alto costo, dejando los contenedores sin protección en momentos críticos en que son susceptibles de contaminarse con drogas.

Según los datos de la Policía de Control de Drogas (PCD), una gran cantidad de cocaína se exporta desde Costa Rica hacia Europa y Estados Unidos, mediante la introducción ilícita de esta en contenedores marítimos. Además de las consecuencias que esto tiene en la reputación de los exportadores y por tanto del país como exportador, potencia los efectos nocivos para la sociedad que implica la existencia del narcotráfico.

1.6 Sistematización del problema

Según Juan Carlos Bonilla, gerente de Operaciones de DOLE Costa Rica (J. C. Bonilla, comunicación personal, 10 de noviembre de 2022), la logística de exportación funciona de la siguiente manera. Cuando un exportador tiene sus productos listos para hacer el envío a su cliente, se comunica con la empresa naviera que le brinda el servicio de transporte de su producto, desde su planta de producción o empaque hasta las instalaciones de su cliente final. Para brindarle el servicio, la compañía naviera le envía el contenedor esterilizado y listo para usarse. Una vez cargado, el contenedor se cierra y se le coloca un dispositivo físico de seguridad pasiva conocido como marchamo de botella, sello, precinto o lacre, que está numerado con un identificador único que se registra en los sistemas informáticos de la naviera y de la Dirección General de Aduanas, este se coloca sobre los mecanismos de cierre para asegurar que estos no se abran sin autorización (adrede o por accidente).

Una vez colocado el dispositivo de seguridad descrito, no puede eliminarse sin provocar su destrucción, es decir, una fuerza física sobre el que produzca su daño y, en consecuencia, haga evidente que fue violentado y evite su futura reutilización (Precintia, 2022). La simplicidad de este sistema tradicional de seguridad facilitó su falsificación

por parte de los delincuentes, haciéndolo inútil para asegurar la inocuidad de los contenedores marítimos y los productos que transporta, así como para garantizar que el contenedor no ha sido contaminado con drogas.

Para mejorar los procesos logísticos de exportación de mercancías en contenedores marítimos, se requiere un producto o servicio que brinde alta visibilidad de los contenedores durante su transporte desde que se cierran en el lugar de carga, durante su traslado a los puertos y hasta el momento en que se embarcan. Esto asegura la inocuidad e integridad física de los productos que transportan y garantiza que no están contaminados con drogas. Las mismas fortalezas que hacen que la solución sea de gran utilidad en la lucha contra el narcotráfico, la hacen ideal para prevenir otros delitos que implican la manipulación de los contenedores marítimos, el irrespeto a las rutas de transporte establecidas y el irrespeto a los tiempos de tránsito definidos según las rutas.

La solución ideal para este fin debe poder utilizarse dentro de los contenedores marítimos, a la vez que permita su geolocalización precisa mediante el uso de tecnologías GNSS. Esto brinda seguridad de que no es susceptible de violentarse o removerse del contenedor al que se le quiere dar seguimiento. El hecho de que este dispositivo esté diseñado para usarse dentro de contenedores marítimos tiene algunas implicaciones: primero, que el equipo no es recuperable y, por lo tanto, su costo debe ser consecuente con ese hecho; segundo, el diseño o disposición de su antena debe permitirle captar señales muy débiles de uno o varios de los servicios GNSS.

La razón por la cual los dispositivos rastreadores colocados en el interior de un contenedor marítimo exportado tienen un costo altísimo de recuperación es que la operación de las empresas navieras, para optimizar el uso de sus contenedores marítimos, aprovecha la ubicación actual de cada contenedor para programar despachos desde esa misma ubicación o ubicaciones cercanas a esta. Por lo anterior, por ejemplo, un contenedor que sale de Costa Rica con productos de exportación y destino final a Europa Occidental viajará hasta el puerto europeo designado y, una vez

en este puerto, puede utilizarse para despachar mercancías que tienen como origen Europa y destino China.

Siguiendo con el ejemplo, una vez que el contenedor se encuentre en China, puede enviarse a cualquier otro lugar del mundo y puede no regresar a Costa Rica en varios meses o incluso no regresar nunca, impidiendo la recuperación sencilla del rastreador. Colaboraciones con otras compañías que tengan la capacidad de recuperar los equipos requieren una logística compleja y costosa como es de suponer.

Entre las principales reglas que un contenedor cargado en tránsito terrestre debe cumplir, están: no debe desviarse de la ruta preestablecida sin autorización previa, una vez que inicia el traslado, no debe detenerse sin autorización y, de detenerse con autorización, estos periodos ociosos del contenedor no pueden superar los 10 min por cada evento. Para que sea posible detectar cada uno de estos eventos con precisión es indispensable contar en todo momento con la ubicación precisa del contenedor, cosa que hasta ahora solo es posible utilizando tecnología GNSS.

Otra característica deseable e importante que debe tener el servicio de seguimiento de contenedores es la detección de la apertura de las puertas del contenedor, esto porque la detención no autorizada puede darse por muchas causas sin que alguna de estas sea necesariamente un evento de contaminación. Una detención no autorizada combinada con la detección de la apertura de las puertas del contenedor definitivamente implica que se dio una anomalía que hace obligatoria la inspección manual de ese contenedor.

Contar con soluciones como la descrita permite a los exportadores y a las autoridades reaccionar oportunamente ante situaciones anómalas que puedan indicar la comisión de delitos de robo de contenedores marítimos y las mercancías que contienen o la contaminación de estos con drogas para su exportación y recibir todos los beneficios que esto implica para el país. El presente proyecto de graduación pretende plantear una solución que satisfaga las necesidades que tiene el mercado en lo referente a la protección de contenedores marítimos, mediante la implementación de tecnologías existentes, combinándolas y adaptándolas al fin descrito.

1.7 Objetivo general

Diseñar un sistema de seguimiento de contenedores marítimos de exportación que sea de bajo costo y facilite monitorearlos, desde su origen hasta que se cargan en los buques que los transportan a su destino final, para evitar que se contaminen con drogas.

1.8 Objetivos específicos

- ❖ Investigar cuáles de las soluciones de seguimiento de activos existentes en el mercado son susceptibles de modificarse o adaptarse para reducir costos en las etapas de diseño, prototipado y producción.
- ❖ Estudiar las dimensiones y partes relevantes de los contenedores marítimos, con el fin de utilizar la información que se recopiló en el diseño de la propuesta.
- ❖ Diseñar un dispositivo rastreador o adaptar uno existente, con la premisa de que quede oculto y protegido por la estructura del contenedor marítimo, pero manteniendo excelente recepción satelital y celular.
- ❖ Estudiar las diferentes plataformas IoT disponibles en el ámbito comercial para determinar si es conveniente para el proyecto utilizar una plataforma existente o si, por el contrario, conviene desarrollar una plataforma propia.

1.9 Estado actual de la investigación

Después de analizar el problema social con sus causas, sus efectos y los *modus operandi* de los grupos de delincuencia organizada para cometer los delitos, se identificaron diferentes estrategias que pretenden dar una solución al problema. Sin embargo, estas soluciones tienen debilidades importantes que las hacen poco aptas para dar seguimiento a contenedores marítimos de exportación a bajo costo, desde su

origen hasta que se cargan en los buques que los llevan a su destino final para evitar que se contaminen con drogas por parte de los grupos delictivos organizados.

Las soluciones existentes en el mercado son:

- ❖ Soluciones pasivas de corto alcance. Las soluciones con base en tecnologías de identificación por radio frecuencia, mejor conocidas como RFID por sus siglas en inglés, son las más populares por su bajo costo. Su implementación se hace principalmente con fines logísticos. Las partes principales de un sistema de este tipo son el denominado TAG o etiqueta RFID, antenas y un dispositivo lector que entrega la información leída a otros sistemas según la necesidad. La etiqueta RFID contiene un *chip* que emite su número de identificación cuando se energiza, no requiere alimentación propia. Sin embargo, hay algunas etiquetas que cuentan con una batería. La energización del *chip* se lleva a cabo cuando la etiqueta es expuesta a la radiación de las antenas, esta radiación se captura y rectifica en la etiqueta y después se envía al *chip* en forma de corriente directa. Como respuesta, el *chip*, que es un transmisor RF, envía a las antenas su identificación y esta lo utiliza el sistema informático de acuerdo con la aplicación. Las principales limitantes de utilizar estos sistemas con fines de protección de mercancías son que la información del *chip* solo puede leerse donde exista la infraestructura requerida, impidiendo la visibilidad de las mercancías cuando estén fuera del alcance de las antenas (12 m).
- ❖ Soluciones activas de corto alcance son las soluciones con base en RF con sistemas activos, por ejemplo, ZigBee, Bluetooth y wifi. Su rango es de unas pocas decenas de metros y se utilizan especialmente en aplicaciones logísticas, su visibilidad es muy baja.
- ❖ Rastreadores autónomos LTE. Estos dispositivos utilizan una de las ventajas que tienen las redes celulares o móviles sobre los sistemas GNSS: las señales provenientes de redes celulares, por tratarse de redes terrestres,

suelen ser mucho más fuertes que las señales satelitales y tienen un ángulo de propagación paralelo a la superficie terrestre. Estas características les permiten a estas señales provenientes de las radiobases celulares, penetrar hacia el interior de los contenedores marítimos a través de las aberturas ubicadas entre las puertas del contenedor y entre estas y el marco estructural que las soporta, quedando disponibles en el interior del contenedor, en la cercanía de esas aberturas, pero con baja potencia. Esta categoría de dispositivos rastreadores opera únicamente usando las redes celulares y los hay diseñados específicamente para instalarse en el interior de los contenedores marítimos siempre que se instalen en las cercanías de las puertas. Las estimaciones de su localización se realizan mediante sistemas con base en la triangulación de señales, utilizando información de la radio base celular a la cual el dispositivo está conectado y su proximidad a otras radiobases para estimar su geolocalización. Una de sus principales desventajas es que la precisión de esta información puede ir desde algunos cientos de metros hasta unos pocos miles (HEAVYAI, 2022). Esa baja precisión hace que esta tecnología sea suficiente para algunos usos logísticos y comerciales, pero completamente inútil para usos que se relacionan con seguridad de mercancías y seguimiento de contenedores marítimos, pues al no brindar una localización exacta, el sistema no cuenta con información suficiente para saber si hubo un desvío de la ruta establecida una parada no autorizada y no se tiene la localización exacta en caso de que sea necesario interceptar el contenedor durante su tránsito.

- ❖ Candados electrónicos (GNSS y LTE). Los candados o precintos electrónicos son de un candado electromecánico controlado por un sistema electrónico que integra un rastreador GNSS y un *modem* celular para transmitir la información de su ubicación y otras variables a un sistema remoto de monitoreo. Su principal ventaja es que, una vez instalado y cerrado, impide que las puertas de los contenedores puedan ser abiertas sin violentarlo, circunstancia a la cual la mayoría de los dispositivos de su clase emite una

alerta indicando ese evento. Entre sus principales desventajas están que, al integrar un mecanismo electromecánico, una batería de polímeros de litio de gran tamaño y otros componentes costosos, su precio se eleva y los modelos de negocio bajo los cuales se usa requieren que el dispositivo sea recuperable para que la prestación del servicio sea rentable. Un ejemplo de este servicio es el denominado marchamo electrónico que ofrecen empresas privadas fungiendo como auxiliares de la función pública, junto con la Dirección General de Aduanas, para contenedores de importación (Poder Judicial, 2022). En este modelo de negocio, el objetivo es detectar si los contenedores se abren antes de que su contenido pague los impuestos de importación correspondientes, se exige que algunos productos que ingresan al país, más fácilmente vendibles en el mercado negro, sean custodiados por un dispositivo de este tipo, desde que salen del puerto hasta que llegan al almacén fiscal, lugar donde se hace el trámite de declaración de impuestos.

- ❖ Rastreadores autónomos (GNSS/LTE) de uso general. Estos son los diseñados para adherirse al cuerpo de un vehículo o en este caso, de un contenedor marítimo. Este tipo de dispositivo, además de no tener ningún mecanismo de seguridad que lo proteja de violentarse o removerse, tiene la debilidad de no ejercer ningún control sobre la apertura de las puertas del contenedor, haciéndolo completamente inútil para esta aplicación. Existe gran variedad de estos dispositivos, algunos son de muy simple construcción y bajo costo y los hay especializados a un alto costo.
- ❖ Rastreadores autónomos (GNSS/LTE/Satelital) especializados se diseñan para instalarse de modo que las antenas LTE y GNSS queden expuestas fuera del contenedor para lograr una buena recepción de señal y el resto del cuerpo dentro del contenedor. Su principal aplicación es logística, son una herramienta para tener visibilidad en todo el trayecto del contenedor hasta la llegada a su país de destino. En algunas versiones funcionan con transmisión dual, LTE/Satelital. No representan una gran ventaja con respecto a la

categoría anterior, son susceptibles de manipularse debido a que sus antenas quedan afuera del contenedor. Por la robustez que requieren para soportar condiciones adversas, especialmente maltrato, la gran autonomía que requiere una batería de alta capacidad y su baja demanda, sus precios son sumamente altos y, ya que no pueden recuperarse con facilidad, el costo para el exportador está fuera de presupuesto de los exportadores.

Para facilitar la evaluación de las diferentes soluciones existentes en el mercado que pretenden resolver problemas similares al propuesto, se definieron en este trabajo tres criterios de evaluación de la tecnología o tecnologías en las que basan su funcionamiento y que deben estar presentes en la solución. Además, se definieron tres grados de afinidad con el criterio (alta, baja y nula), con el fin de identificar sus fortalezas y vulnerabilidades como solución:

- ❖ **Visibilidad.** Para efectos de seguridad y logística, la visibilidad se refiere a los periodos durante los cuales no es posible conocer la ubicación exacta del activo. Es ideal contar con la máxima visibilidad posible. Por ejemplo, un activo rastreado mediante tecnología RFID solo es visible en los momentos en que esté dentro del alcance de las antenas de estos sistemas, máximo de 12 m. Por otro lado, los activos seguidos mediante rastreadores cuya transmisión de ubicación se realiza por medio de redes móviles o satelitales tienen una visibilidad mucho mayor debido a que la cobertura de estas redes es global.
- ❖ **Seguridad.** Para el caso particular del objeto del presente trabajo, un sistema de seguridad es seguro en la medida en que proteja al contenedor marítimo de ser abierto sin que se note por los interesados. Se definen los siguientes parámetros para la evaluación de las soluciones, el grado de seguridad se define como alto si la solución cumple con tres de esos parámetros, bajo si cumple solo dos y, en su defecto, es nulo:

- Resistencia física: capacidad de mantenerse en funcionamiento y adherido o instalado en el contenedor a pesar de los intentos de remoción o destrucción.
 - Pronta detección: se refiere a la capacidad del sistema de detectar comportamientos anormales que indiquen la intención de cometer un delito, para mejorar el tiempo de reacción policial y de los propietarios.
 - Retención activa: detectar apertura de las puertas del contenedor marítimo.
- ❖ **Costo.** Según reuniones sostenidas con el gerente de operaciones de Dole Costa Rica, Juan Carlos Bonilla, y Kenny Chinchilla, de King Ocean Costa Rica, para la mayoría de los exportadores un costo de exportación adicional de un monto mayor que \$100 por cada contenedor se considera inviable para la mayoría de los casos. Se usa entonces para este trabajo el criterio de que una solución cuyo costo total sea superior a \$100 por contenedor no es rentable.

En la siguiente tabla, se resume el resultado del análisis realizado para la evaluación de las opciones disponibles según los criterios antes expuestos. La tabla muestra una comparación de las soluciones de acuerdo con cada criterio, así como un criterio final de si puede considerarse apto para la aplicación o no.

TABLA 1. ANÁLISIS DE AFINIDAD DE LAS SOLUCIONES COMERCIALES AL PROBLEMA

Criterios	Afinidad con Visibilidad	Afinidad con Seguridad	Afinidad con Costo	Aptitud
Sistemas RFID	Baja	Nula	Alta	No Apto
Sistemas corto alcance (ZigBee, Bluetooth y otros)	Baja	Nula	Alta	No Apto
Rastreadores autónomos LTE (sin GNSS)	Baja	Nula	Alta	No Apto

Candados Electrónicos (GNSS y LTE)	Alta	Nula	Nula	No Apto
Rastreadores autónomos (GNSS/LTE) de uso general	Alta	Nula	Alta	No Apto
Rastreadores autónomos (GNSS/LTE/Satelital) especializados	Alta	Baja	Nula	No Apto
Nota. Para que una solución se considere como apta, debe tener algún grado de afinidad con todos los criterios de forma simultánea.				

Según el análisis resumido en la tabla la categoría *Rastreadores autónomos (GNSS/LTE/Satelital) especializados* es la opción más cercana a una solución al problema que se planteó desde las perspectivas de visibilidad y seguridad. Por esta razón, se profundiza todavía más en la investigación de estas pretendiendo encontrar un producto o servicio con un precio cercano al deseable, de acuerdo con el criterio de costo que es el que en la categoría es deficiente.

Los hallazgos se dividen en dos categorías, productos para seguimiento de contenedores y servicios de seguimiento de contenedores.

❖ **Productos:**

- Las empresas T42 (israelí), RSAE (estadounidense) y Concox (China) cuentan con dispositivos especializados para el rastreo de contenedores.

➤ **T42 comercializa los productos (<https://www.t42.co.uk/products>):**

- Tetis 3G Contenedores Secos:
 - Comunicación: Celular + GPS (*built in antenna*).
 - Batería 5200 mAh *battery*.
 - Sensores integrados: Luz, temperatura, acelerómetro e interruptores de detención de apertura de puerta.
 - Costo \$290
- Tetis R 3G Contenedores secos y refrigerados:
 - Comunicación: Celular + GPS (*built in antenna*).

- Batería: 10,400 mAh *battery*.
- Sensores Integrados: Luz, temperatura, acelerómetro e interruptores de detención de apertura de puerta.
- Costo: \$425
- Tetis R Hybrid GSM & Satellite
 - Comunicación: Cellular/Satellite + GPS (built in antenna).
 - Batería: 5,200 mAh.
 - Sensores Integrados: Luz, temperatura, acelerómetro, interruptores de detención de apertura de puerta.
 - Costo: \$870
- **RSAE Labs (<https://rsaelabs.com/product/gs-6c/>):**
 - Global Sentinel® GS-5B
 - Comunicación: GNSS (GPS, Galileo, Glonass, BeiDou), GSM.
 - Batería: Rechargeable NiMH, Low Self-Discharge, Estimated Reports 1200 reports 5+ months.
 - Sensores Integrados: Luz, temperatura, acelerómetro e interruptores de detención de apertura de puerta.
 - Costo: \$600.
- **Concox (<https://www.iconcox.com/products/ct10-3g-container-gps-tracker.html#spec>):**
 - CT10
 - Comunicación: GPS+WiFi+LBS / WCDMA + GSM
 - Batería: 3,800mAh/3.7 V industrial-grade Li-Polymer battery
 - Sensores Integrados: Interruptor de presión, acelerómetro, Giroscopio.
 - Costo: \$180.
- ❖ **Servicios:**
 - Las empresas Avriem y Satlock:
- **Satlock:**

- **Global Container (<https://www.satlock.com/wp/globalcontainer/>)**
 - Utiliza equipos de la marca Concox
 - Considera al equipo desechable y el costo de su monitoreo más el equipo es de \$270 por contenedor, sujeto a volumen no menos de 20 unidades.
- **Arviem (<https://arviem.com/track-and-trace-container-tracking/>):**
 - **Shipping Container Monitoring**
 - Utiliza equipos de las marcas RSAE y T42
 - Cuentan con logística de recuperación de los equipos.
 - El servicio se brinda solo con empresas navieras específicas.
 - El costo del servicio con monitoreo se basa en la cantidad de días de uso empezando en \$20 por día y está sujeto a volumen, no menos de 100 unidades por mes. Un buque tarda aproximadamente dos semanas en trasladarse del puerto de Moín en Costa Rica, al puerto de Amberes en Bélgica.

1.10 Metodológica

El presente trabajo es una investigación aplicada que incluye investigación documental, empírica, experimental y tecnológica, cuyos resultados se utilizan en beneficio de la sociedad. Para determinar la importancia que una propuesta de solución al problema que se planteó puede tener, el primer paso tomado fue investigar los posibles beneficios con los que el desarrollo de la propuesta de solución al problema puede impactar a la sociedad, específicamente en la lucha contra el narcotráfico. La investigación incluyó revisión de entrevistas y audiencias de expertos, entrevista al jefe del Departamento de Inteligencia de la Policía de Control de Drogas, Óscar Abrahams, entrevista al gerente de Operaciones de la empresa Dole, Juan Carlos Bonilla, conversaciones con el gerente de Operaciones de la compañía King Ocean, Kenny Chinchilla, análisis y validación de noticias de prensa, revisión de trabajos documentales, revisión de informes estadísticos y situacionales, documentación técnica y tecnológica, entre otros.

Esta investigación fue de gran utilidad para justificar y motivar el desarrollo de la propuesta, además de sentar las bases para la determinación de las necesidades de los exportadores y la Policía de Control de Drogas. Esta información fue clave al definir los criterios de diseño de la solución y que también se usaron como criterios de evaluación de los productos disponibles en el mercado. Fue en esa etapa donde también se definió que la propuesta debe basar forzosamente su geolocalización en tecnologías GNSS y realizar el envío de información por medio de redes móviles.

Se realizaron dos pruebas experimentales, una con el propósito de conocer las dimensiones de las áreas físicas de interés de los contenedores marítimos, esta consistió en la toma de mediciones y fotografías. La segunda prueba se realizó con el propósito de determinar los niveles de señal de cada una de las tecnologías elegidas en esas mismas áreas y sus alrededores.

Con el análisis de los resultados de estas pruebas se definieron algunos de los criterios para la selección y diseño del *hardware* como las posibles ubicaciones del dispositivo rastreador, las dimensiones del PCB, el tipo de antena por utilizar, especificaciones de la forma de la carcasa plástica, entre otros. Al considerar estos resultados y los criterios de diseño definidos, se eligieron los componentes necesarios para la solución, lo que asegura que cumplan con la funcionalidad requerida y el costo estimado que permita que la solución sea comercialmente viable. Definidos los componentes, se eligió una tarjeta de desarrollo que los integrara y que permitiera el desarrollo del *firmware* de forma sencilla.

La estimación del consumo de energía se realizó una vez definidos los componentes por utilizar y se hizo considerando las diferentes fases por las que debe atravesar el dispositivo. Con la información obtenida se estableció la capacidad mínima de la batería y se buscaron las opciones disponibles comercialmente para evaluar su costo.

Después de estudiar las diferentes plataformas IoT disponibles comercialmente y evaluar los costos de desarrollo de una plataforma propia, se determinó que la opción de hacer un desarrollo propio era costosa e inviable. Se revisaron en detalle las

plataformas más conocidas persiguiendo que la funcionalidad fuera la adecuada y el costo lo más bajo posible. Se evaluaron varias plataformas y destacó una que, por ser de código abierto, permite no solo implementarse con un bajo costo, sino que también es susceptible de modificarse en caso de que se requiera especializarla.

Gracias a que la tarjeta de desarrollo cuenta con documentación suficiente, el desarrollo del *firmware* se redujo a la adaptación de uno de los ejemplos que comprendía toda la funcionalidad requerida. Fue necesario únicamente un cambio estructural con muy poco código añadido.

Capítulo II

2 Marco teórico

2.1 Marco situacional

En América del Sur se produce la totalidad de cocaína que se consume en el ámbito mundial. Es decir, se da la siembra de la planta y la mayor parte de la transformación hasta llegar a la cocaína y se destacan países productores como Bolivia, Colombia y Perú (EL PAcCTO, 2021).

La cocaína es un estimulante extremadamente adictivo que afecta directamente al cerebro. Según el Instituto Nacional sobre el Abuso de Drogas de Estados Unidos (NIH, 2016), la cocaína es una droga clasificada bajo la Lista II (Schedule II) de la Ley sobre Sustancias Controladas de Estados Unidos:

Lo que significa que se considera que tiene un gran potencial para ser abusada, pero que puede ser administrada por un doctor para usos médicos legítimos, por ejemplo, como anestesia local en ciertos tipos de cirugías de los ojos, oídos y garganta (s. p.).

La cocaína se extrae de las hojas de la coca (arbusto eritroxiláceo) que tras someterse a diversos tratamientos químicos se utiliza como droga o como anestésico local en medicina. Como droga, suele presentarse en forma de polvo blanco que se esnifa y es muy tóxica y adictiva (Yépez Maigua, 2018). Hay dos formas químicas de la cocaína que suelen consumirse: la sal de clorhidrato (que es soluble en agua) y los cristales de cocaína o base (que no son solubles en agua), conocidos como *crack* (en referencia al sonido crujiente que se oye cuando se fuma esta mezcla).

La sal de clorhidrato de cocaína, o la forma en polvo de la cocaína, se consume de forma inyectada o inhalada. Los cristales de cocaína han sido procesados con

amoníaco o bicarbonato sódico y agua y luego calentados para eliminar el clorhidrato y producir una sustancia que se puede fumar (NIH, 2016, s. p.).

Durante la década de 2010 y en la actualidad, el uso de cocaína se ha incrementado considerablemente en los países desarrollados, lo que genera gran demanda de la droga. La ley de oferta y demanda se aplica a todos los mercados, tanto lícitos como ilícitos, lo que determina los precios del producto que se pretende obtener. Además, el nivel de riesgo para lograr la entrega del producto al *cliente* incide en el alto precio de la droga. Es decir, la penalización por el tráfico de drogas, el riesgo vinculado con este tipo de ilícito y toda su logística, su consumo y el control de su oferta hacen también que este estupefaciente mantenga un alto precio en el mercado (EL PAcCTO, 2021). Este negocio, al final, es igual a tantos otros y cuanto más lejos estén los países productores de las personas consumidoras más caro es el producto. En el año 2020, en el ámbito mundial se produjeron 1982 t de cocaína pura y existían 21 000 000 personas que la usaban (ONU, 2022).

Con el aumento de la demanda, la producción de cocaína sigue en aumento y se proyecta que la tendencia se mantendrá (ONU, 2022). De acuerdo con la Agencia Europea de la Droga, el aumento de las actividades de producción en Europa (utilizando como materia prima las hojas de coca importadas de Sudamérica) y la colaboración entre grupos delictivos de todo el mundo está creando nuevas amenazas para la seguridad y ampliando el mercado de la cocaína (EMCDDA, 2022).

Según la Organización de las Naciones Unidas (2022), en su Informe Mundial sobre las Drogas 2022, la fabricación potencial de cocaína creció un 11 % en 2020, en comparación con el año anterior, alcanzando un récord de 1.982 t (ajustadas al 100 % de pureza). La fabricación aumentó un 8 % en Colombia y un total combinado de 16.5 % en Perú y el Estado Plurinacional de Bolivia. La fabricación mundial de cocaína se ha duplicado con creces desde el mínimo de 2014. Todo esto a pesar de que la superficie mundial de cultivo de arbusto de coca se mantuvo sin cambios en 2020, en 234.200 ha, un 5 % por debajo del máximo alcanzado en 2018. La disminución de la superficie de cultivo de arbusto de coca en Colombia, del 7.1 % en 2020, se vio

compensada por el aumento de su cultivo en el Perú (13 %) y el Estado Plurinacional de Bolivia (15.3 %). Este aumento de producción sin un incremento en la extensión de las plantaciones se debe al aumento de los rendimientos y a las mayores tasas de eficiencia de los laboratorios. El rendimiento medio de hoja de coca fresca cosechada por hectárea de cultivo de arbusto de coca aumentó un 10 %, pasando de 5,8 t en 2019 a 6,4 t en 2020, mientras que la cantidad global de clorhidrato de cocaína obtenida de una hectárea de cultivo productivo de arbusto de coca aumentó un 18 %, pasando de 6,7 kg en 2019 a 7,9 kg en 2020.

En Costa Rica, el Instituto sobre Alcoholismo y Farmacodependencia (IAFA, 2012) indica que la cocaína, al ser una droga que tiene un mayor costo en el mercado, se asocia con un mayor estatus social y económico y un mayor nivel educativo de las personas consumidoras. En concordancia, los países desarrollados son los principales consumidores de cocaína en el mundo. El destino favorito de la cocaína despachada desde Costa Rica es La Unión Europea debido a que los precios en la calle son más altos en Europa que en Estados Unidos y a que los cárteles colombianos son bloqueados por los cárteles mexicanos que tienen acaparado el mercado de Estados Unidos, dejándoles como principal alternativa la comercialización de la droga en Europa (Vaughn, 2022).

Según cita EL PAcCTO (2021), de acuerdo con el Real Instituto Elcano, un kilo de cocaína de alta pureza vale en España, en la calle, cerca de €80,000. En Colombia, este mismo kilo de cocaína tiene un valor estimado de €1,200, de los que el agricultor productor de coca no cobrará más que €250 por las hojas necesarias para producir un kilo del alcaloide.

Según Álvaro Ramos, exministro de Seguridad y figura pública referente en temas de seguridad en Costa Rica, el país se ha convertido recientemente en el principal receptor de clorhidrato de cocaína en el mundo y en el primer exportador de cocaína a Europa Occidental (Ramos Rechnitz *et al.*, 2022), Espinoza (2022), director del Organismo de Investigación Judicial, también ha indicado esto públicamente. Sin

embargo, ya desde el año 2019, Costa Rica se encontraba entre los cuatro primeros exportadores de cocaína a Europa (Rojas, 2019).

Dos leyes en Costa Rica regulan las actividades que se relacionan con la producción, comercialización y uso de drogas ilícitas: la Ley General de Salud (Ley n.º 5395) y la Ley de Psicotrópicos (Ley n.º 8204). Estas leyes son la base del control de drogas en el país. Han sido promulgadas a partir de las convenciones internacionales, pero se debe aclarar que, en la Ley General de Salud solo menciona la Convención Única de 1961 (art. 126) y la Ley n.º 8204 es la que mayor vigencia tiene y la que se revisa y actualiza con cierta frecuencia (Cortés, 2017).

De acuerdo con Ley n.º 8204 (2002), en Costa Rica:

El comercio, el expendio, la industrialización, la fabricación, la refinación, la transformación, la extracción, el análisis, la preparación, el cultivo, la producción, la importación, la exportación, el transporte, la prescripción, el suministro, el almacenamiento, la distribución y la venta de drogas, sustancias o productos referidos en esta Ley, así como de sus derivados y especialidades, serán actividades limitadas estrictamente a las cantidades necesarias para el tratamiento médico, los análisis toxicológicos y químicos, el entrenamiento de los animales detectores utilizados por los cuerpos de policía y los análisis farmacocinéticos en materia médica o deportiva; para elaborar y producir legalmente medicamentos y otros productos de uso autorizado, o para investigaciones. Solo las personas legalmente autorizadas podrán intervenir en todo lo relacionado con tales sustancias.

Después de su creación, la Ley de Psicotrópicos ha tenido cuatro versiones distintas y, pasó de tener 51 Artículos en su primera versión de 1988 (Ley n.º 7093), a 166 en su cuarta y más reciente versión del 2001 (Ley n.º 8204). Claramente, su evolución ha sido necesaria para enfrentar el creciente problema del narcotráfico. Entre sus cambios más importantes destaca el efectuado en 1998 (Ley n.º 7786), su objetivo fue:

Incluir la Convención Contra el Tráfico Ilícito de 1988 en la legislación nacional mediante los procedimientos policiales de entrega vigilada, encubrimiento y colaboración en investigaciones criminales, controles a personas o instituciones financieras entorno a la ocultación, movilización de capitales provenientes del narcotráfico, control y fiscalización de precursores químicos y mecanismos de colaboración multilateral y extradición de personas (Cortés, 2017, p. 12).

Después de esa modificación, las más significativas son: a la Ley de Psicotrópicos en el 2009 con la Ley n.º 8719, la Ley de Fortalecimiento de la Legislación contra el Terrorismo, que modificó más de 35 artículos de la Ley n.º 8204, Ley contra la Delincuencia Organizada (Ley n.º 8754) que autoriza la intervención de comunicaciones en procesos investigativos que se relacionan con drogas, Ley n.º 9074 del 2012, que modificó los arts. 83, 84, 85 y 87 y agregó los arts. 84 bis y 87, con el fin de otorgarle mayor capacidad de gestión al Instituto Costarricense sobre Drogas con los bienes y dineros decomisados en casos que se relacionan con el tráfico de drogas, y la Ley n.º 9161 del 2013, que introdujo la proporcionalidad y especificidad de género:

Siendo la primera vez que se modifica la legislación costarricense de control de drogas para incluir medidas atenuantes que disminuyeran las penas, aunque esta abarca una minoría de las personas condenadas por delitos de drogas, como son las mujeres detenidas por tratar de introducir drogas a un centro penitenciario (Cortés, 2017, p. 13).

Toda la región centroamericana posee, en mayor o menor medida, una posición geográfica estratégica para el comercio de drogas por ser puente entre América del Norte y América del Sur y por sus estrechas franjas de territorio que permiten cruzar en pocas horas desde las costas del océano Pacífico hacia las costas del océano Atlántico y viceversa. Costa Rica y Panamá particularmente, por su nivel de desarrollo en términos de infraestructura para importaciones y exportaciones marítimas, desempeñan una función de puente entre los productores de cocaína de América del Sur y los principales países consumidores de drogas, a saber, La Unión Europea y Estados Unidos (Saborío, 2019). De acuerdo con Saborío (2019):

El aumento de los controles ejercidos en las fronteras de los países productores de cocaína a partir de los años 90 en el marco de la «guerra contra las drogas», promovida e impulsada por Estados Unidos, representó para los narcotraficantes una razón ulterior para substituir las tradicionales rutas aéreas de la cocaína hacia los Estados Unidos y Europa con rutas marítimas y terrestres, aumentando de esta manera la importancia de Costa Rica en el narcotráfico internacional (s. p.).

Además de contar con esta posición geográfica *privilegiada*, Costa Rica tiene grandes debilidades socioeconómicas que favorecen la instalación y proliferación de actividades y grupos criminales (EL PAcCTO, 2021). Las zonas costeras son un claro ejemplo de esto, así como las zonas rurales y remotas, donde hay una menor presencia administrativa del Estado. Históricamente, las zonas costeras (pacífica y atlántica, es decir, Puntarenas y Limón) son zonas con bajo desarrollo y pocas fuentes de empleo. Además de la actividad portuaria, las principales actividades económicas de estas zonas son la pesca y el turismo, ambas golpeadas por la pandemia de la COVID-19 (Programa Estado de la Nación, 2021). Debido su bajo desarrollo, no son zonas atractivas para la inversión nacional o extranjera, lo que las ha sumido en un círculo vicioso por décadas, impidiendo que puedan desarrollarse adecuadamente y manteniéndolas con altos índices de pobreza.

Según la Encuesta Nacional de Hogares 2022, en la región Pacífico Central el 31 % de la población vive en condiciones de pobreza total, en la región Brunca es el 34 % de la población y en la región Huetar Caribe el 33 %. En contraste, en la región Central solo el 18.1 % de la población vive en condiciones de pobreza total (INEC, 2022). Estas condiciones, es decir, el alto índice de pobreza, las altas tasas de desempleo y el bajo índice de desarrollo humano en general, hacen más susceptible a la población de estas zonas de involucrarse en actividades ilícitas que se relacionan con el narcotráfico, lo que propicia el desarrollo de estas actividades.

Según el Informe Mundial sobre Drogas (ONU, 2020), en el 2020 el total de cocaína decomisada en Costa Rica representó el 3.3 % del total de cocaína

decomisada en el ámbito mundial. En 2021, de acuerdo con O. Abrahams (comunicación personal, 1 de noviembre de 2022), en Costa Rica se decomisó un total de 38.213 kg de cocaína y, para finales de diciembre de 2022, se habían decomisado 21.893 kg.

La cocaína proveniente de Sudamérica ingresa al país vía marítima, tanto por la costa pacífica como por la costa atlántica y en algunos casos por vías aéreas o terrestres. Las variaciones en las rutas del narcotráfico, al igual que las organizaciones criminales son muy dinámicas (Ramos Rechnitz *et al.*, 2022; Baires, 2022). Una vez en el país, la cocaína se moviliza a través de una estructura logística compleja por la vía terrestre hasta ubicaciones estratégicas, por ejemplo, Moín, en la provincia de Limón, donde se encuentra la terminal de Contenedores de Moín que administra la empresa APM Terminals. Desde esos puntos estratégicos, los grupos de delincuencia organizada (GDO) colocan la cocaína en contenedores marítimos tras abordarlos, ya sea en su ruta hacia la terminal portuaria o dentro de esta. Estos contenedores transportan cargas lícitas como piña, banano, café, flores y otros productos de exportación que tienen como destino la Unión Europea y Estados Unidos principalmente (Pomareda, 2022; Ramos Rechnitz *et al.*, 2022). La droga es por lo general introducida en empaques o bolsos y, con menor frecuencia, escondida entre los empaques de los productos por exportar, entre los productos y, en algunos casos, dentro de la estructura del contenedor marítimo (O. Abrahams, comunicación personal, 1 de noviembre de 2022). Indica Pomareda (2022) que, del total de droga decomisada por la Policía de Control de Drogas hasta octubre del año 2022, los decomisos en contenedores marítimos representaron un 67 %.

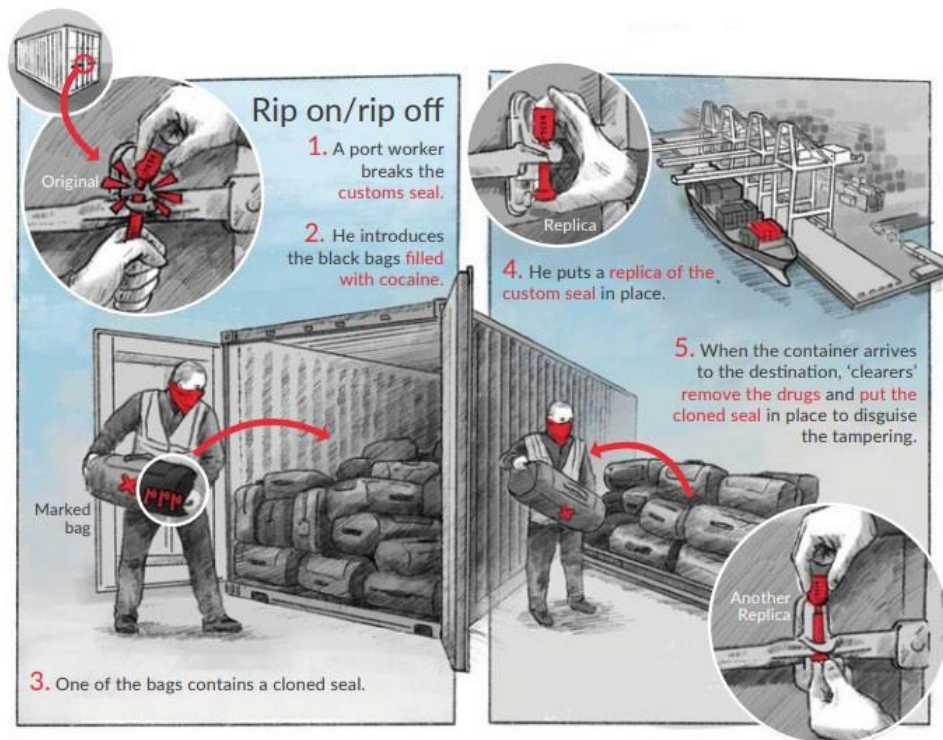
A pesar de los esfuerzos realizados por la Policía de Control de Drogas en colaboración con APM Terminals, hay una cantidad inestimable de cocaína que se exporta a Europa y Estados Unidos. Esta droga es invisible a los controles que se han implementado como producto de la colaboración señalada (O. Abrahams, comunicación personal, 1 de noviembre de 2022).

Pomareda (2022) cita que, de acuerdo con el director de la PCD (Policía de Control de Drogas), Stephen Madden:

Hace unos años la carga de los contenedores era contaminada en las plantas empacadoras exportadoras, pero la situación ha ido cambiando y ahora se está contaminando en el trayecto de la planta exportadora al puerto en predios cercanos al puerto y dentro de la Terminal de Contenedores de Moín (s. p.).

Existen diversos *modus operandi* para realizar la contaminación entre los puertos, que reciben los nombres de gancho ciego, caballo de Troya, intercambio, camuflaje dentro de mercancías lícitas y dentro de la estructura del contenedor (EMCDDA, 2022). El más común de estos métodos es el denominado gancho ciego, que consiste en la apertura de las puertas sin alterar el marchamo o reemplazándolo por una réplica, de este modo, el dueño de las mercancías lícitas no nota la introducción del contenido ilícito dentro del contenedor (EL PAcCTO, 2021).

FIGURA 1. MÉTODO DE CONTAMINACIÓN LLAMADO GANCHO CIEGO



Fuente: McDermott *et al.* (2021).

Se da por sentado que el Centro de Inspección Remoto (CIR) de APM Terminals, al que pertenece el único escáner de rayos X que existe en el país diseñado específicamente para la inspección de contenedores marítimos, está a disposición completa del Estado y la Policía de Control de Drogas (Ramos Rechnitz *et al.*, 2022).

Lo cierto es que el CIR responde a un esfuerzo interinstitucional, y no forma parte de los compromisos con Gobierno en el contrato de concesión con la empresa APM Terminals. Se promueve como una herramienta que apoya los controles interinstitucionales para cumplir de manera mejorada la labor de gestión de riesgo que realizan las autoridades competentes. Además, el servicio es planteado como complementario en el Contrato de Concesión con APM Terminals. Significa que en este momento es voluntario y debe ser solicitado y cancelado por el exportador a APM Terminals (Comex, 2019, s. p.).

En 2021, como resultado de las reuniones sostenidas entre Canapep, APM Terminals, Dirección General de Aduanas y representantes del Ministerio de Hacienda, con el objetivo de garantizar la seguridad e imagen positiva de las exportaciones de Costa Rica en mercados internacionales:

El Gobierno de Costa Rica anunció al mundo la puesta en marcha de una nueva directriz que comprende el escaneo de todos los contenedores relacionados con la exportación de piña fresca, orgánica y subproductos tales como piña seca, congelada, conservas confitadas, compotas, jaleas, mermeladas, puré o pasta de piña, jugos, concentrados y pasteurizados (Piña de Costa Rica, 2021).

A pesar de lo anterior, el escaneo de todos los contenedores marítimos de exportación no es una solución definitiva al problema de la contaminación de contenedores marítimos con cocaína, pues en muchas ocasiones, la droga exportada se mezcla con subproductos de frutas y es indetectable por el CIR. En estos casos solo mediante labores de inteligencia es posible detectar que se ha presentado contaminación de un contenedor (SWI, 2022; O. Abrahams, comunicación personal, 1 de noviembre de 2022).

En otros casos, según cita Pomareda (2022):

Son contenedores que ya han sido escaneados por solicitud de la policía y ya deberían encontrarse totalmente limpios, pero hemos determinado que han sido sacados nuevamente de la terminal. También hemos detectado, lamentablemente, que algunas cargas han ingresado por los puntos de acceso a la Terminal y no solamente cargas de droga para contaminar posteriormente contenedores, sino personas que vienen ocultas en estos cabezales y que han logrado ingresar, indicó Madden (s. p.).

En el año 2017, por Directriz Presidencial n.º 096, se ordenó la formulación del sistema Nacional de Inspección No Intrusiva (SINI), con el fin de proveer las herramientas, equipos, normas y procedimientos necesarios para apoyar a las instituciones en el ejercicio de sus competencias de control aduanero, sanitario,

migratorio y policial en los puntos de ingreso y salida del país. El SINI tiene dos componentes: a) la instalación de equipos de inspección no intrusiva (escáneres) en los puntos de ingreso y salida del país y b) la implementación del CIR para el análisis y la interpretación de las imágenes (Comex, 2019).

El SINI, además de utilizar escáneres de rayos X como el mencionado, al igual que el servicio de marchamos electrónicos actual, utiliza tecnologías que brindan seguimiento de los contenedores hasta que ingresan a la terminal portuaria, haciendo que eventos como la apertura de las puertas de un contenedor dentro de la terminal o la salida no autorizada de un contenedor le sean indetectables. En estas circunstancias, el SINI cumplirá la función del servicio existente actual de marchamo electrónico, que es la de velar porque las mercancías transportadas entre los contenedores marítimos no sean extraídas y vayan a comercializarse en el mercado negro, donde no pagarían impuestos.

El problema central es entonces que, entre las tecnologías disponibles actualmente en el mercado, no existe una tecnología implementada que permita el acompañamiento y monitoreo de los contenedores marítimos, desde que se cargan con las mercancías lícitas hasta que se embarcan y despachan del puerto. Hasta tanto el monitoreo de cada contenedor no se haga, desde el punto en que se carga hasta que sea despachado del puerto, el narcotráfico seguirá utilizando la terminal de contenedores de Moín en la provincia de Limón como su principal punto de exportación de cocaína con destino a Europa Occidental y Estados Unidos.

Según la Evaluación de la Amenaza del Crimen Transnacional Organizado en Latinoamérica, desarrollada por EL PAcCTO (2021), el análisis de los indicadores y del contexto general indica que la mayor amenaza para la región corresponde al narcotráfico. Este es responsable de la mayor violencia existente en Latinoamérica, articulando otras tipologías delictuales subyacentes, conexas y transversales que nutren doblemente los grupos criminales organizados.

El 75 % de los grupos de delincuencia organizada (GDO) de América Latina, tiene como principal actividad delictiva el tráfico de estupefacientes.

Los GDOs actúan con violencia, llegando al extremo del homicidio, y recurriendo con frecuencia a la extorsión y desaparición forzada. Existe un aumento significativo de la utilización de armas de fuego y violencia en la región latinoamericana, especialmente ligada a la comisión de delitos de tráfico de drogas, ajustes de cuentas, territorialidad y delitos contra la propiedad, las cuales generan una amenaza permanente (EL PAcCTO, 2021, p. 16).

En la mayoría de los casos, las organizaciones criminales que operan de manera transversal contratan servicios de grupos delictivos locales para facilitar el control de sus operaciones, ya sea utilizando empresas de transporte, acopio de mercancías, apoyo logístico, legal, tecnológico y financiero, entre otros (EL PAcCTO, 2021).

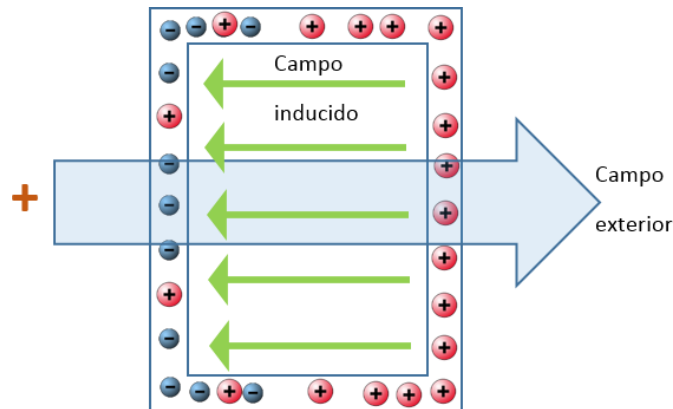
Uno de los principales efectos negativos del narcotráfico para los países de tránsito como Costa Rica es que, tarde o temprano, se vuelven lugares de consumo, pues un porcentaje de la droga que ingresa al país se usa como medio de pago por la logística se brinda a los colaboradores locales (EL PAcCTO, 2021). Esto tiene efectos en el aumento de la delincuencia común y perjudica el bienestar social, pues da lugar al narcomenudeo, que se define como la venta de dosis personales y de aprovisionamiento de drogas en el ámbito local, hecho que desencadena un sinnúmero de ilícitos para el control, tenencia y consumo de drogas.

2.2 Marco conceptual

Existen en el mercado diferentes soluciones para el rastreo de contenedores marítimos, algunas específicas y otras con algún carácter universal o estándar que se adaptan a esta aplicación. En la actualidad, la geolocalización de alta precisión y con cobertura global solo es posible mediante tecnologías globales de navegación por satélite (GNSS). Aun cuando otras tecnologías permiten tener la ubicación de un objeto monitoreado, se encuentra con que, si son precisas no tienen alta cobertura y si tienen alta cobertura no son precisas. Este es el caso de la geolocalización basada en triangulación de radiobases celulares, la geolocalización por wifi y Bluetooth, entre algunas otras. De entre las tecnologías de geolocalización disponibles en el mercado, la que se adapta correctamente a las necesidades de seguimiento y seguridad de contenedores marítimos es únicamente la llamada GNSS, debido a que la cobertura global es una característica primordial en esta aplicación de uso, excepto por el hecho de que los contenedores están contruidos con metal, regularmente acero Corten para los que transportan carga seca y aluminio los que transportan cargas refrigeradas. Este hecho los convierte en una jaula de Faraday impidiendo que penetre en su interior la radiación electromagnética, incluidas las señales emitidas por las constelaciones GNSS.

Los sólidos metálicos son comúnmente buenos conductores eléctricos, ya que sus electrones de valencia están poco ligados a los núcleos atómicos, lo que permite que se muevan con facilidad a través del sólido. Este tipo de electrones poco ligados se denominan electrones libres y cuando se someten a un campo eléctrico empiezan a moverse de un átomo a otro empujados por la fuerza del campo eléctrico. Como su carga es negativa, esta se mueve en sentido contrario al campo eléctrico. Este es el principio de la jaula de Faraday.

FIGURA 2. DIAGRAMA DE UNA JAULA DE FARADAY



Fuente: Sector Electricidad (2021).

A pesar de que la carga eléctrica total del conductor es nula, pues busca el equilibrio electrostático, en uno de los lados de la jaula se concentra un exceso de carga negativa y el lado opuesto queda cargado positivamente. Este movimiento de electrones hace que en el interior de la caja se cree un campo eléctrico de sentido contrario al campo externo, lo que provoca en el interior de la jaula que el campo eléctrico sea nulo. En el interior de la caja no hay campo eléctrico y, por lo tanto, ninguna carga lo puede atravesar (Energía Solar, s. f.).

Por esta razón, los dispositivos con base en tecnologías GNSS usados para dar seguimiento a contenedores marítimos están diseñados para colocarse en el exterior de estos. Lo anterior los hace susceptibles de ser violentados o removidos por los delincuentes o incluso por algún *curioso*.

No se puede afirmar que las tecnologías necesarias para hacer un correcto y seguro seguimiento de contenedores marítimos, desde su origen hasta su destino no existen. Las tecnologías están disponibles, pero en la actualidad, no hay dispositivos que las utilicen o las combinen de forma adecuada con tal fin. Entonces, tanto la tecnología GNSS para la geolocalización como la tecnología celular en todas sus variaciones o generaciones para hacer el envío de la información están disponibles y

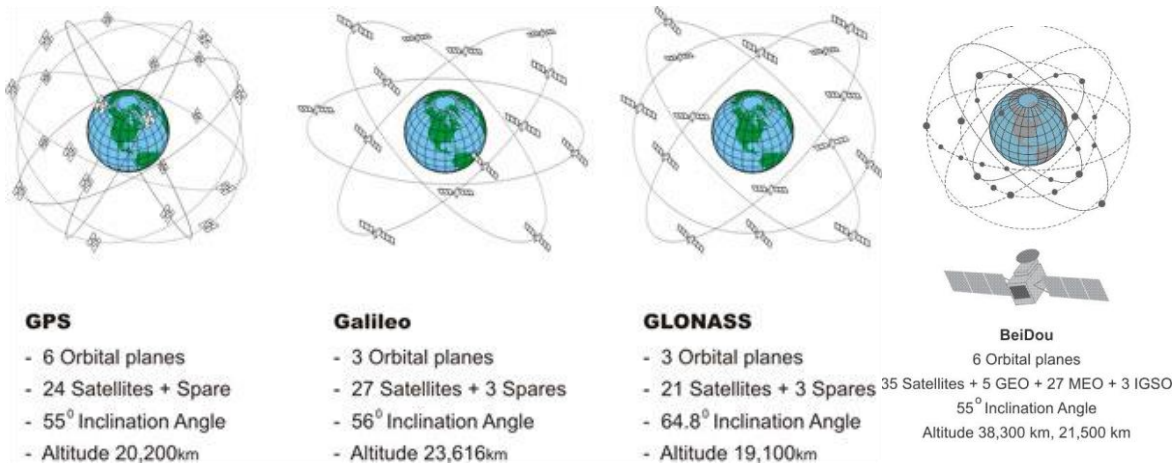
listas para combinarse de forma correcta, con el fin de proveer un servicio especializado de seguimiento de contenedores marítimos.

2.3 Sistemas globales de navegación por satélite (GNSS)

Por décadas se han utilizado tecnologías que implementan Sistemas globales de navegación por satélite (GNSS) para distintos usos civiles. Esta tecnología se ha aplicado, además de al campo militar que le dio origen, a otros muchos campos entre los que destacan: la navegación terrestre, marítima y aérea, la gestión logística y de transporte, la seguridad de personas y mercancías, topografía, agricultura y ganadería. La base de funcionamiento de esta tecnología son agrupaciones de satélites que orbitan la Tierra a las que se conoce como constelaciones. Algunos ejemplos de estas constelaciones son Navstar GPS de EE. UU., Galileo de Europa, BeiDou Navigation Satellite System de China, Global'naya Navigatsionnaya Sputnikovaya Sistema de Rusia (Glonass) y otras que no tienen relevancia para el presente trabajo por no contar con cobertura global.

Cualquier constelación de las indicadas está formada por una red de satélites entre 21 y 30 satélites, Que orbitan a una altura desde la superficie terrestre de entre 21000 km y 25000 km. Cada satélite emite varias señales en la banda L, para la determinación de la distancia satélite-receptor en Tierra, se conoce la posición del satélite, efemérides y se puede medir esta distancia (Berné Valero, 2019).

FIGURA 3. COMPARATIVA DE SISTEMAS GLOBALES DE NAVEGACIÓN POR SATÉLITE



Fuente: Adaptado de Asparuh Kamburov (2018).

El primer sistema GNSS operativo fue el sistema Navstar GPS y se remonta a la segunda guerra mundial, cuando las armadas estadounidense y británica desplegaron sistemas de navegación que utilizaban señales de radio terrestres. Sin embargo, la idea despegó cuando la Unión Soviética lanzó el Sputnik, el primer satélite artificial del mundo, en 1957. Pocos días después del lanzamiento del Sputnik, científicos estadounidenses notaron que podían localizar el satélite con base en la variación en la frecuencia de sus ondas de radio, asociadas con su desplazamiento (efecto Doppler), una medida de cómo las longitudes de onda parecían estirarse o contraerse en función de los movimientos del satélite. Este es el mismo fenómeno que hace que un espectador desde un punto fijo note una diferencia entre el sonido que emite una ambulancia cuando esta se acerca y el que emite cuando se aleja. Esto llevó a las personas investigadoras a pensar en la creación de un sistema de navegación espacial. A finales de la década de 1950, empezaron a desarrollar y probar la tecnología de navegación por satélite y la Marina estadounidense desplegó el sistema operativo de satélites Transit en la década de 1960 (Wall y Harvey, 2022).

Más tarde, en 1973, un grupo de funcionarios del Pentágono decidió crear un *sistema de navegación por satélite para defensa*, sentando las bases del sistema llamado Navstar-GPS, gestionado por el ejército de los Estados Unidos y que después

cambió su nombre a GPS, de sus siglas en inglés Global Positioning System (Wall y Harvey, 2022).

Las fuerzas aéreas estadounidenses pusieron en órbita el primer satélite GPS en 1978, al que siguieron muchos otros lanzamientos a través de los años. A principios de la década de 1990, el sistema ya funcionaba y sus capacidades quedaron demostradas durante la primera guerra del Golfo donde las tropas aliadas se apoyaron en el GPS para navegar por el desierto árabe. En 1995, el satélite GPS N.º 24 fue puesto en órbita, lo que supuso la llegada del sistema a su plena capacidad operativa (Wall y Harvey, 2022).

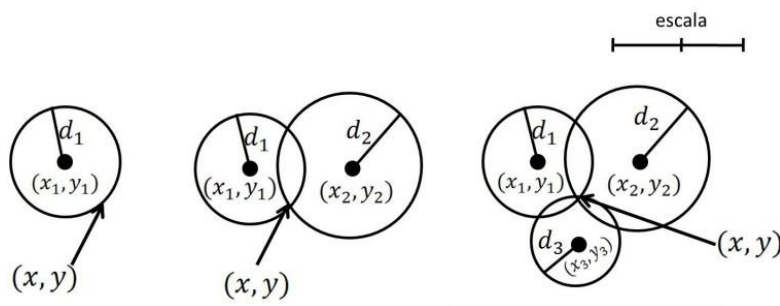
Los satélites GPS emiten dos señales: una para uso militar y otra para aplicaciones civiles. En los primeros años, la señal civil se degradaba intencionadamente por motivos de seguridad nacional. No obstante, eso cambió en 2000, cuando el presidente de los Estados Unidos, Bill Clinton, ordenó que se desactivara la degradación, con lo que el GPS civil pasó a ser mucho más preciso, lo que ha contribuido a que sea una herramienta más fiable para las personas ciudadanas de todo el mundo (Wall y Harvey, 2022). Por haber sido el primero de estos sistemas que conoció la población civil y a pesar de haberse desarrollado los otros sistemas similares desde su creación, en la cultura social es un término tan extendido que se confunde con el término GNSS, que engloba, además del GPS a los otros sistemas de navegación por satélite mencionados.

Comúnmente, se cree que los sistemas GNSS funcionan por triangulación, este es un acercamiento incorrecto porque la triangulación se utiliza para cálculos en dos dimensiones y se basa en la intersección de líneas con base en ángulos y distancias. Los sistemas GNSS son más parecidos a un sistema de trilateración, en el que lo que se mide son las distancias entre tres puntos para conocer la ubicación del objeto. En los sistemas GNSS los satélites funcionan como cada uno de los puntos mencionados y orbitan a una altura y posición relativa fijas sobre la Tierra.

En la figura siguiente se puede observar el planteo desde un enfoque geométrico. Si solamente se conoce la distancia del objeto al primer satélite o punto, en

este caso (x_1, y_1) , el objeto se puede encontrar en cualquier lugar alrededor del círculo de radio d_1 . Si se conoce la distancia del objeto al segundo satélite o punto (x_2, y_2) , para este ejemplo, solamente hay dos puntos en los dos círculos que cumplen con las condiciones de distancia y, por lo tanto, únicamente dos posibles ubicaciones para el objeto, estas son las intersecciones de los círculos. Uno de los dos puntos debe ser la posición del objeto, pero no hay manera de saber cuál de los dos es el verdadero por lo que para determinar cuál es, es necesario contar con una tercera distancia. El tercer círculo centrado, en la posición del tercer satélite (x_3, y_3) , intercepta a los otros dos en la posición del objeto porque este punto es el único que está en los tres círculos y, por lo tanto, cumple con las tres condiciones de distancia (Gómez, 2014).

FIGURA 4. PLANTEAMIENTO GEOMÉTRICO DE TRILATERACIÓN



Fuente: Gómez (2014).

La medición del tiempo es esencial para el cálculo de la posición, pues la distancia es función de la velocidad de una señal electromagnética de frecuencia estable y del tiempo transcurrido, así, el tiempo transcurrido para que la señal electromagnética viaje desde el satélite hasta el receptor es importante. Este debe ser extremadamente preciso para que el cálculo sea correcto.

Con la información del tiempo total transcurrido entre el instante en que una señal sale de un satélite y llega a un receptor multiplicado por la velocidad de la luz, se calcula la distancia entre ambos puntos, esta se conoce como pseudodistancia. Entonces, en teoría, bastaría con solo tres satélites para determinar la posición del punto desconocido, puesto que tres esferoides que se cortan definen un punto y, una

vez obtenidas las distancias desde el punto desconocido a los tres satélites, el receptor en el punto desconocido tiene toda la información necesaria para obtener su ubicación (Gómez, 2014).

No obstante, debido a que en el momento en el que la señal sale del satélite, tanto el satélite como el receptor deben tener exactamente el mismo tiempo (la misma hora) para que el cálculo sea preciso, en la práctica esto exige una altísima precisión y una gran estabilidad de los osciladores, no basta con tres satélites para efectuar el cálculo. Esto porque, aunque los satélites cumplen con las condiciones de precisión requeridas, pues incorporan osciladores atómicos, reconocidos por su extrema precisión, no sucede lo mismo con los receptores. Es inviable desde el punto de vista comercial y práctico equipar con osciladores atómicos a todos los receptores, pues limitaría el campo de uso de las tecnologías GNSS actuales. En el modelo real, para resolver cualquier complicación que pudiera derivar de diferencias de tiempo entre los satélites y los receptores, se utiliza un cuarto satélite que agrega al sistema una variable de tiempo, de modo que los cálculos necesarios para obtener la ubicación del punto desconocido son en esencia un sistema con 4 ecuaciones y 4 incógnitas que se calcularán conociendo las 4 variables: x , y , z y *tiempo* (Gómez, 2014).

A partir del cálculo de la distancia geométrica ρ se plantea el sistema de ecuaciones que permite obtener las coordenadas del receptor y eliminar el error del tiempo receptor δt . Se debe notar que c representa la velocidad de la luz a partir de que la definición de distancia es velocidad multiplicada por tiempo (Gómez, 2014).

$$\begin{aligned} \sqrt{(X - X_1)^2 + (Y - Y_1)^2 + (Z - Z_1)^2} + c\delta t_1 &= \rho_1 \\ \sqrt{(X - X_2)^2 + (Y - Y_2)^2 + (Z - Z_2)^2} + c\delta t_2 &= \rho_2 \\ \sqrt{(X - X_3)^2 + (Y - Y_3)^2 + (Z - Z_3)^2} + c\delta t_3 &= \rho_3 \\ \sqrt{(X - X_4)^2 + (Y - Y_4)^2 + (Z - Z_4)^2} + c\delta t_4 &= \rho_4 \end{aligned}$$

Para obtener esta cuarta variable, los satélites emiten dos portadoras a la misma frecuencia, que están moduladas en fase (BPSK) por diferentes códigos

pseudoaleatorios. El receptor GNSS, por otra parte, calcula la correlación entre el código recibido y el código del satélite cuya señal pretende detectar, lo que le permite separar las señales de los diferentes satélites y obtener, finalmente, el retardo temporal (Gómez, 2014).

El tiempo medido se obtiene comparando la señal recibida por el receptor del satélite y una réplica de dicha señal que genera el receptor. La sincronización entre el código pseudoaleatorio recibido y la réplica generada, se realiza desplazando temporalmente esta última hasta que la correlación entre las dos sea máxima. En el caso de que el reloj del satélite y el del receptor estén sincronizados, el tiempo que habrá que desplazar la réplica será el tiempo de propagación de la señal desde el satélite hasta el receptor (Gómez, 2014, pp. 332-333).

Además de la posible imprecisión de los osciladores en los receptores, la tecnología enfrenta una serie de dificultades que debe resolver para que la información enviada desde los satélites se reciba oportunamente y sea utilizable para realizar los cálculos. Variables como cambios en la presión atmosférica, condiciones climáticas, interferencia y muchas otras exigen el uso de otras técnicas para lograr la precisión máxima.

La medida de distancia con mayor precisión se lleva a cabo con medidas de fase, midiendo el número entero N de longitudes de onda y la parte no entera, una tarea difícil debido a la dificultad de determinar N . A este problema se le llama la determinación de ambigüedades. Se usan las diferencias de fase entre señales repetitivas que emite cada satélite, cálculos que consideran y utilizan el efecto Doppler y otras variaciones de la señal, con el fin de obtener la mejor precisión posible. Esta y otra información de cada uno de los satélites con los que el receptor tiene línea vista se procesa por un sistema electrónico que se basa en un microprocesador para obtener así las coordenadas geográficas del receptor con una altísima precisión, usualmente dentro de un radio de 5 m cuando se usa una sola constelación y decímetros o

centímetros cuando se utiliza una combinación de varias o todas las constelaciones GNSS (Quectel Wireless Solutions, 2022; GPS.GOV, 2022).

A diferencia de lo que la mayoría de la gente cree o infiere con respecto a las tecnologías GNSS, únicamente el sistema Beidou usa algunos satélites en órbita geoestacionaria. Para las demás, es de particular importancia el hecho de que estas tecnologías consideren el efecto Doppler, es decir, el cambio en la frecuencia de una onda como consecuencia del movimiento relativo entre emisor y receptor (SAE), para determinar si el satélite se aleja o se acerca con respecto al receptor.

Las señales provenientes de los satélites contienen entre otra información:

- ❖ La hora actual del satélite, que permite conocer el tiempo en el satélite en el instante en que la señal partió de este.
- ❖ La posición instantánea de un satélite en movimiento. Las coordenadas del satélite en ese momento de la medición son importantes para derivar la posición del receptor, pues los satélites se mueven a una velocidad muy alta en relación con el receptor GPS, por lo que las efemérides (información sobre su posición respecto a la Tierra) deben proporcionar las coordenadas de los satélites en un instante de tiempo.
- ❖ Información sobre las correcciones atmosféricas necesarias. Es necesario comunicar al receptor cierta información sobre la atmósfera, ya que cuando una señal electromagnética atraviesa la atmósfera se ve atenuada por la humedad, la temperatura y la presión barométrica. Por lo tanto, estos datos se introducen en el procesamiento de las distancias.
- ❖ La identificación del satélite que indique al receptor de dónde procede y dónde puede encontrar los demás satélites. Cada distancia que el receptor mide desde cada satélite debe correlacionarse con este. Esto se debe a que el receptor necesitará tener al menos cuatro distancias de al menos cuatro satélites diferentes, necesita ser capaz de asignar el rango apropiado de

distancia o longitud al satélite correcto. Además, debe identificar el origen de cada señal.

Gran parte de la información necesaria procede del Segmento de control. A saber, hay tres segmentos en los sistemas GNSS: el segmento de usuario, el segmento de control y el segmento espacial. El segmento espacial es el conformado por la constelación y el segmento de control son estaciones terrestres, algunas de ellas de monitoreo y otras de carga de información. Los satélites GNSS se rastrean por estas estaciones todo el tiempo para asegurar su estabilidad, correcta sincronización, calcular sus efemérides, entre otros controles (Sickle, s. f.).

El segmento de usuario está conformado por los dispositivos receptores que pueden estar instalados en diversos aparatos, desde teléfonos inteligentes y rastreadores hasta equipos electrónicos de agrimensura, topografía y geología. Su función primaria es recoger y después convertir las señales de los satélites GNSS en mediciones de posición, velocidad y tiempo (Sickle, s. f.).

Dadas las largas distancias que existen entre los satélites GNSS y la superficie terrestre donde se encuentran la mayoría de los receptores que se usan comúnmente, estos enfrentan una de las debilidades de los sistemas GNSS, la baja potencia con que la señal llega a la superficie terrestre. Las señales enviadas por los satélites GNSS que están en órbita tienen forma de cono y este cono cubre una parte sustancial de todo el planeta. Los receptores GNSS típicos tienen una antena pequeña y no direccional. Es decir, un satélite GNSS difunde una señal de baja potencia en una zona extensa en lugar de dirigir una señal de alta potencia a una zona muy concreta como un satélite de comunicaciones típico que no solo tiene mucha más potencia, sino que también emite una señal direccional que se capta en la superficie terrestre mediante el uso de una gran antena parabólica (Sickle, s. f.).

Afortunadamente, las antenas que se utilizan para los receptores GNSS no tienen que apuntar directamente a la fuente de la señal. La señal GNSS también ocupa intencionadamente un ancho de banda mayor del necesario para transportar su

información. Esta característica se utiliza para evitar interferencias y mitigar el multitrayecto, pero lo que es más importante, la propia señal GNSS quedaría oscurecida completamente por la variedad de ruido electromagnético que nos rodea si no fuera una señal codificada de espectro ensanchado. Cuando una señal GNSS llega a un receptor, su potencia es menor que el nivel de ruido del receptor, pero el receptor todavía puede extraer la señal y lograr un seguimiento inequívoco del satélite utilizando técnicas de correlación. Para realizar este trabajo, los elementos de un receptor GNSS funcionan de forma cooperativa e iterativa, eso significa que el flujo de datos se refina repetidamente por los diversos componentes del dispositivo que trabajan juntos a medida que se abre camino a través del receptor (Sickle, s. f.).

Los receptores GNSS están conformados por varios módulos de los cuales el primero es la antena que, a diferencia de las antenas usadas en aplicaciones satelitales, es omnidireccional. La antena recoge las señales del satélite y convierte las ondas electromagnéticas entrantes en corrientes eléctricas sensibles para la sección de RF del receptor. La señal del satélite tiene una densidad de potencia tan baja, sobre todo después de propagarse por la atmósfera, que la eficiencia de la antena es crítica. Por lo tanto, las antenas GNSS deben tener una alta sensibilidad o ganancia.

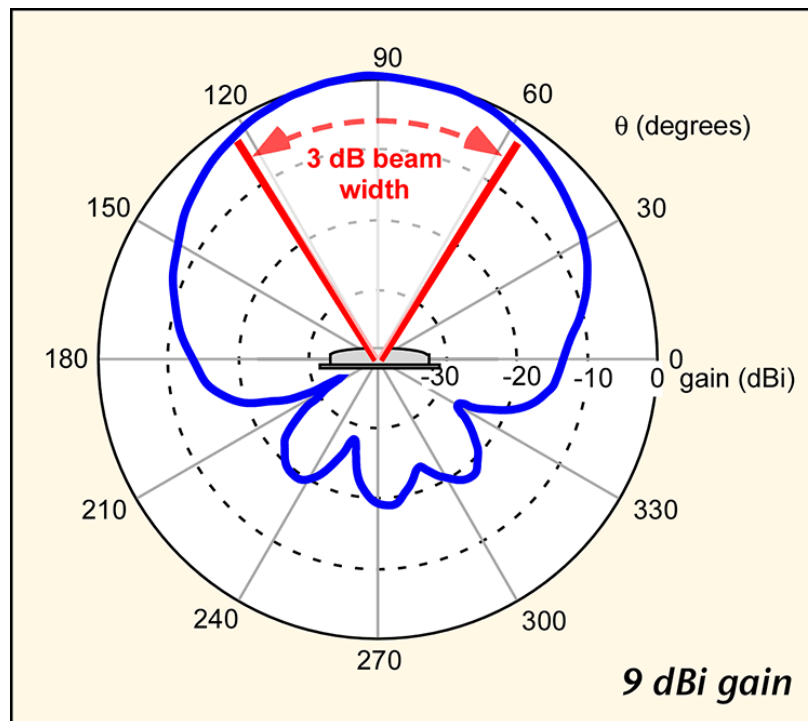
Las ondas polarizadas oscilan en más de una dirección. Los vectores de campo eléctrico de la señal tienen una magnitud constante, pero su dirección gira de modo que el vector de campo eléctrico de la onda describe una hélice en la dirección en la que se propaga. Es decir, las ondas polarizadas circularmente son aquellas en las que el ángulo del vector eléctrico gira alrededor de una línea imaginaria que viaja en la dirección en la que se propaga la onda. La rotación puede ser hacia la derecha o hacia la izquierda. La señal GPS, por ejemplo, es una onda polarizada circularmente a la derecha (Sickle, s. f.).

La mayoría de los receptores tienen una antena integrada, pero muchos también pueden incorporar una antena independiente conectada mediante cables coaxiales. Los cables son un detalle importante, pues cuanto más largo sea el cable, más se perderá

la señal GNSS en su recorrido. Estos suelen tener longitudes estándar para calibrar la impedancia del viaje a través del cable.

Debido a que una antena GNSS está diseñada para ser omnidireccional, su patrón de ganancia debe ser casi un hemisferio completo, pero no perfectamente hemisférico. Una parte de la señal GNSS puede llegar a la antena por debajo del ángulo de máscara, este es un ángulo de entre 10 y 15 grados medidos desde la base que se configura en el receptor a partir del cual se ignora o *enmascara* cualquier señal de satélite, de este modo, se evitan señales reflejas (Nevada Dot, 2017). En la siguiente figura se observa el patrón de radiación típico de una antena GNSS.

FIGURA 5. PATRÓN DE RADIACIÓN IDEAL PARA UNA ANTENA GNSS



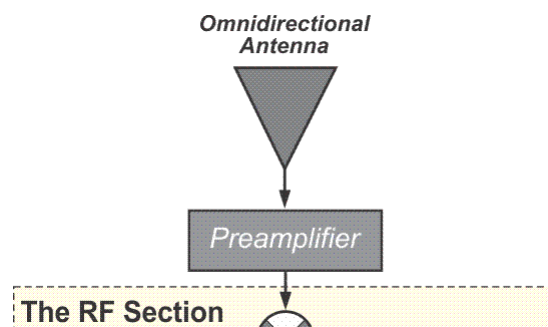
Fuente: Sickle (s. f.).

La ganancia o patrón de ganancia describe la capacidad de una antena para absorber más energía por encima del ángulo de máscara y menos por este. Una ganancia de entre 3-5 decibeles (dB) es típica para una antena GNSS. En este caso, la

ganancia de una antena GNSS real se compara con una antena teórica sin pérdidas que tiene capacidades perfectamente iguales en todas las direcciones (Sickle, s. f.).

En el caso del sistema GPS, las longitudes de onda de las portadoras GPS son de 19 cm (L1), 24 cm (L2) y 25 cm (L5) y las antenas que tienen un cuarto o medio de longitud de onda suelen ser las más prácticas y eficientes, por lo que los elementos de antena GPS pueden ser tan pequeños como 4 o 5 cm. La mayoría de los fabricantes de receptores utilizan una antena *microstrip*, conocidas también como antenas de parche. La *microstrip* puede tener un parche para cada frecuencia, de modo que puede recibir una o todas las portadoras GNSS. Las antenas *microstrip* son duraderas, compactas, de construcción sencilla y perfil bajo. La siguiente antena que más se utiliza se conoce como dipolo. Una antena dipolo tiene un centro de fase estable y una construcción sencilla, pero necesita un buen plano de tierra, es decir, mantenerse paralela a la superficie terrestre. Un plano de tierra también facilita el uso de una antena *microstrip*, ya que no solo mejora el multitrayecto, sino que también tiende a aumentar la ganancia cenital de la antena, es decir, la ganancia de la antena en línea recta. La antena debe tener un ancho de banda de acuerdo con su aplicación. En general, cuanto mayor es el ancho de banda, mejor es el rendimiento, sin embargo, un mayor ancho de banda degrada la relación señal/ruido al incluir más interferencias (Sickle, s. f.).

FIGURA 6. DIAGRAMA GENERAL DE CONSTITUCIÓN DE UN RECEPTOR GNSS (ANTENA)

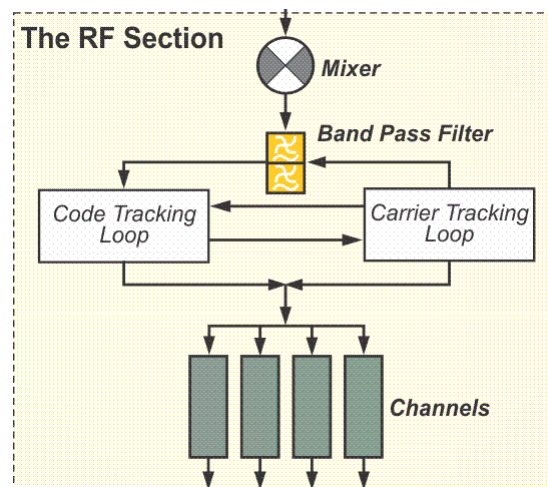


Fuente: Sickle (s. f.),

El segundo elemento del sistema es el preamplificador. Este es necesario debido a la baja potencia de las señales GNSS, su función es aumentar la potencia de la señal

y es importante que la ganancia de la señal preamplificada sea considerablemente superior al ruido. El ruido siempre forma parte de la señal y como su tratamiento es más fácil si las señales que llegan de la antena están en una banda de frecuencias común, parte de la función del preamplificador es combinar la señal entrante con una en frecuencia armónica sinusoidal pura. Esta es la señal de referencia generada por el oscilador del receptor (Sickle, s. f.).

FIGURA 7. DIAGRAMA GENERAL DE CONSTITUCIÓN DE UN RECEPTOR GNSS (SECCIÓN RF)



Fuente: Sickle (s. f.).

Las dos frecuencias se multiplican en un dispositivo llamado mezclador y surgen dos frecuencias: una de ellas es la suma de las dos que entraron y la otra es la diferencia entre ellas. A continuación, las frecuencias suma y diferencia pasan por un filtro paso banda que elimina las frecuencias altas no deseadas, selecciona la más baja de las dos y elimina parte del ruido de la señal. La señal resultante se conoce como frecuencia intermedia (FI) o señal de frecuencia de batido. Esta frecuencia de batido es la diferencia entre la frecuencia portadora desplazada por Doppler procedente del satélite y la frecuencia generada por el oscilador del propio receptor. Para asegurarse de que se abarca toda la gama del efecto Doppler en las señales procedentes de los satélites GPS, el ancho de banda de la propia FI puede variar de 5 a 10 kHz Doppler (Sickle, s. f.).

El siguiente paso en el tratamiento de la señal es la generación de una réplica del código que se utiliza para establecer el bloqueo de la señal e inicializar el bucle de seguimiento en el oscilador del receptor que se correlaciona con la señal de FI. Es en este punto donde se mide el seudorrango, es decir, el desplazamiento temporal necesario para alinear el código generado internamente con la señal de FI, multiplicado por la velocidad de la luz cuyo producto es la distancia recorrida por la señal. En este punto, el receptor genera otra réplica, esta vez una réplica de la portadora. Esta portadora se correlaciona con la señal FI para medir el desfase. Contando los ciclos transcurridos desde el enganche y midiendo la parte fraccionaria de la fase de la portadora generada por el receptor se obtiene el recuento de ciclos observados. A continuación, el receptor reconstruye la onda portadora y extrae la corrección del reloj del satélite, las efemérides y otros datos del mensaje de navegación (Sickle, s. f.).

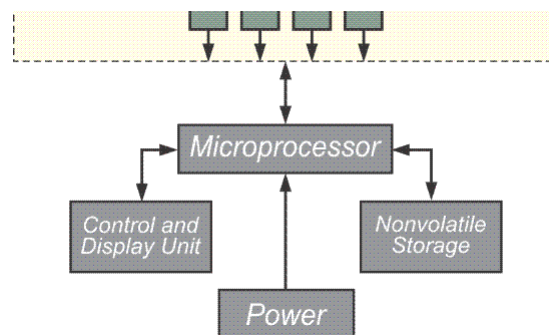
Como los receptores no reciben solo una señal de un satélite, sino un mínimo de cuatro y quizá muchas más provenientes de otros satélites y de forma simultánea, una de las funciones más importantes de los canales de la etapa de radiofrecuencia de los receptores es la identificación de las señales indiferenciadas. Suele haber varias etapas de FI antes de que las copias se envíen a los canales separados, cada uno de los cuales extrae la información de código y portadora de un satélite concreto. Un canal en un receptor GNSS de seguimiento continuo no es diferente de un canal en un televisor. Este es un *hardware* o una combinación de *hardware* y *software*, diseñado para separar una señal de todas las demás. Un receptor puede tener 6 canales, 12 canales o cientos de canales.

En un momento dado una frecuencia de un satélite puede tener su propio canal dedicado y los canales funcionan en paralelo. Este enfoque permite al receptor mantener la precisión cuando se encuentra en una plataforma móvil, proporciona capacidad antiinterferencia y acorta el tiempo hasta la primera fijación (TTFF). Cada canal funciona usualmente de dos maneras: trabajando para adquirir la señal o para rastrearla. Una vez que se adquiere la señal, se rastrea continuamente a menos que se

pierda el bloqueo. Si esto ocurre, el canal vuelve al modo de adquisición y se repite el proceso (Sickle, s. f.).

Por último, el microprocesador de un receptor GNSS gestiona la recepción de datos y controla la multitrayectoria de la señal, es decir, elimina el ruido, extrae las efemérides y el resto de la información del mensaje de navegación o de mensajes de navegación. Controla, además, todo el receptor: los circuitos digitales, el seguimiento y las mediciones. Aunque dispone de almacenamiento para la mayoría de las aplicaciones en la actualidad, se espera que el microprocesador produzca la posición en tiempo real, instantáneamente o casi en tiempo real procesando los datos de alcance, haciendo la conversión del marco de referencia (*datum*) y se envía la posición a la unidad de control y visualización (CDU) que bien puede ser un teléfono inteligente, un rastreador, un equipo de agrimensura o muchos otros tipos de dispositivos electrónicos. La comunicación entre el microprocesador y la CDU es bidireccional: cada uno puede recibir información del otro o enviársela, por lo que los receptores GNSS son completamente controlables por el dispositivo que los tiene integrados (Sickle, s. f.).

FIGURA 8. DIAGRAMA GENERAL DE CONSTITUCIÓN DE UN RECEPTOR GNSS (SECCIÓN DE PROCESAMIENTO)



Fuente: Sickle (s. f.),

2.4 Internet de las cosas (IoT)

Después de la aparición oficial de lo que en la actualidad se conoce como el Internet de las cosas (IoT por las siglas en inglés, Internet of Things), las tecnologías

GNSS, junto con sensores de variables físicas, actuadores y un sinfín de módulos electrónicos, han pasado a ser parte importante de muchos de los dispositivos interconectados, con el fin de informar detalles del entorno en el que se encuentran como la geolocalización, altitud, temperatura y otras variables analógicas, estados lógicos, entre otros, lo que permite generar un ecosistema de servicios alrededor de sus capacidades. Un ecosistema destinado a producir valor para los diferentes sectores de la industria como agricultura, construcción, comercio, salud, educación, seguridad nacional, seguridad ciudadana, transporte y esto por mencionar unos pocos.

El Internet de las cosas fue la evolución natural de la Telemetría, rama de las telecomunicaciones que se encarga de la medición de variables físicas de forma remota. Entre sus usos más populares está el uso de variables meteorológicas. Desde el siglo XIX se habían sentado sus bases con el proyecto de Mont-Blanc de 1874, cuando un grupo de científicos franceses se trasladaron hasta la cima de ese lugar para instalar una serie de sensores con el objetivo de recoger datos meteorológicos como temperatura, la dirección del viento, el espesor de la nieve, entre otros. Toda la información obtenida por los dispositivos se envió por radio hasta la ciudad de París para su análisis (Del Rancho, s. f.).

Según Recuero (2020), los principales avances tecnológicos que hicieron posible el IoT se dieron en los años 60 y 70, con la creación de Arpanet, red telemática operativa del Departamento de Defensa de Estados Unidos, precursora de lo que hoy es el Internet global. Fue en 1969 cuando se envió el primer mensaje a través de Arpanet y en 1973:

Vinton Cerf y Robert E. Kahn, desarrollaron el modelo TCP/IP que describe cómo deben ser tratados los datos (formateados, direccionados, transmitidos, enrutados y recibidos) para proveer conectividad de extremo a extremo entre dos equipos conectados a una red, un avance revolucionario pues, la falta de comunicaciones rápidas y de bajo coste a medias y largas distancias tuvo como consecuencia la creación de redes heterogéneas, totalmente incompatibles entre sí. Esto se tradujo en un ecosistema de silos de equipos conectados de forma

local, normalmente limitados al ámbito académico y militar. En 1983 TCP/IP se convirtió en el corazón de la red ARPANET, reemplazando por completo al protocolo NCP, y la red se separó en dos partes, MILNET, para usos militares, y ARPANET para el resto (Del Rancho, s. f., s. p.).

En la década de los 70, el Departamento de Computer Science del Carnegie Mellon conectó una máquina de Coca-Cola al servidor departamental mediante una serie de *microswitches* de modo que antes de visitar la máquina de bebidas, el interesado podía comprobar desde un computador si quedaban refrescos y si tenían la temperatura adecuada conociendo el tiempo que llevaban enfriándose en la máquina. Cualquier persona conectada con Internet (entonces Arpanet), podía averiguar el estatus de la máquina. Esta máquina expendedora de refrescos se considera el primer dispositivo conectado de la historia, incluso cuando no estuviera conectada con la todavía no existente Internet (Recuero, 2020; Del Rancho, s. f.).

La aparición de Internet como se conoce en la actualidad, al menos en sus aspectos básicos, se dio en los años 90 y, poco después, apareció la World Wide Web (www) cuando Berners-Lee estableció con éxito la primera comunicación entre un cliente Hypertext Transfer Protocol (HTTP) y un servidor a través de Internet. Un año más tarde, creó la primera página web y a partir de ese momento el desarrollo tecnológico vertiginoso dio comienzo a la era de la información. En esa misma época apareció el que se considera el primer dispositivo IoT, una tostadora de pan. John Romkey logró que el aparato, mediante conectividad a través de los protocolos TCP/IP y SNMP, se pudiera controlar desde cualquier computador conectado con la WWW, lo que permite su encendido, apagado y programación del tiempo de *tostado* (Recuero, 2020, s. p.).

Durante esa década continuó la aparición de los proyectos que permitían controlar dispositivos a distancia, obtener datos de variables físicas, transmitir video sobre Internet, entre otros hasta que en el año 2000 LG lanza el primer refrigerador conectado con Internet, el LG Smart DIOS V9100. Debido a su alto precio y la poca

cobertura de Internet en los hogares, el proyecto no tuvo éxito y se dejó de lado (Recuero, 2020).

En 2005, la empresa francesa Violet, lanzó al mercado Nabaztag (liebre en armenio), un dispositivo con forma de conejo que se conectaba a Internet por red wifi. Esta se comunicaba con la persona usuaria mediante mensajes de voz y cambios de color o movimiento de sus orejas, además reproducía, hablaba, escuchaba y respondía a la voz de los usuarios, entre otras funciones avanzadas (Recuero, 2020).

En el 2009 se hace público el término Internet de las cosas (IoT) mediante un artículo de Kevin Ashton, profesor del Massachusetts Institute of Technology (MIT), publicado en el RFID Journal. Ashton indica que cree haber usado ese término públicamente en 1999 como el título de una presentación que hizo en Procter y Gamble (P&G) relacionada con la idea combinar tecnología RFID con Internet (Recuero, 2020). Un hito es que para el momento en que esto sucede ya había más dispositivos conectados a Internet que personas. Durante ese mismo año nuevas aplicaciones del IoT fueron apareciendo en campos tan diversos como el transporte y salud, con proyectos de vehículos autónomos que usaban tecnologías GNSS y conexión celular a Internet y el desarrollo del primer implante cardíaco monitoreado por IoT.

En los años siguientes, con el impulso que dio al desarrollo de nuevas tecnologías la aparición de los teléfonos inteligentes, cada vez más aplicaciones se desarrollaron con nuevos avances tecnológicos en la materia y, para 2014, Intel, Cisco, IBM, GE y AT&T se unen para mejorar la integración de IoT con la industria. Se crea la iniciativa IoT-GSI Global Standards para promover la adopción de estándares para IoT a escala global. A raíz de esa iniciativa se adoptó el protocolo denominado MQTT (Message Queuing Telemetry Transport), propuesto por IBM, que permite que todos los fabricantes puedan participar y soportarlo, lo que facilita la comunicación entre distintos dispositivos de diferentes fabricantes. Este protocolo se ha implementado en muchos de los productos IoT de uso industrial que se utilizan en la actualidad (Del Rancho, s. f.; Recuero, 2020; Gracia, s. f.).

El desarrollo del IoT ha sido tal que en 2016 esta tecnología ya era un blanco importante para ataques cibernéticos debido a sus bajos niveles de seguridad, surgió en ese año Mirai, un *software* malicioso diseñado exclusivamente para atacar dispositivos de IoT. Este programa maligno recopila las contraseñas por defecto que establecen los fabricantes de los dispositivos y que los usuarios muchas veces se olvidan de cambiar y después las utilizaban para acceder a los dispositivos vulnerables para realizar ataques de denegación de servicio (DDoS) (Recuero, 2020).

Para que el IoT haya evolucionado al nivel presente, han debido converger varias tecnologías distintas: las tecnologías de comunicación inalámbrica, los sistemas microelectromecánicos (MEMS), los SoCs (SoC, *System on Chip*) y microservicios de Internet. Además, ha sido de gran relevancia la popularización de plataformas de programación de sistemas embebidos fáciles de usar, que permitieron que más y más personas incursionen en el desarrollo de sistemas IoT, ya sea con fines de aprendizaje, recreacionales o profesionales. Ejemplo de estos son los dispositivos Raspberry Pi y Arduino. Las diferentes condiciones mencionadas han propiciado el ambiente adecuado para que se haya evolucionado desde la comunicación máquina a máquina (M2M), es decir, máquinas conectadas entre sí a través de una red sin interacción humana, hasta convertirse en una red de miles de millones de dispositivos inteligentes que conectan personas, sistemas y otras aplicaciones para recopilar y compartir datos o ejecutar acciones (Recuero, 2020).

Los dispositivos IoT por naturaleza deben interactuar con su entorno, ya sea mediante la adquisición de datos de este o mediante el control sobre elementos del entorno. Para la adquisición de información de su entorno, los dispositivos IoT utilizan sensores. Estos sensores se controlan con un microcontrolador que además controla los dispositivos de comunicaciones para el envío de la información. Para que el microcontrolador pueda operar, este ejecuta internamente un *software* diseñado especialmente para la aplicación IoT requerida, este *software* se conoce como *firmware*.

2.4.1 Sensores

Los sensores o transductores son la conexión de un dispositivo IoT con el entorno, se trata de dispositivos capaces de transformar variables del entorno en información digital que el dispositivo IoT puede usar para ejecutar alguna acción que modifique su entorno a una condición deseada o que informe del estado de esas variables a la plataforma de IoT para que esta analice o muestre la información al usuario, o la procese y analice, con el fin de tomar decisiones que pueden o no afectar al entorno de los dispositivos IoT.

Los sensores pueden captar variables ambientales tan diversas como sea necesario, desde luz, temperatura, presión y humedad, hasta niveles de radiación o concentración de elementos químicos. Un ejemplo que ilustra todo lo mencionado es el proyecto de exploración de Marte Perseverance. Aun cuando alguien puede debatir el hecho de que se trate de un proyecto que integre tecnología IoT porque no tiene una conexión directa a Internet, este robot explorador de la NASA enviado a Marte cuenta con una gran cantidad de módulos diseñados para mantener conexión con una plataforma informática que les instruye sobre las acciones que deben tomar, con base en información que estos recopilan de su entorno mediante el uso de una gran cantidad de sensores y en interacción humana. A la vez, estos dispositivos integrados en el robot utilizan información de su entorno, obtenida mediante el uso de sus sensores, para navegar por la superficie marciana y determinar información del clima, composición de la superficie y muchos más.

En una dimensión mucho menor, un simple termómetro de uso para el hogar, capaz de mostrar el valor de temperatura y humedad de su entorno mediante una aplicación para teléfono inteligente, utiliza sensores de temperatura y humedad para conocer su entorno y las variables específicas que se requieren de este.

Los sensores obtienen los valores de la variable para la que se diseñaron utilizando fenómenos físicos como la variación de la resistividad, capacitancia o inductancia de un componente electrónico al entrar en contacto con la temperatura, luz

o presión de su entorno. Además, se toman en cuenta reacciones químicas, por ejemplo, la oxidación de metales e infinidad de otros fenómenos mucho más complejos y también mucho más simples que los mencionados.

Entre los sensores más comunes destacan:

- ❖ Temperatura: Miden la cantidad de calor generado en un área determinada.
- ❖ Humedad: Miden la cantidad de humedad que se genera en un área determinada.
- ❖ Acelerómetros: Permiten medir la velocidad y aceleración de un objeto.
- ❖ Ubicación: Permiten determinar la ubicación de objetos en el espacio.
- ❖ Ópticos: Miden la presencia y cantidad de luz y la convierten en señales eléctricas.
- ❖ Agua: Permite detectar la presencia o ausencia de agua y los hay diseñados para proporcionar mediciones de la calidad del agua.
- ❖ Imagen: Capturan imágenes ópticas y las convierten en señales electrónicas digitales o análogas.
- ❖ Presión: Se debe diferenciar entre presión física y presión atmosférica. Los sensores de presión física miden la elongación o compresión mientras que los de presión atmosférica miden la presión barométrica.
- ❖ Movimiento: Detecta el movimiento, tanto de personas como de objetos, la detección la llevan a cabo por medios electromecánicos, ópticos o de haz de luz.

2.4.2 Microcontroladores

Toda esta información del entorno se recibe por un microcontrolador, la siguiente parte de la que se compone un dispositivo IoT. Según el tipo de aplicación, este debe ser capaz de funcionar con un sistema operativo de tiempo real rudimentario o con versiones adaptadas o no adaptadas de sistemas operativos como Unix o Linux. Un dispositivo IoT puede tener la misma capacidad de procesamiento que tiene un computador portátil o una capacidad de procesamiento tan limitada que solo le permita acondicionar señales y controlar los sensores y sistemas de transferencia de la información. En la actualidad, existen microcontroladores diseñados especialmente para aplicaciones IoT que son compatibles con los lenguajes de programación que se utilizan para sistemas embebidos más comunes, este es el caso de C/C++ y Python. Entre algunos de estos microcontroladores destacan ESP32 y STM32 con arquitecturas ARM o Xtensa.

Los microcontroladores surgieron como una necesidad para el desarrollo de sistemas embebidos, esto es un sistema de control para un uso particular que puede ser tan simple como el control electrónico de un horno de microondas, hasta el sistema de control del tren de aterrizaje de un avión una aplicación de aviónica. Los sistemas embebidos tienen la ventaja de tener un costo menor que el de un sistema de control general, ya que solo integran los recursos necesarios para la aplicación para la cual se desarrolló. Además, están especializados para esa aplicación integrando los sensores y actuadores necesarios.

Hay muy poca diferencia entre la arquitectura de un computador de uso personal (PC) respecto a un microcontrolador. Un computador de uso personal cuenta con una unidad central de procesamiento (CPU), conocida como microprocesador, memoria RAM, una unidad de almacenamiento y dispositivos periféricos como un teclado, un ratón y una pantalla, . Estos dispositivos periféricos son la forma en la que el PC interactúa con su operador, es decir, su interfaz con el entorno. Un sistema operativo es la base sobre la cual se ejecutan las aplicaciones que la persona usuaria requiere, este les proporciona acceso a los diferentes recursos con los que cuenta el sistema, por

ejemplo, acceso al teclado, ratón y pantalla, entre muchos otros que son invisibles al usuario. Un microcontrolador es también un computador, pero en una escala diferente. Integra un microprocesador, que es la unidad central de proceso, también cuenta con memoria RAM y una unidad de almacenamiento, todo esto integrado dentro de un único *chip* que puede, además de estos componentes, tener otros. La diferencia más notoria yace en el tipo de dispositivos periféricos que integra, pues según su aplicación estos dispositivos pueden ser desde un sensor de concentración de oxígeno hasta un brazo robótico o el motor de un avión.

Al igual que un computador personal, un microcontrolador requiere de un sistema operativo que le permita tener control sobre los recursos disponibles. El sistema operativo de un microcontrolador suele estar integrado con sus aplicaciones que, como ya se explicó, suelen ser específicas y a este conjunto de *software* se denomina *firmware*. Un *firmware* es un *software* específico para alguna aplicación que corre sobre un sistema embebido.

Un dispositivo IoT es también un sistema embebido como los que han existido por muchos años controlando los vehículos, electrodomésticos, juguetes, sistemas industriales y hasta naves aeroespaciales. En este caso, un dispositivo IoT es un sistema embebido que cuenta como una de sus interfaces con su entorno, con un módulo de comunicaciones que le permite interconectarse con otros dispositivos de su misma naturaleza o con sistemas más complejos que reciben su información y le dan instrucciones que este debe seguir.

Los microcontroladores, a lo largo de su historia, han contado con diversas arquitecturas de procesamiento. Algunos ejemplos de estas son x86, ARM, Xtensa, entre otras.

Las primeras arquitecturas de procesamiento de datos binarios son la propuesta por el matemático Von Neumann a mediados de la década de 1940, que hacía posible la ejecución de distintos programas que previamente se podían almacenar en la memoria del computador y la de Harvard, presentada por Howard Aiken (IBM) en 1937.

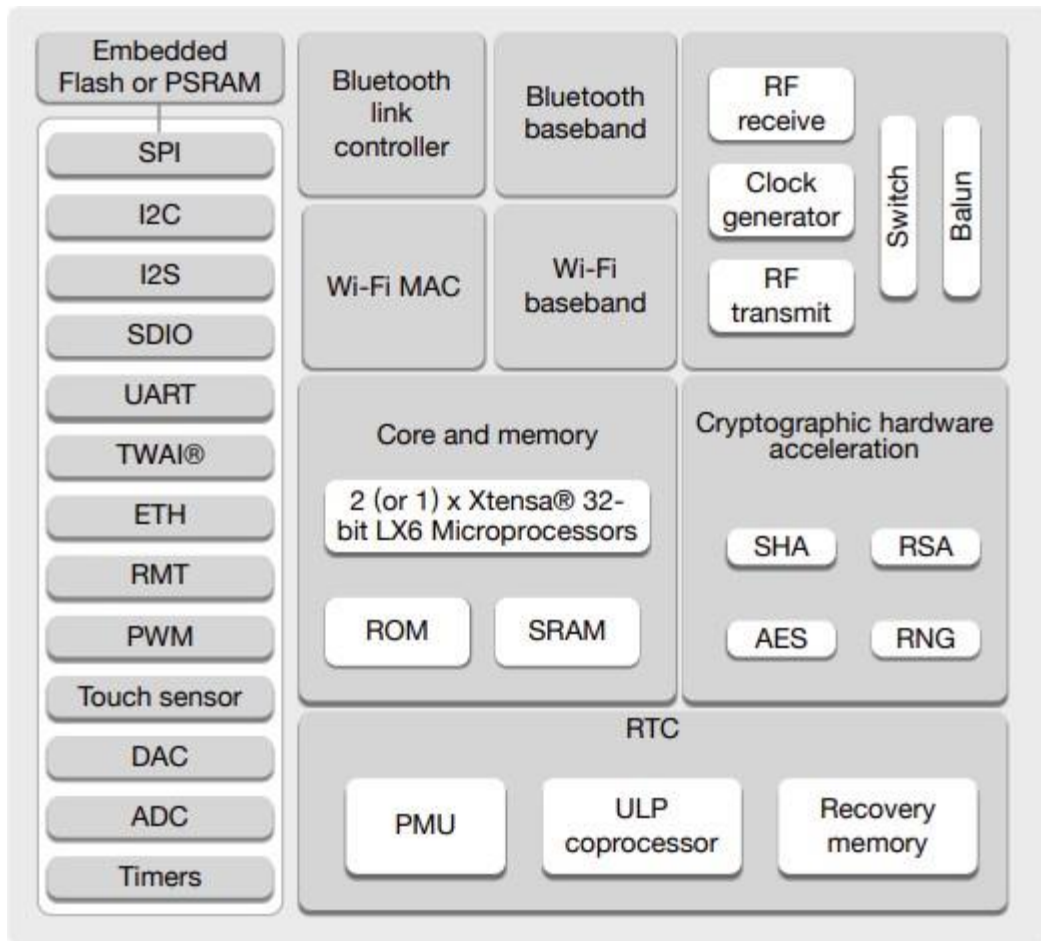
Esta última se diferencia de la Neumann en que usa módulos de memoria separados para almacenar instrucciones y datos (López, 2020).

Posteriormente, se desarrollaron otras arquitecturas como la ARM (Advanced RISC [Reduced Instruction Set Computer] Machine), creada en 1985 por el Acorn Computer Group, que dio origen al primer procesador RISC. La filosofía RISC (Reduced Instruction Set Computer) persigue la eficiencia ejecutando las operaciones de manera simple, esto en contraposición a la filosofía CISC (computadora con *set* de instrucciones complejas), base de la arquitectura x86 de Intel, que se utiliza principalmente en computadores personales, estaciones de trabajo y servidores, aunque también en microcontroladores como el 8051 y su familia. La arquitectura ARM incluye pocos componentes en el *chip*, con el fin de reducir el calentamiento, en consecuencia, su consumo de energía es bajo. Esta última es una de sus características más útiles en las aplicaciones embebidas y, por ende, en IoT (Osio *et al.*, 2020).

Los principales fabricantes de microcontroladores de 32 bits utilizan hoy la arquitectura ARM y cumplen en mayor o menor medida con su filosofía. Sin embargo, desde hace unos años, Espressif, un fabricante de componentes electrónicos de origen chino fundado en 2008 produce una gran variedad de microcontroladores, los conocidos como ESP32 que integran otros periféricos como wifi y bluetooth. Utilizan la arquitectura Xtensa, conocida por permitir la personalización de microprocesadores según su campo de aplicación con bloques o celdas ASIC y FPGA que pueden licenciarse de acuerdo con la aplicación. Estos bloques se denominan SIP por sus siglas en inglés, Semiconductor Intellectual Property. Esta arquitectura había sido usada hasta hace poco, principalmente en sistemas de procesamiento digital de señales y conocida como aceleración por *hardware*, por ejemplo, un decodificador MPEG por *hardware* muy utilizado en tarjetas gráficas para PC para evitar el procesamiento de este tipo de contenido por *software*, liberando recursos del procesador principal, también sistemas de audio, encriptación de datos y muchos otros (Cording, 2022).

En la siguiente imagen se observan los bloques SIP con que cuenta un microcontrolador ESP32. Destaca para efectos ilustrativos el *hardware* específico para criptografía.

FIGURA 9. DIAGRAMA DE BLOQUES DE UN MICROCONTROLADOR ESP32



Fuente: Espressif Systems (2022).

Según el sitio oficial de Cadence, la empresa dueña de la arquitectura, esta arquitectura de *set* de instrucciones Xtensa es una nueva propuesta post-RISC dirigida a productos embebidos, de comunicación y de consumo. La arquitectura de *set* de instrucciones (ISA) está diseñada para proporcionar extensibilidad, alta densidad de código, bajo consumo de energía, alto rendimiento y bajo costo.

Xtensa cuenta con instrucciones de 24 bits para lograr una mayor densidad de código y omite las instrucciones de retardo de bifurcación como los usados por ARM para *rellenar* tiempos muertos. Cuanto menos espacio ocupe una instrucción y más acciones se puedan procesar por ciclo, más denso es su código (Tensilica, 2010).

2.4.3 Firmware

El término *firmware* se explica como *software* firme, es un tipo de *software* que se encuentra integrado en todos los sistemas embebidos y que es inalterable a menos que sea reemplazado. Este término fue concebido por el científico Ascher Opler y se utilizó por primera vez en 1967, en un artículo de la revista Datamation, Firmware de Bios (Tecnología Informática, s. f.)

Este término se usaba en ese entonces para diferenciar entre el sistema operativo de un computador, sus aplicaciones y otros *software*, del *software* almacenado en lo que se conoce como memoria ROM (memoria de un solo acceso). En un computador es un *software* de bajo nivel que *conecta* el *software* con el *hardware*, es decir, administra los recursos del sistema, interactúa directamente con el *software* denominado *controlador* y brinda acceso a información del *hardware*, no es un sistema operativo ni un controlador, tampoco es una aplicación.

En la actualidad, el *firmware* se conoce como soporte lógico inalterable y se refiere al *software* que se ejecuta en cualquier sistema embebido y controla los circuitos electrónicos con un propósito particular, por ejemplo, el control de funcionamiento de un horno de microondas que recibe la información introducida por la persona usuaria y configura temporizadores y activa los elementos de control electromecánico. No es alterable por la persona usuaria y solo puede reemplazarse por otra versión que incluye mejoras o que corrige desperfectos de la versión anterior.

El desarrollo de *firmware* para sistemas embebidos e IoT no es muy diferente del desarrollo de aplicaciones para un computador Windows, Linux o Mac. Asimismo, las aplicaciones para computador se desarrollan en un lenguaje de programación,

orientado generalmente a objetos y después se compila, lo que lo convierte en una aplicación que corre sobre el sistema operativo, un *firmware* se programa en un lenguaje como C++, Python o Java, se compila y se carga a un microcontrolador. No obstante, hace algunos años, los *firmwares* se desarrollaban en lenguaje de muy bajo nivel, conocido como lenguaje ensamblador, donde se trabajaba con las instrucciones del procesador, registros y operaciones binarias, aunque el código programado en lenguaje ensamblador es más eficiente en cuando a consumo de memoria y tiempos de ejecución, aplicaciones complejas requieren mucho tiempo de desarrollo.

Con la popularización de los sistemas IoT han aparecido muchas plataformas que permiten el desarrollo mediante lenguajes de alto nivel. Entre las plataformas más conocidas se encuentran Arduino y Micropython, esta última es nueva, pero ha empezado a tomar relevancia.

Arduino es una plataforma de desarrollo que utiliza C++ como lenguaje de programación. Es muy popular y cuenta con una gran cantidad de librerías disponibles para diferentes aplicaciones y dispositivos. Las librerías son archivos que contienen rutinas (código preprogramado) con un fin específico, por ejemplo, para el control de un MODEM de comunicaciones la rutina ofrece al desarrollador comandos sencillos mientras que sus rutinas pueden ser más complejas y de bajo nivel, por ejemplo, el manejo del MODEM mediante comandos AT.

2.4.4 Conectividad

Como es de suponer, un dispositivo IoT no puede considerarse como tal si no cuenta con una conexión a Internet que para algunas aplicaciones puede ser sustituida por la conexión a una red privada donde se encuentran los servidores y otros dispositivos que son parte del ecosistema IoT. Para dotar de acceso a Internet a un dispositivo IoT se requiere otro de los componentes de un dispositivo de este tipo, el módulo de comunicaciones. Este le permite al dispositivo alcanzar la red o redes en las que se encuentren los servidores y otros elementos del ecosistema para entregar su información y recibir instrucciones.

Existen diversas tecnologías de comunicación disponibles para utilizarse en IoT, muchas de las cuales son diseñadas exclusivamente para esta tecnología. Según el rango de operación y los requerimientos de consumo de energía de un sistema IoT, se selecciona un tipo de red u otra. Entre las redes de corto alcance se tiene, por ejemplo, wifi que hoy es parte de la vida cotidiana de la sociedad, esta se usa en algunos casos en los que la distancia entre el dispositivo IoT y un Access Point wifi permite la comunicación. Al ser esta una tecnología de corto alcance se habla de no mucho más que unas decenas de metros. Muchas de las aplicaciones de campo del IoT que requieren cobertura global por ser de carácter móvil utilizan redes móviles como 2G, 3G, 4G y, más recientemente, 5G. Es importante mencionar que las redes 2G y 3G están en proceso de desconexión en algunos países y ya están deshabilitadas en muchos otros.

Tanto para la interconexión con redes wifi como con las redes móviles se requiere una importante potencia que deriva en un alto consumo de energía por parte del módulo de comunicaciones de un dispositivo IoT si se comparan con las redes que se desarrollaron específicamente para IoT. En el caso de las redes móviles LTE/4G, en su arquitectura se ha considerado su utilización para sistemas IoT, por lo que cuenta con la subred denominada LTE-M (Long Term Evolution for Machines), también conocida como CAT-M1. Esta red utiliza la infraestructura de la red LTE instalada y está diseñada específicamente para funcionar con dispositivos IoT, lo que permite a estos dispositivos enviar y recibir datos, de una forma mucho más eficiente desde el punto de vista energético, lo que les da la posibilidad de tener gran autonomía cuando se alimentan por baterías (Deutsche Telekom, s. f.). Operando sobre redes LTE también hay otra red para uso en aplicaciones IoT, pero no está implementada en Costa Rica por ningún operador, se denomina NB-IoT (banda estrecha para el Internet de las cosas).

En el caso de las redes 5G, se debe tener en cuenta para su uso en aplicaciones IoT que, por su naturaleza de baja latencia y capacidad para permitir altos anchos de banda, esta tecnología utiliza un espectro de alta frecuencia, lo que afecta la cobertura

que se puede lograr. Las más altas frecuencias pueden quedar bloqueadas por objetos ordinarios como árboles y edificios.

Para la conexión e interacción de un dispositivo IoT con redes móviles como LTE, se utiliza un MODEM (modulador/demodulador), conocido también como terminal. Este se trata de un dispositivo de radio frecuencia independiente que se registra en la red móvil pudiendo, por sí solo, usar los servicios de esta, por ejemplo, llamadas de voz, envío de mensajes de texto (SMS) y conexiones de datos. La interfaz de un MODEM con un computador o microcontrolador se lleva a cabo mediante comandos AT.

Los comandos AT son instrucciones codificadas especialmente que conforman un lenguaje de comunicación entre usuario o sistema de control y un MODEM. Fueron desarrollados en 1977 por Dennis Hayes. Los comandos AT se denominan así por la abreviatura de *attention*.

Concebidos inicialmente para la comunicación con MODEM, los comandos AT también se usan en telefonía móvil. Esta los ha adoptado como estándar para poder comunicarse con sus terminales. Todos los teléfonos móviles poseen un juego de comandos AT específico que sirve de interfaz para configurarlos, proporcionarles instrucciones y gestionar el uso de los servicios de red (3Cu Electrónica, s. f.).

Otra de las formas que tiene un dispositivo IoT para acceder a Internet u otra red, es usando redes específicas para IoT, entre estas se pueden mencionar Sigfox (con gran cobertura, tanto en Estados Unidos como en Europa) o LoRaWan. A diferencia de las redes 5G, estas redes utilizan frecuencias más bajas que pueden lograr grandes alcances, cubriendo grandes áreas con pocas radiobases y con menor consumo de energía. Estas redes específicas no se han adoptado en el ámbito global todavía y, en países en desarrollo como Costa Rica, no existen proveedores que cuenten con amplia cobertura. Por lo tanto, solo son una opción para implementaciones industriales de la tecnología IoT que contemplen también la instalación de la infraestructura de alguna de estas tecnologías.

Para casos particulares de aplicaciones de campo o móviles, donde la cobertura de las redes móviles no es suficiente, se utiliza la comunicación satelital bidireccional, utilizando alguna de las redes comerciales disponibles. Entre las redes comerciales más populares destacan Iridium e Immarsat. Para estos casos, el lugar del módulo de comunicaciones es ocupado por un MODEM satelital o, un complemento de un MODEM satelital y otro celular, este último caso para aprovechar la cobertura celular cuando esté disponible, pues por lo general la transmisión de datos vía satélite es mucho más costosa que la transmisión por redes móviles. Es importante tener en cuenta que la transmisión de datos hacia un satélite requiere una relevante cantidad de energía. Por estas últimas dos razones, el envío de información por este medio se hace a intervalos mucho mayores de lo que se haría con redes móviles.

La evolución del IoT no se detiene, la aparición de nuevas aplicaciones con esta tecnología es exponencial y IoT está cada vez más inmersa en la vida cotidiana. Actualmente, se han acuñado términos como SmartHomes, refiriéndose a todas las opciones de domótica disponibles en el mercado integradas mediante IoT, SmartCities o ciudades inteligentes, donde el IoT ha permitido mejorar los servicios ciudadanos de transporte, seguridad, salud y muchos otros, y los llamados *wearables* que son todos aquellos dispositivos IoT que portamos como accesorios o que están incorporados a la ropa.

2.4.5 Baterías

Desde la aparición de las baterías de iones de litio, su continuo desarrollo y su cada vez mayor capacidad de almacenamiento por unidad de volumen o densidad de carga ha permitido que los humanos porten un gran número de aparatos electrónicos y ha hecho posible la movilidad eléctrica y su crecimiento exponencial. Los *wearables*, teléfonos celulares, *tablets*, *laptops* y muchos otros dispositivos no existirían si no se contara con la tecnología en baterías que existe actualmente. Estas capacidades en las baterías con un tamaño reducido permitieron la aparición de muchas aplicaciones de

IoT, ejemplo de estas son los rastreadores autónomos como el que se propone en este trabajo.

La capacidad de una batería se mide en amperios por hora (Ah) y representa el número de horas durante las cuales una batería puede proporcionar una especificada corriente, se mide en amperios porque la corriente se mantiene constante durante la descarga, pero no el voltaje. Por ejemplo, una batería de litio en su estado de máxima carga proporciona un voltaje de 4,2 V y 3.5 V justo antes de perder la capacidad de proporcionar la corriente para la que se diseñó. Esta capacidad depende de la masa de material activo que contiene la batería (litio, por ejemplo). Su capacidad real también puede diferir de la nominal bajo determinadas condiciones específicas, por ejemplo, la temperatura de operación y la de carga, la edad y el historial de la batería y los regímenes de carga o descarga de la batería (PVCDROM, s. f.; Battery University, s. f.).

Como se afirmó antes, la velocidad de carga y descarga afecta a la capacidad nominal de la batería, por ejemplo, si la batería se descarga muy rápidamente, lo que implica alta corriente de descarga, la cantidad de energía que se puede extraer de la batería se reduce y la capacidad de la batería es menor. La causa es que los reactantes no tienen tiempo suficiente para desplazarse a sus posiciones requeridas. Cuando la batería se descarga a un ritmo muy lento utilizando una corriente baja, se puede extraer más energía de la batería y la capacidad de la batería es mayor. Se concluye entonces que la capacidad de la batería debe incluir también la velocidad de carga/descarga y, por esta razón, además de la corriente se indica el tiempo sugerido de descarga (PVCDROM, s. f.).

Como ya se indicó, la temperatura de una batería afecta a la energía que se puede extraer de ella. A temperaturas más altas, la capacidad de la batería suele ser mayor que a temperaturas más bajas.

La edad y el historial de la batería tienen un gran impacto en su capacidad, la capacidad de la batería se mantiene en su valor nominal o cerca de este durante un número limitado de ciclos de carga/descarga. El historial de la batería tiene un impacto adicional en la capacidad, si se ha forzado la batería al proporcionar corriente con una

velocidad alta, la capacidad de la batería puede reducirse prematuramente. Se recomienda entonces respetar los parámetros establecidos por el fabricante para prolongar la vida útil de la batería (PVCDROM, s. f.).

2.4.6 Plataforma IoT

Por último, dentro de un ecosistema IoT, en el extremo opuesto a los dispositivos, se encuentra una plataforma informática capaz de recopilar toda la información proveniente de los sensores y procesarla para convertirla en información útil y con propósito. Estas plataformas y herramientas de IoT se consideran el componente más importante del ecosistema de IoT, pues llenan la brecha que hay entre los sensores del dispositivo y las redes de datos y el uso o aprovechamiento de la información. Según la aplicación, las plataformas pueden solo ser un sistema que muestra en un portal web los datos provenientes de los sensores o sistemas complejos que utilizan inteligencia artificial, Machine Learning y *big data* para analizar la información y convertirla en indicadores para la toma de decisiones o incluso procesarla y analizarla para tomar decisiones por sí mismos.

Las plataformas informáticas para IoT suelen tener una estructura particular debido al hecho de que deben recibir y procesar grandes volúmenes de información. Entre sus componentes, destaca el servicio de recepción de datos de los dispositivos del ecosistema, esta es usualmente una aplicación servidor que efectúa el proceso de escucha, validación y almacenamiento de la información. Por lo general, el proceso de escucha se lleva a cabo mediante llamadas HTTP GET/POST efectuadas, ya sea por los dispositivos cuando deben enviar información o por el servidor cuando requiere consultar algún dato de los dispositivos remotos. Además, es común que se utilicen *web sockets*, esta es una comunicación directa entre el equipo IoT y el servidor de escucha en un puerto TCP o UDP específico. Por último, existe un protocolo desarrollado especialmente para aplicaciones IoT denominado MQTT.

Otra parte importante de una plataforma IoT es la interfaz con la persona usuaria, en esta se muestra toda la información que se recopiló por los dispositivos IoT, ya sea

que esta se haya procesado bajo algún requerimiento específico o que se muestre tal cual se recibe para que la persona pueda organizarla y utilizarla.

2.5 Automated Vehicle Location

Como se mencionó, el precursor del IoT es la telemetría. Las primeras aplicaciones comerciales de telemetría que se relacionan con los sistemas GNSS fueron los sistemas AVL (Automated Vehicle Location). Antes de la aparición de las GNSS, estos sistemas utilizaban diferentes métodos para determinar la ubicación de un vehículo, pero después de la aparición del primer sistema GNSS para uso civil en el año 1995 (el GPS), el principal elemento de un sistema AVL pasó a ser un receptor GNSS. Una vez resuelta la geolocalización del vehículo, un microcontrolador acondicionaba la información de posición y la pasaba a un módulo de comunicaciones que, finalmente, la enviaba mediante algún sistema de radio frecuencia a una estación central. En esta estación central, la información era decodificada y se mostraba en un mapa con la ubicación del vehículo (Okunieff, 1997).

A partir de la aparición de las redes móviles de datos, los sistemas AVL adoptaron Internet como medio de envío de su ubicación y otras variables, convirtiéndolos en una de las primeras y más populares aplicaciones comerciales y logísticas del IoT. En la actualidad, gracias a los importantes avances en el almacenamiento de energía en pilas de alta densidad energética y a la aparición de los SoCs, los sistemas AVL se han evolucionado hacia sistemas de control de activos, lo que permite que los dispositivos IoT para rastreo sean autónomos en lo que a energía se refiere. Esto da la posibilidad de que puedan usarse, además de en flotas vehiculares, en todo tipo de objetos que requieren protección como mercancías, personas, mascotas y contenedores marítimos (con las restricciones mencionadas) (Okunieff, 1997).

2.6 Hipótesis

La implementación de un dispositivo rastreador que brinde visibilidad, seguridad y bajo costo puede incidir en una disminución del trasiego de drogas desde la terminal de contenedores de Moín. Esto protege a los exportadores contra pérdidas millonarias en producto, a sus clientes de no recibir sus productos a tiempo, del daño a su imagen ante su mercado meta y la imagen del país.

2.7 Limitaciones

El sistema propuesto en el presente proyecto no pretende acabar con el narcotráfico en el país, sino ser una valiosa ayuda para atacar una de las tantas formas de tráfico de drogas que afectan al país y ser una herramienta más en la prevención del robo de contenedores y mercancías que se venden en el mercado negro.

2.8 Alcances

- ❖ Para efectos de este proyecto final de graduación se plantea el desarrollo del sistema únicamente, profundizando hasta los componentes principales del *firmware*, dejando para una etapa posterior su prototipado.
- ❖ Se definen los requisitos que debe cumplir la construcción de la carcasa protectora. Sin embargo, al no haber una versión final del producto que garantice que los componentes seleccionados son los que se incluyan en el diseño final, no se profundiza en el diseño detallado de esta previendo modificaciones.
- ❖ El ámbito de utilización del dispositivo es el territorio costarricense, para uso fuera de Costa Rica, se debe estudiar el comportamiento ante temperaturas elevadas y la contratación de SIM globales.

Capítulo III

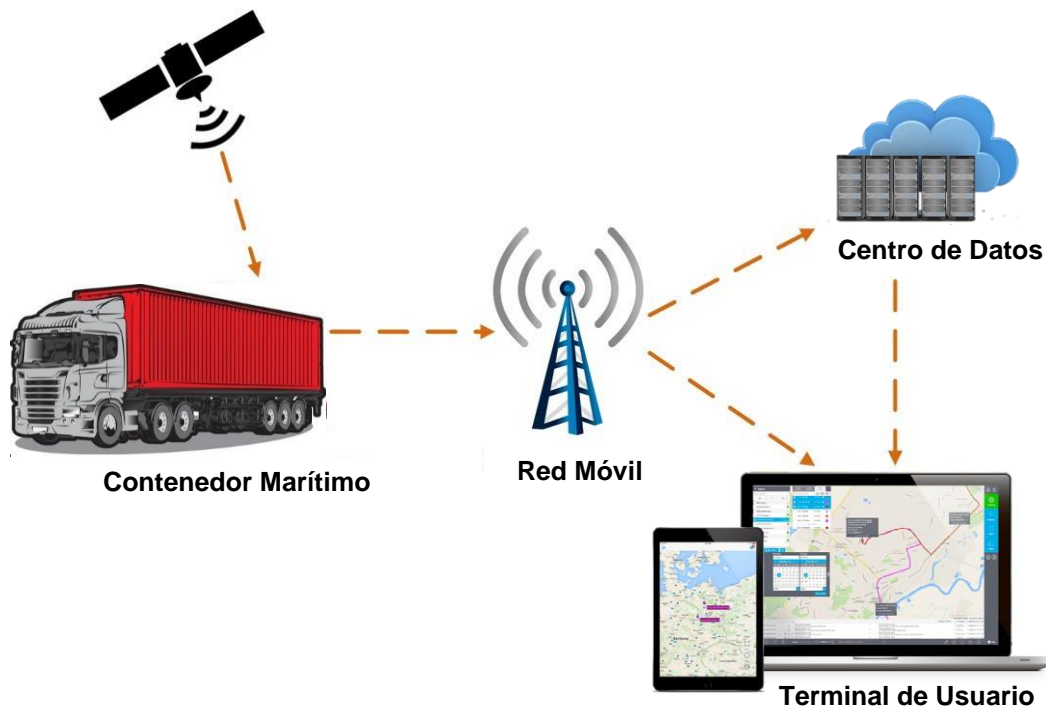
3 Propuesta

Usando como base los criterios de evaluación expuestos en el Capítulo I, en el apartado 1.9, se busca en este capítulo que la propuesta de solución al problema aporte tres beneficios primordiales:

- ❖ **Visibilidad** del contenedor durante todo el trayecto hasta cargarse en el buque para detectar cualquier variación en el patrón esperado de ejecución de la ruta. Para esto, es necesario que el sistema permita consultar la geolocalización de los contenedores marítimos en todo momento.
- ❖ **Seguridad** de las puertas del contenedor. Esto se logra con la detección en tiempo real de la apertura de las puertas y la detección de estacionamiento del contenedor.
- ❖ **Bajo costo** para el exportador, de modo que sea rentable para estos adquirir la solución. Para esto, es ideal que todos los componentes del sistema tengan un bajo costo y que los servicios elegidos tengan también un costo bajo.

Anteriormente, se explicó que un sistema IoT está compuesto por uno o varios dispositivos IoT, generalmente dispersos en un área determinada y que se conectan mediante Internet o una red privada a una plataforma de *software*, hospedada usualmente en *la nube*. Como se puede observar en la siguiente figura, el Sistema de Rastreo y Alerta de Apertura No Autorizada de Contenedores Marítimos no es la excepción y en este capítulo se describe el abordaje realizado para definir cada una de sus partes.

FIGURA 10. SISTEMA DE RASTREO Y ALERTA DE APERTURA NO AUTORIZADA DE CONTENEDORES MARÍTIMOS



Fuente: Adaptado de MEMUK Magazine (2017).

Se plantea como parte del sistema el diseño de un dispositivo rastreador (dispositivo IoT) que, al instalarse en un contenedor marítimo, ya sea seco o refrigerado, quede oculto a la vista del observador, protegido de personas mal intencionado por el cuerpo del contenedor, pero con antenas externas ocultas que permitan la recepción y transmisión de las señales necesarias para brindar visibilidad del contenedor.

El siguiente elemento del sistema es una plataforma IoT que permite la visualización en un mapa de los dispositivos instalados en los contenedores. Esto demuestra, además de la información de la geolocalización de cada contenedor, otra información relevante, como la fecha y hora del último reporte y el estado del dispositivo, si está conectado con la red y si está detenido o en movimiento. Esta

plataforma debe ser capaz también de generar notificaciones de eventos relevantes que reporte el dispositivo IoT, por ejemplo, la apertura de las puertas del contenedor, asimismo, debe analizar la información para detectar otros eventos como paradas fuera de los lugares permitidos y salidas de la ruta establecida.

Con respecto a las comunicaciones, las redes móviles son el medio de comunicación predilecto para aplicaciones IoT cuyos dispositivos se desplazan por grandes regiones, pues la cobertura que requieren para mantener comunicación constante con el servidor debe ser total. Debido al bajo consumo de datos que tiene la presente aplicación y el hecho de que el equipo es desechado una vez que haya cumplido con su función se utilizan líneas prepago para lograr la comunicación.

3.1 Plataforma IoT

Se mencionó en el capítulo anterior que toda plataforma IoT, consta de dos componentes principales, el servidor de escucha que recibe toda la información de los dispositivos IoT y la almacena en una base de datos y una aplicación web que, según la interacción del usuario, muestra la ubicación de los dispositivos y otra información relevante como el estado de sus puertos digitales y señales que monitorean. La plataforma por utilizar en el presente proyecto debe estar alineada con los criterios de visibilidad, seguridad y costo definidos. Para lograrlo, debe cumplir con los siguientes requisitos:

- ❖ Mostrar la geolocalización exacta de cada uno de los dispositivos actualizando en tiempo real la información que se muestra con la información recibida de los dispositivos.
- ❖ Permitir la configuración de cercas electrónicas o geocercas, estas son áreas marcadas en el mapa como cercas virtuales de modo que cuando un dispositivo las invade o sale de ellas el sistema genera una alerta. Esto según una regla que la persona usuaria haya programado para tal efecto.

- ❖ Ser compatible con la detección de la activación de entradas digitales para que pueda ser útil ante un evento de apertura de puertas de un contenedor.
- ❖ Capacidad de detectar, con base en la información enviada por el dispositivo IoT, la detención del contenedor en lugares no autorizados.
- ❖ Capacidad de enviar notificaciones web y de *e-mail* sobre los eventos mencionados.
- ❖ Permitir la modificación de su código para el desarrollo de aplicaciones específicas o, en su defecto, contar con una API que permita extraer la información para que otras aplicaciones puedan usarla para aplicaciones específicas.
- ❖ Ser compatible con protocolos HTTP GET/POST para la recepción de datos de los dispositivos IoT.

Existen en el mercado diversas plataformas IoT para rastreo de activos y flotas vehiculares. Para el uso de la mayoría de estas, es necesario comprar una suscripción y contar con una cantidad mínima de equipos matriculados. Por corresponder a características de la funcionalidad básica de este tipo de aplicaciones, la mayoría de estas cumple con los criterios de visibilidad y seguridad. Entre las plataformas más populares se encuentran:

- ❖ GpsGate:
 - Cumple con los criterios de visibilidad y seguridad.
 - Cuenta con un API adecuado.
 - Su suscripción tiene un costo de \$500.
 - El costo mensual por dispositivo matriculado es \$3.
 - Cantidad mínima de equipos contratados 100.

❖ GURTAM:

- Cumple con los criterios de visibilidad y seguridad.
- Cuenta con un API adecuado.
- Su suscripción tiene un costo de \$1,000.
- El costo mensual por dispositivo matriculado es \$3.
- Cantidad mínima de equipos contratados 100.
- Requiere exclusividad por región, ya está disponible en Costa Rica.

❖ 3D tracking

- Cumple con los criterios de visibilidad y seguridad.
- Cuenta con un API adecuado.
- Su suscripción tiene un costo de \$700.
- El costo mensual por dispositivo matriculado es \$5.
- Cantidad mínima de equipos contratados 100.

❖ NAVIXY

- Cumple con los criterios de visibilidad y seguridad.
- Cuenta con un API adecuado.
- Su suscripción tiene un costo de \$500.
- El costo mensual por dispositivo matriculado es \$3.
- Cantidad mínima de equipos contratados 100.

❖ Traccar

- Cumple con los criterios de visibilidad y seguridad.
- Cuenta con un API adecuado, además, permite la modificación de su código fuente.
- No requiere suscripción obligatoria. Opcionalmente, el costo de un servidor virtual es de \$40 mensuales.
- No tiene costo mensual.
- No hay cantidad mínima de equipos, solo depende de la capacidad del servidor.

3.2 Selección de la plataforma

De las opciones que se estudian destaca Traccar por dos de sus características más relevantes para este proyecto. La primera, que es una plataforma de uso libre y código abierto, permite la modificación de su código fuente según lo desee la persona usuaria. En segundo lugar, puede hospedarse en un servidor propio, es necesario cubrir únicamente el costo de implementación y costos del hospedaje.

Según la información revisada sobre esta plataforma es un referente en temas de plataformas IoT para rastreo de activos. Es ampliamente usada, reconocida y recomendada por algunos fabricantes de equipos IoT, por ejemplo, Fifotrack (s. f.). Otras plataformas incluso se basan en el código fuente de Traccar, este es el caso de la plataforma Latam GPS (s. f.).

Al considerar el importante aporte que tiene para el presente proyecto el uso de una plataforma de tan bajo costo y que facilita el desarrollo de futuras características o funcionalidades, se verificó que esta cumpla a cabalidad con los criterios definidos. Entre sus características relevantes se encuentran:

Monitoreo

Posee una interfaz gráfica que cuenta con todas las funciones básicas de una plataforma de seguimiento de activos, tanto en su versión web como en su versión móvil que está disponible para Android y iOS. Permite observar la geolocalización de los activos rastreados en tiempo real y sin retrasos y cuenta con varias opciones de mapas, lo que incluye mapas de carreteras e imágenes de satélite. El servidor de escucha puede manejar una amplia variedad de sensores e información adicional suministrada por los dispositivos IoT.

Alertas

La plataforma Traccar proporciona notificaciones web instantáneas, además tiene la funcionalidad de enviarlas por correo electrónico y SMS si se contrata el servicio de un tercero que sea compatible con los protocolos SMTP y SMPP. Esto permite el envío de alertas sobre eventos ocurridos que puedan indicar que se da un evento de contaminación.

Informes

Permite la generación de informes simples de historial de localización, viajes, paradas, entre otros. Los resultados pueden verse directamente en la interfaz web o en la aplicación móvil y también se pueden exportar y descargar como un archivo de Microsoft Excel. El historial también se puede proyectar en el mapa proporcionando una representación visual de la actividad de los dispositivos.

Recepción de datos

Además de ser compatible con una amplia variedad de marcas de dispositivos IoT, la plataforma permite interactuar con su servidor por medio de llamadas HTTP usando un protocolo estándar llamado OsmAnd (OSM Automated Navigation Directions). Este es un protocolo de código abierto que se utiliza para interactuar con aplicaciones de navegación que utilizan la librería de mapas Open Street Maps (OsmAnd, s. f.).

Se concluye del análisis que la plataforma Traccar no solo es adecuada para utilizarse como plataforma IoT, sino que tiene una serie de ventajas adicionales. Esta plataforma, además de tener un bajo costo que genera ahorros que se trasladarán al usuario final, cuenta con aplicaciones móviles de uso libre para dispositivos móviles y permite la modificación de estas y de cualquier componente de la plataforma, dejando el camino libre para la mejora o desarrollo de etapas futuras.

3.3 Diseño de hardware

Ante la ausencia en el mercado de un dispositivo que cumpla con los criterios definidos, se fundaron las bases para iniciar el proceso de diseño de la solución. Para esto, la investigación continuó mediante dos pruebas de campo con carácter experimental para tomar algunas mediciones físicas de los contenedores marítimos y verificar los niveles de potencia de señal de las tecnologías que, según los resultados de la investigación inicial, se ajustan a los requerimientos para solucionar el problema propuesto, GNSS y redes móviles.

3.3.1 Primera prueba experimental

La primera prueba experimental consistió en la exploración física de un contenedor marítimo estándar para determinar la mejor ubicación en la que se debe colocar un dispositivo de seguimiento, así como determinar si el mecanismo de cierre de los contenedores marítimos tiene características que faciliten la colocación estratégica de un mecanismo de detección de apertura de este. Una vez ubicados los lugares estratégicos en el contenedor y estudiado el mecanismo de cierre, se procedió a tomar medidas de las dimensiones físicas de los espacios disponibles, así como de la separación de las puertas entre sí, con respecto al marco estructural que las soporta y medidas de otras estructuras aledañas a las puertas. De los datos que se obtienen, se resumen los más relevantes en la siguiente tabla.

TABLA 2. RESULTADOS DE MEDICIONES IMPORTANTES

Descripción	Resultado
Separación de puertas	
Entre puertas	9 mm
Puerta/marco estructural	7 mm
Grososres	
Puertas	80 mm
Marco	135 mm

3.3.2 Segunda prueba experimental

Con los datos de la primera prueba experimental se definieron los pasos para realizar una segunda prueba experimental, esta vez con el objetivo de determinar los niveles de señal GNSS y de redes móviles dentro de los contenedores marítimos, entre las ranuras de sus puertas y en el exterior de estos. Las mediciones se hicieron utilizando un dispositivo rastreador de la marca Concox, modelo Wetrack (1) (Concox, s. f.). Este dispositivo permite determinar fácilmente si los niveles de recepción de señales GNSS y red móvil son aceptables para decodificar la información GNSS y transmitir la información mediante la red móvil. Su tamaño es apropiado para colocarse en las ranuras que separan las puertas del marco estructural que las soporta.

FIGURA 11. CONCOX, WETRACK



Fuente: Concox (s. f.).

Con base en los hallazgos durante la fase de investigación documental y en la experiencia del autor, se determinó que al encontrar una ubicación para la antena GNSS automáticamente se tendría una buena ubicación para la antena LTE, por lo que las pruebas se centraron en la obtención de los valores de esa señal y verificando que en los lugares donde la señal GNSS era más fuerte también lo fuera la señal de la red móvil. Con base en la observación de las posibles ubicaciones de la antena GNSS y a partir de la premisa de que cuanto más expuesta la antena mejor es la recepción, se definió medir en tres ubicaciones:

- ❖ Dentro del contenedor, exactamente en dirección a la ranura que separa ambas puertas.
- ❖ Entre la puerta derecha y el marco que la soporta.
- ❖ Bajo el empaque exterior de la puerta derecha.

Al enviar la consulta de estado al dispositivo mediante SMS, este contesta con información relevante. A continuación, un ejemplo:

Battery:3.59V,LOW; GPRS:Link Up GSM Signal Level:Strong; GPS:Successful positioning; SVS Used in fix:5(7); , GPS Signal Level:35,34,32,37,27 Defense:OFF;

La siguiente tabla muestra los posibles valores de cada uno de los parámetros relevantes.

TABLA 3. RESPUESTA A LA CONSULTA DE ESTADO DE WETRACK

Parámetro	Posibles valores
GSM Signal Level	Strong, Good, Weak
GPS	Successful positioning, Searching satellite, <i>OFF</i>
SVS Used in fix	Satélites usados (satélites visibles)
GPS Signal Level	La ganancia de la señal recibida de cada satélite en dB

Fuente: Concox (s. f.).

Se aclara con respecto a la tabla anterior que los parámetros *GPS* y *SVS Used in fix* están ligados intrínsecamente. Además, los valores del parámetro *GPS* se basan en los de *SVS Used in fix*. Solo uno de estos parámetros se muestra en la tabla, *SVS Used in fix*. Los resultados de la prueba fueron los siguientes:

TABLA 4. RESULTADOS OBTENIDOS EN LA PRUEBA

Lugar de medición	Valor de señal GPS para cada satélite usado	Satélites visibles vs. usados	Valor de señal celular
Dentro del contenedor	1. -	0(4)	Weak
	2. -	0(3)	Weak
	3. -	0(4)	Weak
Entre puerta y marco	1. 36,34,36,30	4(5)	Good
	2. 36,34,36,30	4(5)	Good
	3. 35,34,32,37,27	5(7)	Good
Bajo el empaque exterior	1. 23,29,34,37,38,44,40,40,44,43	10(12)	Strong
	2. 22,32,35,36,38,43,39,39,43,42	10(12)	Strong
	3. 24,30,39,32,41,39,40,40,41,40	10(12)	Strong

3.3.3 Análisis de resultados de las pruebas

Con la información obtenida durante las pruebas, se llegó a las siguientes conclusiones:

- ❖ Se confirma que la antena GNSS no debe estar dentro del contenedor debido a que la intensidad de la señal recibida es débil.
- ❖ La ubicación entre la puerta y el marco es una opción viable, aunque puede haber periodos en los que la recepción no sea suficiente, por ejemplo, cuando el contenedor se encuentre rodeado de otros contenedores.
- ❖ La antena GNSS del tipo cerámica es menos adecuada para implementarla en el presente proyecto debido a que, de las opciones encontradas en los sitios de los principales distribuidores de componentes electrónicos, el grosor

de la más delgada es 4 mm, sumado al del PCB (~2 mm) y la carcasa plástica supera los 6 mm.

- ❖ El área bajo el empaque de la puerta es suficiente para colocar una antena, lo que la ocultaría por completo y tendría excelente recepción por estar completamente fuera del contenedor.
- ❖ El tipo y dimensiones de la antena GNSS deben ser el punto de partida para el diseño, pues es el principal diferenciador de la solución propuesta con respecto a las existentes en el mercado. De la elección y la ubicación correcta de la antena dependen la visibilidad y la seguridad que la solución aporte.
- ❖ Cuando un contenedor marítimo se cierra, dentro de este no existe ninguna abertura al exterior que permita la entrada de luz o aire.
- ❖ La apertura de la puerta izquierda está condicionada a la apertura de la puerta derecha. Es decir, no se puede abrir la puerta izquierda si no se abre antes la puerta derecha. Se define izquierdo y derecho en función de la perspectiva de un observador ubicado de frente a las puertas.

3.3.4 Selección de hardware

Al hacerse evidente que la construcción del contenedor y las tecnologías elegidas hacen factible el diseño e implementación de un dispositivo que cumpla con los criterios de visibilidad y seguridad, se investiga sobre las opciones disponibles en el mercado que permitan cumplir con los criterios de diseño.

3.3.4.1 Criterios de selección de hardware

Después de investigar sobre las opciones de componentes disponibles comercialmente que permiten cumplir con los criterios de diseño, se definieron los siguientes criterios para la búsqueda y evaluación de estos:

- ❖ Usar un *chipset* que integre un receptor GNSS y un *modem* LTE, cuando menos e idealmente de alguna de estas marcas Quectel, Telit, Qualcomm y U-blox, por ser las de más renombre en el sector. Esto da el beneficio de un costo bajo por los dos módulos GNSS y LTE.
- ❖ Usar un microcontrolador basado en arquitecturas ARM o Xtensa. Para este requisito las opciones más destacadas son la serie ESP32 (de Espressif Systems), que utiliza arquitectura Xtensa y STM32 (de STMicroelectronics) que usa arquitectura ARM. En ambos casos se trata de microcontroladores optimizados para aplicaciones IoT, por lo que su consumo de energía es bajo (especialmente el ESP32).
- ❖ El precio de los componentes debe, a la vez, ser el menor posible.
- ❖ Qué exista una tarjeta o *kit* de desarrollo que integre estos componentes o la mayoría de estos y permita programarlos con plataformas de desarrollo como Arduino C/C++, Espressif IDF (IoT Development Framework) o Micropython para aprovechar la cantidad de librerías disponibles existentes para estos entornos de desarrollo. No se descarta el uso de Raspberry Pi Pico, un *kit* de desarrollo que utiliza un sistema operativo que se basa en Linux y permite la creación de aplicaciones IoT.
- ❖ Los esquemáticos de los circuitos del *kit* de desarrollo, así como los diagramas del PCB deben estar disponibles y ser de uso libre, de modo que puedan usarse para la etapa de diseño del PCB.
- ❖ El *kit* de desarrollo debe permitir su uso en pruebas de campo, no puede tener elementos que sobresalgan de forma importante de la superficie del PCB. Esto pensando principalmente en que, si una parte de este debe quedar necesariamente ubicada entre la puerta del contenedor y el marco, solo hay 7 mm de espacio para este y algún tipo de aislante que evite su contacto con el metal del contenedor.

- ❖ Es ideal que el *kit* de desarrollo tenga solo los elementos necesarios para este proyecto y que físicamente tenga una forma regular que permita adoptar su diseño dentro de la carcasa plástica del prototipo. Este hecho reduce el proceso de diseño y la necesidad de modificaciones a los esquemáticos.
- ❖ Que cuente al menos con una entrada digital o analógica, con el fin de usarla para detectar la apertura de las puertas del contenedor. Afortunadamente, esta característica es parte de la naturaleza de los microcontroladores y es improbable encontrar uno que no la tenga.

3.3.4.2 Proceso de búsqueda de hardware

Con los criterios definidos se inició la búsqueda de un *kit* de desarrollo que cumpla con estos. Se realizaron dos tipos de búsqueda, una exacta con el requerimiento del proyecto y otra flexible, utilizando palabras clave que se relacionan, con la intención de tener mayores resultados similares. Las búsquedas realizadas fueron las siguientes:

TABLA 5. CRITERIOS DE BÚSQUEDA DE COMPONENTES

STM32 OR ARM +	LTE + GNSS	Búsqueda exacta
	GPS + LTE	Búsquedas flexibles
	Glonass + LTE	
	GSM + GNSS	
	GSM + GPS	
	GSM + Glonass	
ESP32 +	LTE + GNSS	Búsqueda exacta
	GPS + LTE	Búsquedas flexibles
	Glonass + LTE	
	GSM + GNSS	
	GSM + GPS	
	GSM + Glonass	
Raspberry + pi +	LTE + GNSS	Búsqueda exacta
	GPS + LTE	Búsquedas flexibles
	Glonass + LTE	
	GSM + GNSS	

	GSM + GPS	
	GSM + Glonass	

A continuación, los sitios de búsqueda con el resultado de las búsquedas:

Sparkfun

Las búsquedas exactas no muestran resultados.

El resultado más relevante de la búsqueda flexible fue:

SparkFun LTE GNSS Breakout-SARA-R5.

Este resultado corresponde a un módulo adicional compatible con ESP32, STM32 y Raspberry Pi.

Jameco

Las búsquedas exactas no muestran resultados.

No hubo resultados relevantes para la búsqueda flexible.

Silicon Labs

Las búsquedas exactas no muestran resultados.

No hubo resultados relevantes para la búsqueda flexible.

Waveshare

Las búsquedas exactas no muestran resultados.

El resultado más relevante de la búsqueda flexible fue:

- SIM7600G-H 4G HAT For Raspberry Pi, LTE Cat-4 4G/3G/2G Support.
- SIM7080G NB-IoT/Cat-M(eMTC)/GNSS Module for Raspberry Pi Pico, Global Band Support.

Ambos casos corresponden a módulos que pueden añadirse a una tarjeta de desarrollo básica, no a un *kit* de desarrollo.

Mouser

Las búsquedas exactas no muestran resultados.

No hubo resultados relevantes para la búsqueda flexible.

Adafruit

Las búsquedas exactas no muestran resultados.

No hubo resultados relevantes para la búsqueda flexible.

DigiKey

Las búsquedas exactas no muestran resultados.

No hubo resultados relevantes para la búsqueda flexible.

Aliexpress

La búsqueda exacta muestra resultados exactos:

- TTGO-SIM7600SA-H ESP32, 4G, LTE, Cat4, multibanda, LTE, TDD, FDD, posicionamiento satelital múltiple, GNSS, GPS, GLONASS.

El resultado más relevante de la búsqueda flexible fue:

- Raspberry Pi Pico SIM868 GSM/GPRS/GPS/GNSS módulo de conexión Bluetooth

Este último corresponde al mismo resultado de búsqueda obtenido en Waveshare, un módulo y no un *kit* completo.

Amazon

La búsqueda exacta muestra resultados exactos:

- LILYGO Solar Charge Development Board Module ESP32-WROVER-B Chip Wireless Module WiFi BLE 18560 Battery Holder TTGO T-SIM7000G SIM GPS Antenna CH9102F 16 MB.

No hubo resultados relevantes después de flexibilizar la búsqueda.

Los resultados de las últimas dos búsquedas exactas corresponden al mismo producto. De la búsqueda se concluye que:

- ❖ Los fabricantes más conocidos de *kits* de desarrollo no cuentan con uno que se adapte a las necesidades de este trabajo.
- ❖ Las opciones que ofrecen los fabricantes más conocidos de *kits* de desarrollo son módulos integrados GNSS/LTE, que pueden usarse mediante una tarjeta de desarrollo que se debe integrar por separado, lo que aumenta el tamaño del área de PCB y la altura considerablemente.
- ❖ La única opción disponible en el mercado es del fabricante LilyGo, hasta ahora desconocida para el autor.
- ❖ Existe un fabricante adicional de dispositivos RF llamado Simcom, de calidad comparable a las preferidas al inicio de la búsqueda.

3.3.4.3 Análisis de las Opciones Disponibles

Las especificaciones del dispositivo TTGO-SIM7600X-H son las siguientes (LilyGo, s. f.):

- Voltaje de alimentación: 3.3 V DC o 5 V DC
- ESP32 *chip* (WROVER-B Module) (240 MHz procesador de doble núcleo)
- Memoria Flash: 4 MB
- PSRAM: 8 MB
- SRAM: 520KB
- Wifi Integrado
- Bluetooth Integrado
- Puerto USB: CP2104 or CH9102 (*drivers*)
- Módulo de comunicaciones SIM7000G

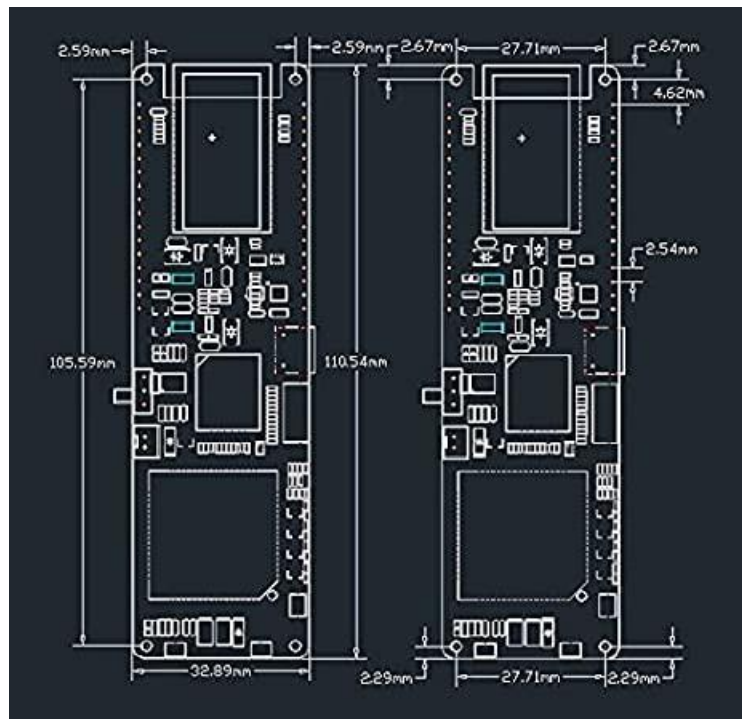
- Puerto para nano SIM integrado
- Antena LTE: puerto para antena LTE
- Antena GNSS: Puerto para antena GNSS
- Circuito de carga de la batería:
 - Tipo de batería
 - Circuito de protección DW01A
 - Interfaz para panel solar de 4.4-6.8 V CN3065
 - Receptáculo para batería 18650
 - Conector 2p JST-PH para panel solar
- Puerto Micro SD integrado
- Interruptor *on/off* integrado

Se evalúa la viabilidad de utilizar la única solución que se encuentra. El análisis consiste en validar los criterios de selección mencionados, además de una investigación de la calidad del producto.

- ❖ Integra un *chipset* GNSS/LTE. La marca es Simcom y el modelo SIM7600X-H
- ❖ Se basa en un microcontrolador de arquitectura ESP32 por lo que puede programarse con Arduino C/C++, Espressif IDF (IoT Development Framework) o Micropython y tiene bajo consumo de energía.
- ❖ El chipset T-SIM7600X-H tiene un costo de \$40 en Digikey y \$35 en Waveshare. Evidentemente, la compra en grandes cantidades hará que el precio mejore considerablemente.
- ❖ No tiene tarjetas superpuestas o módulos independientes. El componente que más sobresale del PCB es el puerto USB tipo C, cuya altura es de 3 mm. Sumado al grosor de la tarjeta PCB la altura total es de 5.29 mm.
- ❖ El microcontrolador ESP32 cuenta con un módulo bluetooth/wifi, innecesario para la aplicación, pero que puede resultar útil durante la fase de prototipado.

- ❖ Los diagramas esquemáticos y ejemplos de código específicos del módulo se encuentran publicados en GitHub y son de uso libre (LilyGO, s. f.).
- ❖ El PCB es una sola placa alargada de dimensiones: largo 110.5 mm, ancho 32.89 mm y grosor 2.29 mm.

FIGURA 12. DIMENSIONES DEL PCB DE LA TARJETA DE DESARROLLO ELEGIDA



Fuente: LilyGO (s. f.).

- ❖ El consumo de energía cuando el microcontrolador está en modo *sleep* y el módulo GNSS/LTE (consumo 20 μ A) está apagado desde 300 μ A.

Con respecto a la calidad, el análisis se basa en el renombre de las empresas fabricantes:

SIMCom Wireless Solutions Limited

Tiene 20 años de experiencia con el suministro de una gran variedad de módulos y soluciones inalámbricas, lo que incluye 5G, 4G, LPWA, LTE-A, 3G, 2G y GNSS. Según el último informe M2M de ABI Research Inc., una conocida empresa estadounidense de investigación de mercado, SIMCom ha despachado los mayores envíos de módulos inalámbricos durante 4 años consecutivos.

LilyGO:

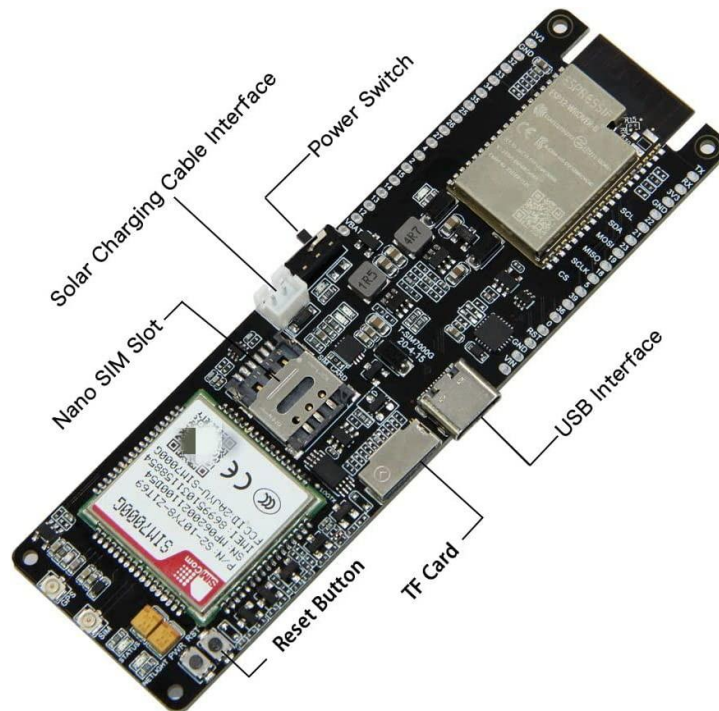
No se encontró información relevante del proveedor LilyGO. Se consultó a la tienda local MicroJPM, quienes comercializan sus productos desde hace 2 años e indican que no han tenido devolución de productos durante todo el tiempo que han comercializado la marca y que han vendido importantes cantidades, principalmente módulos ESP32 con pantalla integrada. Adicionalmente, la marca aparece listada como fabricante de módulos ESP32 en el sitio oficial: <http://esp32.net/>

3.3.4.4 Selección de hardware

Con base en los hallazgos se decide utilizar el *kit* de desarrollo T-SIM7600G-H R2, versión de *hardware* 1.4, para diseñar de la solución, valorando la conveniencia del *kit* de desarrollo al tener todos los componentes integrados y por encima de la incertidumbre existente sobre la calidad.

La elección presenta el inconveniente de que no tiene una hoja de datos de la tarjeta de desarrollo, por lo que es necesario revisar las hojas de datos individuales de cada componente para reunir las características eléctricas relevantes.

FIGURA 13. TARJETA DE DESARROLLO ELEGIDA



Fuente: LilyGO (s. f.).

3.3.4.5 Selección de antenas

La antena incluida con el *kit* es cerámica, del tipo *microstrip* o parche, por lo que se reemplazará por una antena tipo dipolo de dimensiones similares. La antena que se seleccionó es de la marca Quectel, modelo YFGA003AA. Esta fue elegida por su tamaño, 39.45 mm × 13.25 mm × 0.13 mm y su ganancia 6 dBi, la impedancia es la requerida según la hoja de datos del SIM7600G-H, 50 Ω (Quectel, 2021; SIMCom, 2020). La antena LTE incluida con el *kit* es la usada para el desarrollo y se estudia la necesidad de cambiarla según el desempeño en las pruebas.

3.3.4.6 Apertura de puertas

Se observó durante las pruebas experimentales que la puerta izquierda de un contenedor no puede ser abierta si antes no se abre la puerta derecha. La relevancia de este hecho, sumada a la conveniencia de integrar el sistema de detección de apertura

de puertas dentro de la carcasa del rastreador, condiciona la ubicación del rastreador a los alrededores de la puerta derecha del contenedor. Se evaluaron tres opciones posibles, detectando la presencia de luz al abrirse una puerta y utilizando un interruptor electromecánico que se liberaría cuando se abriera la puerta.

3.3.4.6.1 Sensor de luz

Ventajas de utilizar un sensor de luz:

- ❖ No tiene partes móviles que puedan fallar o estropearse durante la manipulación del equipo, durante una caída del dispositivo o debidas a la vibración durante el transporte.
- ❖ Mientras el contenedor está cerrado hay oscuridad total dentro de este de modo que cualquier presencia de luz es atribuible a una intrusión, no se limita solo a la puerta.
- ❖ Bajo costo.
- ❖ No limita la condición de impermeable del dispositivo al no requerir contacto directo con el ambiente externo a la carcasa.
- ❖ Es casi imposible de engañar.

Desventajas de utilizar un sensor de luz:

- ❖ Bajo algunas circunstancias desconocidas que no se estén considerando, la cantidad de luz disponible en el ambiente puede no ser la adecuada para detectar la intrusión. Sin embargo, esto es poco probable considerando que las variaciones se consideran intrusión.
- ❖ El diseño de la carcasa debe contar con una ventana que puede encarecer la producción.

3.3.4.6.2 Interruptor electromecánico

Ventajas de utilizar un interruptor electromecánico:

- ❖ Bajo consumo de energía

Desventajas de utilizar un interruptor electromecánico:

- ❖ Podría dañarse en una caída o de forma intencional por manipulación haciendo que el dispositivo no pueda utilizarse o que se utilice de forma incorrecta.
- ❖ Complica y encarece el diseño y producción de la carcasa plástica.
- ❖ Puede engañarse fácilmente.

3.3.4.6.3 Análisis de viabilidad

Por costo y conveniencia, el sensor de luz es la solución más viable, sus desventajas no elevan el costo del proyecto.

3.3.4.6.4 Diseño del circuito de detección de apertura de puertas

Gracias a que el microcontrolador ESP32 cuenta con un coprocesador de consumo ultrabajo de energía (ULP) que, permanece encendido durante el modo de sueño profundo del procesador principal (Deep Sleep), es posible desarrollar aplicaciones que despiertan al procesador principal de su modo de sueño profundo. Esto mediante la activación de una entrada digital (Espressif Systems, 2022).

FIGURA 14. FUENTES DE REACTIVACIÓN DEL CPU

31.3.10 Wakeup Source

The ESP32 supports various wake-up sources, which could wake up the CPU in different sleep modes. The wake-up source is determined by `RTC_CNTL_WAKEUP_ENA`, as shown in Table 31-2.

Table 31-2. Wake-up Source

WAKEUP_ENA	Wake-up Source	Light-sleep	Deep-sleep	Hibernation	Notes*
0x1	EXT0	Y	Y	-	1
0x2	EXT1	Y	Y	Y	2
0x4	GPIO	Y	Y	-	3
0x8	RTC timer	Y	Y	Y	-
0x10	SDIO	Y	-	-	4
0x20	Wi-Fi	Y	-	-	5
0x40	UART0	Y	-	-	6
0x80	UART1	Y	-	-	6
0x100	TOUCH	Y	Y	-	-
0x200	ULP co-processor	Y	Y	-	-
0x400	BT	Y	-	-	5

Notes*:

1. EXT0 can only wake up the chip in light-sleep/deep-sleep mode. If `RTC_CNTL_EXT_WAKEUP0_LV` is 1, it is pad high-level triggered; otherwise, it is low-level triggered. Users can set `RTC_CNTL_EXT_WAKEUP0_SEL[4:0]` to select one of the RTC PADS to be the wake-up source.
2. EXT1 is especially designed to wake up the chip from any sleep mode, and it also supports multiple pads' combinations. First, `RTC_CNTL_EXT_WAKEUP1_SEL[17:0]` should be configured with the bitmap of PADS selected as a wake-up source. Then, if `RTC_CNTL_EXT_WAKEUP1_LV` is 1, as long as one of the PADS is at high-voltage level, it can trigger a wake-up. However, if `RTC_CNTL_EXT_WAKEUP1_LV` is 0, it needs all selected PADS to be at low-voltage level to trigger a wake-up.
3. In Deep-sleep mode, only RTC GPIOs (not DIGITAL GPIOs) can work as wakeup source.

Fuente: Espressif Systems (2022).

Como se observa en la figura anterior, solamente las entradas/salidas (GPIO) que pertenecen al núcleo del reloj en tiempo real (RTC) pueden reactivar el procesador principal. Como se observa en la siguiente imagen, las opciones disponibles son: 0-5, 34-39.

FIGURA 15. SECCIÓN DE LA CONFIGURACIÓN DEL MULTIPLEXOR DE GPIO

Power Domain	Analog Function0	Analog Function1	Analog Function2	RTC Function0	RTC Function1	Function0	Type
VDDA supply in							
VDD3P3							
VDD3P3 supply in							
VDD3P3 supply in							
VDD3P3_RTC		ADC1_CH0		RTC_GPIO0		GPIO36	I
VDD3P3_RTC		ADC1_CH1		RTC_GPIO1		GPIO37	I
VDD3P3_RTC		ADC1_CH2		RTC_GPIO2		GPIO38	I
VDD3P3_RTC		ADC1_CH3		RTC_GPIO3		GPIO39	I
VDD3P3_RTC							
VDD3P3_RTC		ADC1_CH6		RTC_GPIO4		GPIO34	I
VDD3P3_RTC		ADC1_CH7		RTC_GPIO5		GPIO35	I
VDD3P3_RTC	XTAL_32K_P	ADC1_CH4	TOUCH9	RTC_GPIO9		GPIO32	I/O/T
VDD3P3_RTC	XTAL_32K_N	ADC1_CH5	TOUCH8	RTC_GPIO8		GPIO33	I/O/T
VDD3P3_RTC	DAC_1	ADC2_CH8		RTC_GPIO6		GPIO25	I/O/T
VDD3P3_RTC	DAC_2	ADC2_CH9		RTC_GPIO7		GPIO26	I/O/T

Para este proyecto se eligió el GPIO34 por no tener funciones secundarias y no contar con resistores *pull-up* o *pull-down*. Este GPIO es exclusivamente una entrada digital como lo indica la imagen anterior. Procurando que el diseño sea simple, se utiliza un foto-resistor (LDR) para lograr la activación del GPIO34 que, a la vez, despertará al procesador principal.

FIGURA 16. CARACTERÍSTICAS ELÉCTRICAS DE LOS GPIO

Table 15: DC Characteristics (3.3 V, 25 °C)

Symbol	Parameter	Min	Typ	Max	Unit	
C_{IN}	Pin capacitance	-	2	-	pF	
V_{IH}	High-level input voltage	$0.75 \times VDD^1$	-	$VDD^1 + 0.3$	V	
V_{IL}	Low-level input voltage	-0.3	-	$0.25 \times VDD^1$	V	
I_{IH}	High-level input current	-	-	50	nA	
I_{IL}	Low-level input current	-	-	50	nA	
V_{OH}	High-level output voltage	$0.8 \times VDD^1$	-	-	V	
V_{OL}	Low-level output voltage	-	-	$0.1 \times VDD^1$	V	
I_{OH}	High-level source current ($VDD^1 = 3.3$ V, $V_{OH} \geq 2.64$ V, output drive strength set to the maximum)	VDD3P3_CPU power domain ^{1, 2}	-	40	-	mA
		VDD3P3_RTC power domain ^{1, 2}	-	40	-	mA
		VDD_SDIO power domain ^{1, 3}	-	20	-	mA
I_{OL}	Low-level sink current ($VDD^1 = 3.3$ V, $V_{OL} = 0.495$ V, output drive strength set to the maximum)	-	28	-	mA	
R_{PU}	Resistance of internal pull-up resistor	-	45	-	k Ω	
R_{PD}	Resistance of internal pull-down resistor	-	45	-	k Ω	
V_{IL_nRST}	Low-level input voltage of CHIP_PU to power off the chip	-	-	0.6	V	

tes:

1. Please see Table IO_MUX for IO's power domain. VDD is the I/O voltage for a particular power domain of pins.

Fuente: Espressif Systems (2022).

En la figura anterior se muestran los valores de corriente y voltaje de activación para los GPIO. Para este caso VDD es 3.3 V, el valor mínimo para V_{IH} es 2.47 V, es decir, sobre ese valor el microcontrolador considera que su entrada está en estado lógico 1 y el valor máximo para V_{IL} es 0.82 V, es decir, bajo ese valor el microcontrolador considera la señal como un 0 lógico. El fotorresistor elegido es el modelo PDV-P9203 de Advanced Photonix cuyas características se muestran en la siguiente tabla:

FIGURA 17. ESPECIFICACIONES DEL FOTORESISTOR PDV-P9203

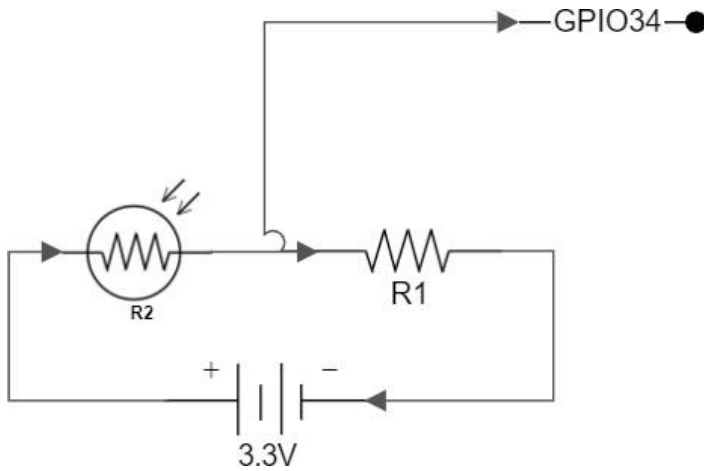
Typical Electro-Optical Specifications at $T_A=23\text{ }^\circ\text{C}$

Parameter	Test Conditions	Symbol	Min	Typ	Max	Unit
Dark Resistance	After 10sec. @10Lux @ 2856°K	R_D	5	-	-	MΩ
Illuminated Resistance	10Lux @ 2856°K	R_{IL}	10	-	30	KΩ
Sensitivity	$\frac{\text{Log}(R100) - \text{Log}(R10)**}{\text{Log}(E100) - \text{Log}(E10)***}$	S	-	0.90	-	Ω/Lux
Spectral Peak	-	λ_p	-	570	-	nm
Rise Time	10Lux @ 2856°K	T_R	-	60	-	ms
Fall Time	After 10Lux @ 2856°K	T_F	-	25	-	ms

**R100, R10: cell resistances at 100 Lux and 10 Lux at 2856 K respectively.
 ***E100, E10: luminances at 100 lux and 10 lux @2856 K respectively

De la tabla anterior se obtienen los valores de impedancia del fotorresistor elegido para la condición de oscuridad, 5 MΩ y el valor máximo de resistencia para condiciones de luz, a partir de 10 Lux, es 30 KΩ. Se utiliza un divisor de tensión para enviar al microcontrolador la señal correcta, según corresponda para eso se calcula el elemento faltante, la resistencia R1. A continuación, se muestra el cálculo de este valor.

FIGURA 18. DIVISOR DE TENSION



$$R2 = \frac{W_{DDD} \times R1}{W1} - R1$$

$$R1 = \frac{3.3V \times 10000\Omega}{2.47V} - 10000\Omega$$

$$R1 = 19759\Omega$$

3.3.4.7 Consumo de energía y elección de la batería

Los principales componentes del *kit* de desarrollo son el microcontrolador ESP32 Wrover y el módulo de comunicaciones SIM7600G-H. A continuación, se analizan los consumos de corriente de forma detallada para cada uno de estos.

3.3.4.7.1 Consumo del microcontrolador ESP32

El microcontrolador tiene la capacidad de apagarse por completo, situación en la cual su consumo de energía es de 1 μ A según la hoja de datos. Sin embargo, al estar apagado por completo no es capaz de despertar cuando el acelerómetro detecte movimiento, es por esta razón que el modo en el que funcionará para este proyecto es el denominado Deep-Sleep modo 1, en este modo el coprocesador ULP se mantiene encendido consumiendo 150 μ A. Durante el funcionamiento activo, el consumo típico del microcontrolador es de 40 mA (Espressif Systems, 2022).

3.3.4.7.2 Análisis de la comunicación de datos LTE

El módulo de comunicaciones consume 20 μ A en modo dormido. En modo activo el consumo oscila entre 2 mA y 17 mA en modo de espera y 720 mA durante el pico de transmisión. La trama de datos, es decir, la cadena de datos para enviar cada vez que se actualiza la posición tiene un tamaño aproximado de 28 *bytes*. A continuación, se presenta el detalle:

TABLA 6. ESTIMACIÓN DE LA CANTIDAD DE DATOS DE LA TRAMA

Bytes	Descripción
4 <i>bytes</i>	Tiempo actual del dispositivo, por lo general se utiliza formato EPOCH
4 <i>bytes</i>	Tiempo en que se hizo la última actualización de posición, también en formato EPOCH.
4 <i>bytes</i>	Latitud
4 <i>bytes</i>	Longitud
4 <i>bytes</i>	Altitud
4 <i>bytes</i>	Velocidad
2 <i>bytes</i>	Ángulo de orientación

1 <i>byte</i>	Cantidad de satélites visible
1 <i>byte</i>	Entradas digitales

Fuente: Elaboración propia

A estos 28 *bytes* se le debe sumar el espacio que usan los protocolos, incluso así es una cantidad de datos muy pequeña que no afecta el tiempo de conexión. El módem entonces se registra en la red, hará el envío cerrará la conexión y se apagará. El tiempo de transmisión mínimo típico es de 100 ms, sin embargo, el tiempo de registro en la red celular es de aproximadamente 20 s, por lo tanto, es el tiempo que se debe usar en los cálculos de consumo de energía (How to Electronics, 2022).

3.3.4.7.3 Análisis de la adquisición de datos de posición GNSS

Para adquirir la posición, el módulo GNSS debe activarse, obtener la posición y después desactivarse. Según la hoja de datos, el valor TTFF, de sus siglas en inglés Time To First Fix, que significa tiempo necesario para obtener la primera posición si el receptor tiene línea vista al cielo es menor que 35s y la corriente consumida por el módulo es de 100 mA mientras está activo (Sección 4.3.1).

3.3.4.7.4 Cantidad de activaciones para el envío de información

Es ideal que el dispositivo esté despierto únicamente durante los periodos de movimiento del contenedor y que pueda despertar cuando se da una activación de las entradas digitales. Como escenario base, se usó el trayecto más largo posible que pudiera seguir un contenedor de exportación dentro del territorio nacional, este tendría como origen Paso Canoas en la frontera con Panamá y como destino la terminal de contenedores de Moín, en Limón, la distancia más larga recorrida por un contenedor de exportación es de 512 km. A una velocidad promedio de 40 km/h se estima que el recorrido puede tardar 12 horas. Si se desea que el dispositivo reporte su ubicación cada 3 minutos, la cantidad de reportes que deben hacerse durante esas 12 horas (720 minutos) es 240 transmisiones en total (720/3).

3.3.4.7.5 Cálculo de consumo de corriente

Por lo general, se indica la capacidad de las baterías en amperios por hora (Ah). Es decir, el valor de corriente que puede suministrar esa batería por periodo de una hora. Entonces, si lo que se tiene es el valor de consumo de corriente instantánea, dado ese valor, al multiplicarlo por la cantidad de tiempo en horas durante el cual se requiere ese flujo de energía de forma sostenida se obtiene la capacidad de la batería requerida para lograrlo.

$$C_{consumo} (mA) \times t (h) = C_{batería} (mAh) \quad * \quad C_{consumo} (mA) \times t (h) = C_{batería} (mAh)$$

Para el cálculo de la capacidad de la batería requerida para este proyecto se tiene hasta ahora el valor de tiempo, 12 horas. Se debe tener en cuenta que, como se mencionó, para tener un reporte de actividad cada 3 minutos el dispositivo tiene ciclos en los que está activo por cerca de un minuto y dormido por dos minutos, 33 % del tiempo activo y 66 % del tiempo dormido. En horas, 3.96 horas activo y 7.92 horas dormido. En la siguiente tabla se muestran los resultados de los cálculos de consumo para cada módulo y fase y al final la capacidad que debe tener la batería desde el punto de vista teórico.

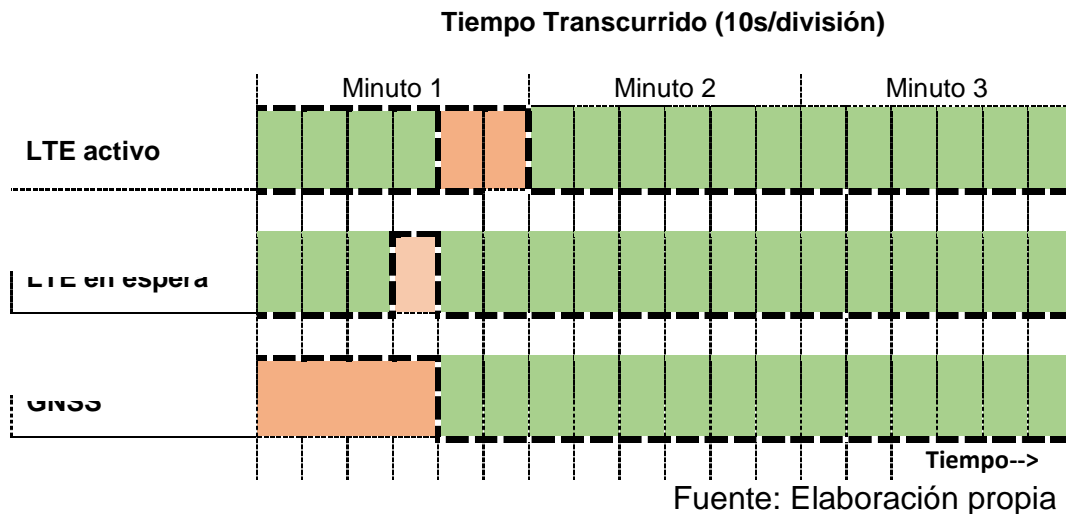
TABLA 7. CÁLULO DE CORRIENTE INDIVIDUAL POR MÓDULO

	Dormido	Espera	Activo
ESP32	150 μ A		40 mA
	1.8 mAh		480 mAh
LTE	20 μ A	17 mA	720 mA
	0.24 mAh	204 mAh	8640 mAh
			48 mAh (20)
GNSS			100 mA
			1200 mAh
			11.66 mAh (35) s
Total	2.04 mAh	204 mAh	~540 mAh
	~746 mAh		

Fuente: Elaboración propia

Los periodos de actividad del módulo de comunicaciones son más cortos que los periodos de inactividad, por esta razón, se calcularon solamente para el periodo de actividad, a diferencia de los demás periodos. La siguiente tabla ilustra los periodos durante los cuales cada módulo está activo, en espera y dormido.

FIGURA 19. TIEMPOS DE ACTIVIDAD DE LOS DIFERENTES MÓDULOS



Se debe considerar que los cálculos mostrados son teóricos y no consideran el consumo de los demás componentes del dispositivo, por esta razón, se debe estimar que hay un 20 % de consumo adicional en potencia disipada en otros componentes pasivos. Adicionalmente, se trabajó con los valores ideales de tiempos de registro en la red y TTFF, estos valores no siempre son los ideales y pueden extenderse. Para referencia, las dimensiones físicas de una batería a base de iones de litio con capacidad de 1500 mAh son 52 mm (largo) x 35 mm (ancho) x 6 mm (espesor), un dato importante en el momento de diseñar la carcasa de protección.

3.3.5 Diseño de la carcasa de protección y soporte

Por ser uno de los dispositivos que se adapta mejor al requerimiento expuesto, se obtuvo acceso a un dispositivo de la marca T42, el modelo Tetis 3G, para analizar la construcción de su carcasa y usarlo como base para el diseño preliminar. Como ya se analizó antes, sus principales desventajas son el precio y el hecho de que sus antenas

quedan expuestas al instalarlo en el contenedor. Para evitar cometer los mismos errores, se propone ocultar las antenas bajo el empaque de la puerta, cuyo tamaño es suficiente para cubrirlas. El diseño propuesto funciona tanto en contenedores secos como refrigerados.

La fijación al contenedor el Tetis 3G la logra mediante magnetos que lo fijan al marco de las puertas del contenedor, que es de acero, pero este método de fijación solo funciona en contenedores secos. Existe una importante diferencia entre un contenedor seco y uno refrigerado, este último es de aluminio casi en su totalidad por lo que usar magnetos no es una alternativa viable. La fijación del dispositivo propuesto se hace con una combinación de un adhesivo de grado industrial, probablemente de la familia Tesa ACX y la presión ejercida por la puerta del contenedor. La función del adhesivo es sostener el dispositivo mientras la puerta está abierta, una vez cerrada la puerta, la sujeción se logra por la presión que ejerce la puerta sobre la carcasa.

Para que el diseño de la propuesta de solución sea adaptable, tanto a contenedores secos como refrigerados, su largo no debe exceder el ancho del marco del contenedor seco que es de 11,5 cm.

FIGURA 20. FOTOGRAFÍAS DE LAS PRINCIPALES MEDICIONES

Dispositivo Tetis 3G en contenedor seco.



El grosor de la puerta del contenedor es de 8 cm.



Dispositivo Tetis 3G desarmado parcialmente, colocado en contenedor refrigerado con la puerta abierta.



La distancia utilizable para el diseño es de 11,5 cm para que el diseño se adapte a ambos tipos de contenedor.



Dispositivo Tetis 3G desarmado parcialmente colocado en contenedor refrigerado con la puerta cerrada para validar el grosor de la abertura.



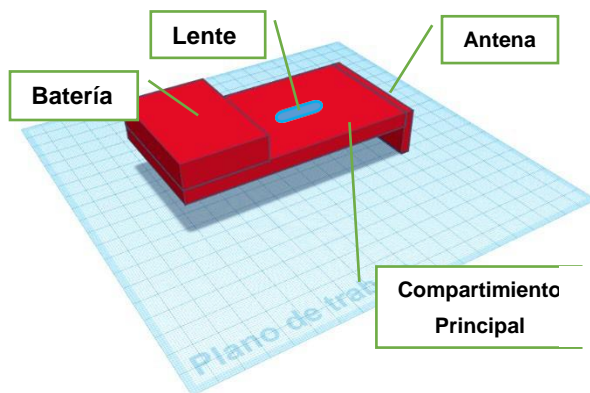
El espacio bajo el empaque es ideal para colocar una antena pequeña sin que sea visible. Como se puede ver, las antenas del Tetis 3G quedan por fuera.



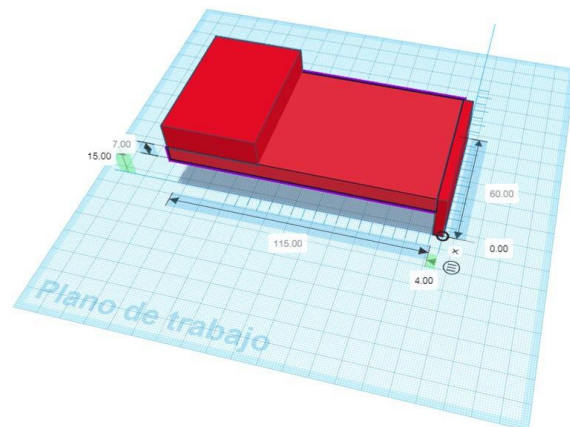
Como se pudo observar en la figura anterior, la forma física del dispositivo Tetis 3G es una buena propuesta si se adaptara a ambos tipos de contenedor y si sus antenas no fueran visibles. Con base en las observaciones del ajuste de este equipo, tanto en contenedores secos como refrigerados, se buscó innovar su diseño eliminando sus debilidades.

FIGURA 21. DISEÑO PROPUESTO PARA LA CARCASA PLÁSTICA

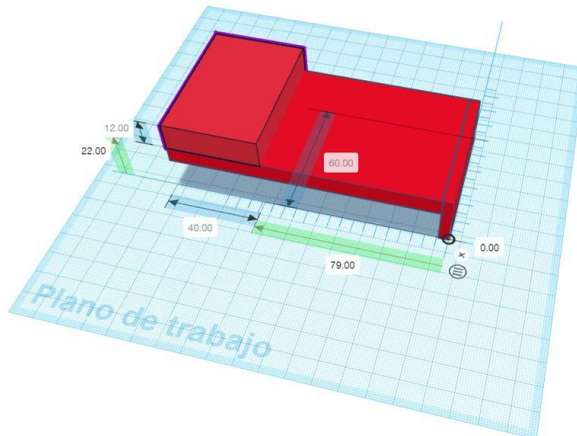
Consta de tres partes



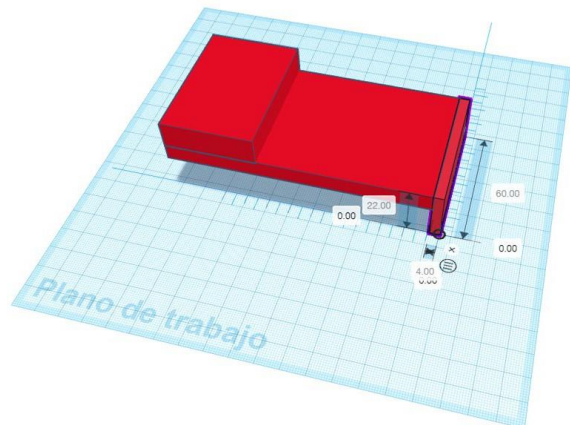
Compartimiento de PCB 115x60x7mm



Compartimiento para la batería 60x40x12mm



Compartimiento de antenas 60x22x4mm



Fuente: Elaboración propia

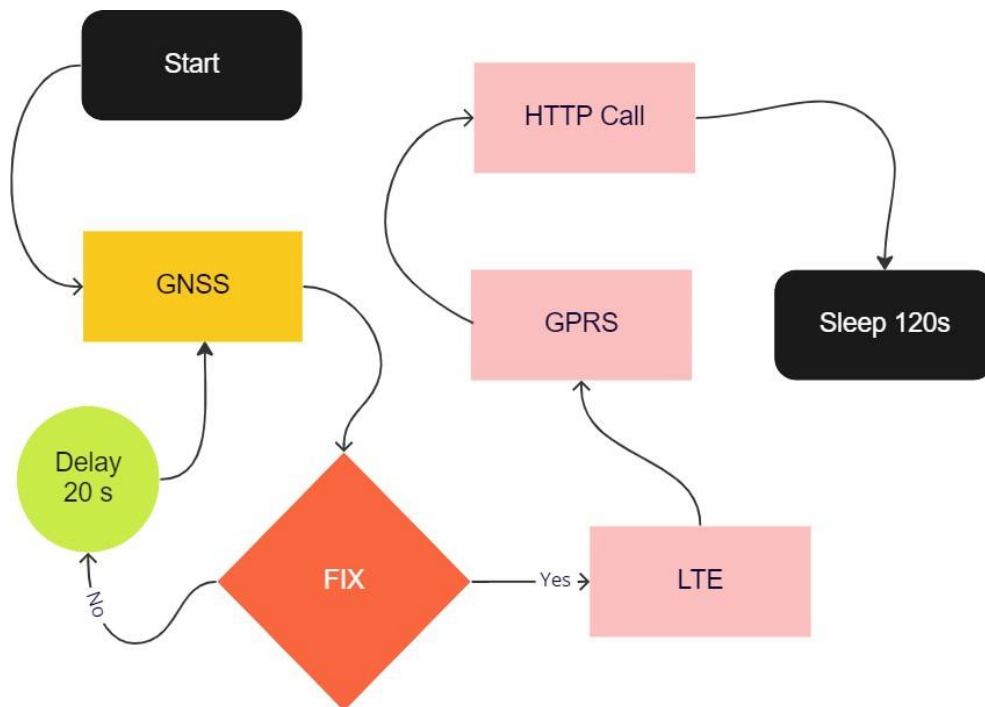
En la figura anterior se observa una propuesta de diseño preliminar que cumple con los criterios de visibilidad y seguridad. Brinda visibilidad por tener sus antenas externas. Brinda seguridad porque las antenas se encuentran ocultas y el cuerpo del dispositivo se mantiene en el interior del contenedor.

3.3.6 Firmware del dispositivo IoT

3.3.6.1 Requerimiento del firmware

Para lograr el envío de posición actual a la plataforma IoT cada 3 minutos, el *software* que corre en el microcontrolador debe seguir una secuencia en la que active el módulo GNSS y espere confirmación de que se ha efectuado un FIX, es decir, que se ha adquirido una posición e inmediatamente debe desactivar el módulo GNSS. Estos datos de posición deben enviarse a la plataforma mediante una llamada HTTP, para esto, debe activar el módulo LTE, efectuar el registro en la red y establecer una conexión de datos para después ejecutar la llamada. De inmediato debe desactivar el MODEM y activar el modo dormido para este y para el microcontrolador. A continuación, se presenta un diagrama de flujo para la secuencia descrita:

FIGURA 22. DIAGRAMA DE FLUJO DEL FIRMWARE PROPUESTO



El fabricante LilyGO tiene a disposición de los desarrolladores códigos de ejemplo para el desarrollo de *firmware* para sus productos. Estos ejemplos, así como la documentación técnica de los productos, se encuentran en GitHub, un repositorio para desarrolladores donde se puede compartir código (LilyGO, s. f.). Los ejemplos publicados en Github son para uso en la plataforma Arduino. Para simplificar el proceso de desarrollo y ante la ausencia de algún inconveniente que impida su uso para este desarrollo, se usa también la plataforma Arduino para el planteo del *firmware* del dispositivo.

Es importante tener presente que para controlar los MODEM se utilizan comandos AT. Estos se envían a través del puerto serial y también por medio de este se recibe la respuesta del módem y la información requerida. El listado de comandos para el MODEM Simcom se puede descargar del sitio web del fabricante. Existen varias notas de aplicación con comandos importantes según el uso requerido.

3.3.6.2 Librería para control del módem

Para efectos prácticos, sin embargo, se utiliza una biblioteca que actúa como intérprete de comandos AT, específicamente la TinyGSM que está diseñada para que las comunicaciones con MODEM sean más sencillas. Esta se encarga de enviar el comando correcto según la función deseada o solicitada por el desarrollador y es capaz de gestionar las respuestas AT para proporcionar la retroalimentación necesaria. Esta librería está creada para la interfaz estándar Arduino y es compatible con una gran cantidad de MODEM de diferentes marcas. Esta se trata de una librería que se ha usado por años, pero se mantiene actualizada con los últimos modelos de MODEM.

Es importante aclarar que pese a estar actualizada en cuanto a dispositivos de reciente fabricación, los comandos no han sufrido mayores cambios por lo que con GSM se refiere a cualquiera de las tecnologías vigentes, GPRS se refiere a la conexión de datos y GPS se usa para referirse a GNSS. Adicionalmente, no todos los comandos AT tienen una instrucción asociada, para esos casos se utiliza la instrucción `modem.sendAT("el comando AT requerido")`.

3.3.6.3 Librería para interacción con servidores web

Para efectuar la llamada HTTP al servidor, requerida para cargar en este la información de posición, se utiliza la librería `ArduinoHttpClient.h`. Esta está diseñada para facilitar la interacción con servidores web desde la plataforma Arduino.

A este respecto, se debe tener presente que, para que un dispositivo envíe información a la plataforma Traccar. Este hace una consulta HTTP POST, es decir, una llamada como las que se hacen en la barra de direcciones de un navegador de Internet; la diferencia radica en que, al hacerla, la información se recibe en el servidor y se almacena en la base de datos con la hora y fecha en la que se realizó.

Esta librería brinda soporte para el protocolo HTTP, lo que permite al ESP32 hacer este tipo de conexión con servidores de Internet. Para el caso particular de este proyecto, la URL de esta llamada tiene el formato siguiente:
`http://ipDelServidor:Puerto/?id=idDelDispositivo&lat={0}&lon={1}×tamp={2}&hdop={3}&altitude={4}&speed={5}` (Traccar, s. f.). Con esta llamada el dispositivo IoT debe enviar a la dirección IP del servidor un identificador único, su latitud, su longitud, la hora y fecha en la que se generó el reporte y otros datos.

A continuación, un ejemplo:

Las coordenadas de la sede central de la Universidad Latina son:
9.985593311266486, -84.10866469844667.

FIGURA 23. COORDENADAS DE LA ULATINA



Recuperado el 24 de diciembre de 2022 de <https://maps.google.com>

Al utilizar un generador de hora en formato Epoch se obtiene que el tiempo actual es: 1671855553.

FIGURA 24. TIEMPO UNIX PARA EL EJEMPLO

la marca de tiempo Unix actual **1671855790**

Convertir epoch a fecha normal

Admite marcas de tiempo Unix en segundos, milisegundos y microsegundos.

Tiempo Unix en **segundos**:

GMT/UTC : sábado, 24 de diciembre de 2022 4:19:13 AM

En su tiempo : viernes, 23 de diciembre de 2022 10:19:13 PM GMT-06:00

Relativo : hace unos segundos

Año Mes Día Hora Min Seg GMT

2022 - 12 - 24 4 : 19 : 13 GMT

Recuperado el 24 de diciembre de 2022, desde <https://espanol.epochconverter.com/>

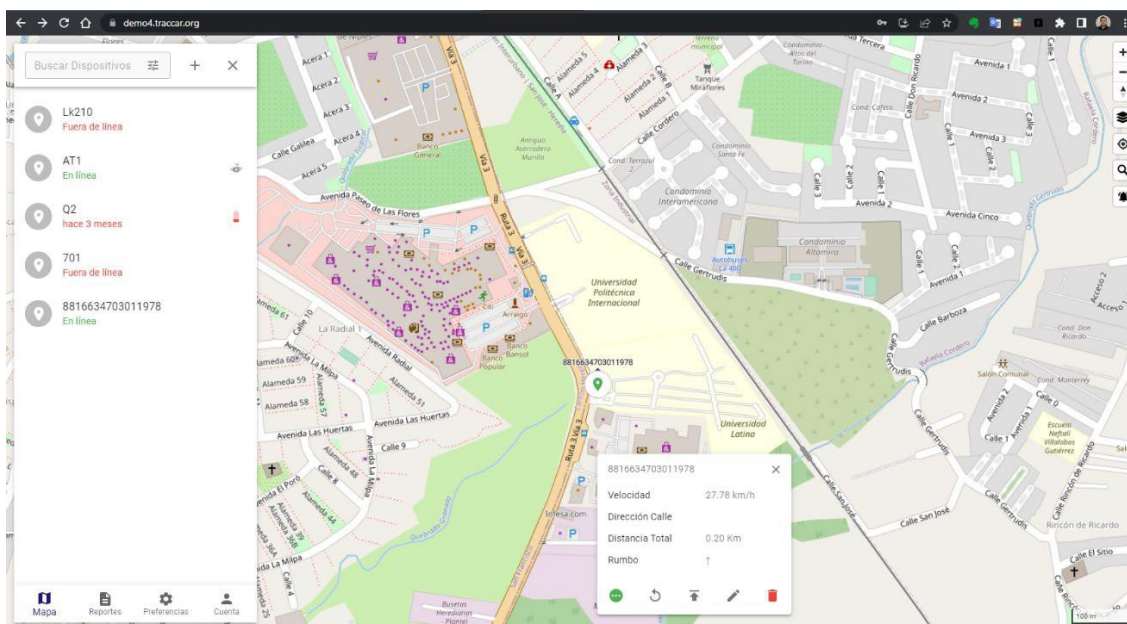
Se crea un identificador único y se matricula en una instancia demo de la plataforma Traccar: 8816634703011978

Con esta información se genera la URL que queda de la siguiente forma:
<http://demo4.traccar.org:5055/?id=8816634703011978&lat=9.983818167881154&lon=-84.10872908221025×tamp=1671854398&hdop=9&altitude=1500&speed=15>

Se coloca esa URL en el navegador, la respuesta es una página en blanco.

En la plataforma se observa la ubicación del dispositivo ficticio como si estuviera en la Universidad Latina:

FIGURA 25. GEOLOCALIZACIÓN SEGÚN LOS DATOS ENVIADOS A LA PLATAFORMA



Fuente: Recuperado el 11 de diciembre de 2022, desde <https://traccar.org>

3.3.6.4 Librería para funciones de tiempo

El tiempo que se debe enviar al servidor debe indicarse en tiempo UNIX o Epoch. Este corresponde a la cantidad de segundos transcurridos desde las 00:00:00 UTC horas del 1 de enero del año 1970 hasta la actualidad. Este se trata de un formato de tiempo estándar que no depende de zonas horarias ni configuraciones regionales de algún otro tipo, se usa ampliamente en desarrollo de *software*, bases de datos y

sistemas embebidos. En la plataforma Arduino para utilizar funciones de tiempo es necesario implementar una librería, en este caso se usa la librería llamada time.h.

3.3.6.5 Planteo del firmware

El ejemplo más relevante para este proyecto es el llamado Arduino_TinyGSM, que establece comunicación con el módem y adquiere la posición del módulo GNSS y una conexión de datos LTE. Este ejemplo se usó como base para el planteamiento del *firmware* de este proyecto. Los cambios que se hicieron al *software* original son:

- ❖ Se establecen los parámetros de configuración según el operador de telefonía móvil y los requerimientos del proyecto.
- ❖ Se elimina el código que no es relevante para el proyecto, por ejemplo, las partes que permiten enviar SMS y gestionar llamadas de voz.
- ❖ Se cambia el orden de ocurrencia de cada evento según el diagrama de flujo. se anida dentro de una sola función todo el proceso para activar el módulo GNSS, adquisición de coordenadas, inicialización del MODEM, establecimiento de conexión de datos, establecimiento de conexión TCP y envío TCP.
- ❖ Se introduce una función que convierte el tiempo recibido del receptor GNSS a tiempo UNIX.

En el Anexo II se incluye una copia del código propuesto y también una copia del archivo original.

3.4 Análisis de costos

Al considerar que uno de los criterios de diseño para este proyecto es el costo, a continuación, se proyecta el costo final del dispositivo en tres escenarios posibles. En todos los escenarios se considera despreciable el costo de la plataforma IoT por representar menos del 0.1 % del precio de venta final de cada dispositivo.

Escenario 1

Se consultó a Apple Ko, representante del fabricante chino de quipos IoT EELINK, por el costo estimado de cada equipo según la documentación actual e indica que no pueden dar un precio porque el proceso de evaluación tiene un costo y varias fases, costos en los que no se puede incurrir para esta etapa del proyecto, ir más allá queda fuera del alcance del presente trabajo. Informalmente, sin embargo, accedió a hacer una estimación con base en un producto suyo de similares características que se puede adaptar para funcionar del modo que se planteó en este documento, el modelo GPT49 e indica lo siguiente, el precio es de \$35 por dispositivo más \$2,500 que se pagan una única vez por concepto de diseño de moldes, PCB y otros costos. Se deben comprar 3000 unidades la primera vez. Estima que la diferencia en precio puede ser +\$10. El *firmware* quedaría precargado y el producto empacado para su venta, además es posible enviar las tarjetas SIM previamente para que se instalen durante el proceso de manufactura. En este escenario el margen de utilidad parece ser bueno.

Escenario 2

Buscando los costos por componente con diferentes proveedores para tener una idea más clara del costo de manufactura, se halló que del proveedor Mouser se puede obtener el microcontrolador por \$6 y las antenas \$4 y \$8. Del proveedor Wareshare es posible obtener el MODEM por \$35. En total \$52 sin considerar el proceso de manufactura. Si se añade mano de obra para la manufactura y carcasa plástica los costos superarían fácilmente los \$100.

Escenario 3

El *kit* de desarrollo usado que incluye las antenas, el módem y el procesador tiene un costo de \$52 en Amazon. Esta tarjeta contiene todos los componentes requeridos para el proyecto y ya ha atravesado por el proceso de manufactura. Es posible obtener mejores precios por volumen de compra.

Se consultó a la empresa local Plasti Lang para obtener una estimación del costo de la carcasa plástica, pero indican que lo que se tiene de la carcasa hasta el momento no es suficiente para brindar un precio. Según el diseño 3D enviado y la descripción que se brinda, estiman que cada carcasa puede costar de ₡1.500 a ₡2.500 y que la cantidad mínima que fabrican es de 1000 unidades.

Se estima la mano de obra de soldar la fotorresistencia y armar el dispositivo en \$2.5 por unidad que se basa en el costo de la hora de trabajo de personal calificado (MTSS, 2022). Se plantea, a continuación, el escenario más pesimista en el que se debe usar la tarjeta de desarrollo como PCB y la carcasa plástica se compraría localmente.

TABLA 8. RESUMEN DE COSTOS ESCENARIO 3

Ítem	Costo
SIM	\$0.90
Carcasa plástica	\$4.16
Tarjeta LilyGO	\$52.50
Impuestos de importación 15 %	\$8.10
Sensor de luz	\$2.5
Mano de obra	\$5.00
Total	\$73.16

En este escenario hay un margen de utilidad bajo. Se debe considerar que se trata del peor de los casos, pero que es posible conseguir mejores precios de los

componentes por volumen y exonerar un porcentaje de impuestos si se utilizan fondos de la iniciativa banca para el desarrollo.

Conclusiones

- ❖ La tecnología disponible es suficiente para el desarrollo de una solución de seguimiento de contenedores que cumpla con los criterios de visibilidad, seguridad y bajo costo, lo que hace que la propuesta de este trabajo sea una solución viable.
- ❖ No existe en el mercado una solución susceptible de modificarse, con el fin de evitar un diseño del sistema desde cero, pero herramientas de desarrollo que facilitan el diseño y prototipado de la solución.
- ❖ Las posibles ubicaciones para un dispositivo rastreador dentro de un contenedor, que permiten protegerlo de violentarse manteniendo la visibilidad, se limitan a los alrededores de las aberturas ubicadas entre las puertas y el marco.
- ❖ Existe gran cantidad de plataformas IoT para rastreo en modo renta y existe al menos una solución de código abierto y que cumple con los criterios de visibilidad, seguridad y costo.

Recomendaciones

- ❖ Para implementar la solución es importante considerar que la ubicación ideal del dispositivo es la más alta posible. Se debe buscar que la antena sea paralela al suelo para optimizar al máximo la recepción de la señal GNSS.
- ❖ El equipo debe considerarse como desechable, se recomienda evaluar la viabilidad de utilizar una batería tipo desechable, con el fin de reducir costos. Una combinación de pilas AA o AAA parece ser viable. Se debe tener en cuenta el reemplazo de la circuitería de regulación y carga según convenga.

- ❖ El presente proyecto tiene todo lo necesario para permitir el rastreo de los contenedores en el ámbito mundial, basta con alargar la vida de la batería cambiando la frecuencia de reporte en el océano debido a que no hay señal de redes móviles ahí. Además, se debe usar una SIM global para lo que hay varios proveedores.

Referencias

Bibliografía citada:

3Cu Electrónica. (s. f.). *Comandos AT*.

<https://sites.google.com/site/3cuelelectronica/home/comandos-at-1>

Asparuh Kamburov. (2018). *Manual para la práctica docente sobre redes geodésicas de referencia Y GNSS*. https://mgu.bg/wp-content/uploads/2022/06/manual_practica_docente.pdf

Baena Capilla, M. (2007). *Desarrollo de un Software para la Gestión de Correcciones RTCM de la Red Andaluza de Posicionamiento para Navegadores de Código (GEORAP)*. Universidad de Sevilla. Biblioteca de Ingeniería.
<https://biblus.us.es/bibing/proyectos/abreproy/11417/fichero/Cap%C3%ADtulos+%252F2-+Sistema+de+Navegacion+con+ayuda+de+sat%C3%A9lites.pdf>

Baires, L. (2022, 19 de septiembre). *Costa Rica combate narcotráfico en el Pacífico*. *Diálogo Américas*. <https://dialogo-americas.com/es/articles/costa-rica-combate-narcotrafico-en-el-pacifico/#.Y4Gp43bMK71>

Bartlett, C. (2022). *Container tracking 'a train not going to stop', predicts Drewry*. *The Load Star*. <https://theloadstar.com/container-tracking-a-train-not-going-to-stop-predicts-drewry/>

Battery University. (s. f.). *BU-409: Charging Lithium-ion*.

<https://batteryuniversity.com/article/bu-409-charging-lithium-ion>

Berné Valero, J. L.; Garrido Villen, N. y Capilla Roma, R. (2019). *GNSS: GPS, GALILEO, Glonass, BEIDOU Fundamentos y métodos de posicionamiento*. Universitat Politècnica de València.

- Comex. (2019). *Comunicado de Prensa. Centro de Monitoreo de imágenes no forma parte de compromisos del gobierno con APM Terminals*.
<https://www.comex.go.cr/sala-de-prensa/comunicados/2019/mayo/cp-2367-centro-de-monitoreo-de-im%C3%A1genes-no-forma-parte-de-compromisos-del-gobierno-con-apm-terminals/>
- Concox. (s. f.). *WeTrack Lite Mini Vehicle GPS tracker*.
<https://www.iconcox.com/products/wetrack-lite-mini-vehicle-gps-tracker.html>
- Cording, S. (2022). *What Is the ESP32? Elektor Magazine*.
<https://www.elektormagazine.com/articles/what-is-the-esp32>
- Cortés, E. (2017). *Política Criminal y Encarcelamiento por Delitos Relacionados con Drogas en Costa Rica*. Colectivo de Estudios de Drogas y Derecho (CEDD).
http://fileserv.idpc.net/library/Costa_Rica.pdf
- Del Rancho, J. (s. f.). *Historia Del Internet of Things*.
<https://www.timetoast.com/timelines/2731679>
- Deutsche Telekom. (s. f.). *Easy y simple: LTE-M*.
<https://www.telekom.com/en/company/details/long-term-evolution-for-machines-563208>
- Energía Solar. (s. f.). *Jaula de Faraday: definición y funcionamiento*. <https://solar-energia.net/electricidad/leyes/ley-de-faraday/jaula-de-faraday>
- Espinoza, W. (2022, 10 de octubre). *Corte Plena. Sesión Ordinaria n.º 51-2022* [Grabación en Video de la Sesión]. Poder Judicial.
<https://livestream.com/poderjudicial-costarica/events/10644108/videos/233266945>

- Espressif Systems. (2022). *ESP32 Series Datasheet Versión 4.1*.
https://www.espressif.com/sites/default/files/documentation/esp32_datasheet_en.pdf
- Espressif Systems. (2022). *ESP32 Technical Reference Manual Versión 4.8*.
https://www.espressif.com/sites/default/files/documentation/esp32_technical_reference_manual_en.pdf#
- Europa-Latinoamérica Programa de Asistencia contra el Crimen Transnacional Organizado (EL PAcCTO). (2021). *Evaluación de la amenaza del crimen transnacional organizado en Latinoamérica*. https://www.elpaccto.eu/wp-content/uploads/2021/07/Documento-web-2.MB_.pdf
- Fifotrack. (s. f.). *Platform Partners*. <https://www.fifotrack.com/platform-partners>
- Fundación Marviva (2022). *Índice de Progreso Social en Puntarenas: una visión del sector pesquero*. https://www.incae.edu/sites/default/files/iindice-de-progreso-social-en-puntarenas-una-visioin-del-sector-pesquero-feb-2022_0.pdf
- García, D. (2008). *Sistema GNSS (Global Navigation Satellite System) (Proyecto de fin de Carrera, Universidad Autónoma de Madrid)*.
<http://arantxa.ii.uam.es/~jms/pfcsteleco/lecturas/20080125DavidGarcia.pdf>
- Garita, L. (2016). *Guía Trabajos de Graduación*. Instituto Tecnológico de Costa Rica.
- Garrido-Villén, N. (2014, 9 de septiembre). *Sistemas GNSS. Introducción a los sistemas de posicionamiento global (4). Investigando sobre GNSS y delimitación de la propiedad*. <https://nagarvil.webs.upv.es/sistemas-gnss-introduccion/>
- Gómez, E. (2014). *Trilateración: Sismos, GPS, rayos y teléfonos celulares y la XIX Olimpiada de Ciencias de la Tierra*.
<https://www.ugm.org.mx/publicaciones/geos/pdf/geos14-2/trilateracion-34-2.pdf>

González, M. (2021, 13 de octubre). *Puntarenas en Costa Rica: la zona más pobre del país más próspero de Centroamérica (y el contraste con el lujo turístico)*. BBC News Mundo. <https://www.bbc.com/mundo/noticias-america-latina-58798999>

Gracia, M. (s. f.). *IoT-Internet of Things*. Deloitte. <https://www2.deloitte.com/es/es/pages/technology/articles/loT-internet-of-things.html>

HEAVY.AI. (2022). *Location-Based Services Definition*. <https://www.heavy.ai/technical-glossary/location-based-services>

How To Electronics. (2022). *SIM7600 4G LTE GSM módem Tutorial with Arduino | AT Commands, Call, SMS, HTTP Internet*. <https://youtu.be/v1eSL9aCPEg>

Instituto Nacional de Estadística y Censos (INEC). (2022). *Encuesta Continua de Empleo. Tercer trimestre Julio - agosto - Setiembre 2022. Resultados generales*. https://admin.inec.cr/sites/default/files/2022-11/ECE_III%20T_2022.pdf

Instituto Nacional de Estadística y Censos (INEC). (2022). *Encuesta Nacional de Hogares julio 2020: Resultados generales*. <https://admin.inec.cr/sites/default/files/2022-10/reenaho2022.pdf>

Instituto Nacional Sobre el Abuso de Drogas de Estados Unidos (NIH). (2016). *Cocaína: Abuso y adicción - Reporte de investigación*. <https://nida.nih.gov/es/publicaciones/serie-de-reportes/cocaina-abuso-y-adiccion/que-es-la-cocaina>

Instituto Sobre Alcoholismo y Farmacodependencia. (2012). *Consumo de drogas en Costa Rica*. Encuesta Nacional 2010. <https://www.icd.go.cr/portalicd/images/docs/uid/investigaciones/EncuestaNac2010/Fascculo%204%20Consumo%20de%20%20Cocana%20y%20Crack.pdf>

Latam GPS. (s. f.). *Sistema de rastreo satelital*. <https://latamgps.com/plataforma/>

- Ley n.º 8204. (2001). *Ley sobre Estupefacientes, Sustancias Psicotrópicas, Drogas de Uso no Autorizado, Actividades Conexas, Legitimación de Capitales y Financiamiento al Terrorismo.*
- LilyGO. (s. f.). *TinyGSM Getting Started Guide*. https://github.com/Xinyuan-LilyGO/T-SIM7600X/tree/master/examples/Arduino_TinyGSM/AllFunctions
- López, J. (2020). *John von Neumann, el Genio que Diseñó la Arquitectura de Nuestros Ordenadores*. <https://www.xataka.com/historia-tecnologica/john-von-neumann-genio-que-diseno-arquitectura-nuestros-ordenadores-hizo-hace-75-anos-este-solo-uno-sus-logros>
- McDermott, J.; Bargent, J.; Den Held, D. y Ramírez, M. (2021). *The Cocaine Pipeline to Europe*. <https://globalinitiative.net/wp-content/uploads/2021/02/The-cocaine-pipeline-to-Europe-GI-TOCInsightCrime.pdf>
- MEMUK Magazine. (2017). *End-to end GPS Technology Offers Solution for Cargo Tracking*. <https://www.memuk.org/technology/end-end-gps-technology-offers-solution-cargo-tracking-42120>
- Ministerio de Trabajo y Seguridad Social MTSS. (2022). *Decreto de Salarios Mínimos n.º 43633-MTSS*. https://www.mtss.go.cr/temas-laborales/salarios/decretos/decreto_43633_MTSS.pdf
- Nevada Dot. (2017). *Global Positioning System (GPS)*. State of Nevada Department of Transportation Construction. <https://www.dot.nv.gov/home/showpublisheddocument/9212/63645150998827000#:~:text=Nearly%20all%20GPS%20receivers%2C%20inexpensive,between%2010%20and%2015%20degrees.>
- Observatorio de la Violencia. (2022). *Homicidios según móvil*. <http://observatorio.mj.go.cr/recursos/tablas-y-graficos#>

Oficina de Coordinación Nacional de Posicionamiento, Navegación, y Cronometría por Satélite (GPS.GOV). (2022, 24 de agosto). *Sistema de Posicionamiento Global*. <https://www.gps.gov/spanish.php>

Okunieff, P. (1997). *Synthesis of Transit Practice 24, AVL Systems for Bus Transit*. Cambridge Systematics, Inc. https://onlinepubs.trb.org/onlinepubs/tcrp/tcrp_syn_24.pdf

Organización de las Naciones Unidas (ONU). (2022). *Informe Mundial sobre las Drogas 2022*. Tendencias del Mercado. https://www.unodc.org/res/wdr2022/MS/WDR22_Booklet_4.pdf

Osio, J.; Aróztegui, W. y Rapallini, J. (2020). *Sistemas Digitales Basados en Microcontroladores*. Editorial de la Universidad Nacional de La Plata (EDULP). <https://doi.org/10.35537/10915/95305>

Osmand. (s. f.). *Build OsmAnd, Tools and SDK & API Samples*. <https://osmand.net/docs/technical/build-osmand/>

Pathak, A. (2022, 18 de agosto). *Tecnología GNSS vs. GPS: Conozca las diferencias clave*. Geekflare. <https://geekflare.com/es/gnss-vs-gps-technology/>

Piña de Costa Rica. (2021, 26 de marzo). *Sector piñero protege sus exportaciones*. <https://www.pinadecostarica.com/2021/03/sector-pinero-protege-sus-exportaciones>

Poder Judicial. (2022). *Diccionario usual del Poder Judicial*. <https://dictionariosusual.poder-judicial.go.cr/index.php/diccionario/42908:marchamo%20electr%C3%B3nico%20para%20control%20aduanero>

Pomareda, F. (2022, 26 de octubre). *Droga encontrada en contenedores es un 67% del total capturado en el país. Cocaína decomisada aumentó hasta en 1.376% desde*

- que APM opera terminal de Moín. *Semanario Universidad*.
<https://semanariouniversidad.com/pais/cocaina-decomisada-aumento-hasta-en-1-376-desde-que-apm-opera-terminal-de-moin/>
- Precintia. (2022). *Qué es un precinto sello lacre o marchamo de seguridad*.
<https://www.precintia.com/blog/que-es-un-precinto-sello-lacre-o-marchamo-de-seguridad/>
- Programa de las Naciones Unidas para el Desarrollo (PNUD). (2021). *Atlas de Desarrollo Humano Cantonal*. <https://pnud-conocimiento.cr/proyecto/atlas-de-desarrollo-humano-cantonal/>
- Programa Estado de la Nación. (2021). *Estado de la nación 2021: versión completa Programa Estado de la Nación*. Consejo Nacional de Rectores.
<https://estadonacion.or.cr/wp-content/uploads/2021/11/estado-nacion2021.pdf>
- PVCDROM. (s. f.). *Battery Capacity*. <https://www.pveducation.org/pvcdrom/battery-characteristics/battery-capacity>
- Quectel Wireless Solutions. (2022). *Quectel releases dual-band high-precision GNSS module LC29H with RTK and DR technologies*. <https://www.quectel.com/news-and-pr/gnss-lc29h-launch>
- Quectel. (2021). *Antenna YFGA003AA Datasheet v1.1*. https://cnquectel-my.sharepoint.com/:b:/g/personal/arturo_proskauer_quectel_com/EYNS8GHkaHFMv4SdHpV9sYwBs93feuW6rCNBT99d7GT4Nw?e=fgQN2b
- Ramos Rechnitz, A.; Mata Vega, G. y Méndez Retana, J. R. (2022, 09 de junio). *Para referirse a la penetración del narcotráfico en Costa Rica*. [Grabación en Video de la Audiencia]. Asamblea Legislativa, Comisión de Seguridad y Narcotráfico.
<https://www.youtube.com/watch?v=2blf4eRZExE>

- Recuero, P. (2020, 22 de septiembre). *Breve historia de Internet de las cosas (IoT)*. Telefónica S. A. <https://empresas.blogthinkbig.com/breve-historia-de-internet-de-las-cosas-iot/>
- Rojas, P. (2019, 3 de octubre) Costa Rica: el tercer país que más envía cocaína al principal puerto europeo. En 9 meses casi 7 t de esa droga llegaron a puerto de Amberes desde territorio tico. País supera en envíos a Colombia, está por detrás de Brasil y Ecuador. *CRHoy*. <https://www.crhoy.com/nacionales/costa-rica-el-tercer-pais-que-mas-envia-cocaina-al-principal-puerto-europeo/>
- Saborío, S. (2019). Estado del arte sobre narcoviolenca en Costa Rica. *Revista Reflexiones*, 98(2).
https://www.scielo.sa.cr/scielo.php?script=sci_arttext&pid=S1659-28592019000200023
- SEA. (s. f.). *Efecto Doppler*. <https://www.sea-astronomia.es/glosario/efecto-doppler>
- Sector Electricidad. (2021). *Jaula de Faraday*. <https://www.sectorelectricidad.com/wp-content/uploads/2021/02/jaula-de-faraday1.png>
- Shibo, X.; Peng, N.; Wensheng, C.; Qingzhou, L.; Xianfeng, Z. (2016). *The Application of Ad-Hoc Network in Smart Container Tracking System*. China Waterborne Transport Research Institute. DOI: 10.1109/TrustCom.2016.0317
- Sickle, J. (s. f.). *GEOG 862-GPS and GNSS for Geospatial Professionals*. The Pennsylvania State University. <https://www.e-education.psu.edu/geog862/node/1899>
- SIMCom Wireless Solutions Limited (SIMCom). (2020). *SIM7600G(-H) SIM7600NA(-H) Hardware Design v1.6*. https://mt-system.ru/sites/default/files/documents/sim7600g-h_sim7600na-h_hardware_design_v1.06.pdf

- Tecnología Informática. (s. f.). *¿Qué es firmware?* <https://www.tecnologia-informatica.com/que-es-firmware/>
- Tensilica, Inc. (2010). *Xtensa Instruction Set Architecture (ISA) Reference Manual*. <https://www.linkedin.com/pulse/five-reasons-we-lack-container-tracking-simple-solution-higgins/>
- The European Monitoring Centre for Drugs and Drug Addiction (EMCDDA). (2022, 6 de mayo). *Europe and the global cocaine trade*. https://www.emcdda.europa.eu/publications/eu-drug-markets/cocaine/europe-and-global-cocaine-trade_en
- The European Monitoring Centre for Drugs and Drug Addiction (EMCDDA). (2022, 6 de mayo). *Europe changing role in expanding cocaine and methamphetamine markets*. https://www.emcdda.europa.eu/news/2022/5/eu-drug-markets-cocaine-and-methamphetamine_en.
- Traccar. (2022). *Modern GPS Tracking Platform*. <https://www.traccar.org/>
- Unece. (2012). *Guía de implementación de la facilitación del comercio*. <https://tfig.unece.org/SP/contents/TIR-convention.htm>
- Universidad de Costa Rica. (2018). *Desarrollo y empleo en Puntarenas, reto social e institucional: memoria del foro*. <https://www.srp.ucr.ac.cr/sites/default/files/MemoriasJornadasdeInvestigacion/Repositorio/Memoria.pdf>
- Vaughn, C. (2022, 10 de noviembre). *Limon: The New gateway Port For Cocaine Leaving Costa Rica*. *Costa Rica Star News*. <https://news.co.cr/limon-the-new-gateway-port-for-cocaine-leaving-costa-rica/79128/>
- Vecchio, R.; Martínez, E. y Cosentino, J. P. (2017). *Internet de la Cosas (IoT)*. <http://repositorio.ub.edu.ar/handle/123456789/8484>

Wall, M. y Harvey, A. (2022). *GPS: Everything you need to know about the space-based technology keeping us on track*. Space.com. <https://www.space.com/gps-what-is-it>

Yépez Maigua, A. C. (2018). *Consumo de sustancias psicotrópicas/ estupefacientes y su incidencia en el comportamiento de los estudiantes dentro del aula, de los octavos y novenos años de educación básica, de la Unidad Educativa “Luis Ulpiano de la Torre”, cantón Cotacachi período 2014-2015* (Tesis de pregrado, Universidad Técnica del Norte).
<http://repositorio.utn.edu.ec/handle/123456789/8389>

Bibliografía consultada:

Genoma del Robo. (2020, 21 de noviembre). *Seguridad Residencial con defensa en Profundidad*. <https://www.genomadelrobo.com/blog/seguridad-residencial-defensa-profundidad/>

Newton, E. (2021, 16 de julio). *What IoT sensors are onboard NASA’s Perseverance rover?* Techfruit. <https://techfruit.com/2021/07/16/what-iot-sensors-are-onboard-nasas-perseverance-rover/>

Random Nerd Tutorials. (s. f.). *ESP32 HTTP GET and HTTP POST with Arduino IDE (JSON, URL Encoded, Text)*. <https://randomnerdtutorials.com/esp32-http-get-post-arduino/>

Random Nerd Tutorials. (s. f.). *Getting Started with LILYGO T-SIM7000G ESP32 (LTE, GPRS, and GPS)*. <https://randomnerdtutorials.com/lilygo-t-sim7000g-esp32-lte-gprs-gps/>

Unidad Empresarial de la Sociedad Suiza de Radio y Televisión (SWI). (2022, 24 de octubre). *Hallan en Costa Rica 400 kilos de cocaína en un contenedor que iba a Bélgica*. https://www.swissinfo.ch/spa/costa-rica-narcotr%C3%A1fico_hallan-en-

costa-rica-400-kilos-de-coca%C3%ADna-en-un-contenedor-que-iba-a-
b%C3%A9lgica/48004084

Glosario

Código abierto: Conocido también como Open Source, se refiere al código fuente de un *software* cuyo uso es libre en su estado actual y puede modificarse según el gusto o necesidad de un particular. Además, ya sea en su estado original o con modificaciones, puede distribuirse de forma libre por cualquier persona.

PCB: Circuito impreso o tarjeta electrónica

Kit de desarrollo o tarjeta de desarrollo: Un circuito impreso que contiene los componentes necesarios para el desarrollo de sistemas electrónicos con base en esos componentes.

Librerías: Son archivos con funciones que se desarrollaron específicamente para administrar y controlar, tanto el microcontrolador como los módulos que se requieran para un proyecto. Además, existen las que se desarrollan para la implementación de protocolos de comunicación. Sin librerías el desarrollo de un proyecto es mucho más complejo.

Decibel: El decibelio es la décima parte de una campana, que debe su nombre a Alexander Graham Bell. Es una unidad logarítmica adimensional que se utiliza para hacer una comparación. Un aumento de 3 decibelios indica una duplicación de la intensidad de la señal y una disminución de 3 decibelios indica una reducción a la mitad de la intensidad de la señal.

Anexos

```
/******
```

TinyGSM Getting Started guide:
<https://tiny.cc/tinygsm-readme>

NOTE:
Some of the functions may be unavailable for your modem.
Just comment them out.

https://simcom.ee/documents/SIM7600C/SIM7500_SIM7600%20Series_AT%20Command%20Manual_V1.01.pdf

```
*****/
```

```
#define TINY_GSM_MODEM_SIM7600
```

```
// Set serial for debug console (to the Serial Monitor, default speed 115200)
#define SerialMon Serial
```

```
// Set serial for AT commands (to the module)
// Use Hardware Serial on Mega, Leonardo, Micro
#define SerialAT Serial1
```

```
// See all AT commands, if wanted
#define DUMP_AT_COMMANDS
```

```
// Define the serial console for debug prints, if needed
#define TINY_GSM_DEBUG SerialMon
```

```
/*
  Tests enabled
*/
#define TINY_GSM_TEST_GPRS      true
#define TINY_GSM_TEST_TCP      true
// #define TINY_GSM_TEST_CALL   true
// #define TINY_GSM_TEST_SMS    true
// #define TINY_GSM_TEST_USSD   true
// #define TINY_GSM_TEST_TEMPERATURE true
// #define TINY_GSM_TEST_TIME   true
#define TINY_GSM_TEST_GPS      true
// powerdown modem after tests
#define TINY_GSM_POWERDOWN     true
// #define TEST_RING_RI_PIN     true
```

```
// set GSM PIN, if any
#define GSM_PIN                ""
```

```
// Set phone numbers, if you want to test SMS and Calls
// #define SMS_TARGET "+380xxxxxxxx"
// #define CALL_TARGET "+380xxxxxxxx"
```

```
// Your GPRS credentials, if any
const char apn[] = "YourAPN";
// const char apn[] = "ibasis.iot";
const char gprsUser[] = "";
const char gprsPass[] = "";
```



```

// Server details to test TCP/SSL
const char server[] = "vsh.pp.ua";
const char resource[] = "/TinyGSM/logo.txt";

#include <SPI.h>
#include <SD.h>
#include <Ticker.h>
#include <TinyGsmClient.h>
#include "utilities.h"

#ifdef DUMP_AT_COMMANDS
#include <StreamDebugger.h>
StreamDebugger debugger(SerialAT, SerialMon);
TinyGsm modem(debugger);
#else
TinyGsm modem(SerialAT);
#endif

void setup()
{
  // Set console baud rate
  SerialMon.begin(115200);
  delay(10);

  // Set GSM module baud rate
  SerialAT.begin(UART_BAUD, SERIAL_8N1, MODEM_RX, MODEM_TX);

  /*
   The indicator light of the board can be controlled
  */
  pinMode(LED_PIN, OUTPUT);
  digitalWrite(LED_PIN, HIGH);

  /*
   MODEM_PWRKEY IO:4 The power-on signal of the modulator must be given to it,
   otherwise the modulator will not reply when the command is sent
  */
  pinMode(MODEM_PWRKEY, OUTPUT);
  digitalWrite(MODEM_PWRKEY, HIGH);
  delay(300); //Need delay
  digitalWrite(MODEM_PWRKEY, LOW);

  /*
   MODEM_FLIGHT IO:25 Modulator flight mode control,
   need to enable modulator, this pin must be set to high
  */
  pinMode(MODEM_FLIGHT, OUTPUT);
  digitalWrite(MODEM_FLIGHT, HIGH);

  //Initialize SDCard
  SPI.begin(SD_SCLK, SD_MISO, SD_MOSI, SD_CS);
  if (!SD.begin(SD_CS)) {
    Serial.println("SDCard MOUNT FAIL");
  } else {
    uint32_t cardSize = SD.cardSize() / (1024 * 1024);
    String str = "SDCard Size: " + String(cardSize) + "MB";
    Serial.println(str);
  }
}

```

```

}

// Uncomment below will perform loopback test
// while (1) {
//     while (SerialMon.available()) {
//         SerialAT.write(SerialMon.read());
//     }
//     while (SerialAT.available()) {
//         SerialMon.write(SerialAT.read());
//     }
// }
}

void light_sleep(uint32_t sec )
{
    esp_sleep_enable_timer_wakeup(sec * 1000000ULL);
    esp_light_sleep_start();
}

void loop()
{
    bool res ;

    // Restart takes quite some time
    // To skip it, call init() instead of restart()
    DBG("Initializing modem...");
    if (!modem.init()) {
        DBG("Failed to restart modem, delaying 10s and retrying");
        return;
    }
    //
    // // Restart takes quite some time
    // // To skip it, call init() instead of restart()
    // DBG("Initializing modem...");
    // if (!modem.restart()) {
    //     DBG("Failed to restart modem, delaying 10s and retrying");
    //     // restart autobaud in case GSM just rebooted
    //     return;
    // }
}

#if TINY_GSM_TEST_GPRS
/* Preferred mode selection : AT+CNMP
2 – Automatic
13 – GSM Only
14 – WCDMA Only
38 – LTE Only
59 – TDS-CDMA Only
9 – CDMA Only
10 – EVDO Only
19 – GSM+WCDMA Only
22 – CDMA+EVDO Only
48 – Any but LTE
60 – GSM+TDSCDMA Only
63 – GSM+WCDMA+TDSCDMA Only
67 – CDMA+EVDO+GSM+WCDMA+TDSCDMA Only

```

```

    39 – GSM+WCDMA+LTE Only
    51 – GSM+LTE Only
    54 – WCDMA+LTE Only
*/
String ret;
// do {
//     ret = modem.setNetworkMode(2);
//     delay(500);
// } while (ret != "OK");
ret = modem.setNetworkMode(2);
DBG("setNetworkMode:", ret);

//https://github.com/vshymansky/TinyGSM/pull/405
uint8_t mode = modem.getGNSSMode();
DBG("GNSS Mode:", mode);

/**
CGNSSMODE: <gnss_mode>,<dpo_mode>
This command is used to configure GPS, GLONASS, BEIDOU and QZSS support mode.
gnss_mode:
    0 : GLONASS
    1 : BEIDOU
    2 : GALILEO
    3 : QZSS
dpo_mode :
    0 disable
    1 enable
*/
modem.setGNSSMode(1, 1);
light_sleep(1);

String name = modem.getModemName();
DBG("Modem Name:", name);

String modemInfo = modem.getModemInfo();
DBG("Modem Info:", modemInfo);

// Unlock your SIM card with a PIN if needed
if (GSM_PIN && modem.getSimStatus() != 3) {
    modem.simUnlock(GSM_PIN);
}

DBG("Waiting for network...");
if (!modem.waitForNetwork(600000L)) {
    light_sleep(10);
    return;
}

if (modem.isNetworkConnected()) {
    DBG("Network connected");
}
#endif

#if TINY_GSM_TEST_GPRS
DBG("Connecting to", apn);

```

```

if (!modem.gprsConnect(apn, gprsUser, gprsPass)) {
    light_sleep(10);
    return;
}

res = modem.isGprsConnected();
DBG("GPRS status:", res ? "connected" : "not connected");

String ccid = modem.getSimCCID();
DBG("CCID:", ccid);

String imei = modem.getIMEI();
DBG("IMEI:", imei);

String imsi = modem.getIMSI();
DBG("IMSI:", imsi);

String cop = modem.getOperator();
DBG("Operator:", cop);

IPAddress local = modem.localIP();
DBG("Local IP:", local);

int csq = modem.getSignalQuality();
DBG("Signal quality:", csq);
#endif

#if TINY_GSM_TEST_USSD && defined TINY_GSM_MODEM_HAS_SMS
String ussd_balance = modem.sendUSSD("*111#");
DBG("Balance (USSD):", ussd_balance);

String ussd_phone_num = modem.sendUSSD("*161#");
DBG("Phone number (USSD):", ussd_phone_num);
#endif

#if TINY_GSM_TEST_TCP && defined TINY_GSM_MODEM_HAS_TCP
TinyGsmClient client(modem, 0);
const int port = 80;
DBG("Connecting to ", server);
if (!client.connect(server, port)) {
    DBG("... failed");
} else {
    // Make a HTTP GET request:
    client.print(String("GET ") + resource + " HTTP/1.0\r\n");
    client.print(String("Host: ") + server + "\r\n");
    client.print("Connection: close\r\n\r\n");

    // Wait for data to arrive
    uint32_t start = millis();
    while (client.connected() && !client.available() &&
        millis() - start < 30000L) {
        delay(100);
    };

    // Read data
    start = millis();
    while (client.connected() && millis() - start < 5000L) {

```

```

while (client.available()) {
  SerialMon.write(client.read());
  start = millis();
}
}
client.stop();
}
#endif

#if TINY_GSM_TEST_CALL && defined(CALL_TARGET)

  DBG("Calling:", CALL_TARGET);
  SerialAT.println("ATD"CALL_TARGET";");
  modem.waitResponse();
  light_sleep(20);
#endif

#if TINY_GSM_TEST_GPS && defined TINY_GSM_MODEM_HAS_GPS
  DBG("Enabling GPS/GNSS/GLONASS");
  modem.enableGPS();
  light_sleep(2);

  float lat2    = 0;
  float lon2    = 0;
  float speed2  = 0;
  float alt2    = 0;
  int  vsat2   = 0;
  int  usat2   = 0;
  float accuracy2 = 0;
  int  year2   = 0;
  int  month2  = 0;
  int  day2    = 0;
  int  hour2   = 0;
  int  min2    = 0;
  int  sec2    = 0;
  DBG("Requesting current GPS/GNSS/GLONASS location");
  for (;;) {
    digitalWrite(LED_PIN, !digitalRead(LED_PIN));
    if (modem.getGPS(&lat2, &lon2, &speed2, &alt2, &vsat2, &usat2, &accuracy2,
                    &year2, &month2, &day2, &hour2, &min2, &sec2)) {
      DBG("Latitude:", String(lat2, 8), "\tLongitude:", String(lon2, 8));
      DBG("Speed:", speed2, "\tAltitude:", alt2);
      DBG("Visible Satellites:", vsat2, "\tUsed Satellites:", usat2);
      DBG("Accuracy:", accuracy2);
      DBG("Year:", year2, "\tMonth:", month2, "\tDay:", day2);
      DBG("Hour:", hour2, "\tMinute:", min2, "\tSecond:", sec2);
      break;
    } else {
      light_sleep(2);
    }
  }
  DBG("Retrieving GPS/GNSS/GLONASS location again as a string");
  String gps_raw = modem.getGPSraw();
  DBG("GPS/GNSS Based Location String:", gps_raw);
  DBG("Disabling GPS");
  modem.disableGPS();
#endif

```

```

#if TINY_GSM_TEST_TIME && defined TINY_GSM_MODEM_HAS_TIME
  int year3 = 0;
  int month3 = 0;
  int day3 = 0;
  int hour3 = 0;
  int min3 = 0;
  int sec3 = 0;
  float timezone = 0;
  for (int8_t i = 5; i; i--) {
    DBG("Requesting current network time");
    if (modem.getNetworkTime(&year3, &month3, &day3, &hour3, &min3, &sec3,
                             &timezone)) {
      DBG("Year:", year3, "\tMonth:", month3, "\tDay:", day3);
      DBG("Hour:", hour3, "\tMinute:", min3, "\tSecond:", sec3);
      DBG("Timezone:", timezone);
      break;
    } else {
      DBG("Couldn't get network time, retrying in 15s.");
      light_sleep(15);
    }
  }
  DBG("Retrieving time again as a string");
  String time = modem.getGSMDateTime(DATE_FULL);
  DBG("Current Network Time:", time);
#endif

#if TINY_GSM_TEST_GPRS
  modem.gprsDisconnect();
  light_sleep(5);
  if (!modem.isGprsConnected()) {
    DBG("GPRS disconnected");
  } else {
    DBG("GPRS disconnect: Failed.");
  }
#endif

#if TINY_GSM_TEST_TEMPERATURE && defined TINY_GSM_MODEM_HAS_TEMPERATURE
  float temp = modem.getTemperature();
  DBG("Chip temperature:", temp);
#endif

#ifdef TEST_RING_RI_PIN
#ifdef MODEM_RI
  //Set RI Pin input
  pinMode(MODEM_RI, INPUT);

  Serial.println("Wait for call in");
  //When is no calling ,RI pin is high level
  while (digitalRead(MODEM_RI)) {
    Serial.print('.');
    delay(500);
  }
  Serial.println("call in ");

  //Wait for 5 seconds to connect the call
  delay(5000);
#endif

```

```

//Accept call
SerialAT.println("ATA");

// Hang up after 20 seconds of talk time
delay(20000);

SerialAT.println("ATH");

#endif //MODEM_RI
#endif //TEST_RING_RI_PIN

#ifdef MODEM_DTR1

modem.sleepEnable();

delay(100);

// test modem response , res == 0 , modem is sleep
res = modem.testAT();
Serial.print(" Test AT result -> ");
Serial.println(res);

delay(1000);

Serial.println("Use DTR Pin Wakeup");
pinMode(MODEM_DTR, OUTPUT);
//Set DTR Pin low , wakeup modem .
digitalWrite(MODEM_DTR, LOW);

// test modem response , res == 1 , modem is wakeup
res = modem.testAT();
Serial.print(" Test AT result -> ");
Serial.println(res);

#endif

#if TINY_GSM_POWERDOWN
// Try to power-off (modem may decide to restart automatically)
// To turn off modem completely, please use Reset/Enable pins
modem.poweroff();
DBG("Poweroff.");
#endif

SerialMon.printf("End of tests. Enable deep sleep , Will wake up in %d seconds", TIME_TO_SLEEP);

//Wait moden power off
light_sleep(5);

esp_sleep_enable_timer_wakeup(TIME_TO_SLEEP * uS_TO_S_FACTOR);
delay(200);
esp_deep_sleep_start();

while (1);
}

```



```
/******
```

Propuesta de un rastreador GNSS utilizando un microcontrolador ESP32 y un módulo de comunicaciones SIM7600G-H que reportará su posición a la plataforma traccar.

Basado en el ejemplo https://github.com/Xinyuan-LilyGO/T-SIM7600X/tree/master/examples/Arduino_TinyGSM

```
*****/
```

```
#define TINY_GSM_MODEM_SIM7600
// Configurar serial para consola de depuración (al Monitor Serial, velocidad por defecto 115200)
#define SerialMon Serial
// Configurar puerto serie para enviar comandos AT al MODEM
#define SerialAT Serial1
// Ver todos los comandos AT, si se desea
#define DUMP_AT_COMMANDS
// Definir puerto de consola serie para depuración, si es necesario
#define TINY_GSM_DEBUG SerialMon
// Funciones del módulo de comunicaciones que se van a utilizar
#define TINY_GSM_TEST_GPRS true
#define TINY_GSM_TEST_TCP true
#define TINY_GSM_TEST_GPS true
#define TINY_GSM_POWERDOWN true
// PIN del SIM
#define GSM_PIN "1111"
/*
```

Se establece el nombre del punto de acceso y sus credenciales. Debido a que en Costa Rica únicamente Claro cuenta con una red CAT-M, se usará un SIM de este operador celular. Para esto el APN es datos.claro y no requiere credenciales de acceso.

```
*/
const char apn[] = "datos.claro";
const char gprsUser[] = "";
const char gprsPass[] = "";
```

```
// Librerías requeridas
#include <TinyGsmClient.h>
#include <ArduinoHttpClient.h>
#include <TimeLib.h>
#include <SPI.h>
#include <Ticker.h> // Funciones especiales de ESP32 para Arduino.
#include <TinyGsmClient.h>
#include <utilities.h>
```

```
// Si previamente de eligió ver todos los comandos AT enviados en el puerto de consola aquí se indica
#ifdef DUMP_AT_COMMANDS
#include <StreamDebugger.h>
StreamDebugger debugger(SerialAT, SerialMon);
TinyGsm modem(debugger);
#else
TinyGsm modem(SerialAT);
#endif
```

```
// Configuración
void setup()
{
```

```
// Se establece la velocidad del puerto de consola
SerialMon.begin(115200);
delay(10);
```

```
// Se establece la velocidad del puerto del MODEM y los parámetros de conexión serial
SerialAT.begin(UART_BAUD, SERIAL_8N1, MODEM_RX, MODEM_TX);
```

```
// Se configura el LED multipropósito incluido en la tarjeta de desarrollo
pinMode(LED_PIN, OUTPUT);
digitalWrite(LED_PIN, HIGH);
```

```
// MODEM_PWRKEY IO:4 Se define el comando que activa el MODEM
pinMode(MODEM_PWRKEY, OUTPUT);
digitalWrite(MODEM_PWRKEY, HIGH);
delay(300); //Need delay
digitalWrite(MODEM_PWRKEY, LOW);
```

```
// MODEM_FLIGHT IO:25 Se define el comando que activa el modo avión
pinMode(MODEM_FLIGHT, OUTPUT);
digitalWrite(MODEM_FLIGHT, HIGH);
}
```

```
void light_sleep(uint32_t sec )
{
    esp_sleep_enable_timer_wakeup(sec * 1000000ULL); //unsigned long long
    esp_light_sleep_start();
}
```

```
// Ciclo principal
void loop()
{
    bool res ;
```

```
// Inicialización del MODEM
DBG("Iniciando MODEM...");
if (!modem.init()) {
    DBG("Error al iniciar MODEM, intentando de nuevo...");
    return;
}
```

```
/*
    Se establece el modo de conexión. El MODEM SIMCOM soporta conexión LTE y también GSM (2G). Se
    debe indicar el modo que se usará. Los valores posibles son 2 Selección automática, 3 solo GSM, 38 solo
    LTE, 51 GSM y LTE. Para nuestro caso usaremos selección automática.
*/
```

```
#if TINY_GSM_TEST_GPRS
String ret;
ret = modem.setNetworkMode(2);
DBG("setNetworkMode:", ret);
```

```
uint8_t mode = modem.getGNSSMode();
DBG("GNSS Mode:", mode);
```

```

/**
CGNSSMODE: <gnss_mode>,<dpo_mode>
Configuración del modo GNSS. GPS + GLONASS, BEIDOU and QZSS support mode.
gnss_mode:
  0 : GLONASS
  1 : BEIDOU
  2 : GALILEO
  3 : QZSS
dpo_mode :
  0 disable
  1 enable
*/
modem.setGNSSMode(0, 1);
light_sleep(1);

// Descloquear el SIM de ser requerido
if (GSM_PIN && modem.getSimStatus() != 3) {
  modem.simUnlock(GSM_PIN);
}

// Registro en la red
DBG("Esperando red celular...");
if (!modem.waitForNetwork(600000L)) {
  light_sleep(10);
  return;
}

if (modem.isNetworkConnected()) {
  DBG("Conexión establecida");
}
#endif

// Inicia conexión de datos
#ifdef TINY_GSM_TEST_GPRS
if (!modem.gprsConnect(apn, gprsUser, gprsPass)) {
  light_sleep(10);
  return;
}

//Muestra información de conexión
res = modem.isGprsConnected();
DBG("Estado GPRS:", res ? "connectado" : "no connectado");

String ccid = modem.getSimCCID();
DBG("CCID:", ccid);

String imei = modem.getIMEI();
DBG("IMEI:", imei);

String imsi = modem.getIMSI();
DBG("IMSI:", imsi);

String cop = modem.getOperator();
DBG("Operador:", cop);

IPAddress local = modem.localIP();
DBG("IP Local:", local);

```

```
int csq = modem.getSignalQuality();
DBG("Calidad de la Señal:", csq);
#endif
```

```
// Obtiene coordenadas de geolocalización
```

```
#if TINY_GSM_TEST_GPS && defined TINY_GSM_MODEM_HAS_GPS
```

```
DBG("Activando GNSS");
modem.enableGPS();
light_sleep(2);
```

```
tmElements_t te;
time_t unixTime;
```

```
float lat2 = 0;
float lon2 = 0;
float speed2 = 0;
float alt2 = 0;
int vsat2 = 0;
int usat2 = 0;
float accuracy2 = 0;
int year2 = 0;
int month2 = 0;
int day2 = 0;
int hour2 = 0;
int min2 = 0;
int sec2 = 0;
```

```
DBG("Obteniendo coordenadas GNSS");
```

```
for (;;) {
    digitalWrite(LED_PIN, !digitalRead(LED_PIN));
    if (modem.getGPS(&lat2, &lon2, &speed2, &alt2, &vsat2, &usat2, &accuracy2,
                    &year2, &month2, &day2, &hour2, &min2, &sec2)) {
        DBG("Latitude:", String(lat2, 8), "\tLongitude:", String(lon2, 8));
        DBG("Speed:", speed2, "\tAltitude:", alt2);
        DBG("Visible Satellites:", vsat2, "\tUsed Satellites:", usat2);
        DBG("Accuracy:", accuracy2);
        DBG("Year:", year2, "\tMonth:", month2, "\tDay:", day2);
        DBG("Hour:", hour2, "\tMinute:", min2, "\tSecond:", sec2);
```

```
/* El siguiente es un struc para "armar" el tiempo Epoch/UNIX
```

```
Se debe enviar al servidor en tiempo en formato UNIX
```

```
*/
```

```
te.Second = sec2;
te.Hour = hour2;
te.Minute = min2;
te.Day = day2;
te.Month = month2;
te.Year = year2 - 1970;
fixTime = makeTime(te);
```

```
break;
```

```
} else {
    light_sleep(2);
}
```

```
}
```

```
// Inicia conexión TCP
```

```
#if TINY_GSM_TEST_TCP && defined TINY_GSM_MODEM_HAS_TCP
/*
```

A continuación se declaran las variables globales necesarias y se indican, la dirección del servidor y el puerto, además de los parámetros necesarios para efectuar la llamada HTTP

Para referencia se recuerda el ejemplo utilizado en la sección anterior

```
http://demo4.traccar.org:5055/?
```

```
id=8816634703011978&lat=9.983818167881154&lon=-84.10872908221025&timestamp=1671854398&hdop=9&altitude=1500&speed=15
```

```
*/
    const char server[] = "demo4.traccar.org";
    const char resource[] = "/?
id=8816634703011978&lat="&lat2&"&lon="&lon2&"&timestamp="&fixTime&"&hdop="&accuracy2&"&altitude="&alt2&"&speed="&speed2;
    const int port = 5055;
    TinyGsmClient client(modem, 0);
    DBG("Conectando a ", server);
    if (!client.connect(server, port)) {
        DBG("... error");
    } else {
        // Hace la llamada HTTP
        client.print(String("GET ") + resource + " HTTP/1.0\r\n");
        client.print(String("Host: ") + server + "\r\n");
        client.print("Conexión: terminada\r\n\r\n");

        // Espera confirmación de entrega
        uint32_t start = millis();
        while (client.connected() && !client.available() &&
            millis() - start < 30000L) {
            delay(100);
        };
        client.stop();
    }
#endif
#endif
```

```
// Desconexión de datos
```

```
#if TINY_GSM_TEST_GPRS
```

```
modem.gprsDisconnect();
```

```
light_sleep(5);
```

```
if (!modem.isGprsConnected()) {
```

```
    DBG("GPRS desconectado");
```

```
} else {
```

```
    DBG("Error de desconexión GPRS.");
```

```
}
```

```
#endif
```

```
// Apaga el MODEM
```

```
#if TINY_GSM_POWERDOWN
```

```
modem.poweroff();
```

```
DBG("Poweroff.");
```

```
#endif
```

```
SerialMon.printf("El dispositivo despertará dentro de: ", TIME_TO_SLEEP);
```

```
//Wait moden power off
```

```
light_sleep(5);
```

```
esp_sleep_enable_timer_wakeup(TIME_TO_SLEEP * uS_TO_S_FACTOR);  
// TIME_TO_SLEEP * uS_TO_S_FACTOR se definen en utilities.h
```

```
delay(200);  
esp_deep_sleep_start();
```

```
while (1);  
}
```

```
#define uS_TO_S_FACTOR    1000000ULL /* Conversion factor for micro seconds to seconds */
#define TIME_TO_SLEEP    30    /* Time ESP32 will go to sleep (in seconds) */

#define UART_BAUD        115200

#define MODEM_TX         27
#define MODEM_RX         26
#define MODEM_PWRKEY     4
#define MODEM_DTR        32
#define MODEM_RI         33
#define MODEM_FLIGHT     25
#define MODEM_STATUS     34

#define SD_MISO          2
#define SD_MOSI          15
#define SD_SCLK          14
#define SD_CS            13

#define LED_PIN          12
```