Decanato de Ingeniería e Informática
Escuela de Informática

Trabajo de Grado para optar por el título de:
Ingeniería de Sistemas de Computación

Tema:

Análisis y diseño de un sistema web y móvil para el control de disponibilidad de estacionamientos apoyado en el internet de las cosas, en los centros comerciales de la ciudad de Santo Domingo durante el periodo mayo-agosto 2018 (caso de estudio Ágora Mall).

Sustentantes:

Br. Randol Mariano Frías Taveras	**2014-2499**
Br. Smiley Rafael Mariñez Mota	**2014-2052**
Br. Brayler Sánchez Peguero	**2014-2571**

Asesor:
Freddy Jiménez

Santo Domingo, Distrito Nacional
República Dominicana
Julio, 2018

Análisis y diseño de un sistema web y móvil para el control de disponibilidad de estacionamientos apoyado en el internet de las cosas, en los centros comerciales de la ciudad de santo domingo durante el periodo mayo-agosto 2018 (caso de estudio ágora mall).

ÍNDICE

ÍNDICE DE GRÁFICAS

ÍNDICE DE TABLAS

DEDICATORIAS

Gracias al esfuerzo y a la dedicación que tuve a la hora de cursar esta carrera y de realizar este trabajo, puedo dedicar el mismo a toda mi familia, a todos mis amigos y a todos aquellos profesores de UNAPEC que ayudaron a enriquecer y pulir mi conocimiento.

En primer lugar, le hago una dedicación especial a mi madre, Miriam Peguero, quien desde pequeño me inculcó la importancia del saber y de las adversidades que iba enfrentar durante el transcurso de mi vida.

A mi padre, Youel Sánchez, quien siempre me ha dado su apoyo incondicional y quien desde pequeño me fue mostrando de qué consiste la informática y de cómo la misma revolucionaria el mundo. Gracias por siempre estar para mi.

A mi hermana, Yoleymi Sánchez, por ofrecerme su cariño y apoyo. Comparto este éxito contigo, por siempre estar dispuesta a ayudarme.

A mis compañeros de carrera de UNAPEC, quienes aportaron su granito de arena para poder llegar hasta aquí y presentar este trabajo de grado.

Brayler Sánchez Peguero

Este trabajo de grado el cual es un resumen de todo un conjunto de conocimientos, esfuerzo, dedicación y el producto de una etapa de mi vida que finalizo con gran satisfacción.

Por tal motivo lo dedico a mi madre, Altagracia Taveras. Mi mayor ejemplo para seguir, responsable de formar quien soy, palabras me faltarían para decirte y reconocerte todo lo que haz hecho por mi. Amor, dedicación, entrega y perseverancia para llevarme a donde estoy hoy.

Mi hermana, Julissa Castillo. A pesar de la distancia siempre he podido contar contigo, tu apoyo no me ha faltado en ningún momento, tu cariño siempre no importando que y ayuda incondicional.

Kyoko Murata, mi amada esposa. Porque siempre has creído en mi, sacando a flote esas cualidades que están escondida. Tu apoyo ha sido siempre, a pesar de las circunstancias la ayuda que me das me impulsa a seguir adelante en cada uno de mis planes y metas.

Randol M. Frías

En primer lugar, dedico este logro a Dios, ya que gracias a Él he logrado concluir mis estudios universitarios.

A mi madre Isabel Mota por ser mi motor y mi razón para seguir adelante.

A mi padre Paulino Mariñez por sus palabras de aliento y por todo el apoyo que me brindó en el transcurso de mi vida universitaria. Por enseñarme con su ejemplo el valor del sacrificio y el trabajo arduo.

A mi hermana Annette Mariñez por ser un ejemplo a seguir y porque a pesar de la distancia siempre me transmite su amor, confianza y aprecio.

Por último, quiero dedicar este logro a todas las personas que al igual que yo se vieron en la necesidad de estudiar y trabajar al mismo tiempo para poder salir adelante. Este trabajo de grado es una muestra fehaciente de que es posible lograr todo lo que uno se propone si se tiene constancia, dedicación, esfuerzo, sacrificio y sobre todo el favor de Dios.

Smiley Mariñez

AGRADECIMIENTOS

A Ágora Mall por facilitarnos las informaciones, gráficas y fotografías para la elaboración de esta investigación.

A todas las empresas e instituciones que nos brindaron los datos necesarios para el desarrollo de los temas presentados en este trabajo de grado.

A mi familia, la cual me inculcó los valores necesarios para prepararme para la vida, gracias por su paciencia y apoyo incondicional. Ustedes son los responsables de mis logros y sin su apoyo nada de esto hubiera sido posible.

A mis amigos, por apoyarme en las buenas y en las malas, por estar ahí siempre y cuando los he necesitado. Ustedes también son una parte fundamental de este éxito.

A mis compañeros de carrera, quienes junto a ellos viví buenas experiencias en la universidad, muchas gracias por su amistad.

A UNAPEC y sus profesores, quienes me sirvieron desde el inicio como guías para obtener el conocimiento necesario, y a prepararme para la vida y el campo laboral. Gracias por enseñarme tanto en lo moral como en lo laboral.

Les deseo a cada uno de ustedes, todo mi agradecimiento.

Brayler Sánchez Peguero

A Dios en primer lugar, porque este ha sido su voluntad y su tiempo para finalizar esta etapa. Por ponerme en mi la sabiduría para poder vencer cada uno de los obstáculos, que se han presentado en este camino.

A mi familia, especialmente a las tres mujeres mas importante que tengo en la vida. Mi madre, Altagracia Taveras, como maestra sembraste en mi el amor por los estudios, tu dedicación, amor y entrega son el mejor regalo que he podido recibir, definitivamente sin esto no seria hoy una realidad. Mi hermana, Julissa Castillo, agradecido inmensamente por tu dedicación hacia mi, no como una hermana mas bien como una segunda madre. Mi esposa, Kyoko Murata, has tomado esta carrera como si fuera tuya, me has apoyado, me has ayudado. Has sido un motor que me impulsa a seguir para darme cuenta de todo lo que puedo dar. A mi padre, porque a pesar de las circunstancias, a pesar de las situaciones, se que puedo contar contigo.

A mis amigos y compañeros, ustedes hacen que este camino se haga mas corto, y fácil de llevar, por su apoyo y amistad que supieron darme durante este trayecto les estaré siempre agradecidos.

A UNAPEC y a sus profesores, en especial a nuestro asesor Freddy Jiménez por servirnos como fuente e instrumento de enseñanza y conocimientos durante gran parte de este desafío.

Randol M. Frías

A Dios por haberme dado salud y fuerzas para llegar hasta este punto.

A mis padres por siempre apoyarme y estar para mí cuando los necesitaba. Por darme motivos para seguir hacia adelante, por los consejos, las felicitaciones y los regaños. Por existir y por darme la vida.

A mi familia por ser un pilar fundamental en mi formación. Por enseñarme a darle más valor a una persona con un corazón noble, bondadoso, cálido y sincero que a una persona de éxito.

A mi tía Daysi Alexandra Mota por su apoyo constante en mi formación profesional.

Al Ministerio de Educación Superior, Ciencia y Tecnología (MESCyT) por hacerme recipiente de media beca para mis estudios de grado.

A mis amigos, compañeros de universidad, colegas y a la Universidad APEC y sus docentes, especialmente a aquellos que con pasión y entrega ponen sus conocimientos a disposición de los estudiantes y que con su vocación inspiran a la siguiente generación de profesionales a ser mejores cada día, a producir entregables de calidad y de alto nivel y a trabajar con pasión y empeño en pro de los objetivos propios y comunes.

Smiley Mariñez

RESUMEN EJECUTIVO

Entre los problemas que se presenta actualmente en la población de Santo Domingo debido al crecimiento del número vehicular en los últimos años podemos mencionar la dificultad para obtener un espacio para estacionarse en la ciudad, sumando al aumento de la población y pocos lugares diseñados para esto. Llevando al taponamiento de las vías y permanecer por un tiempo prolongado a la espera que se desocupo un estacionamiento.

La presente investigación propone un sistema web y móvil para la gestión de parqueos en los centros comerciales, tomando como referencia el caso Ágora Mall. Esto resulta útil especialmente en la época en la que vivimos en la que el índice de adquisición de vehículos aumenta con cada año que pasa; sin embargo, la cantidad de parqueos disponibles permanece invariante. Alrededor del 30% del mercado automotriz de la República Dominicana se concentra en el Distrito Nacional, por lo que es preciso implementar medidas que ayuden a mejorar el manejo de parqueos en Santo Domingo.

Ágora Mall dispone de 1,800 parqueos (1,400 propios y 400 de la Dirección General de Aduanas disponibles en horario no laborables de la entidad oficial) distribuidos en sus 8 niveles, de los cuales 6 son en una torre y 2 son soterrados. Este centro comercial cuenta con más de 180 establecimientos comerciales que atraen a un promedio de 30 mil visitas diarias. Alojar esta enorme cantidad de personas al día resulta un reto para cualquier institución.

Con el sistema propuesto en esta investigación se dotará de información de valor tanto al centro comercial como al visitante, de manera que ambos puedan tomar las mejores decisiones en lo que respecta a los parqueos de Ágora Mall, ya que entre las facilidades que ofrece el sistema se encuentra poder realizar estudios o análisis de reportes basados en los datos generados, tanto por la entrada y salida de vehículos lo que significa que se logrará medir de manera eficiente en el caso de entidades comerciales como plazas o tiendas, cuáles son los horarios o días en los que reciben mayor o menor cantidad de visitas. Del lado del conductor o usuario, este le permitirá ver la disponibilidad de parqueos, tanto cantidad como ubicación de los mismos.

Entre los beneficios principales del sistema se encuentran:

- Rápida ubicación de parqueos disponibles, lo que se traduce en menor tráfico de vehículos dentro de la plaza y por tanto menores embotellamientos;
- Mejor experiencia de usuario a nivel general al no ser necesario invertir tiempo adicional localizando plazas de parqueos;
- Reducción del dióxido de carbono (CO_2) emitidos por los vehículos dentro de la plaza, lo que representa un impacto positivo en el medio ambiente.

INTRODUCCIÓN

En los últimos años el aumento vehicular ha provocado un sin número de embotellamientos y dificultades a la hora de estacionarse en lugares públicos o privados, como son los centros comerciales. Cada una de estas dificultades han causado que las personas se vean obligadas a invertir tiempo valioso en la búsqueda de estacionamientos debido a la falta de un sistema de monitoreo que contabilice los mismos.

Dicha contabilización puede ser lograda mediante el uso de tecnologías que detectan la entrada y/o salida de vehículos de cualquiera de estos lugares, cómo son los radares y las redes inalámbricas. Las redes inalámbricas se han vuelto muy populares debido a la facilidad de uso y de movilidad que tienen las personas cuando la utilizan, mientras que los radares no son más que aquellos sistemas que utilizan ondas electromagnéticas con el fin de realizar mediciones de distancia, dirección, altitud y velocidad de objetos que se encuentran de forma estática o en movilización.

La utilización de las dos tecnologías mencionadas anteriormente y de otras más, no menos importantes, han llevado a esta investigación a enfocarse en el diseño de un sistema de control de parqueos en los centros comerciales de Santo Domingo, que hará posible solventar las dificultades y/o problemáticas que tienen los ciudadanos al estacionarse en centros comerciales.

Dicho sistema tendrá como propósito principal llevar a cabo la contabilización de los parqueos de manera automática, con el fin de realizar una mejor gestión y de notificar a los dueños de vehículos la disponibilidad de los parqueos, dando como resultado una mayor facilidad para la obtención de los mismos y menos pérdida de tiempo a la hora de estacionarse.

METODOLOGÍA

El objetivo de este trabajo es analizar y diseñar una solución informática enfocado en plataformas web y móvil para la gestión de parqueos en los centros comerciales de la ciudad de Santo Domingo.

En base al grado de profundidad con que se abordará este tema se estará implementado y/o realizando un tipo de estudio o investigación descriptiva. Además, se trabajará aplicando el Método de Análisis, utilizando la Encuesta como técnica para la recolección de la información, con un enfoque cualitativo para la investigación.

Se estará implementado o utilizando tres tipos de estudios: Descriptivo, de este modo se dará a conocer la información que actualmente existe sobre el tema de los parqueos, identificar las debilidades de los actuales procesos y desarrollar las acciones necesarias que mejorarían el problema, utilizando distintas fuentes para recolectar las informaciones necesarias para poder detallar de forma precisa los componentes del diseño a desarrollar.

Exploratorio, de manera que se pueda tener una visión general de tipo aproximativo sobre la realidad de los parqueos de Ágora Mall, se puedan identificar tendencias de horarios de embotellamientos y relaciones potenciales entre las variables involucradas en la causa de la congestión.

Documental, para recopilar adecuadamente datos e información sobre la problemática por analizar mediante el uso de documentos impresos, electrónicos

o gráficos, compararlos y llegar a una conclusión que respalde o no la hipótesis planteada.

El método de investigación será el de Análisis, mediante este método o proceso se identificarán cada una de las partes que conforman el tema presentado y sus respectivas características. Para de esa forma establecer una relación de causa y efecto entre los elementos que componen dicho caso.

CAPÍTULO I.

ANTECEDENTES DE ÁGORA MALL

1.1 Introducción

Cuando hablamos de verde nos llega a la mente imágenes de árboles, bosques y naturaleza. Cosas hermosas que crean un ambiente limpio y delicado, suave y natural. Poder relajarse uno al caminar, observar un hermoso ambiente mientras compramos, compartimos con la familia o almorzamos en alguna reunión de trabajo. Esa es la idea principal de lo que es Ágora Mall: el primer centro comercial verde de la República Dominicana. Una propuesta exquisita para pasar un buen momento en un ambiente relajado y de confort en donde las personas pueden encontrar en un solo lugar los establecimientos idóneos para satisfacer sus necesidades comerciales.

1.2 Historia

Ágora Mall es un centro comercial que fue inaugurado el 23 de agosto del 2012. Mide 120,000 metros y tiene tres entradas y tres salidas diseñadas para que sus clientes disfruten de un acceso cómodo, rápido y seguro:

Entradas:

- Av. Abraham Lincoln
- Calle Filomena Gómez de Cova
- Av. John F. Kennedy

Ágora Mall dispone de un total de 1,800 estacionamientos con accesos directos a cada uno de sus niveles. Los visitantes acceden a más de 180 establecimientos comerciales a través de 10 ascensores y 20 escaleras eléctricas.

En este centro comercial el público dominicano puede encontrar todo lo que busca en un mismo lugar con más de 120 mil metros cuadrados de construcción y que aloja 180 locales comerciales con la oferta de productos y servicios más completa del país.

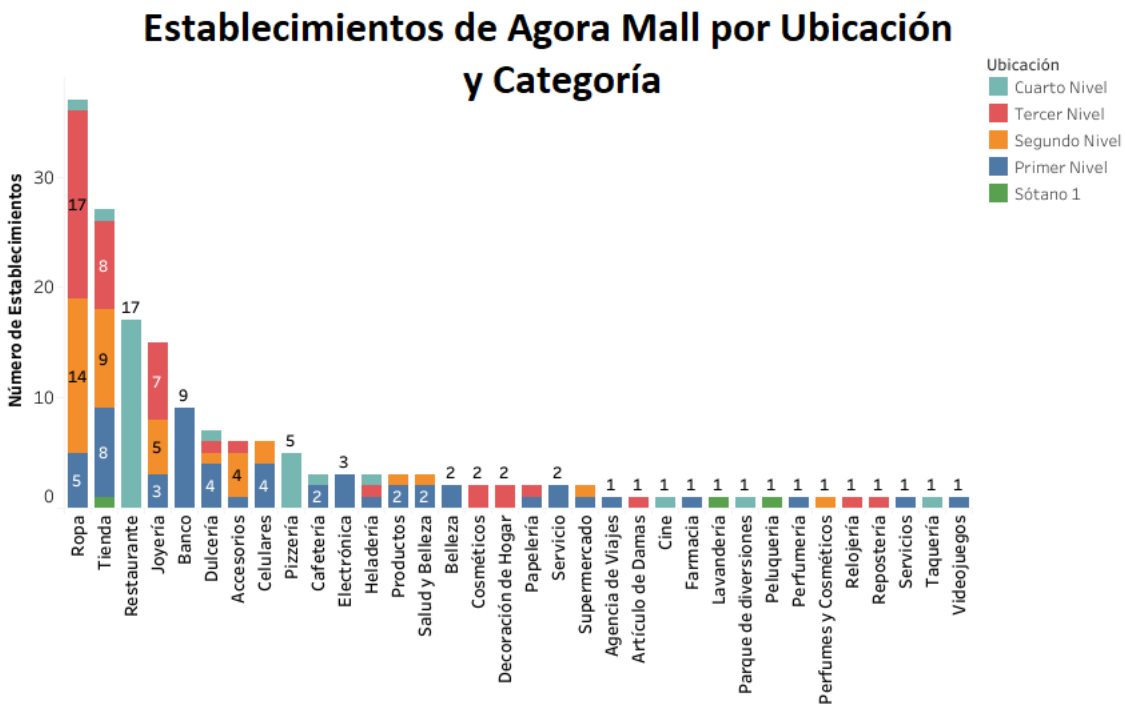

Figura 1.1 Categorización por Piso de los Establecimientos de Ágora Mall **Fuente**: Autores

Ágora Mall se construyó con una inversión de US$120, el centro comercial tiene mayor incidencia en un área de tres millas donde se concentran alrededor de medio millón de habitantes.

El centro comercial Ágora Mall Santo Domingo está ubicado en la intersección de las avenidas Abraham Lincoln con John F. Kennedy. Es además el primer edificio verde de la República Dominicana y cuenta con una moderna infraestructura de cuatro niveles con una torre de parqueos con capacidad para más de 1,400 vehículos.

La mejor mezcla de ofertas de establecimientos comerciales es Ágora Mall. Desde una de las grandes tiendas por departamento del país incluyendo establecimientos con ofertas especializadas como artículos para el hogar, artículos deportivos, servicios bancarios, telecomunicaciones, sala de bellezas, tiendas de moda nacional e internacional, joyería, calzado, farmacia, restaurantes y centros de diversión.

Dada a su privilegiada ubicación a este centro comercial se puede acceder a través del Metro de Santo Domingo, en la estación Pedro Mir de la Línea 2.

Figura 1.2 Vista Externa de Ágora Mall **Fuente**: Arquitexto.com

Ágora Mall es un centro comercial de Santo Domingo que gracias a su proceso de construcción, diseño y gestión está certificado bajo los estándares del programa LEED, desarrollado por el Consejo de la Construcción Verde de Estados Unidos. Esta certificación lo avala como una edificación verde, la primera de este tipo en el país. Su diseño simple responde a la modalidad fast-

track o pista de carrera, que consiste en poner tiendas ancla en los extremos y distribuir pequeñas tiendas entre ellas

Las características clave de esta certificación son la correcta selección del emplazamiento, el ahorro de agua, la eficiencia energética y el uso de materiales renovables, reciclados y no contaminantes.

La obra de Ágora Mall es una estructura de hormigón armado de 130,000 m2 de construcción, dividida en tres edificios separados por juntas de construcción. Consta de un edificio de estacionamiento de once niveles (tres soterrados), con muros, zapatas, columnas y vigas de hormigón armado, y losa alveolada (hollow-core); un edificio de tiendas ancla de seis niveles (dos soterrados), con entrepisos de forjado metálico (metal decking), y un edificio de tiendas medianas y pequeñas también de seis niveles (dos soterrados) con losa aligerada tipo waffle.

Planos de Ágora Mall

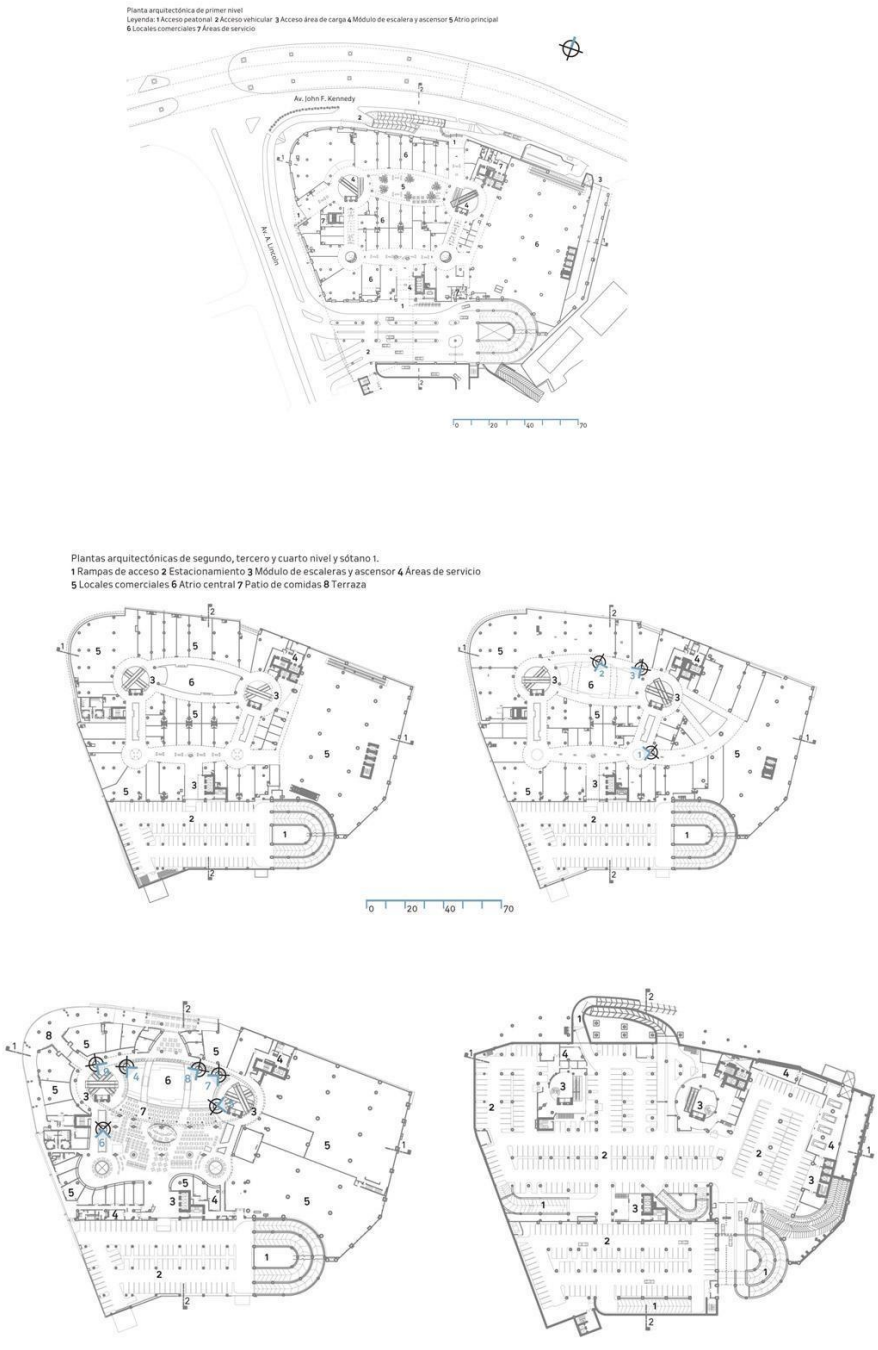

Figura 1.3 Planos Arquitectónicos de Ágora Mall **Fuente**: Arquitexto.com

El atrio central tipo lucernario (sky-light) tiene forma de elipse de 40 x 60 m; cerca de 2,400 m2 techado con sistema ETFE, soportado en vigas que alcanzan longitudes en vuelo de hasta 7 m. El EFTE es un fluoroplástico usado originalmente para la arquitectura naval que se caracteriza por su excelente resistencia eléctrica y química, baja fricción y estabilidad sobresaliente a altas temperaturas. Los materiales de construcción utilizados son reciclados en un 90%: yeso, fibra de vidrio y metal (se supone que un 35% del acero empleado es de contenido reciclado).

El edificio cuenta con una certificación del programa LEED (Leadership in Energy and Enviromental Design) del Consejo de la Construcción Verde de Estados Unidos (United States Green Building Council), lo que lo respalda como un edificio sostenible. Esta certificación como “Green Building” tiene como objetivo transformar la forma en que los edificios y las comunidades son diseñadas y operadas haciendo conciencia medio ambiental y contribuyendo a un ambiente más saludable que mejore la calidad de vida de las personas.

Este proceso implica:

- **Emplazamiento/ ubicación**, que mide el impacto que tiene la selección del lugar en el que se realiza la edificación sobre el medio ambiente local;
- **Gestión de agua**, que incluye la integración de tecnologías y estrategias para reducir la cantidad de agua potable consumida en el edificio;

- **Calidad ambiental interior**, que tiene en cuenta el uso de luz natural, criterios de confort térmico, acústico, ventilación y otros aspectos que inciden sobre la salud ambiental de un espacio;
- **Materiales**, que promueven las prácticas de reducción de deshecho de la construcción, de reciclado doméstico así como el uso de materiales reciclados o rápidamente renovables para la construcción;
- **Energía y atmósfera**, en esta parte se mide la eficiencia y comportamiento energético del edificio y que promueve la integración de energías renovables.

Estos renglones forman parte del procedimiento de operaciones con el que se gestiona esta infraestructura cuya construcción inició en noviembre de 2009, convirtiéndose en el centro comercial más completo del país, localizado en una de la zona de mayor tráfico de la ciudad. 120 mil metros cuadrados de construcción que alojan 180 establecimientos comerciales y reciben un promedio de 30 mil visitas diarias.

Visitas por Día a Ágora Mall

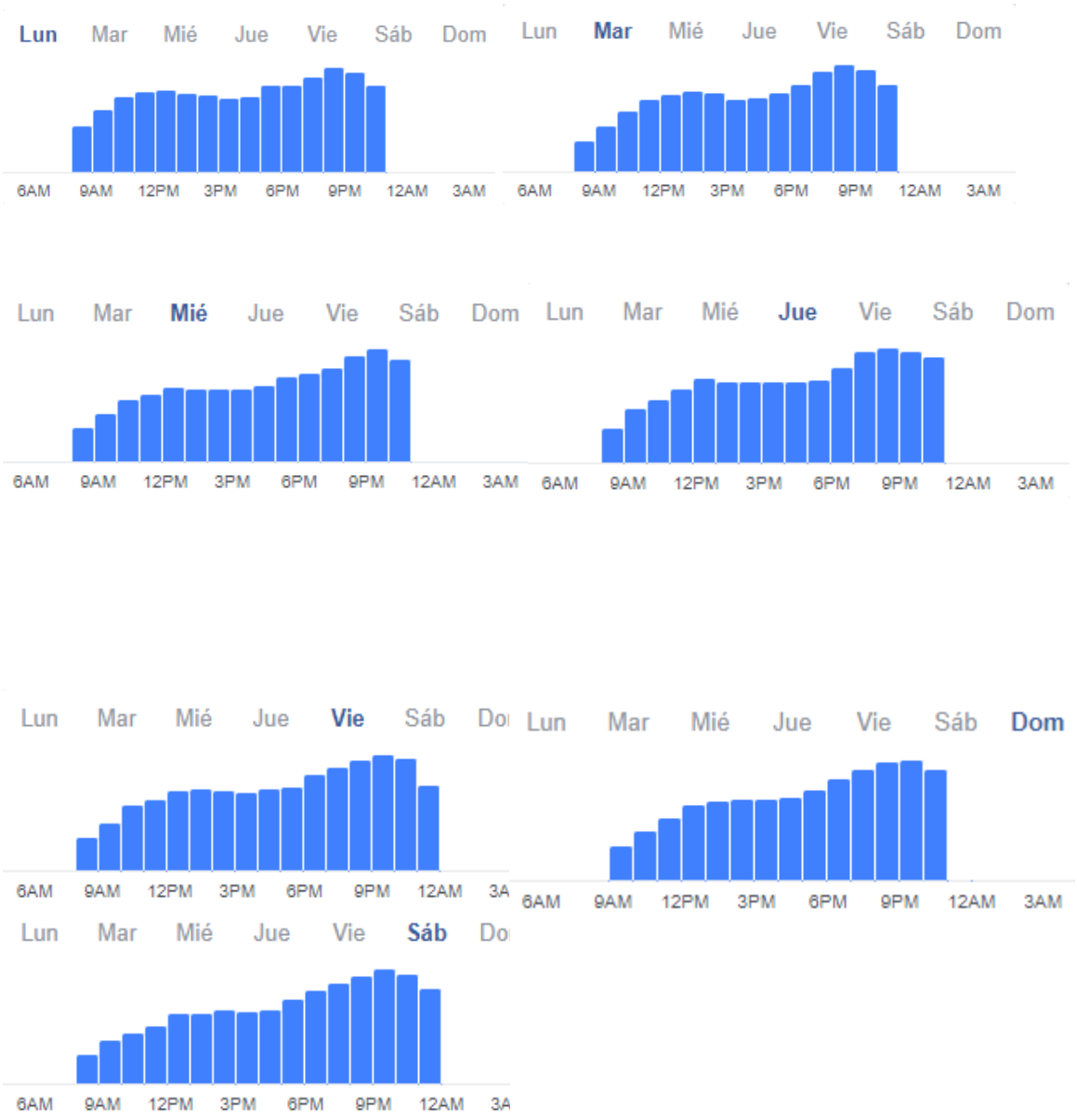

Figura 1.4 Horarios más concurridos de Ágora Mall **Fuente**: Página de Facebook de Ágora Mall

1.3 Misión

Convertirse en el nuevo corazón de Santo Domingo, con pasión y excelencia. Ser el primer edificio comercial verde.

1.4 Visión

Impresionar a sus clientes siendo el lugar favorito para comprar, divertirse y compartir, promoviendo que cada comercio sea rentable y que su gente se sienta orgullosa de pertenecer a la comunidad Ágora en un espacio donde se contribuye con la sostenibilidad del medio ambiente.

1.5 Valores

- Enfoque de Servicio al Cliente
- Excelencia
- Honestidad
- Afabilidad
- Compromiso
- Colaboración

1.6 Filosofía Institucional

La filosofía que Ágora Mall ha adoptado como institución se basa en ofrecer a sus clientes servicios variados y de calidad que satisfagan sus necesidades a la vez que se mantiene la armonía con el medio ambiente a través de la reutilización de recursos.

1.7 Objetivos

Crear una cultura de valores que promueva el desarrollo de sus integrantes desde la óptica personal y profesional, siguiendo las mejores prácticas y normas y creando un mecanismo de comunicación e interacción entre todos.

1.8 Organigrama Institucional

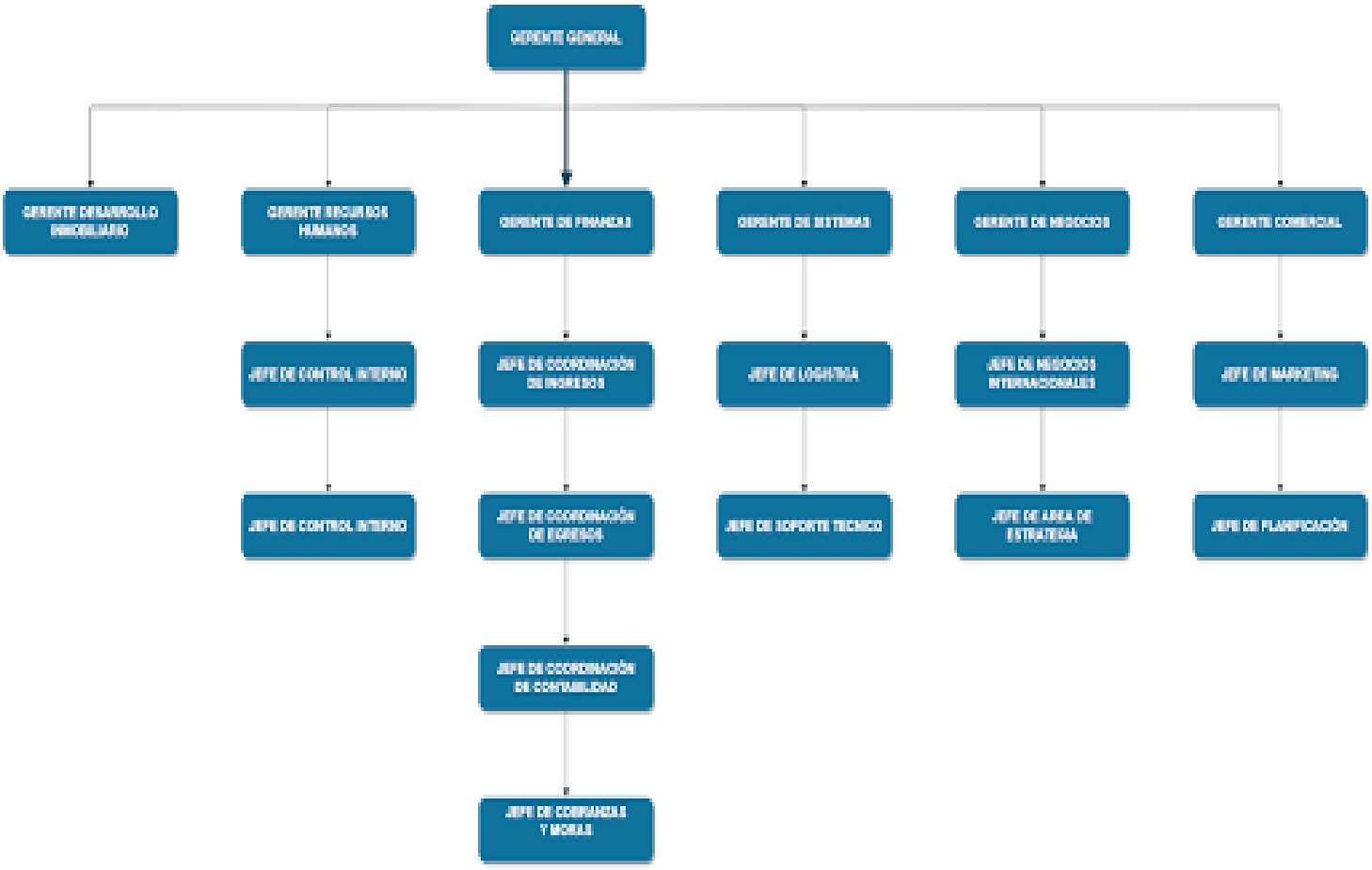

Figura 1.5 Organigrama de Ágora Mall **Fuente**: Autores

Ágora Mall es una propuesta atractiva y variada que vino a dinamizar las opciones comerciales de los consumidores dominicanos. Posee una ubicación estratégica de fácil acceso para todos los clientes independientemente de que los mismos lleguen o no en vehículo. Ágora Mall posee cuatro niveles en los que operan más de 180 establecimientos de diversas categorías.

Ágora Mall destaca especialmente por ser el primer centro comercial verde del país. Esta certificación fue lograda a través del aprovechamiento y especialización de los recursos utilizados en la construcción del centro comercial. Esta certificación de edificio sostenible fue otorgada por el programa LEED (Leadership in Energy and Enviromental Design).

CAPÍTULO II.

INTERNET DE LAS COSAS (IoT)

2.1 Introducción

El Internet de las cosas es un término que ha ido evolucionando durante el pasar de los años y se ha ido incorporando en la sociedad. Esta tecnología viene con el fin de proporcionar un sin número de posibilidades y mejoras a la vida diaria del ser humano, la misma busca hacer que las cosas sean realizadas de una manera más rápida conectando todo hacia internet, de modo que todos los dispositivos sean uno mismo.

Muchas compañías han empezado a explotar el Internet de las cosas de una manera significativa, ya que es una de las cosas que se quieren plantear en el futuro próximo. Algunas de estas compañías son: Amazon con Alexa, Apple con Siri, Microsoft con Cortana y un sin número de compañías que buscan extender esta tecnología por todo el mundo.

Gracias al Internet de las cosas en un futuro las personas serán capaces de utilizar dispositivos completamente conectados a Internet que mejoren nuestra calidad de vida y que cosas rutinarias como realizar la lista de compras, subir o bajar la temperatura del aire, según el tiempo en el momento, apagar las luces de las habitaciones, entre otras cosas, sean aún más fáciles, debido a que estos dispositivos serán capaces de realizar cada una de estas cosas con una mayor exactitud.

2.2 Historia

A partir de 2016, la visión de Internet de las cosas ha evolucionado debido a la convergencia de múltiples tecnologías, incluida la comunicación inalámbrica ubicua, análisis en tiempo real, aprendizaje automático, sensores de productos básicos y sistemas integrados. Esto significa que los campos tradicionales de los sistemas integrados, las redes de sensores inalámbricos, los sistemas de control, la automatización (incluida la automatización del hogar y la construcción) y otros contribuyen a habilitar el Internet de las cosas.

El concepto de una red de dispositivos inteligentes se discutió ya en 1982, con una máquina de Coke modificada en la Universidad Carnegie Mellon convirtiéndose en el primer electrodoméstico conectado a Internet, capaz de informar su inventario y si las bebidas recién cargadas estaban frías. El influyente trabajo de Mark Weiser de 1991 sobre computación ubicua, "La computadora del siglo XXI", así como lugares académicos como UbiComp y PerCom produjeron la visión contemporánea de IoT. En 1994 Reza Raji describió el concepto en IEEE Spectrum como "[moviendo] pequeños paquetes de datos a un gran conjunto de nodos, para integrar y automatizar todo, desde electrodomésticos hasta fábricas enteras". Entre 1993 y 1996, varias compañías propusieron soluciones como Microsoft's at Work o Novell's NEST. Sin embargo, sólo en 1999 el campo comenzó a cobrar impulso. Bill Joy visualizó la

comunicación Dispositivo a Dispositivo (D2D) como parte de su marco de "Seis Webs", presentado en el Foro Económico Mundial en Davos en 1999.

Figura 2.1 - Logotipo de IEEE Spectrum. **Fuente**: thearcticinstitute.org

El concepto de Internet de las cosas se hizo popular en 1989 a través del Auto-ID Center en MIT y publicaciones relacionadas de análisis de mercado. Kevin Ashton (uno de los fundadores del Auto-ID Center original) vio la identificación de radiofrecuencia (RFID) como un requisito previo para el Internet de las cosas en ese punto. Ashton prefiere la frase "Internet para cosas". Si todos los objetos y personas de la vida diaria estuvieran equipados con identificadores, las computadoras podrían administrarlos y almacenarlos. Además del uso de RFID, el etiquetado de las cosas se puede lograr a través de tecnologías tales como comunicación de campo cercana, códigos de barras, códigos QR y marcas de agua digitales.

Una transformación significativa es extender "cosas" desde los datos generados desde los dispositivos a los objetos en el espacio físico. El modelo de pensamiento para el futuro entorno de interconexión se propuso en 2004. El modelo incluye la noción de que el universo ternario consiste en el mundo físico, el mundo virtual y el mundo mental y una arquitectura de referencia de niveles múltiples con la naturaleza y dispositivos en el nivel inferior por el nivel de Internet, redes de sensores y redes móviles, y comunidades inteligentes de personas y máquinas en el nivel superior, que permite a los usuarios geográficamente dispersos realizar tareas de forma cooperativa y resolver problemas utilizando la red para promover activamente el flujo de material, energía , técnicas, información, conocimiento y servicios en este entorno. Este modelo de pensamiento visualizó la tendencia de desarrollo de Internet de las cosas.

2.3 Definición

Es un término ambiguo, pero se está volviendo rápidamente una tecnología tangible que puede ser aplicada en los centros de datos para recolectar información sobre casi cualquier cosa que las TI quieran controlar.

La internet de las cosas (IoT) es esencialmente un sistema de máquinas u objetos equipados con tecnologías de recopilación de datos, de manera que esos objetos pueden comunicarse entre sí. Los datos de máquina a máquina (M2M) que se generan tienen una amplia gama de usos, pero comúnmente se

ven como una forma de determinar la salud y el estado de las cosas, inanimadas o con vida.

El internet de las cosas no es más que la utilización del internet en cualquier dispositivo o cosa donde se haga posible realizar una conexión de modo que los datos sean compartidos y procesados.

2.4 Características

Hay 7 características cruciales en el Internet de las cosas:

1. **Conectividad.** Esto no necesita mucha explicación adicional. Dispositivos, sensores, necesitan estar conectados: a un elemento, a los demás, a los actuadores, a un proceso ya "Internet" u otra red.
2. **Cosas.** Cualquier cosa que pueda ser etiquetada o conectada como tal, ya que está diseñada para ser conectada. Desde sensores y electrodomésticos hasta ganado marcado. Los dispositivos pueden contener sensores o materiales de detección que se pueden conectar a dispositivos y artículos.
3. **Datos.** Los datos son el pegamento del Internet de las cosas, el primer paso hacia la acción y la inteligencia.
4. **Comunicación.** Los dispositivos se conectan para que puedan comunicar datos y estos datos pueden analizarse.

5. **Inteligencia.** El aspecto de la inteligencia como en las capacidades de detección en dispositivos de IoT y la inteligencia recopilada a partir del análisis de datos (también inteligencia artificial).
6. **Acción.** La consecuencia de la inteligencia. Esto puede ser una acción manual, una acción basada en debates sobre fenómenos (por ejemplo, en decisiones sobre cambio climático) y automatización, a menudo la pieza más importante.
7. **Ecosistema.** El lugar del Internet de las cosas desde una perspectiva de otras tecnologías, comunidades, objetivos y la imagen en la que encaja Internet de las cosas. La dimensión Internet de Todo, la dimensión de la plataforma y la necesidad de alianzas sólidas.

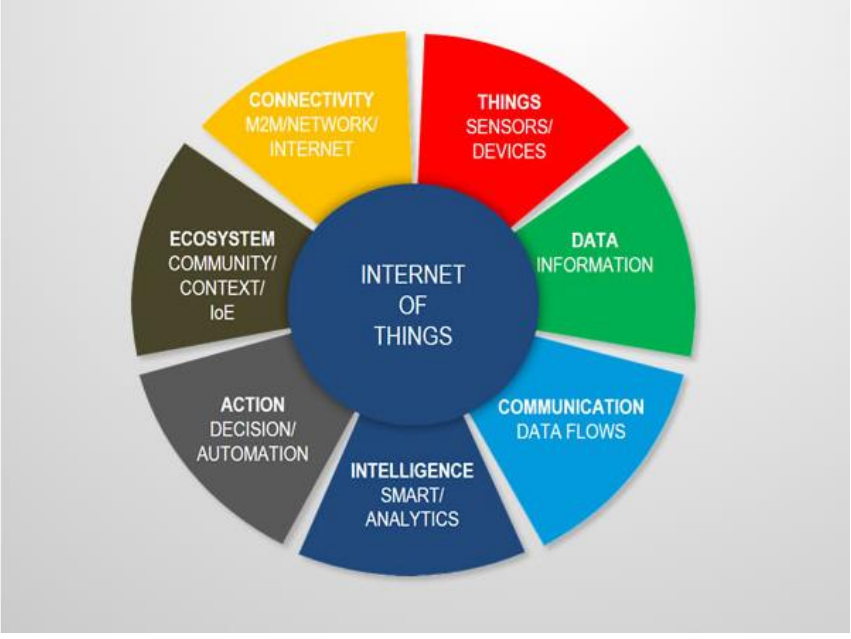

Figura 2.2 - Las 7 características del IoT. **Fuente**: i-scoop.eu

2.5 Ventajas

Comunicación

IoT fomenta la comunicación entre dispositivos, también conocida como comunicación de máquina a máquina (M2M). Debido a esto, los dispositivos físicos pueden permanecer conectados y, por lo tanto, la transparencia total está disponible con menores ineficiencias y mayor calidad.

Figura 2.3 - Punto máquina a máquina. **Fuente**: coherentchronicle.com

Automatización y control

Debido a que los objetos físicos se conectan y controlan digital y centralmente con la infraestructura inalámbrica, existe una gran cantidad de automatización y control en el funcionamiento. Sin la intervención humana, las máquinas son

capaces de comunicarse entre sí, lo que permite un resultado más rápido y oportuno.

Información

es obvio que tener más información ayuda a tomar mejores decisiones. Ya se trate de decisiones mundanas como la necesidad de saber qué comprar en la tienda de comestibles o si su empresa tiene suficientes widgets y suministros, el conocimiento es poder y más conocimiento es mejor.

Monitor

La segunda ventaja más obvia de IoT es el monitoreo. Conocer la cantidad exacta de suministros o la calidad del aire en su hogar, puede proporcionar más información que no se pudo recolectar fácilmente con anterioridad. Por ejemplo, saber que tiene poca leche o tinta de impresora podría ahorrarle otro viaje a la tienda en el futuro cercano. Además, monitorear la caducidad de los productos puede mejorar la seguridad y lo hará.

Tiempo

La cantidad del tiempo ahorrado debido a IoT podría ser bastante grande. Y en la vida moderna de hoy, todos podríamos usar más tiempo.

Dinero

La mayor ventaja de IoT es ahorrar dinero. Si el precio del equipo de etiquetado y monitoreo es menor que la cantidad de dinero ahorrado, entonces el Internet de las cosas será ampliamente adoptado. IoT fundamentalmente demuestra ser muy útil para las personas en sus rutinas diarias al hacer que los dispositivos se comuniquen entre sí de manera efectiva, ahorrando y conservando energía y costos. Permitir que los datos se comuniquen y compartan entre los dispositivos y luego se traduzcan de la manera requerida, hace que nuestros sistemas sean eficientes.

La automatización de las tareas diarias conduce a un mejor control de los dispositivos

El IoT le permite automatizar y controlar las tareas que se realizan a diario, evitando la intervención humana. La comunicación máquina a máquina ayuda a mantener la transparencia en los procesos. También conduce a la uniformidad en las tareas. También puede mantener la calidad del servicio. También podemos tomar medidas necesarias en caso de emergencias.

Eficiente y ahorra tiempo

La interacción máquina a máquina proporciona una mejor eficiencia, por lo tanto; resultados precisos pueden obtenerse rápidamente. Esto se traduce en un

ahorro de tiempo valioso. En lugar de repetir las mismas tareas todos los días, permite a las personas hacer otros trabajos creativos.

Ahorra dinero

Se puede lograr una utilización óptima de la energía y los recursos adoptando esta tecnología y manteniendo los dispositivos bajo vigilancia. Podemos alertarnos en caso de posibles cuellos de botella, averías y daños en el sistema. Por lo tanto, podemos ahorrar dinero utilizando esta tecnología.

Mejor calidad de vida

Todas las aplicaciones de esta tecnología culminan en una mayor comodidad, conveniencia y una mejor gestión, mejorando así la calidad de vida.

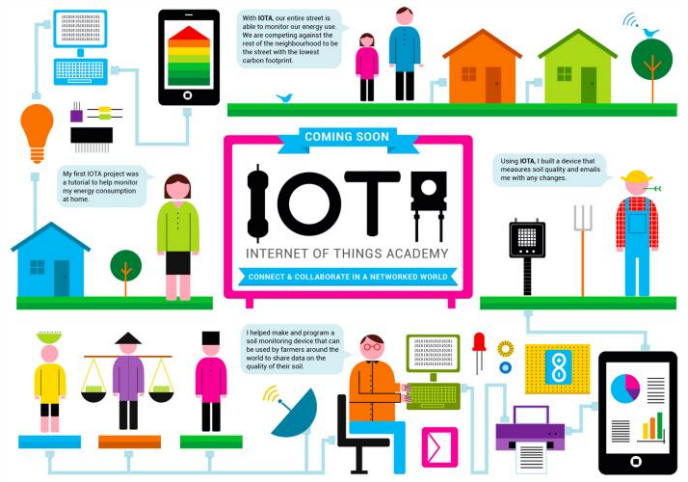

Figura 2.4 - Ahorro Del tiempo y calidad de vida. **Fuente**: soloelectronicos.com

2.6 Desventajas

Compatibilidad

Actualmente, no existe un estándar internacional de compatibilidad para los equipos de etiquetado y monitoreo. Creo que esta desventaja es la más fácil de superar. Las empresas de fabricación de estos equipos solo necesitan aceptar un estándar, como Bluetooth, USB, etc. Esto no es nada nuevo o innovador.

Complejidad

Como con todos los sistemas complejos, hay más oportunidades de falla. Con Internet of Things, las fallas podrían dispararse. Por ejemplo, supongamos que tanto usted como su cónyuge reciben un mensaje que indica que su leche ha expirado y ambos se detienen en una tienda de camino a casa, y ambos compran leche. Como resultado, usted y su cónyuge han comprado el doble de la suma que ambos necesitan. O tal vez un error en el software termina ordenando automáticamente un nuevo cartucho de tinta para su impresora cada hora por unos días, o al menos después de cada falla de energía, cuando solo necesita un reemplazo único.

Privacidad

Con todos estos datos de IoT que se transmiten, aumenta el riesgo de perder privacidad. Por ejemplo, ¿cuán bien encriptada se guardarán y transmitirán los

datos? ¿Desea que sus vecinos o empleadores sepan qué medicamentos está tomando o su situación financiera?

Seguridad

imagínese si un pirata informático notorio cambia su receta. O si una tienda le envía automáticamente un producto equivalente al que es alérgico, o un sabor que no le gusta, o un producto que ya ha expirado. Como resultado, la seguridad está en última instancia en manos del consumidor para verificar cualquier automatización.

Como todos los electrodomésticos, maquinaria industrial, servicios del sector público como el suministro de agua y el transporte, y muchos otros dispositivos, todos están conectados a Internet, hay mucha información disponible en él. Esta información es propensa a ser atacada por hackers. Sería muy desastroso si intrusos no autorizados acceden a información privada y confidencial.

Figura 2.5 - Brechas de seguridad en IOT. **Fuente**: oasys-sw.com

Desempleo

Los trabajadores no calificados y los ayudantes pueden terminar perdiendo sus trabajos en el efecto de la automatización de las actividades diarias. Esto puede conducir a problemas de desempleo en la sociedad. Este es un problema con el advenimiento de cualquier tecnología y se puede superar con la educación. Con las actividades diarias automatizadas, naturalmente, habrá menos requisitos de recursos humanos, principalmente trabajadores y personal con menos educación. Esto puede crear un problema de desempleo en la sociedad.

La tecnología toma el control de la vida

Nuestras vidas estarán cada vez más controladas por la tecnología y dependerán de ella. La generación más joven ya es adicta a la tecnología para todo. Tenemos que decidir cuánto de nuestra vida cotidiana estamos dispuestos a mecanizar y controlar mediante la tecnología.

2.7 Aplicaciones

2.7.1 Consumidor

Más o menos hace 5 años, los consumidores rara vez vieron lo que el Internet de las cosas significaría para sus vidas privadas. Hoy en día, lo hacen cada vez más: no solo porque están interesados en la tecnología, sino principalmente porque una gama de nuevas aplicaciones y dispositivos conectados ha llegado al mercado.

Estos dispositivos y sus posibilidades están recibiendo mayor atención en prácticamente todos los sitios de noticias y sitios web que cubren la tecnología. Wearables y relojes inteligentes, aplicaciones domésticas conectadas e inteligentes (con Google's Nest siendo popular, pero ciertamente no el primero): hay muchos ejemplos conocidos..

Figura 2.6 - Termostato 3ra generación. **Fuente**: i-scoop.eu

Aunque se dice que aparece algo de fatiga tecnológica, la combinación de aplicaciones en un contexto de consumo y de fascinación por la tecnología, sin duda, juega un papel en la creciente atención para Internet de las cosas. Ese aspecto de fascinación del consumidor se suma a todas las posibilidades de la vida real a medida que comienzan a implementarse y las realidades contextuales y tecnológicas, haciendo que el Internet de las Cosas sea uno de esos muchos términos tecnológicos generalizados. Obviamente, el mercado de Internet de las cosas para el consumidor no solo está impulsado por la

fascinación por las nuevas tecnologías: sus fabricantes presionan mucho al mercado, ya que la adopción significa nuevas posibilidades comerciales con un papel clave para los datos.

El consumidor de Internet de las cosas y la electrónica de consumo

Con el Internet de las cosas para el consumidor, estamos estrictamente en una realidad de electrónica de consumo.

El 47% de los consumidores están preocupados por cuestiones de privacidad y seguridad relacionadas con el Internet de las cosas

Si bien algunas de las aplicaciones en este espacio ya son populares (salud física y personal, por ejemplo), el crecimiento real todavía tiene que llegar.

A continuación se presentan algunos desafíos de la electrónica de consumo para abordar primero:

- **Dispositivos más inteligentes**. Los consumidores están esperando generaciones inteligentes de productos wearables e Internet de las cosas, que puedan cumplir más funciones sin depender demasiado de los teléfonos inteligentes, como es el caso de muchos de estos dispositivos en la actualidad (piensen en las primeras generaciones de relojes inteligentes que necesitan un teléfono inteligente).

- **Seguridad**. Los consumidores aún no confían en el Internet de las cosas, lo cual se ve reforzado por las infracciones y la cobertura de estas infracciones. Además, no se trata solo de la seguridad de los dispositivos, sino también, entre otros, de la seguridad de los protocolos de comunicación de datos bajos (y de los sistemas operativos Internet of Things). Un ejemplo: el estándar de automatización del hogar Zigbee fue probado como fácil de descifrar en noviembre de 2016.
- **Datos y privacidad.** Además de las preocupaciones de seguridad, también existen preocupaciones con respecto al uso de datos y la privacidad. La falta de confianza con respecto a los datos, la privacidad y la seguridad ya era un problema antes de estas infracciones, como lo abordamos en nuestra descripción general de las evoluciones del mercado de productos electrónicos de consumo.
- **Una "razón convincente para comprar"**. Los dispositivos actuales que se clasifican como dispositivos de Internet del consumidor de las cosas son todavía relativamente caros, "tontos" y difíciles de usar. También a menudo carecen de un beneficio único que hace que los consumidores los compren masivamente.

El mercado de Internet de las cosas para el consumidor

Mientras que el enfoque del Internet industrial de las cosas se centra más en los beneficios de las aplicaciones, el Internet de las cosas para el consumidor se trata más de experiencias nuevas e inmersivas centradas en el cliente.

Las compras de Internet para las compras de los consumidores, el cuarto segmento de mercado más grande en 2016, se convertirán en el tercer segmento más grande para 2020 (IDC, 2017) se espera que el mercado comience a mejorar a partir de finales de 2017 o 2018, cuando el Internet de las cosas para el consumidor crezca rápidamente en varios tipos de dispositivos y aplicaciones, una vez que los fabricantes puedan enfrentar los diversos desafíos.

Como se mencionó, el Internet de las cosas para consumidores generalmente trata de dispositivos portátiles inteligentes y dispositivos electrodomésticos inteligentes, pero también de televisores inteligentes, drones para aplicaciones de consumo y una amplia gama de dispositivos con conectividad de Internet de las cosas.

Es importante tener en cuenta que de hecho el Internet de las cosas de los consumidores se superpone con el uso de Internet de las cosas en varias industrias.

Además de ejemplos como los contadores inteligentes, como se explicó anteriormente, está claro que el CIoT ofrece a los fabricantes de dispositivos y aplicaciones oportunidades importantes para aprovechar los datos para generar nuevas fuentes de ingresos e incluso nuevas asociaciones y ecosistemas para aprovechar estos datos de diversas maneras. La privacidad y la seguridad de los datos seguirán siendo un desafío durante varios años, pero al mismo tiempo nuevas generaciones de dispositivos con beneficios claros y un enfoque en la experiencia del consumidor impulsarán el mercado.

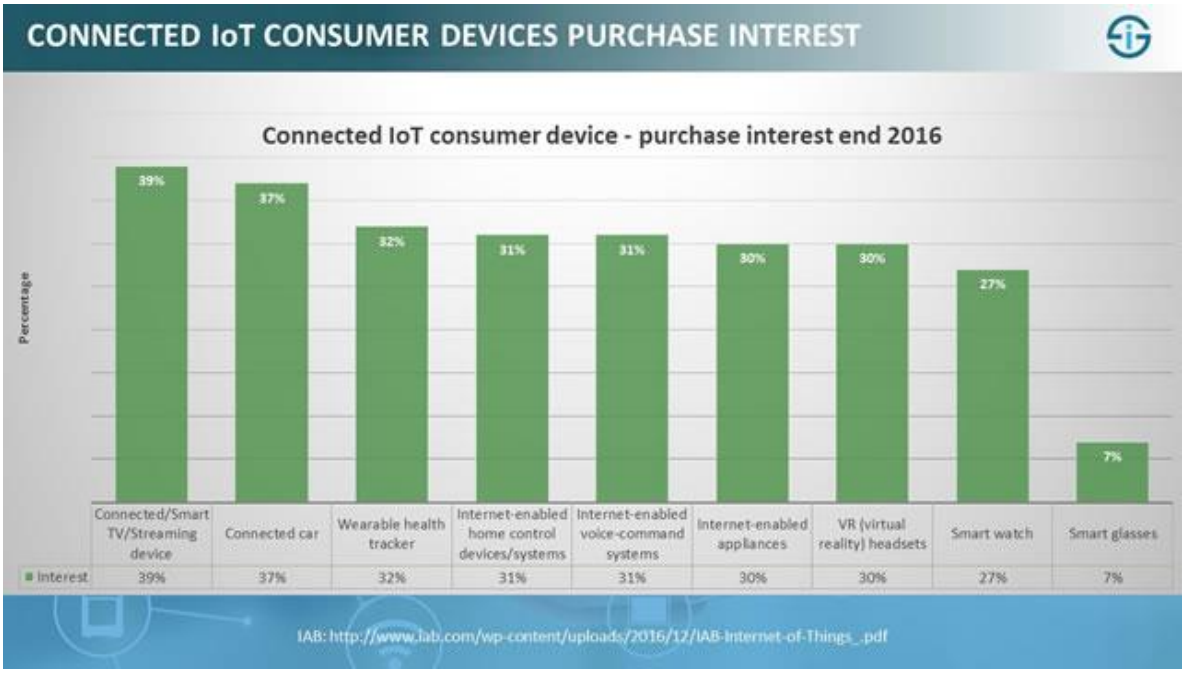

Figura 2.7 - Consumidores conectados por dispositivos. **Fuente**: iab.com

2.7.2 Empresas

El Internet of Things de la empresa será el mayor de los tres sectores principales de IoT: empresa, hogar y gobierno, según lo define BI Intelligence, el servicio de investigación de Business Insider.

Eso es porque las empresas tienen el capital y el alcance para comprar dispositivos y servicios de IoT a gran escala. Verán que los beneficios del IoT se acumulan lo suficientemente rápido como para estimular la adopción y la inversión.

Los dispositivos IoT van desde unidades similares a robots hasta diminutos chips que se conectan a máquinas industriales o de oficina, lo que permite al usuario controlar completamente el dispositivo o simplemente recopilar datos específicos del mismo.

La empresa será el mayor mercado de dispositivos IoT: habrá un total de 23.300 millones de dispositivos IoT conectados en 2019 en todos los sectores, estimamos. De esos 23.300 millones de dispositivos, el mercado empresarial representará alrededor del 40% del total o 9.100 millones de dispositivos, lo que lo convierte en el mayor de los tres sectores de la IoT.

La empresa IoT será masiva por sí misma, más grande que el mercado móvil estrictamente definido. Eso también significa que en 2019, el IoT de la empresa

por sí solo será más grande, combinados todos los mercados de teléfonos inteligentes y tabletas, que las previsiones de BI Intelligence incluirán alrededor de 6 mil millones de dispositivos para 2019.

En un nuevo informe IoT de BI Intelligence, dimensionamos el mercado de IoT de la empresa, destacando el desglose entre el hardware frente al gasto de software y determinando qué industrias se actualizarán primero al IoT. Examinamos cómo las empresas ya están utilizando los sistemas de IoT y qué barreras aún podrían obstaculizar las actualizaciones de la empresa IoT.

Aquí hay más hallazgos clave del informe BI Intelligence:

- El sector empresarial representará el 39% de los aproximadamente 23 mil millones de dispositivos activos de IoT que esperamos para el año 2019. Creemos que será el más grande de los tres mercados principales de IoT, incluidas las empresas, el hogar y el gobierno.
- El gasto en productos y servicios de IoT para empresas alcanzará los 255 mil millones de dólares en todo el mundo en 2019, frente a los $ 46.200 millones de este año, según nuestras estimaciones. Esto representa una CAGR de 5 años del 40%.
- Los proveedores de software de Enterprise IoT ganarán mucho más que aquellos que proporcionan hardware de IoT. Las ventas de software y servicios de IoT enfocadas en la empresa llegarán a $ 43.9 mil millones

para fin de año, mientras que el hardware representará aproximadamente $ 2.3 mil millones en ingresos, de acuerdo con nuestras estimaciones.

- Los sectores de fabricación, transporte y almacenamiento e información invertirán más en sistemas y dispositivos de IoT en los próximos cinco años, estimamos. Actualmente, los fabricantes son la industria líder en el uso de dispositivos IoT y estimamos que la inversión total en IoT alcanzará los $ 140,000 millones en los próximos 5 años.
- Las principales barreras para instalar el IoT dentro de las empresas incluyen los altos costos de instalación y la creciente vulnerabilidad a un ciberataque.

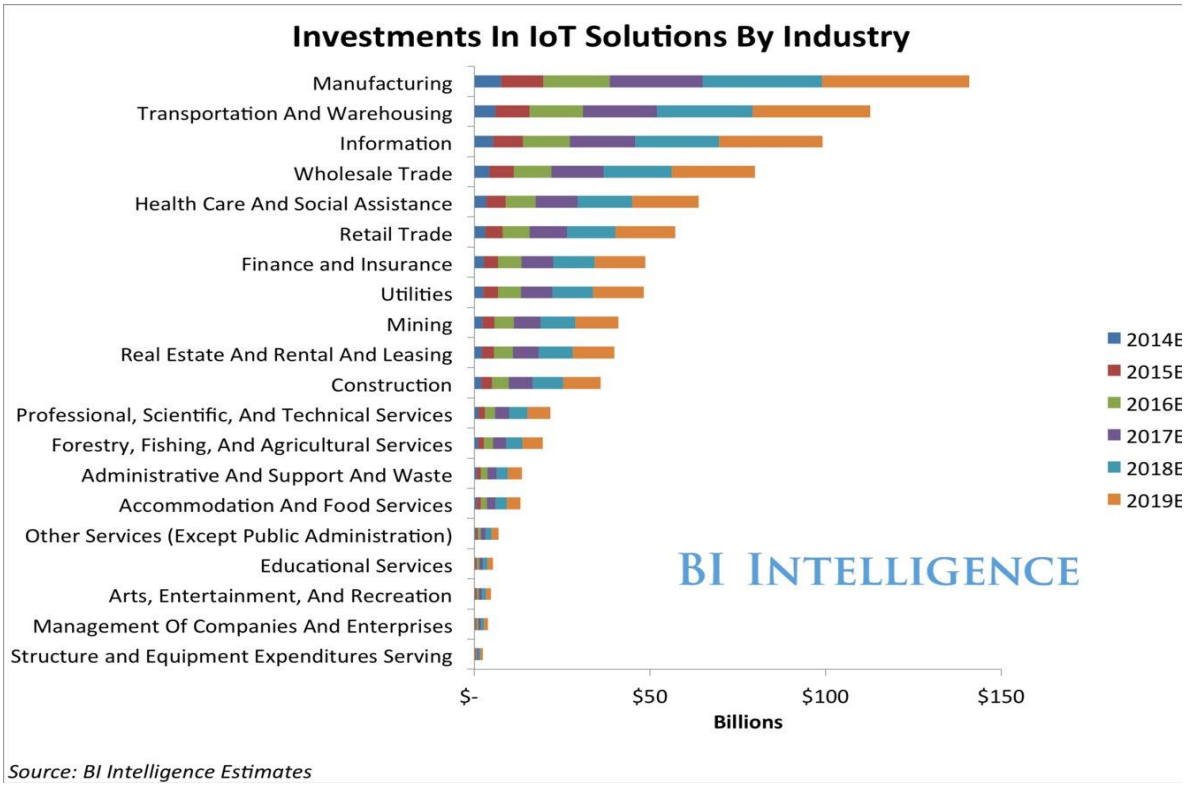

Figura 2.8 - Reporte BI Intelligence. **Fuente**: intelligence.businessinsider.com

2.7.3 Infraestructura

El monitoreo y control de operaciones de infraestructura urbana y rural como puentes, vías férreas y parques eólicos es una aplicación clave de IoT. La infraestructura de IoT puede utilizarse para monitorear cualquier evento o cambio en las condiciones estructurales que puedan comprometer la seguridad e incrementar el riesgo.

También puede utilizarse para planificar actividades de reparación y mantenimiento de manera eficiente, coordinando tareas entre diferentes proveedores de servicios y los usuarios de las instalaciones. Otra aplicación de los dispositivos de IoT es el control de infraestructura crítica, como puentes para permitir el pasaje de embarcaciones. El uso de dispositivos de IoT para el monitoreo y operación de infraestructura puede mejorar el manejo de incidentes, la coordinación de la respuesta en situaciones de emergencia, la calidad y disponibilidad de los servicios, además de reducir los costos de operación en todas las áreas relacionadas a la infraestructura. Incluso áreas como el manejo de desperdicios puede beneficiarse de la automatización y optimización que traería la aplicación de IoT.

2.8 Tendencias

2.8.1 Inteligencia

La inteligencia ambiental y el control autónomo no son parte del concepto original de Internet de las cosas. La inteligencia ambiental y el control autónomo tampoco requieren necesariamente estructuras de Internet. Sin embargo, hay un cambio en la investigación para integrar los conceptos del Internet de las cosas y el control autónomo, con resultados iniciales en esta dirección, considerando a los objetos como la fuerza impulsora del IoT autónomo. La mayoría de los trabajos relacionados con IoT inteligente explotan las capacidades de la computación en la nube para realizar el análisis y devolver el resultado a los dispositivos IoT si es necesario. Sin embargo, los intentos están llevando a cierto nivel de inteligencia y aprendizaje automático en los dispositivos con recursos limitados, nodos de computación de borde y niebla.

En el futuro, Internet of Things puede ser una red no determinista y abierta en la que las entidades autoorganizadas o inteligentes (servicios web, componentes SOA) y objetos virtuales (avatares) serán interoperables y capaces de actuar de forma independiente (persiguiendo su propio objetivos o compartidos) según el contexto, las circunstancias o los entornos. El comportamiento autónomo mediante la recopilación y el razonamiento de la información de contexto así como la capacidad del objeto para detectar cambios en el entorno (fallas que afectan a los sensores) e introducir medidas de mitigación adecuadas constituye

una importante tendencia de investigación, claramente necesaria para proporcionar credibilidad a la tecnología IoT. Los productos y soluciones de IoT modernos en el mercado utilizan una variedad de tecnologías diferentes para admitir dicha automatización basada en el contexto, pero se solicitan formas de inteligencia más sofisticadas para permitir el despliegue de unidades de sensores en entornos reales.

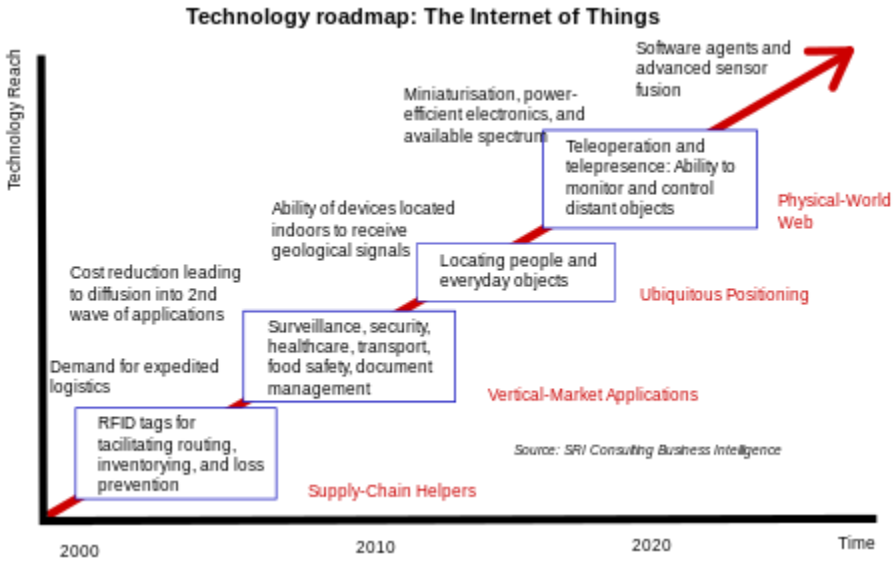

Figura 2.9 - Crecimiento del internet de las cosas. **Fuente:** intelligence.businessinsider.com

2.8.2 Arquitectura

Ciudades inteligentes

Una ciudad inteligente recopila y analiza datos de los sensores y cámaras de video de IoT. En esencia, "detecta" el entorno para que el operador de la ciudad pueda decidir cómo y cuándo actuar. Algunas acciones se pueden realizar de

forma automática. Por ejemplo, un contenedor de basura público puede ponerse en contacto con la ciudad para obtener servicio cuando está cerca de la capacidad en lugar de esperar una recogida programada.

¿Cuáles son los beneficios de una ciudad inteligente?

- **Para las agencias de la ciudad**: obtenga más participación ciudadana y optimice las operaciones a través de la inteligencia de datos en tiempo real y la colaboración dentro de la agencia.
- **Para los ciudadanos**: mejorar la vida diaria a través de los servicios de la ciudad. Las ciudades inteligentes ofrecen visibilidad de los datos de la ciudad en tiempo real para mejorar la movilidad, la conectividad y los servicios de seguridad.
- **Para empresas**: impulse nuevas fuentes de ingresos y desarrollo económico mejorando la conciencia sobre la actividad y el comportamiento de los clientes.
- **Para desarrolladores y vendedores**: Desarrollo de aplicaciones de combustible de datos de la ciudad. Ayude a la ciudad a mejorar la eficiencia operativa, involucrar a los ciudadanos y aumentar la viabilidad económica.

Tipos

1. **Calidad del aire**: controle el aire para saber cuándo regular las emisiones.
2. **Arquitectura de comunicación**: conéctate con ciudadanos y turistas a través de kioscos interactivos y aplicaciones móviles, ofreciendo información en función de su ubicación.
3. **Medio ambiente**: visualice y analice todos los datos de la ciudad para decidir mejor cuándo y cómo actuar.
4. **Iluminación**: menor consumo de energía, reducción de costos y simplificación del mantenimiento.
5. **Estacionamiento**: Genere ingresos con estacionamiento basado en la demanda y reduzca el tiempo de búsqueda de espacio para estacionamiento para los ciudadanos.
6. **Wi-Fi público**: el Wi-Fi de toda la ciudad conecta los sensores pero, lo que es más importante, también proporciona una manera para que las personas se conecten con el mundo.
7. **Seguridad y protección**: proteja contra la delincuencia, el terrorismo y los disturbios civiles y responda más rápidamente a las emergencias con análisis de video avanzados.
8. **Transporte**: reduzca la congestión y la contaminación a través de la gestión del tráfico.

9. Movilidad urbana: comprender dónde se mueven las personas y pasar su tiempo y utilizar esas ideas para la planificación de la ciudad.
10. **Gestión de residuos**: cuando los contenedores de basura están conectados, los trabajadores de la ciudad pueden recogerlos según sea necesario. Ahorre tiempo y recursos del personal.
11. **Gestión del agua**: el flujo de agua seguro y eficiente es un recurso esencial para cualquier ciudad.

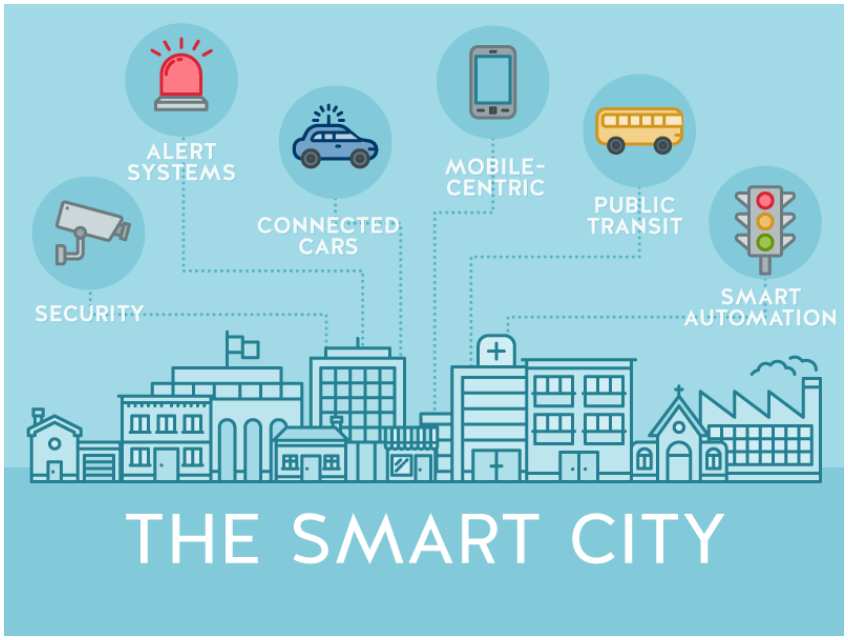

Figura 2.10 - Concepto de ciudad inteligente. **Fuente**: informationsecuritybuzz.com

2.8.3 Estándares

A continuación se encuentra una lista parcial de las normas IEEE relacionadas con el Internet de las cosas.

1. IEEE 754 ™ -2008 - Estándar IEEE para aritmética de coma flotante.

2. IEEE 802.1AS ™ -2011 - Estándar IEEE para redes de área local y metropolitana - Sincronización y sincronización para aplicaciones con tiempo limitado en redes de área local puenteadas.

3. IEEE 802.1Q ™ -2011 - Estándar IEEE para redes de área local y metropolitana - Puentes de control de acceso a medios (MAC) y redes de área local con puente virtual.

4. IEEE 802.3 ™ -2012 - IEEE Standard para Ethernet.

5. IEEE 802.3.1 ™ -2011 - Definiciones del estándar IEEE para la base de información de gestión (MIB) para Ethernet.

6. IEEE 802.11 ™ -2012 - Estándar IEEE para tecnología de la información - Telecomunicaciones e intercambio de información entre sistemas - Redes de área local y metropolitana - Requisitos específicos Parte 11: Especificaciones de control de acceso (MAC) y capa física (PHY) LAN inalámbrica Enmienda 10 : Redes de malla.

7. IEEE 802.11ad ™ -2012 - Estándar IEEE para redes de área local y metropolitana - Requisitos específicos - Parte 11: Especificaciones de control de acceso (MAC) y capa física (PHY) de LAN inalámbrica - Enmienda 3: Mejoras para rendimiento muy alto en 60 GHz Banda.

8. IEEE 802.15.1 ™ -2005 - Estándar IEEE para tecnología de la información - Telecomunicaciones e intercambio de información entre sistemas - Redes de área local y metropolitana - Requisitos específicos. - Parte 15.1: Especificaciones de control de acceso inalámbrico (MAC) y capa física (PHY) para redes inalámbricas de área personal (WPAN).

9. IEEE 802.15.2 ™ -2003 - Práctica recomendada de IEEE para tecnología de la información - Telecomunicaciones e intercambio de información entre sistemas - Redes de área local y metropolitana - Requisitos específicos Parte 15.2: Coexistencia de redes inalámbricas de área personal con otros dispositivos inalámbricos que operan en bandas de frecuencias sin licencia.

10. IEEE 802.15.3 ™ -2003 - Estándar IEEE para la tecnología de la información - Telecomunicaciones e intercambio de información entre sistemas - Redes de área local y metropolitana - Requisitos específicos Parte 15.3: Control de acceso medio inalámbrico (MAC) y capa física

(PHY) Especificaciones para alta velocidad inalámbrico Redes de área personal (WPAN) Enmienda 1: Subcapa de Mac.

11. IEEE 802.15.3c ™ -2009 - Estándar IEEE para tecnología de la información-- Redes de área local y metropolitana-- Requisitos específicos-- Parte 15.3: Enmienda 2: Extensión de capa física alternativa basada en ondas milimétricas.

12. IEEE 802.15.4 ™ -2011 - Estándar IEEE para redes de área local y metropolitana - Parte 15.4: Redes inalámbricas de área personal de baja velocidad (LR-WPAN).

13. IEEE 802.15.4e ™ -2012 - Estándar IEEE para redes de área local y metropolitana - Parte 15.4: Redes inalámbricas de área personal de baja velocidad (LR-WPAN) Enmienda 1: subcapa MAC.

14. IEEE 802.15.4f ™ -2012 - Estándar IEEE para redes de área local y metropolitana-- Parte 15.4: Redes de área personal inalámbricas de baja velocidad (LR-WPAN) Enmienda 2: Sistema de identificación de frecuencia de radio activa (RFID) Capa física (PHY).

15. IEEE 802.15.4g ™ -2012 - Estándar IEEE para redes de área local y metropolitana - Parte 15.4: Redes de área personal inalámbricas de baja

velocidad (LR-WPAN) Enmienda 3: Especificaciones de capa física (PHY) para velocidad de datos baja, inalámbrico, Smart Metering Utility Networks.

16. IEEE 802.15.4j ™ -2013 - Estándar IEEE para tecnología de la información - Telecomunicaciones e intercambio de información entre sistemas - Redes de área local y metropolitana - Requisitos específicos - Parte 15.4: Control de acceso medio inalámbrico (MAC) y Capa física (PHY) Especificaciones para tarifa baja Enmienda de Redes de área personal inalámbricas (WPAN): Extensión de capa física alternativa para admitir servicios de red de área de cuerpo médico (MBAN) que operan en la banda de 2360-2400 MHz.

17. IEEE 802.15.5 ™ -2009 - Práctica recomendada de IEEE para tecnología de la información-Telecomunicaciones e intercambio de información entre sistemas-Redes de área local y metropolitana-Requisitos específicos Parte 15.5: Capacidad de topología de malla en redes inalámbricas de área personal (WPAN).

18. IEEE 802.15.6 ™ -2012 - Estándar IEEE para tecnología de la información - Telecomunicaciones e intercambio de información entre sistemas - Redes de área local y metropolitana - Requisitos específicos - Parte 15.6: Control de acceso medio inalámbrico (MAC) y Capa física

(PHY) Especificaciones para personal inalámbrico Redes de área (WPAN) usadas en o alrededor de un cuerpo.

19. IEEE 802.15.7 ™ -2011 - Estándar IEEE para redes de área local y metropolitana - Parte 15.7: Comunicación óptica inalámbrica de corto alcance usando luz visible.

20. IEEE 802.16 ™ -2012 - Estándar IEEE para interfaz aérea para sistemas de acceso inalámbrico de banda ancha.

21. IEEE 802.16p ™ -2012 - IEEE Standard for Air Interface para sistemas de acceso inalámbrico de banda ancha Enmienda: mejoras para admitir aplicaciones de máquina a máquina.

22. IEEE 802.16.1b ™ -2012 - Estándar IEEE para WirelessMAN-Interfaz aérea avanzada para sistemas de acceso inalámbrico de banda ancha - Enmienda: mejoras para admitir aplicaciones de máquina a máquina.

23. IEEE 802.22 ™ -2011 - Estándar IEEE para tecnología de la información - Telecomunicaciones e intercambio de información entre sistemas Redes inalámbricas de área regional (WRAN) - Requisitos específicos Parte 22: Cognitivo inalámbrico RAN Control de acceso medio (MAC) y capa física

(PHY) Especificaciones: Políticas y procedimientos para la operación en las bandas de TV.

24. IEEE 802.22.1 ™ -2010 - Estándar IEEE para tecnología de la información - Telecomunicaciones e intercambio de información entre sistemas - Redes de área local y metropolitana - Requisitos específicos Parte 22.1: Estándar para mejorar la protección contra interferencias dañinas para dispositivos con bajo consumo de energía que operan en TV Bandas de difusión.

25. IEEE 802.22.2 ™ -2012 - Estándar IEEE para tecnología de la información - Telecomunicaciones e intercambio de información entre sistemas - Redes de área local y metropolitana - Requisitos específicos Parte 22.2: Instalación y despliegue de sistemas IEEE 802.22.

26. IEEE 1284 ™ -2000 - Método de señalización estándar IEEE para una interfaz paralela bidireccional paralela para ordenadores personales.

27. IEEE 1285 ™ -2005 - Estándar IEEE para interfaz de almacenamiento escalable (S / SUP 2 / I).

28. IEEE 1301.3 ™ -1992 - Estándar IEEE para una práctica de equipos métricos para microcomputadoras: refrigeración por convección con conectores de 2.5 mm.

29. IEEE 1377 ™ -2012 - Estándar IEEE para la capa de aplicación de protocolo de comunicación de medición de la industria de servicios públicos (tablas de datos del dispositivo final).

30. IEEE 1394 ™ -2008 - Estándar IEEE para un bus serie de alto rendimiento.

31. IEEE 1451.0 ™ -2007 - Estándar IEEE para una interfaz de transductor inteligente para sensores y actuadores - Funciones comunes, protocolos de comunicación y formatos de hoja de datos electrónicos del transductor (TEDS).

32. IEEE 1547 ™ -2003 - Estándar IEEE para la interconexión de recursos distribuidos con sistemas de energía eléctrica.

33. IEEE 1547.1 ™ -2005 - Procedimientos de prueba de conformidad estándar de IEEE para equipos que interconectan recursos distribuidos con sistemas de energía eléctrica.

34. IEEE 1547.2 ™ -2008 - Guía de aplicaciones IEEE para IEEE Std 1547 ™, estándar IEEE para la interconexión de recursos distribuidos con sistemas de energía eléctrica.

35. IEEE 1547.3 ™ -2007 - Guía IEEE para monitoreo, intercambio de información y control de recursos distribuidos interconectados con sistemas de energía eléctrica.

36. IEEE 1547.4 ™ -2011 - Guía IEEE para el diseño, operación e integración de sistemas de isla de recursos distribuidos con sistemas de energía eléctrica.

37. IEEE 1547.6 ™ -2011 - Práctica recomendada IEEE para la interconexión de recursos distribuidos con distribución de sistemas de energía eléctrica Redes secundarias.

38. IEEE 1609.2 ™ -2013 - Estándar IEEE para acceso inalámbrico en entornos vehiculares - Servicios de seguridad para aplicaciones y mensajes de gestión.

39. IEEE 1609.3 ™ -2010 - Estándar IEEE para acceso inalámbrico en entornos vehiculares (WAVE) - Servicios de red.

40. IEEE 1609.4 ™ -2010 - Estándar IEEE para acceso inalámbrico en entornos vehiculares (WAVE) - Operación multicanal.

41. IEEE 1609.11 ™ -2010 - Estándar IEEE para acceso inalámbrico en entornos vehiculares (WAVE) - Protocolo de intercambio de datos de pago electrónico inalámbrico para sistemas de transporte inteligentes (ITS).

42. IEEE 1609.12 ™ -2012 - Estándar IEEE para acceso inalámbrico en entornos vehiculares (WAVE) - Asignación de identificadores.

43. IEEE 1675 ™ -2008 - Estándar IEEE para banda ancha sobre hardware Powerline 1900.1-2008 Definiciones y conceptos estándar IEEE para

acceso dinámico al espectro: terminología relacionada con redes inalámbricas emergentes, funcionalidad del sistema y gestión del espectro.

44. IEEE 1701 ™ -2011 - Estándar IEEE para el protocolo de comunicación de puerto óptico para complementar las tablas de datos del dispositivo final de la industria de servicios públicos.

45. IEEE 1702 ™ -2011 - Estándar IEEE para el protocolo de comunicación del módem telefónico para complementar las tablas de datos del dispositivo final de la industria de servicios públicos.

46. IEEE 1703 ™ -2012 - Estándar IEEE para red de área local / red de área amplia (LAN / WAN) Protocolo de comunicación de nodo para complementar las tablas de datos de dispositivo final de la industria de servicios públicos.

47. IEEE 1775 ™ -2010 - Estándar IEEE para equipos de comunicación de línea de alimentación - Requisitos de Compatibilidad Electromagnética (EMC) - Métodos de prueba y medición.

48. IEEE 1815 ™ -2012 - Estándar IEEE para comunicaciones de sistemas de energía eléctrica - Protocolo de red distribuida (DNP3) 2200-2012 Protocolo estándar IEEE para gestión de flujo en dispositivos cliente de medios.

49. IEEE 1888 ™ -2011 - Estándar IEEE para el Protocolo de red de control comunitario verde omnipresente.

50. IEEE 1900.1 ™ -2008 - Definiciones y conceptos del estándar IEEE para el acceso dinámico al espectro: terminología relacionada con las redes inalámbricas emergentes, la funcionalidad del sistema y la gestión del espectro.

51. IEEE 1900.2 ™ -2008 - Práctica recomendada por IEEE para el análisis de la interferencia y coexistencia de banda adyacente y en banda entre sistemas de radio.

52. IEEE 1900.4 ™ -2009 - Estándar IEEE para Building Blocks arquitectónicos que permite la toma de decisiones distribuidas por dispositivos de red para optimizar el uso de recursos de radio en redes de acceso inalámbricas heterogéneas.

53. IEEE 1900.4a ™ -2011 - Estándar IEEE para Building Blocks arquitectónicos que permite la toma de decisiones distribuidas por dispositivos de red para el uso optimizado de recursos de radio en redes de acceso inalámbricas heterogéneas. Enmienda 1: Arquitectura e interfaces para redes de acceso de espectro dinámico en bandas de frecuencias espaciales en blanco.

54. IEEE 1901 ™ -2010 - Estándar IEEE para redes de banda ancha sobre redes eléctricas: control de acceso medio y especificaciones de capa física.

55. IEEE 1902.1 ™ -2009 - Estándar IEEE para protocolo de red inalámbrica de longitud de onda larga.

56. IEEE 1905.1 ™ -2013 - Estándar de borrador IEEE para una red doméstica digital convergente para tecnologías heterogéneas.

57. IEEE 2200 ™ -2012 - Protocolo estándar IEEE para la gestión de flujo en dispositivos cliente de medios.

58. IEEE 2030 ™ -2011 - Guía IEEE para interoperabilidad de red inteligente de tecnología de energía y operación de tecnología de información con el sistema de energía eléctrica (EPS), aplicaciones de uso final y cargas

59. IEEE 2030.5 ™ -2013 - Adopción IEEE del estándar de protocolo de aplicación Smart Energy Profile 2.0.

60. IEEE 11073-00101 ™ -2008 - Estándar IEEE para Informática de la Salud - Comunicación con dispositivos médicos PoC - Parte 00101: Guía - Pautas para el uso de la tecnología inalámbrica RF.

61. IEEE 11073-10102 ™ -2012 - Estándar IEEE para informática sanitaria - Comunicación de dispositivo médico en punto de atención - Nomenclatura - ECG anotado.

62. IEEE 11073-10103 ™ -2012 - Estándar IEEE para informática sanitaria - Comunicación de dispositivo médico en punto de atención - Nomenclatura - Dispositivo implantable, cardíaco.

63. IEEE 11073-10201 ™ -2004 - Estándar IEEE para Informática de la Salud - Comunicación de dispositivos médicos en punto de atención - Parte 10201: Modelo de información de dominio.

64. IEEE 11073-10404 ™ -2010 - Estándar IEEE para informática de salud-Comunicación de dispositivo de salud personal Parte 10404: Especialización de dispositivo-Oxímetro de pulso.

65. IEEE 11073-10406 ™ -2011 - Estándar de IEEE para informática de la salud - Comunicación de dispositivos de salud personal Parte 10406: Especialización de dispositivos - Electrocardiógrafo básico (ECG) (ECG de 1 a 3 derivaciones).

66. IEEE 11073-10407 ™ -2010 - Estándar IEEE para informática de la salud Comunicación de dispositivos de salud personal Parte 10407: Especialización del dispositivo Monitor de presión arterial.

67. IEEE 11073-10408 ™ -2010 - Estándar IEEE para informática de salud Comunicación de dispositivo de salud personal Parte 10408: Termómetro de especialización de dispositivo.

68. IEEE 11073-10415 ™ -2010 - Estándar IEEE para informática de la salud Comunicación de dispositivos de salud personal Parte 10415: Especialización del dispositivo Balanza de pesaje 11073-10420-2010 Norma IEEE para informática de la salud - Comunicación de dispositivos de salud personales Parte 10420: Especialización del dispositivo - Analizador de composición corporal.

69. IEEE 11073-10417 ™ -2011 - Estándar IEEE para informática de la salud Comunicación de dispositivos de salud personal Parte 10417: Especialización del dispositivo Medidor de glucosa.

70. IEEE 11073-10418 ™ -2011 - Estándar IEEE para informática de salud - Comunicación de dispositivos de salud personales - Especialización de dispositivos - Monitor de relación internacional normalizada (INR).

71. IEEE 11073-10420 ™ -2010 - Estándar IEEE para informática de la salud - Comunicación entre dispositivos de salud personal Parte 10420: Especialización de dispositivos - Analizador de composición corporal.

72. IEEE 11073-10441 ™ -2008 - Estándar IEEE para Informática de la Salud - Comunicación del Dispositivo de Salud Personal - Parte 10441:

Especialización del Dispositivo - Monitor de Actividad y Aptitud Cardiovascular.

73. IEEE 11073-30300 ™ -2004 - Estándar IEEE para informática de salud - Comunicación de dispositivo médico en punto de atención - Perfil de transporte - Infrarrojo.

74. IEEE 11073-30400 ™ -2010 - Estándar IEEE para informática sanitaria - Comunicación de dispositivos médicos en punto de atención Parte 30400: Perfil de interfaz - Ethernet con cables.

75. IEEE 14575 ™ -2000 - Estándar IEEE para interconexión heterogénea (HIC) (interconexión serial escalable de bajo costo y baja latencia para la construcción de sistemas paralelos).

76. IEEE 21450 ™ -2010 - Estándar IEEE para tecnología de la información - Interfaz de transductor inteligente para sensores y actuadores - Funciones comunes, protocolos de comunicación y formatos de hoja de datos electrónicos del transductor (TEDS).

77. IEEE 21451-1 ™ -2010 - Estándar IEEE para tecnología de la información - Interfaz de transductor inteligente para sensores y actuadores - Parte 1: Modelo de información del procesador de aplicaciones compatible con la red (NCAP).

78. IEEE 21451-2 ™ -2010 - Estándar IEEE para tecnología de la información - Interfaz de transductor inteligente para sensores y actuadores - Parte 2: Transductores a protocolos de comunicación de microprocesador y formatos de hoja de datos electrónicos del transductor (TEDS).

79. IEEE 21451-4 ™ -2010 - Estándar IEEE para tecnología de la información - Interfaz de transductor inteligente para sensores y actuadores - Parte 4: Protocolos de comunicación de modo mixto y formatos de hoja de datos electrónicos del transductor (TEDS).

80. IEEE 21451-7 ™ -2011 - Estándar IEEE para interfaz de transductor inteligente para sensores y actuadores - Transductores para sistemas de identificación por radiofrecuencia (RFID) Protocolos de comunicación y formatos de hoja de datos electrónicos para transductor.

2.9 Privacidad y Seguridad

Internet de las cosas está conectando más dispositivos cada día, y nos dirigimos hacia un mundo que tendrá 24 mil millones de dispositivos de IoT para 2020. Este crecimiento conlleva varios beneficios, ya que cambiará la forma en que las personas llevan a cabo las tareas cotidianas y potencialmente transforman el mundo. Tener un hogar inteligente es indudablemente genial y atraerá la atención de sus invitados, pero una iluminación inteligente puede reducir el consumo total de energía y reducir su factura de electricidad.

Los nuevos desarrollos permitirían a los automóviles conectados conectarse con la infraestructura de ciudad inteligente para crear un ecosistema completamente diferente para el conductor, que simplemente está acostumbrado a la forma tradicional de llegar del Punto A al Punto B.

Y los dispositivos de salud conectados le dan a la gente una mirada más profunda y completa sobre su propia salud, o la falta de ella, que nunca antes.

Pero con todos estos beneficios viene el riesgo, ya que el aumento de dispositivos conectados brinda a los piratas informáticos y ciber-delincuentes más puntos de entrada.

A fines del año pasado, un grupo de hackers derribó una red eléctrica en una región del oeste de Ucrania para causar el primer apagón de un ciberataque. Y

esto probablemente sea solo el comienzo, ya que estos hackers están buscando más formas de atacar infraestructuras críticas, como redes eléctricas, represas hidroeléctricas, plantas químicas y más.

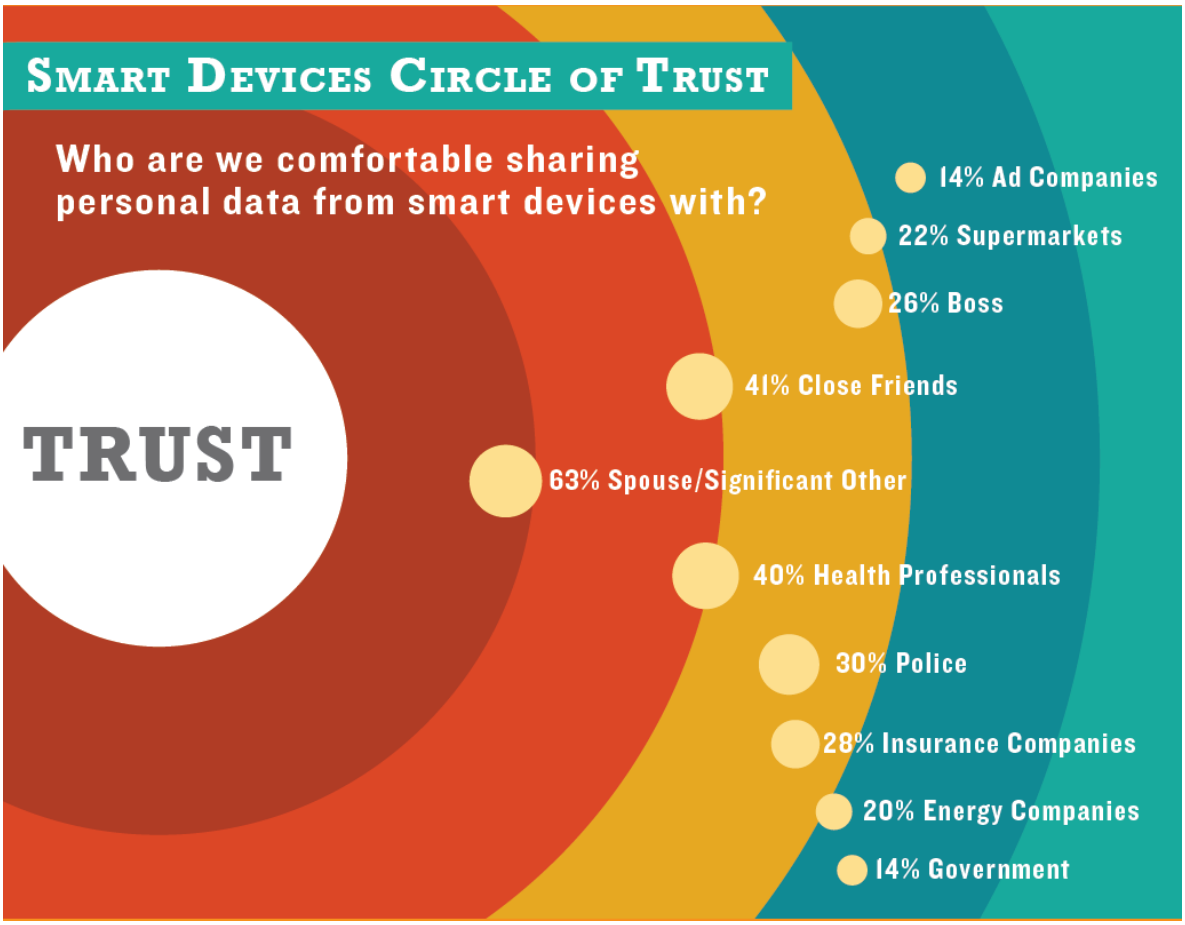

Figura 2.11 - Círculo de confianza. **Fuente**: trustarc.com

Además de estos problemas de seguridad, el consumidor medio está preocupado por su privacidad. Después de todo, si gran parte de la vida del consumidor está conectada, entonces ¿qué está fuera de los límites?

A continuación, hemos compilado una lista de algunos de los mayores problemas de seguridad y privacidad de IoT a medida que nos dirigimos hacia este mundo verdaderamente conectado.

Cuestiones de seguridad de IoT

- **Percepción pública**: si el IoT realmente va a despegar realmente, este debe ser el primer problema que aborden los fabricantes. El estudio 2015 del estado del Smart Home de Icontrol descubrió que el 44% de todos los estadounidenses estaban "muy preocupados" por la posibilidad de que su información fuera robada de su casa inteligente, y el 27% estaba "algo preocupado". Con ese nivel de preocupación, los consumidores dudarían en comprar dispositivos conectados.

- **Vulnerabilidad a la piratería**: los investigadores han podido hackear dispositivos reales en el mercado con suficiente tiempo y energía, lo que significa que los hackers probablemente puedan replicar sus esfuerzos. Por ejemplo, un equipo de investigadores de Microsoft y la Universidad de Michigan descubrió recientemente una gran cantidad de agujeros en la seguridad de la plataforma inteligente para el hogar SmartThings de Samsung, y los métodos estaban lejos de ser complejos.

- **¿Están las empresas preparadas?**: El Informe de introspección sobre seguridad cibernética de AT & T encuestó a más de 5.000 empresas en todo el mundo y descubrió que el 85% de las empresas están en el proceso o la intención de implementar dispositivos IoT. Sin embargo, solo el 10% de los encuestados confía en que podrían proteger esos dispositivos contra los piratas informáticos.

- **True Security**: Jason Porter, VP de soluciones de seguridad de AT & T, le dijo a BI Intelligence, el servicio de investigación premium de Business Insider, que asegurar dispositivos IoT significa más que simplemente proteger los dispositivos en sí mismos. Las empresas también necesitan crear seguridad en aplicaciones de software y conexiones de red que se vinculen a estos dispositivos.

Problemas de privacidad de IoT

- **Demasiados datos**: la enorme cantidad de datos que los dispositivos de IoT pueden generar es asombrosa. Un informe de la Comisión Federal de Comercio titulado "Internet de las cosas: privacidad y seguridad en un mundo conectado" descubrió que menos de 10,000 hogares pueden generar 150 millones de puntos de datos discretos por día. Esto crea más puntos de entrada para los piratas informáticos y deja vulnerable la información sensible.

- **Perfil público no deseado**: indudablemente, usted estuvo de acuerdo con los términos de servicio en algún momento, pero ¿alguna vez ha leído un documento completo? El mencionado informe de la FTC descubrió que las empresas pueden usar los datos recopilados que los consumidores ofrecen voluntariamente para tomar decisiones de empleo. Por ejemplo, una compañía de seguros puede recopilar información sobre sus hábitos de manejo a través de un automóvil conectado al calcular su tasa de seguro. Lo mismo podría ocurrir para la salud o el seguro de vida gracias a los rastreadores de fitness.

- **Escuchando espías**: los fabricantes o los hackers podrían usar un dispositivo conectado para invadir virtualmente la casa de una persona. Los investigadores alemanes lograron esto al interceptar datos no cifrados de un dispositivo de medidor inteligente para determinar qué programa de televisión estaba viendo alguien en ese momento.

- **Confianza del consumidor**: cada uno de estos problemas podría hacer mella en el deseo de los consumidores de comprar productos conectados, lo que evitaría que el IoT cumpliera con su verdadero potencial.

El crecimiento del IoT es inevitable y todos deben adaptarse a esta tecnología que es bastante revolucionaria, y que promete un sin número de ventajas a la hora de realizar muchas actividades cotidianas e incluso actividades que son difíciles o tediosas de realizar. Este término o mejor dicho este hecho conlleva un proceso largo para su desarrollo debido a que deben realizarse las medidas necesarias para hacer que los usuarios que utilicen esta tecnología no se vean expuestos en cuanto a vulnerabilidades de Seguridad y que cada aspecto de su privacidad sea respetado en cuanto a las leyes se habla.

Hay muchos aspectos que hacen que el IoT sea un término que conlleva a un futuro prometedor y convincente para los usuarios. Hoy en dia hay muchos dispositivos que las personas utilizan que son considerados en el ámbito del IoT, un ejemplo común son los relojes inteligentes, estos ayudan a disminuir el uso de los dispositivos móviles, ya que mediante estos es posible realizar ciertas funciones básicas, como tomar una llamada, enviar textos cortos e incluso visualizar de una manera rápida cualquier documento que se desee ver en el momento.

Figura 2.12 - Vulnerabilidades del IOT. **Fuente:** bizreport.com

CAPÍTULO III.

TECNOLOGÍAS DE RADAR Y REDES INALÁMBRICA

3.1 Radar

3.1.1 Historia

La historia del radar comenzó con experimentos de Heinrich Hertz a fines del siglo XIX que demostraron que las ondas de radio se reflejaban en objetos metálicos. Esta posibilidad fue sugerida en el trabajo seminal de James Clerk Maxwell sobre electromagnetismo. Sin embargo, no fue hasta principios del siglo XX que los sistemas capaces de utilizar estos principios se volvieron ampliamente disponibles, y fue el inventor alemán Christian Hülsmeyer quien los utilizó por primera vez para construir un dispositivo de detección de buques simple para evitar colisiones en la niebla (Reichspatent Nr 165546). Numerosos sistemas similares, que proporcionaron información direccional a objetos de corto alcance, se desarrollaron durante las siguientes dos décadas.

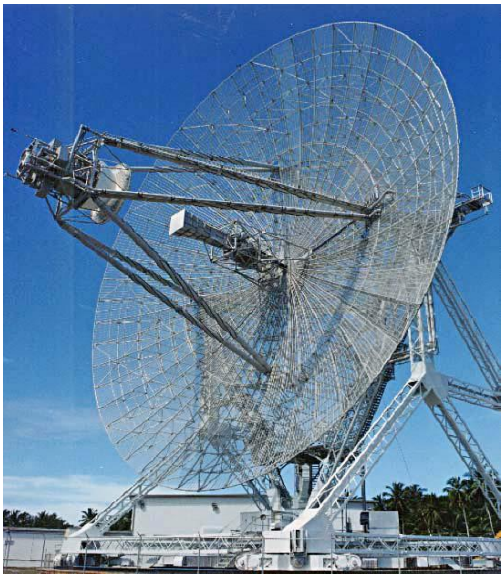

Figura 3.1 Una antena de radar de detección a larga distancia. **Fuente**: SMDC

El desarrollo de sistemas capaces de producir pulsos cortos de energía de radio fue el avance clave que permitió la creación de sistemas de radar modernos. Al temporizar los pulsos en un osciloscopio, se pudo determinar el alcance y la dirección de la antena reveló la ubicación angular de los objetivos. Los dos, combinados, produjeron una "solución", ubicando el objetivo relativo a la antena. En el período de 1934-1939, ocho naciones desarrollaron de manera independiente, y en gran secreto, sistemas de este tipo: el Reino Unido, Alemania, los Estados Unidos, la URSS, Japón, los Países Bajos, Francia e Italia. Además, Gran Bretaña compartió su información con los Estados Unidos y cuatro países de la Commonwealth: Australia, Canadá, Nueva Zelanda y Sudáfrica, y estos países también desarrollaron sus propios sistemas de radar. Durante la guerra, Hungría se agregó a esta lista. El término RADAR fue acuñado en 1939 por los Estados Unidos Signal Corps ya que trabajó en estos sistemas para la Marina.

El progreso durante la guerra fue rápido y de gran importancia, probablemente uno de los factores decisivos para la victoria de los Aliados. Un desarrollo clave fue el magnetrón en el Reino Unido, que permitió la creación de sistemas relativamente pequeños con una resolución por debajo del metro. Al final de las hostilidades, Gran Bretaña, Alemania, Estados Unidos, la URSS y Japón tenían una gran diversidad de radares terrestres y marítimos, así como pequeños sistemas aerotransportados. Después de la guerra, el uso del radar se amplió a numerosos campos que incluyen: aviación civil, navegación marítima, radar en

forma de pistola para la policía, meteorología e incluso medicina. Desarrollos clave en el período de la posguerra incluyen el tubo de ondas progresivas como una forma de producir grandes cantidades de microondas coherentes, el desarrollo de sistemas de retardo de señal que conducen a radares phased array, y frecuencias cada vez mayores que permiten resoluciones más altas. Los aumentos en la capacidad de procesamiento de la señal debido a la introducción de computadoras de estado sólido también han tenido un gran impacto en el uso del radar.

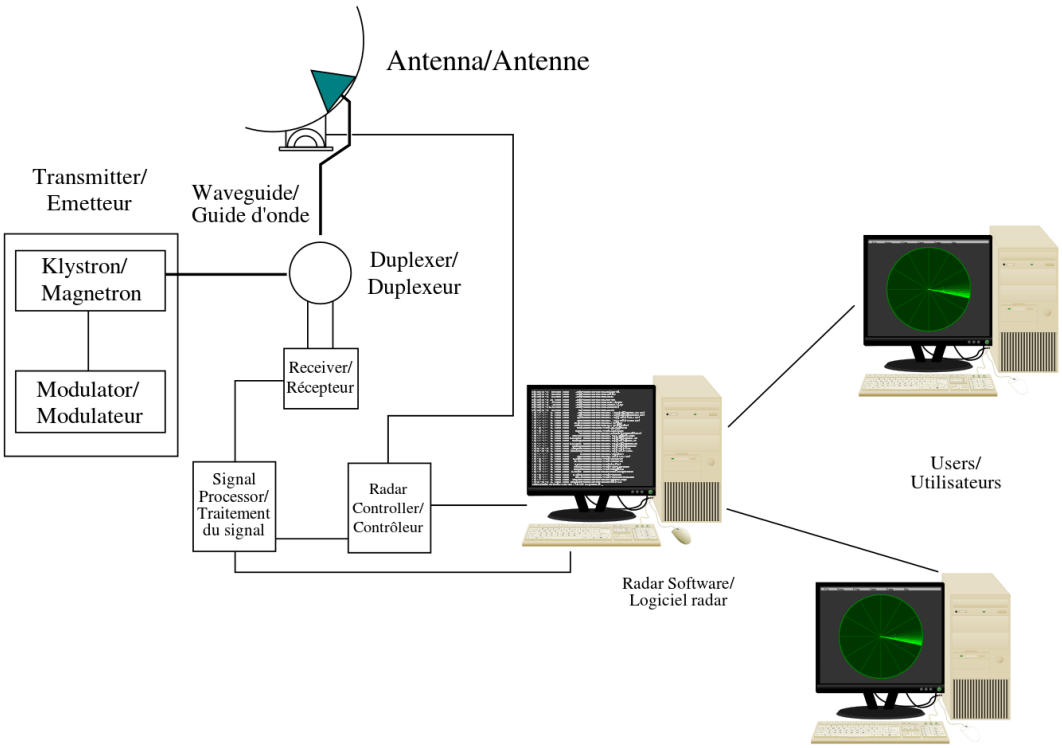

Figura 3.2 Componentes de un radar. **Fuente**: Wikimedia

3.1.2 Principios

Un sistema de radar tiene un transmisor que emite ondas de radio llamadas señales de radar en direcciones predeterminadas. Cuando entran en contacto con un objeto, generalmente se reflejan o dispersan en muchas direcciones. Pero algunos de ellos absorben y penetran en el objetivo hasta cierto punto. Las señales de radar se reflejan especialmente bien con materiales de considerable conductividad eléctrica, especialmente en la mayoría de los metales, en el agua de mar y en el suelo húmedo. Algunos de estos hacen posible el uso de altímetros de radar. Las señales de radar que se reflejan hacia el transmisor son las deseables que hacen que el radar funcione. Si el objeto se mueve hacia o desde el transmisor, hay un ligero cambio equivalente en la frecuencia de las ondas de radio, causado por el efecto Doppler.

Los receptores de radar suelen estar, pero no siempre, en la misma ubicación que el transmisor. Aunque las señales de radar reflejadas capturadas por la antena receptora suelen ser muy débiles, pueden reforzarse con amplificadores electrónicos. También se utilizan métodos más sofisticados de procesamiento de señales para recuperar señales de radar útiles.

La débil absorción de ondas de radio por el medio a través del cual pasa es lo que permite a los conjuntos de radar detectar objetos a rangos relativamente largos, rangos en los que otras longitudes de onda electromagnéticas, como luz visible, luz infrarroja y luz ultravioleta, están demasiado atenuadas. Los

fenómenos meteorológicos tales como la niebla, las nubes, la lluvia, la nieve que cae y el agua de nieve que bloquean la luz visible suelen ser transparentes para las ondas de radio. Ciertas frecuencias de radio que son absorbidas o dispersadas por el vapor de agua, gotas de lluvia o gases atmosféricos (especialmente oxígeno) se evitan en el diseño de radares, excepto cuando se pretende su detección.

La frecuencia del radar, la forma del pulso, la polarización, el procesamiento de la señal y la antena determinan lo que puede observar.

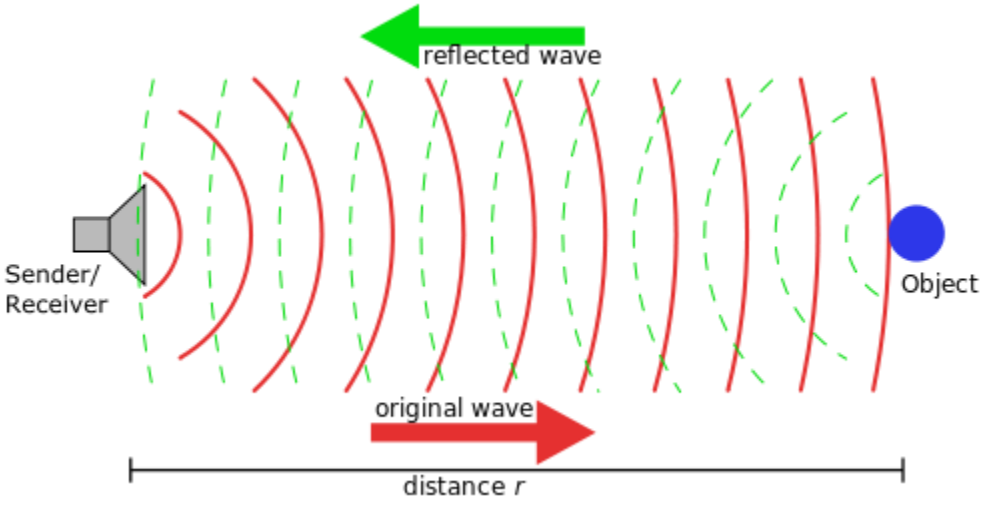

Figura 3.3 Principio de un sonar o radar de medición de distancia. **Fuente**: Inkscape

Si las ondas electromagnéticas que viajan a través de un material se encuentran con otro material, teniendo una constante dieléctrica o constante diamagnética diferente de la primera, las ondas se reflejarán o se dispersarán desde el límite

entre los materiales. Esto significa que un objeto sólido en el aire o en el vacío, o un cambio significativo en la densidad atómica entre el objeto y lo que lo rodea, generalmente dispersará las ondas de radar (radio) de su superficie. Esto es particularmente cierto para los materiales eléctricamente conductores como el metal y la fibra de carbono, lo que hace que el radar sea adecuado para la detección de aeronaves y barcos. El material absorbente del radar, que contiene sustancias resistivas y a veces magnéticas, se utiliza en vehículos militares para reducir la reflexión del radar. Este es el equivalente radial de pintar algo de un color oscuro para que no pueda ser visto por el ojo por la noche.

Las ondas de radar se dispersan en una variedad de formas dependiendo del tamaño (longitud de onda) de la onda de radio y la forma del objetivo. Si la longitud de onda es mucho más corta que el tamaño del objetivo, la onda rebotará de forma similar a la luz reflejada por un espejo. Si la longitud de onda es mucho más larga que el tamaño del objetivo, el objetivo puede no ser visible debido a la mala reflexión. La tecnología de radar de baja frecuencia depende de las resonancias para la detección, pero no la identificación, de los objetivos. Esto se describe mediante la dispersión de Rayleigh, un efecto que crea el cielo azul de la Tierra y los atardeceres rojos. Cuando las dos escalas de longitud son comparables, puede haber resonancias. Los primeros radares usaban longitudes de onda muy largas que eran más grandes que los objetivos y recibían una señal vaga, mientras que muchos sistemas modernos usan longitudes de onda

más cortas (unos pocos centímetros o menos) que pueden captar objetos tan pequeños como una barra de pan.

Las ondas de radio cortas se reflejan desde curvas y esquinas de una manera similar al destello de una pieza de vidrio redondeada. Los objetivos más reflectantes para longitudes de onda cortas tienen ángulos de 90° entre las superficies reflectantes. Un reflector de esquina consiste en tres superficies planas que se encuentran como la esquina interior de una caja. La estructura reflejará las ondas que entran en su abertura directamente de regreso a la fuente. Se usan comúnmente como reflectores de radar para facilitar la detección de objetos difíciles de detectar. Los reflectores de esquina en barcos, por ejemplo, los hacen más detectables para evitar colisiones o durante un rescate.

3.1.3 Diseño

Un radar consta de los siguientes bloques lógicos:

- Un transmisor que genera las señales de radio por medio de un oscilador controlado por un modulador.
- Un receptor en el que los ecos recibidos se llevan a una frecuencia intermedia con un mezclador. No debe añadir ruido adicional.
- Un duplexor que permite usar la antena para transmitir o recibir.
- Hardware de control y de procesado de señal.
- Interfaz de usuario.

Oscilador

El núcleo del transmisor lo forma un dispositivo oscilador. La elección de este se realiza en virtud de las características que se requieren del sistema radar (coste, vida útil, potencia de pico, longitud de los pulsos, frecuencia, etc.) Los osciladores más utilizados son:

- Magnetrón: es el más utilizado a pesar de que se trata de una tecnología algo vieja. Son pequeños y ligeros. Pueden funcionar a frecuencias de entre 30 MHz y 100 GHz y proporcionan buena potencia de salida.
- Klistrón: algo más grandes que los anteriores, llegan a funcionar solamente hasta los 10 GHz. La potencia de salida que proporcionan puede quedarse corta en algunos casos.
- TWT (Tubo de ondas progresivas): para radares de 30 MHz a 15 GHz, buena potencia de salida.

Modulador

El modulador o pulsador es el elemento encargado de proporcionar pequeños pulsos de potencia al magnetrón. Esta tecnología recibe el nombre de "potencia pulsada". Gracias al modulador, los pulsos de RF que emite el oscilador están limitados a una duración fija. Estos dispositivos están formados por una fuente de alimentación de alto voltaje, una red de formación de pulsos (PFN) y un conmutador de alto voltaje (como un tiratrón). Si en lugar de magnetrón se usa

un tubo klistrón, este puede actuar como amplificador, así que la salida del modulador puede ser de baja potencia.

Diseño de la antena

Las señales de radio difundidas (broadcast) por una sola antena se propagan en todas las direcciones y, del mismo modo, una antena recibirá señales desde cualquier dirección. Esto hace que el radar se encuentre con el problema de saber dónde se ubica el blanco.

Los primeros sistemas solían utilizar antenas omnidireccionales, con antenas receptoras directivas apuntando en distintas direcciones. Por ejemplo, el primer sistema que se instaló (Chain Home) utilizaba dos antenas receptoras cuyas direcciones de observación formaban un ángulo recto, cada una asociada a una pantalla diferente. El mayor nivel de eco se obtenía cuando la dirección de observación de la antena y la línea radar-blanco formaban ángulo recto y, por el contrario, era mínimo cuando la antena apuntaba directamente hacia el objetivo.

Una importante limitación de este tipo de solución era que el pulso se transmitía en todas las direcciones, de modo que la cantidad de energía en la dirección que se examinaba era solo una pequeña parte de la transmitida. Para que llegue una potencia razonable al blanco se requieren antenas direccionales.

Figura 3.4 Radar de pistola para la medición de velocidad. **Fuente**: US Air Force

3.1.4 Clasificación

Se puede hacer una clasificación general de los radares en función de una serie de aspectos básicos:

Según el número de antenas

- Monoestático: una sola antena transmite y recibe.
- Biestático: una antena transmite y otra recibe, en un mismo o diferentes emplazamientos.
- Multiestático: combina la información recibida por varias antenas.

Según el blanco

- Radar primario: funciona con independencia del blanco, dependiendo solamente de la RCS del mismo.
- Radar secundario: el radar interroga al blanco, que responde, normalmente con una serie de datos (altura del avión, etc.). En el caso de vehículos militares, se incluye el identificador amigo-enemigo.

Según la forma de onda

- Radar de onda continua (CW): transmite ininterrumpidamente. El radar de la policía suele ser de onda continua y detecta velocidades gracias al efecto Doppler.
- Radar de onda continua con modulación (CW-FM, CW-PM): se le añade a la señal modulación de fase o frecuencia con objeto de determinar cuando se transmitió la señal correspondiente a un eco (permite estimar distancias).
- Radar de onda pulsada: es el funcionamiento habitual. Se transmite periódicamente un pulso, que puede estar modulado o no. Si aparecen ecos de pulsos anteriores al último transmitido, se interpretarán como pertenecientes a este último, de modo que aparecerán trazas de blancos inexistentes.

Según su finalidad

- Radar de seguimiento: es capaz de seguir el movimiento de un blanco. Por ejemplo, el radar de guía de misiles.
- Radar de búsqueda: explora todo el espacio, o un sector de él, mostrando todos los blancos que aparecen. Existen radares con capacidad de funcionar en ambos modos.

3.2 Redes Inalámbricas

3.2.1 Conceptos

Una red inalámbrica es una red informática que utiliza conexiones de datos inalámbricas entre nodos de red. La red inalámbrica es un método mediante el cual los hogares, las redes de telecomunicaciones y las instalaciones comerciales evitan el costoso proceso de introducir cables en un edificio o una conexión entre varias ubicaciones de equipos. Las redes de telecomunicaciones inalámbricas generalmente se implementan y administran mediante comunicación por radio. Esta implementación tiene lugar en el nivel o capa físico de la estructura de red del modelo OSI.

Los ejemplos de redes inalámbricas incluyen redes de teléfonos celulares, redes de área local inalámbricas (WLAN), redes de sensores inalámbricas, redes de comunicación por satélite y redes de microondas terrestres.

Por el otro lado, existen algunas cuestiones relacionadas con la regulación legal del espectro electromagnético. Las ondas electromagnéticas se transmiten a través de muchos dispositivos (de uso militar, científico y de aficionados), pero son propensos a las interferencias. Por esta razón, todos los países necesitan regulaciones que definan los rangos de frecuencia y la potencia de transmisión que se permite a cada categoría de uso.

Además, las ondas hertzianas no se confinan fácilmente a una superficie geográfica restringida. Por este motivo, un *hacker* puede, con facilidad, escuchar una red si los datos que se transmiten no están codificados. Por lo tanto, se deben tomar medidas para garantizar la privacidad de los datos que se transmiten a través de redes inalámbricas.

3.2.2 Tipos de Redes

3.2.2.1 Redes WAN (Wide Area Network)

Una red de área extensa (WAN) es una red de telecomunicaciones o una red de computadoras que se extiende a una gran distancia geográfica. Las redes de área amplia a menudo se establecen con circuitos de telecomunicación arrendados. Las entidades empresariales, educativas y gubernamentales utilizan redes de área amplia para transmitir datos al personal, estudiantes, clientes, compradores y proveedores de varios lugares en todo el mundo. En esencia, este modo de telecomunicación permite a una empresa llevar a cabo de

manera efectiva su función diaria independientemente de su ubicación. Internet puede considerarse una WAN.

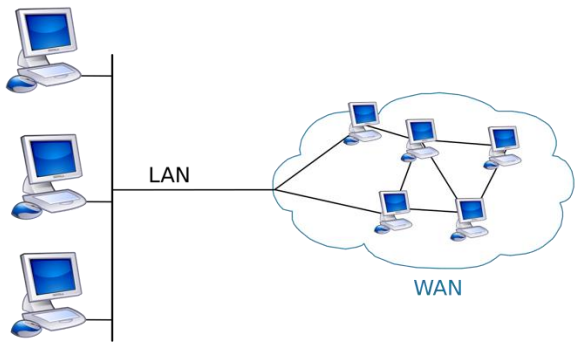

Figura 3.5 Interconexión entre la red de área local (LAN) y la red de área amplia (WAN) **Fuente:** Wikipedia

3.2.2.2 Redes MAN (Metropolitan Area Network)

Una red de área metropolitana (MAN) es una red informática que interconecta usuarios con recursos informáticos en un área geográfica o región mayor que la cubierta incluso por una gran red de área local (LAN) pero menor que el área cubierta por una red de área extensa (WAN) El término MAN se aplica a la interconexión de redes en una ciudad en una única red más grande que puede ofrecer también una conexión eficiente a una red de área amplia. También se usa para referirse a la interconexión de varias redes de área local en un área metropolitana mediante el uso de conexiones punto a punto entre ellas. Este último uso también se conoce como una red de campus.

3.2.2.3 Redes LAN (Local Area Network)

Una red de área local (LAN) es una red informática que interconecta las computadoras dentro de un área limitada, como una residencia, escuela, laboratorio, campus universitario o edificio de oficinas. Por el contrario, una red de área amplia (WAN) no solo cubre una distancia geográfica mayor, sino que también generalmente involucra circuitos de telecomunicación arrendados.

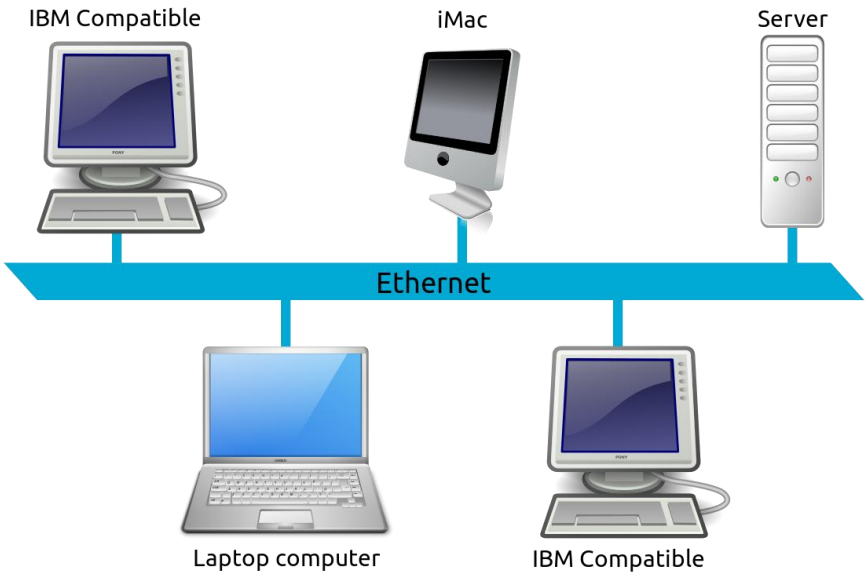

Figura 3.6 Un diagrama conceptual de una red de área local **Fuente:** Wikipedia

3.2.2.4 Redes NAN (Near-me Area Network)

Una red de área cercana a mí (NAN) es una red de comunicación que se enfoca en la comunicación inalámbrica entre dispositivos en las proximidades. A diferencia de las redes de área local (LAN), donde los dispositivos están en el mismo segmento de red y comparten el mismo dominio de difusión, los

dispositivos en una NAN pueden pertenecer a diferentes infraestructuras de red propietarias (por ejemplo, diferentes operadores de telefonía móvil). Si dos dispositivos están geográficamente cerca, la ruta de comunicación entre ellos podría, de hecho, atravesar una larga distancia, ir desde una LAN, a través de Internet y a otra LAN.

3.2.2.5 Redes PAN (Personal Area Network)

Una red de área personal (PAN) es una red informática utilizada para la transmisión de datos entre dispositivos tales como computadoras, teléfonos, tabletas y asistentes digitales personales. Los PAN pueden utilizarse para la comunicación entre los propios dispositivos personales o para conectarse a una red de nivel superior e Internet (un enlace ascendente) donde un dispositivo maestro asume el rol de puerta de enlace. Un PAN puede transportarse a través de buses de computadora cableados como USB.

Una red de área personal inalámbrica (WPAN) es un PAN de baja potencia que se transporta a través de una tecnología de red inalámbrica de corta distancia, como IrDA, USB inalámbrico, Bluetooth y ZigBee. El alcance de un WPAN varía de unos pocos centímetros a unos pocos metros.

3.2.3 Estándares de Redes Inalámbricas

3.2.3.1 IEEE 802.11a

IEEE 802.11a-1999 o 802.11a fue una enmienda a las especificaciones de red local inalámbrica IEEE 802.11 que definió los requisitos para un sistema de comunicación de multiplexación por división de frecuencia ortogonal (OFDM). Originalmente fue diseñado para admitir comunicaciones inalámbricas en las bandas de infraestructura de información nacional (U-NII) sin licencia (en el rango de frecuencias de 5-6 GHz) reguladas en los Estados Unidos por el Código de Regulaciones Federales, Título 47, Sección 15.407.

Originalmente descrito como la cláusula 17 de la especificación de 1999, ahora se define en la cláusula 18 de la especificación de 2012 y proporciona protocolos que permiten la transmisión y recepción de datos a velocidades de 1.5 a 54Mbit / s. Se ha visto una implementación mundial extendida, particularmente dentro del espacio de trabajo corporativo. Si bien la modificación original ya no es válida, los fabricantes de puntos de acceso inalámbrico (tarjetas y enrutadores) todavía usan el término "802.11a" para describir la interoperabilidad de sus sistemas a 5,8 GHz, 54 Mbit / s (54 x 106 bits por segundo).

3.2.3.2 IEEE 802.11b

IEEE 802.11b-1999 o 802.11b, es una enmienda a la especificación de red inalámbrica IEEE 802.11 que extiende el rendimiento de hasta 11 Mbit/s utilizando la misma banda de 2.4GHz. Se incorporó una enmienda relacionada en el estándar IEEE 802.11-2007.

802.11b tiene una velocidad de datos en bruto máxima de 11 Mbit/s y utiliza el mismo método de acceso a medios CSMA/CA definido en la norma original. Debido a la sobrecarga del protocolo CSMA/CA, en la práctica, el rendimiento máximo de 802.11b que puede alcanzar una aplicación es de aproximadamente 5,9 Mbit/s con TCP y 7,1 Mbit/s con UDP.

Los productos 802.11b aparecieron en el mercado a mediados de 1999, ya que 802.11b es una extensión directa de la técnica de modulación DSSS (espectro ensanchado de secuencia directa) definida en la norma original. El Apple iBook fue la primera computadora convencional vendida con una red 802.11b opcional. Técnicamente, el estándar 802.11b usa codificación de código complementario (CCK) como su técnica de modulación. El aumento dramático en el rendimiento de 802.11b (en comparación con el estándar original) junto con las reducciones de precio sustanciales simultáneas llevaron a la rápida aceptación de 802.11b como la tecnología de LAN inalámbrica definitiva.

3.2.3.3 IEEE 802.11g

IEEE 802.11g-2003 o 802.11g es el tercer estándar de modulación para LAN inalámbricas. Funciona en la banda de 2,4 GHz (como 802.11b) pero opera a una tasa máxima de datos brutos de 54 Mbit/s. Utilizando el esquema de transmisión CSMA/CA, 31,4 Mbit/s es el rendimiento neto máximo posible para paquetes de 1500 bytes de tamaño y una velocidad inalámbrica de 54 Mbit/s (idéntica al núcleo 802.11a, excepto por algunos gastos generales heredados adicionales para compatibilidad con versiones anteriores). En la práctica, los puntos de acceso pueden no tener una implementación ideal y, por lo tanto, no pueden alcanzar incluso un rendimiento de 31,4 Mbit/s con paquetes de 1500 bytes.

1500 bytes es el límite habitual para los paquetes en Internet y, por lo tanto, un tamaño relevante para comparar. Los paquetes más pequeños ofrecen un rendimiento teórico aún menor, hasta 3 Mbit/s con una velocidad de 54 Mbit/s y paquetes de 64 bytes. Además, el rendimiento disponible se comparte entre todas las estaciones que transmiten, incluido el AP, por lo que el tráfico descendente y ascendente está limitado a un total compartido de 31,4 Mbit/s utilizando paquetes de 1500 bytes y velocidad de 54 Mbit/s.

3.2.3.4 IEEE 802.11n

IEEE 802.11n-2009, comúnmente acortado a 802.11n, es un estándar de red inalámbrica que usa múltiples antenas para aumentar las velocidades de datos. A veces denominado MIMO, que significa "entrada múltiple y salida múltiple", es una enmienda al estándar de red inalámbrica IEEE 802.11-2007. Su objetivo es mejorar el rendimiento de la red en comparación con las dos normas anteriores, 802.11a y 802.11g, con un aumento significativo en la velocidad máxima de datos netos de 54 Mbit/s a 600 Mbit/s (tasa de bits bruta ligeramente más alta que incluye, por ejemplo, error códigos de corrección y rendimiento máximo ligeramente más bajo) con el uso de cuatro flujos espaciales a un ancho de canal de 40 MHz. Soporte estandarizado 802.11n para múltiples entradas de múltiples salidas, agregación de cuadros y mejoras de seguridad, entre otras características. Se puede usar en las bandas de frecuencia de 2,4 GHz o 5 GHz.

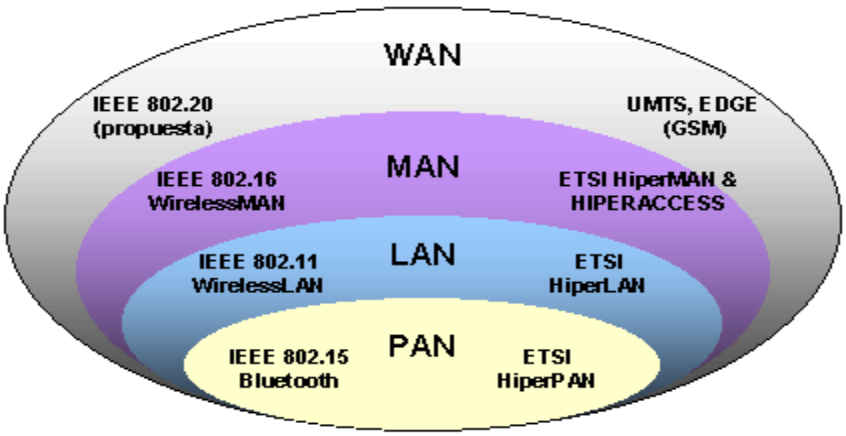

Figura 3.7 Cobertura y estándares. **Fuente**: Wikimedia

3.2.3.5 IEEE 802.11ac

IEEE 802.11ac es un estándar de red inalámbrica en la familia 802.11, que proporciona redes inalámbricas de área local de alto rendimiento (WLAN) en la banda de 5 GHz. El estándar se desarrolló a partir de 2008 (PAR aprobado el 26-09-2008) hasta 2013 y se publicó en diciembre de 2013 (aprobado por ANSI el 12-12-2013).

La especificación tiene un rendimiento de múltiples estaciones de al menos 1 gigabit por segundo y un rendimiento de enlace único de al menos 500 megabits por segundo (500 Mbit/s). Esto se logra ampliando los conceptos de la interfaz aérea incluidos en 802.11n: ancho de banda de RF más amplio (hasta 160 MHz), más flujos espaciales MIMO (hasta ocho), MIMO multiusuario de enlace descendente (hasta cuatro clientes) y alta velocidad. modulación de densidad (hasta 256-QAM).

Las mejoras de enlace único y multi-estación compatibles con 802.11ac permiten varios escenarios nuevos de uso de WLAN, como transmisión simultánea de video de alta definición a múltiples clientes en el hogar, sincronización rápida y respaldo de archivos de datos grandes, pantalla inalámbrica, gran campus / auditorio implementaciones y automatización de pisos de fabricación.

3.2.4 Protocolos de Seguridad de Redes Inalámbricas

3.2.4.1 WEP

Wired Equivalent Privacy (WEP) es un algoritmo de seguridad para redes inalámbricas IEEE 802.11. Introducido como parte del estándar 802.11 original ratificado en 1997, su intención era proporcionar confidencialidad de datos comparable a la de una red cableada tradicional. WEP, reconocible por su clave de 10 o 26 dígitos hexadecimales (40 o 104 bits), en un tiempo fue ampliamente utilizado y, a menudo, fue la primera opción de seguridad presentada a los usuarios por las herramientas de configuración del enrutador.

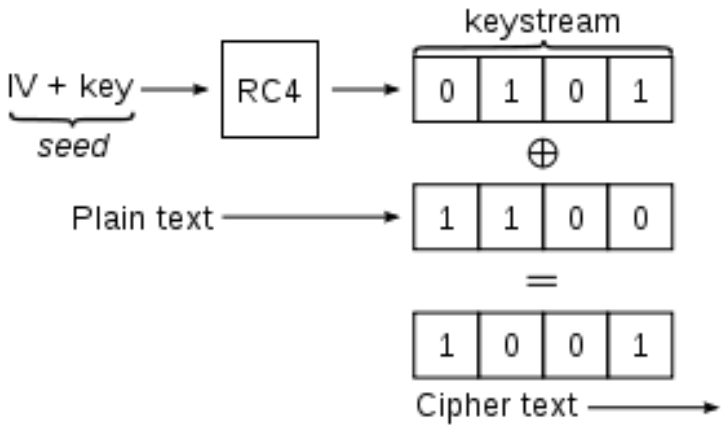

Figura 3.8 Cifrado WEP básico **Fuente**: Wikimedia

En 2003, Wi-Fi Alliance anunció que WEP había sido reemplazado por Wi-Fi Protected Access (WPA). En 2004, con la ratificación del estándar 802.11i completo (es decir, WPA2), el IEEE declaró que tanto WEP-40 como WEP-104

han quedado obsoletos. WEP era el único protocolo de cifrado disponible para dispositivos 802.11ay 802.11b construidos antes del estándar WPA, que estaba disponible para dispositivos 802.11g. Sin embargo, algunos dispositivos 802.11b recibieron actualizaciones de firmware o software para habilitar WPA, y los dispositivos más nuevos lo tenían incorporado.

3.2.4.2 WPA

Wi-Fi Protected Access (WPA) es un protocolo de seguridad y un programa de certificación de seguridad desarrollado por Wi-Fi Alliance para proteger las redes de computadoras inalámbricas. La Alianza los definió en respuesta a las serias deficiencias que los investigadores habían encontrado en el sistema anterior, Wired Equivalent Privacy (WEP). El método de cifrado de WPA es el Protocolo de Integridad de Clave Temporal (TKIP). TKIP incluye una función de mezcla por paquete, una verificación de integridad de mensaje, un vector de inicialización extendido y un mecanismo de reingreso. WPA proporciona autenticación de usuario sólida basada en 802.1xy el protocolo de autenticación extensible (EAP). WPA depende de un servidor de autenticación central, como RADIUS, para autenticar a cada usuario.

Las actualizaciones de software que permiten que las computadoras cliente y servidor implementen WPA se volvieron ampliamente disponibles durante 2003. Los puntos de acceso (consulte los puntos críticos) pueden operar en modo mixto WEP/WPA para admitir clientes WEP y WPA. Sin embargo, el modo mixto

proporciona de manera efectiva solo seguridad de nivel WEP para todos los usuarios. Los usuarios domésticos de puntos de acceso que usan solo WPA pueden operar en un modo de hogar especial en el cual el usuario solo necesita ingresar una contraseña para conectarse al punto de acceso. La contraseña activará la autenticación y el cifrado TKIP.

3.2.4.3 WPA2

WPA2, que requiere pruebas y certificación por Wi-Fi Alliance, implementa los elementos obligatorios de IEEE 802.11i. En particular, incluye soporte obligatorio para CCMP, un modo de cifrado basado en AES con una gran seguridad. La certificación comenzó en septiembre de 2004; desde el 13 de marzo de 2006, la certificación WPA2 es obligatoria para que todos los dispositivos nuevos lleven la marca de Wi-Fi. La WPA, desde 2006, ha sido reemplazada oficialmente por WPA2. Uno de los cambios más importantes entre WPA y WPA2 es el uso obligatorio de algoritmos AES y la introducción de CCMP (modo de contador de cifrado con protocolo de código de autenticación de mensaje de encadenamiento de bloque) como reemplazo de TKIP. Sin embargo, TKIP todavía se conserva en WPA2 como un sistema alternativo y para la interoperabilidad con WPA.

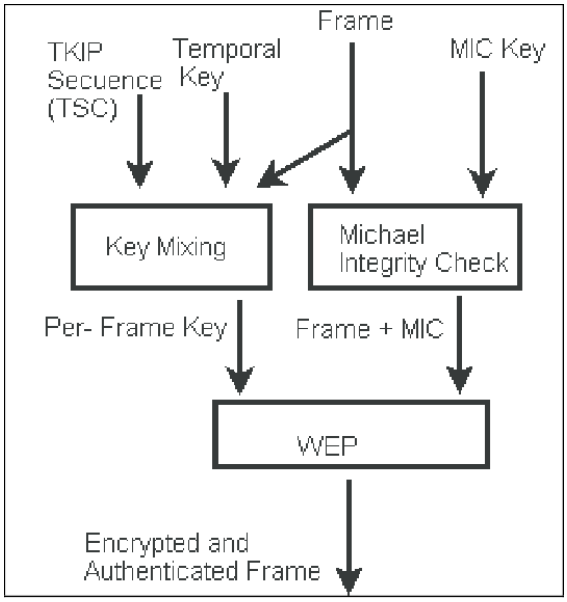

Figura 3.9 WI-FI Protected Access 2 (WPA-2) **Fuente**: Research Gate

Actualmente, la vulnerabilidad de seguridad primaria al sistema WPA2 real es oscura (y requiere que el atacante ya tenga acceso a la red Wi-Fi segura para obtener acceso a ciertas claves y luego perpetuar un ataque contra otros dispositivos en la red) Como tal, las implicaciones de seguridad de las vulnerabilidades conocidas de WPA2 están limitadas casi por completo a las redes de nivel empresarial y merecen poca o ninguna consideración práctica con respecto a la seguridad de la red doméstica.

3.2.3.4 WPA3

En octubre de 2017, los investigadores hicieron pública una vulnerabilidad grave en WPA2, el protocolo de seguridad que protege la mayoría de las redes WiFi

actuales. Este descubrimiento puso la seguridad del protocolo en el punto de mira y condujo a discusiones sobre la necesidad de un nuevo estándar.

Finalmente, WiFi Alliance, la organización que certifica los dispositivos WiFi, anunció WPA3, un protocolo de autenticación nuevo y mejorado que se lanzó en enero del 2018. Esta nueva versión no está destinada a mejorar la reputación de WPA2, ya que varios fabricantes están parcheando la vulnerabilidad revelada en sus actualizaciones. En cambio, busca implementar nuevas características y aumentar la seguridad de un protocolo que no se ha mejorado en los últimos 13 años.

Este nuevo protocolo busca traer mejoras en la autenticación y el cifrado al tiempo que facilita la configuración de redes inalámbricas. De manera crucial para mejorar el cifrado, el nuevo protocolo de seguridad contará con un cifrado de 192 bits. Aunque la Alianza no lo declaró explícitamente, es seguro asumir que, al igual que su predecesor y como se utiliza en WPA, WPA3 también usará un vector de inicialización de 48 bits. De esta forma, este nuevo protocolo cumple con los más altos estándares de seguridad y es apto para su uso en redes con los requisitos de seguridad más estrictos, como los de gobiernos, defensa o sistemas industriales.

Otra característica notable de WPA3 es la implementación del protocolo Dragonfly, también conocido como Autenticación Simultánea de Iguales (SAE). Esto tiene como objetivo mejorar la seguridad en el momento del handshake, que es cuando se intercambia la llave. Como resultado, WPA3 está preparado para proporcionar una seguridad robusta incluso si se usan contraseñas cortas o débiles, es decir, aquellas que no contienen una combinación de letras, números y símbolos.

3.2.3.5 EAP

El Protocolo de Autenticación Extensible, o EAP, es un marco de autenticación utilizado frecuentemente en redes inalámbricas y conexiones punto a punto. Se define en RFC 3748, que hizo que RFC 2284 sea obsoleto, y se actualiza mediante RFC 5247.

EAP es un marco de autenticación para proporcionar el transporte y el uso del material de claves y los parámetros generados por los métodos de EAP. Hay muchos métodos definidos por los RFC y una cantidad de métodos específicos del vendedor y existen nuevas propuestas. EAP no es un protocolo de conexión; en su lugar, solo define los formatos de mensaje. Cada protocolo que usa EAP define una forma de encapsular los mensajes EAP dentro de los mensajes de ese protocolo.

EAP está en uso amplio. Por ejemplo, en IEEE 802.11 (WiFi) los estándares WPA y WPA2 han adoptado IEEE 802.1X con cien tipos de EAP como mecanismos de autenticación oficiales.

EAP es un marco de autenticación, no un mecanismo de autenticación específico. Proporciona algunas funciones comunes y la negociación de métodos de autenticación llamados métodos EAP. Actualmente hay unos 40 métodos diferentes definidos. Los métodos definidos en IETF RFCs incluyen EAP-MD5, EAP-POTP, EAP-GTC, EAP-TLS, EAP-IKEv2, EAP-SIM, EAP-AKA y EAP-AKA '. Además, existe una cantidad de métodos específicos del vendedor y nuevas propuestas. Los métodos modernos comúnmente utilizados que pueden funcionar en redes inalámbricas incluyen EAP-TLS, EAP-SIM, EAP-AKA, LEAP y EAP-TTLS. Los requisitos para los métodos EAP utilizados en la autenticación de LAN inalámbrica se describen en RFC 4017. La lista de códigos de tipo y de paquetes utilizados en EAP está disponible en el Registro IAP EAP.

3.3 Tecnología Wimag

3.3.1 Definición

Wimag es un sistema de detección alternativo que usa pequeños magnetómetros a batería, integrados en la carretera superficie, para detectar vehículos y comunicar la detección eventos a un controlador de host, sin la necesidad de una amplia cableado o conductos. El sensor del magnetómetro es

un dispositivo equivalente a un bucle que utiliza perturbaciones en el campo magnético de la tierra para detectar

vehículos de paso y/o estacionarios. Simplemente se instala por 'coring' un agujero de diámetro apropiado en la calzada y fijación en el lugar con una resina epoxi dedicada compuesto. Los sensores tienen una conexión inalámbrica de baja potencia incorporada transmisor/receptor y una batería dedicada de larga duración para transmitir datos de detección a un punto de acceso asociado o reloj de repetición.

El punto de acceso es una puerta de enlace inalámbrica que mantiene enlaces inalámbricos bidireccionales a sensores y repetidores dentro de el sistema. El punto de acceso Siemens tiene un cable conexión ethernet para transmitir el sensor del magnetómetro datos de detección a un controlador de tráfico en la carretera a través de una tarjeta de interfaz. Se pueden usar múltiples puntos de acceso si necesario para proporcionar conectividad a muchos magnetómetros. Por lo general, los sensores deben ubicarse a unos 40m de un punto de acceso para garantizar que la conexión inalámbrica confiable la comunicación se mantiene en todo momento. Por aplicaciones donde se necesitan mayores distancias a repetidor puede ser utilizado. El repetidor puede usarse para ampliar la distancia que puede instalarse un magnetómetro desde un punto de acceso, hasta aproximadamente 300m.

Se pueden instalar dos repetidores que funcionan en tándem entre un sensor y punto de acceso para ampliar aún más el rango a aproximadamente 600m si es necesario.

3.3.2 Tipos de Wimag

Recopilación de datos de tráfico confiables en las intersecciones pide una tecnología diferente que monitorear la ocupación de HGV plazas de aparcamiento. Y detectando bicicleta el tráfico es algo totalmente diferente todavía. Dentro de la familia Sitraffic Wimag de detectores, encontrará el óptimo detector diseñado para cada uno de estos usos. Sitraffic Wimag VD, por ejemplo, es un detector de tráfico que proporciona información precisa datos de tráfico en movimiento como entrada para conmutación óptima de fase verde.

El nuevo Sitraffic Wimag PD es un estacionamiento detector que usa dos tecnologías diferentes para la detección confiable de autos, vehículos pesados y motocicletas estacionados en los espacios equipados con el sistema. Sitraffic Wimag MR es un "MicroRadar" especial versión capaz de detectar usuarios de carretera "pequeños" como los ciclistas, incluso aquellos que pedalean justo al borde del carril. Los tres tipos de detectores pueden integrarse en un solo sistema porque comparten la misma tecnología de transmisión, incluidos repetidores, estación base y dedicado software.

Sitraffic Wimag VD: campo magnético para la detección que asegura altas tasas de detección en el tráfico en movimiento. El uso de la tecnología de campo magnético hace que este detector de tráfico (VD) sea superior a la mayoría de otros tipos de detectores para esta aplicación. Como Sitraffic Wimag VD está integrado en el asfalto justo en el centro del carril, los vehículos pasan directamente sobre el sensor. Por lo tanto, es virtualmente imposible para que el sensor "pierda" un vehículo o "detectar" una inexistente. El detector también funciona sustancialmente mejor que detectores de techo convencionales cuando se trata de registrar las diferencias de tiempo entre vehículos individuales, incluso cuando los espacios de tiempo ocurren a distancias bastante grandes desde la línea de stop.

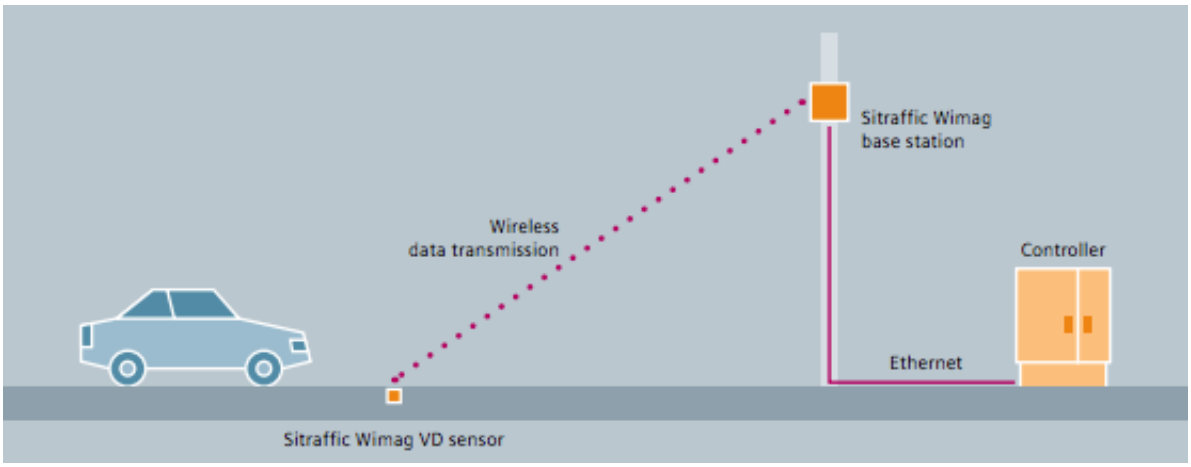

Figura 3.10 Funcionamiento del sensor Wimag VD **Fuente:** Siemens

Sitraffic Wimag MR: Con muchos tipos de detectores, la activación del mensaje de solicitud de fase verde en la línea de parada es cualquier cosa menos una cosa segura cuando el vehículo que se acerca es una bicicleta.

Porque muchos sistemas no pueden distinguir entre el carril bici y el general carril de tráfico al lado. Sin embargo, para Sitraffic Wimag MR esto es lo más fácil en el mundo. El detector usa MicroRadar (MR) la tecnología y su zona de detección puede ajustarse para extenderse exactamente hasta el borde del carril En caso de cambios en la disposición del carril, la zona del detector puede ser reajustado incluso después de la instalación del detector.

Sitraffic Wimag PD: Tecnología del campo magnético más MicroRadar para la detección rentable de vehículos estacionados. Una función que se ha usado durante mucho tiempo en aparcamientos ahora también es posible en espacios de estacionamiento al aire libre: estacionamiento individual monitoreo espacial Sitraffic Wimag PD es el costo efectivo y fácil de instalar solución para la detección confiable

de vehículos estacionados. El sensor está empotrado en la superficie de la carretera en frente o detrás del estacionamiento Como usa tanto la tecnología de campo magnético y MicroRadar, es capaz de identificar confiablemente el estado actual de ocupación en cualquier clima y en todas las estaciones. Como

para todos Sitraffic Wimag detector de tipos, instalación no requiere costoso y consume mucho tiempo

El cableado funciona porque los mensajes de estado se transmiten a través de la radio móvil. Sitraffic Wimag PD puede detectar automóviles, vehículos pesados y motocicletas.

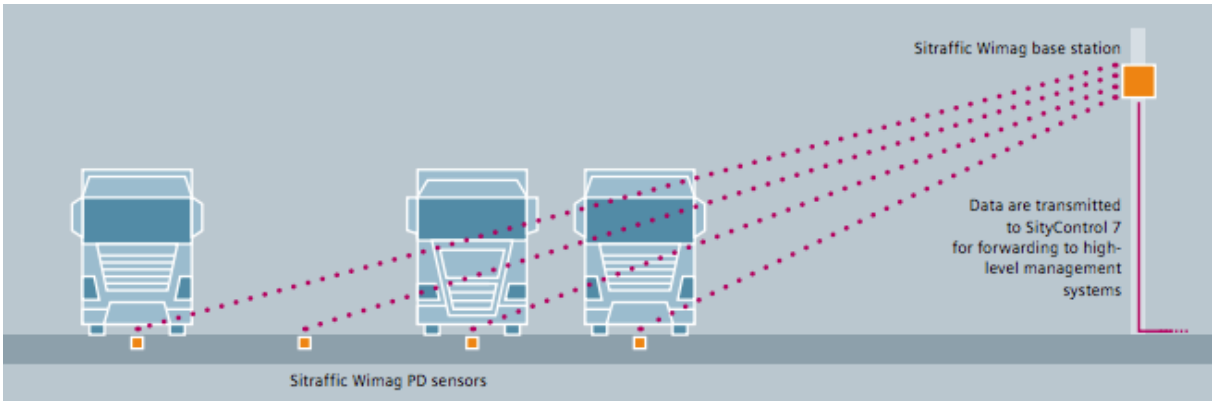

Figura 3.11 Funcionamiento del sensor Wimag PD **Fuente:** Siemens

Esto permite una cantidad de muy útil aplicaciones tales como:

• Reportar espacios de estacionamiento de vehículos pesados en las estaciones de descanso de la autopista al tráfico sistemas de gestión e información

• Detección del estado de ocupación de espacios de estacionamiento dentro y fuera de la calle.

• Monitorear áreas que no deben ser bloqueado por vehículos estacionados.

3.4 Seguridad en las Redes

3.4.1 Vulnerabilidades en una Red

Una vulnerabilidad es todo aquello que amenaza la estabilidad o la seguridad de algo pudiéndose considerar como un punto débil del sistema. Las vulnerabilidades son muy variadas y al igual que las amenazas poseen una clasificación de acuerdo con su origen.

Las amenazas pueden ser constantes y ocurrir en cualquier momento. Ya que todo sistema de información presenta un riesgo mínimo o relativamente grande; lo cual representa la probabilidad de que una amenaza se concrete por medio de una vulnerabilidad o punto débil.

Las Amenazas en redes se dividen en tres grandes grupos:
-Intencionales: son amenazas provocadas o deliberadas, como fraudes, vandalismo, sabotajes, espionaje, invasiones y ataques, robos y hurtos de información.

-Involuntarias: son amenazas causadas como resultantes de acciones inconscientes de usuarios, a través de software electrónico o fallos en el uso, muchas veces causadas por la falta de conocimiento de lo que se está manejando.

-Físicas: son aquellos presentes en los ambientes en los cuales la información se está manejando o almacenando físicamente, como ejemplos de este tipo de vulnerabilidad se distinguen en compartimiento de identificadores tales como nombre de usuario o credencial de acceso, etc.

Tipos de Vulnerabilidades:

-Naturales: son todas aquellas vulnerabilidades que están relacionados con las condiciones de la naturaleza ya que no es constante y pueden colaborar en riesgo la información. Estas amenazas naturales son principalmente determinante por la elección del lugar y montaje de un sistema, por lo cual se deberán tomar cuidados especiales con el local, como por ejemplo: Ambientes sin protección contra incendios prevención de los mismos, infraestructura incapaz de resistir a las manifestaciones de la naturaleza como terremotos, maremotos, huracanes, etc.

-Hardware: en este tipo de vulnerabilidad es causado por los posibles defectos de fabricación o configuración de los equipos que utilice un sistema, los cuales puedan permitir el ataque o alteración de estos. Por ello, la seguridad de la información busca evaluar: si el hardware utilizado está dimensionado correctamente para sus funciones. Si posee área de almacenamiento suficiente, procesamiento y velocidad adecuados. Elementos que pueden causar el mal Funcionamiento del Equipo Hardware:

La ausencia de actualizaciones conforme con las orientaciones de los fabricantes de programas y hardware que se utiliza, conservación inadecuada de los equipos, la falta de configuración de respaldo, equipos de contingencia, baja calidad de los elementos electrónicos utilizados, etc.

-Almacenamiento: los medios de almacenamiento son principalmente los soportes físicos o magnéticos que se utilizan para almacenar la información. Si los soportes que almacenan información, no se utilizan de forma adecuada, el contenido en los mismos podrá estar vulnerable a una serie de factores que podrán afectar la integridad, disponibilidad y confidencialidad de la información.

-Comunicación: la información se puede transmitir por distintos medios físicos, ya sea vía cable, satélite, fibra óptica u ondas de radio, para ello y por ello debe existir seguridad. El éxito en el tránsito de los datos es un aspecto crucial en la implementación de la seguridad de la información. En un sistema como por ejemplo una empresa, puede haber un gran intercambio de datos a través de medios de comunicación que rompen barreras físicas tales como teléfono, Internet, WAP, fax, télex etc.

Siendo estos medios considerados los más vulnerables en la comunicación de la información, por lo que deberán recibir tratamiento de seguridad adecuado con el propósito de evitar que: Cualquier falla en la comunicación haga que una

información quede no disponible para sus usuarios, o por el contrario, estar disponible para quien no posee derechos de acceso.

La ausencia de sistemas de encriptación en las comunicaciones que pudieran permitir que personas ajenas a la organización obtengan información privilegiada.

La mala elección de sistemas de comunicación para envío de mensajes de alta prioridad de la empresa puede provocar que no se alcanzará el destino esperado o bien se interceptó el mensaje en su tránsito.

-Humanas: este tipo de vulnerabilidad está relacionada con los daños que las personas pueden causar a la información y al ambiente tecnológico que la soporta. Este tipo de vulnerabilidades de tipo humana pueden ser intencionales o no.

La mayor vulnerabilidad es el desconocimiento de las medidas de seguridad adecuadas para ser adoptadas por cada elemento constituyente, principalmente los miembros internos de una empresa.

Entre los puntos débiles humanos por su grado de frecuencia están: la falta de capacitación específica para la ejecución de las actividades o funciones de cada uno y la falta de conciencia de seguridad para las actividades de rutina, los errores, omisiones, insatisfacciones etc, de origen externo tenemos vandalismo, fraude, extorsión, invasiones, etc.

-Software: considerados como puntos débiles en aplicaciones o programas que permiten que ocurran accesos indebidos a sistemas informáticos incluso y normalmente sin el conocimiento de un usuario o administrador de red. Una de las causas principales de este tipo de vulnerabilidad es la descarga de programas de sitios no confiables, configuración e instalaciones indebidas de estos u otros programas no testados en un PC, que podrán llevar al uso abusivo de los recursos por parte de usuarios malintencionados. A veces la libertad de uso implica el aumento del riesgo.

Un ejemplo son las aplicaciones que realizan la lectura de información y que permiten el acceso de los usuarios a dichos datos en medio electrónico y, por esta razón, se convierten en el objetivo predilecto de agentes causantes de amenazas, como por ejemplo:

- Programas lectores de e-mail que permiten la ejecución de códigos maliciosos.
- Editores de texto que permiten la ejecución de virus de macro etc.
- Programas para la automatización de procesos
- Los sistemas operativos conectados a una red.
- Falta de uso de criptografía en la comunicación.

3.4.2 Métodos de Control

La seguridad informática suele dividirse en tres categorías importantes, comúnmente conocidas como controles:

- Físicos
- Técnicos
- Administrativos

Estas tres categorías definen los objetivos principales de una implementación correcta de seguridad. Dentro de dichos controles existen las sub-categorías que más adelante describen los controles y su implementación.

-Controles físicos: control físico es la implementación de medidas de seguridad en una estructura definida utilizada para impedir el acceso no autorizado a material confidencial. A continuación, ejemplos de controles físicos:

- Vigilancia de cámaras de circuito cerrado
- Sistemas de alarma térmica o de movimiento
- Guardias de seguridad
- ID de retratos
- Puertas de acero cerradas y cerrojos de seguridad con punto muerto
- Biometría (incluye huellas digitales, voz, cara, iris, tipo de letra y otros métodos usados de identificación)

-Controles técnicos: los controles técnicos usan tecnología como base para controlar el acceso y uso de datos confidenciales a través de la estructura física y la red. Los controles técnicos son de gran alcance y abarcan tecnologías tales como:

- Cifrado
- Tarjetas inteligentes
- Autenticidad de redes
- Listas de control de acceso (ACL)
- Software de auditoría de integridad de archivos

-Controles administrativos: los controles administrativos definen los factores de seguridad humanos. Dichos controles involucran a todos los niveles de personal de una organización y determinan qué usuarios tienen acceso a los recursos e información por medios tales como:

- Formación y reconocimiento
- Preparación para desastres y planes de recuperación
- Reclutamiento de personal y estrategias de separación
- Registro de personal y contabilidad

3.4.3. Firewalls

La protección de seguridad comúnmente se considera más un proceso que un producto. Sin embargo, las implementaciones de seguridad estándar suelen emplear alguna forma de mecanismo dedicado para controlar privilegios de acceso y restringir recursos de redes a usuarios autorizados, identificables y rastreables.

Los cortafuegos son uno de los componentes de implementación de seguridad de redes. Varios proveedores ponen a disposición soluciones de cortafuegos para todos los niveles del mercado: desde los usuarios de hogares para proteger un computador personal hasta soluciones de centros de datos que protegen información vital empresarial. Los cortafuegos pueden ser soluciones de hardware autónomas tales como dispositivos de cortafuegos de Cisco, Nokia, y Sonicwall. Los proveedores tales como Checkpoint, McAfee, y Symantec también han desarrollado cortafuegos de software de propietario para hogares y mercados comerciales.

Se pueden crear reglas más elaboradas para controlar el acceso a subredes específicas o incluso nodos específicos, dentro de una LAN. También puede restringir el contacto a su servidor de algunas aplicaciones dudosas o programas tales como troyanos, worms u otros virus de cliente y servidor. Por ejemplo, algunos troyanos escanean redes de servicios en puertos de 31337 a 31340 (llamados los puertos elite en terminología de ciberpiratas).

Puesto que no hay servicios ilegítimos que se comuniquen a través de estos puertos no estándar, el bloquearlos puede disminuir efectivamente las posibilidades de que nodos infectados en su red se comuniquen de forma independiente con sus servidores maestros remotos.

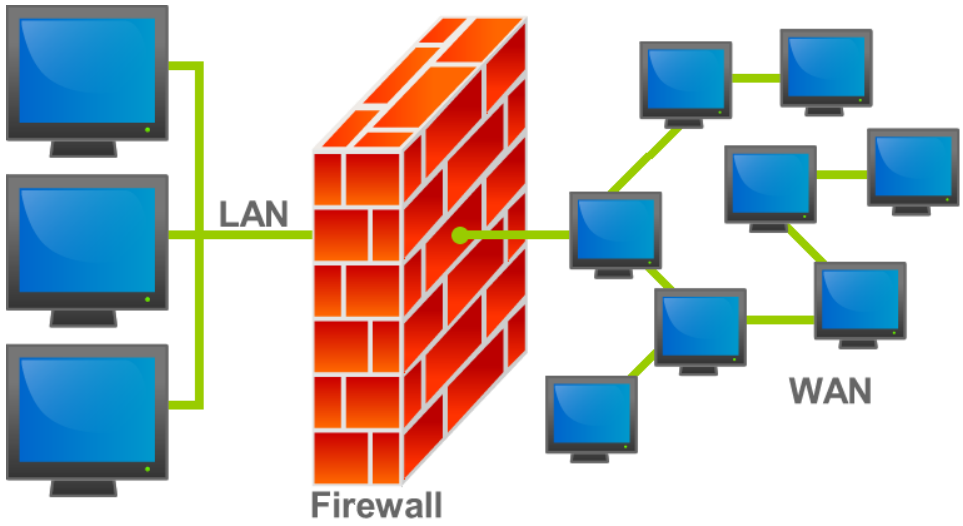

Figura 3.12 Ilustración de dónde se ubicaría un cortafuegos en una red **Fuente**: Wikimedia

También puede bloquear conexiones externas que intenten suplantar rangos de direcciones IP privadas para infiltrar su LAN.

Por ejemplo, si su LAN usa el rango 192.168.1.0/24, usted puede diseñar una regla que instruya al dispositivo de red de Internet (por ejemplo, eth0) para que descargue los paquetes a ese dispositivo con una dirección en su rango IP de LAN.

Puesto que, como política predeterminada, se recomienda rechazar los paquetes reenviados, cualquier otra dirección IP engañosa para el dispositivo externo (eth0) es rechazada automáticamente.

3.4.4 Tipos de Virus

Un virus es un software que tiene por objetivo de alterar el funcionamiento normal de cualquier tipo de dispositivo informático, sin el permiso o el conocimiento del usuario, principalmente para lograr fines maliciosos sobre el dispositivo. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en una computadora, aunque también existen otros más inofensivos, que solo producen molestias.

Existen diversos tipos de virus, varían según su función o la manera en que este se ejecuta en nuestra computadora alterando la actividad de la misma, entre los más comunes están:

- **Recycler:** Consiste en crear un acceso directo de un programa y eliminar su aplicación original, además al infectar un pendrive convierte a toda la información en acceso directo y oculta el original de modo que los archivos no puedan ser vistos, pero con la creación de un archivo batch que modifique los atributos de los archivos contenidos en el pendrive, estos podrían ser recuperados.

- **Troyano:** Consiste en robar información o alterar el sistema del hardware o en un caso extremo permite que un usuario externo pueda controlar el equipo.
- **Bombas lógicas o de tiempo**: Son programas que se activan al producirse un acontecimiento determinado. La condición suele ser una fecha (bombas de tiempo), una combinación de teclas, o ciertas condiciones técnicas (bombas lógicas). Si no se produce la condición permanece oculto al usuario.
- **Gusano**: Tiene la propiedad de duplicarse a sí mismo.
- **Hoax**: Los hoax no son virus ni tienen capacidad de reproducirse por sí solos. Son mensajes de contenido falso que incitan al usuario a hacer copias y enviarla a sus contactos. Suelen apelar a los sentimientos morales («Ayuda a un niño enfermo de cáncer») o al espíritu de solidaridad («Aviso de un nuevo virus peligrosísimo») y, en cualquier caso, tratan de aprovecharse de la falta de experiencia de los internautas novatos.
- **Joke**: Al igual que los hoax, no son virus, pero son molestos, un ejemplo: una página pornográfica que se mueve de un lado a otro, y si se le llega a dar a cerrar es posible que salga una ventana que diga error.

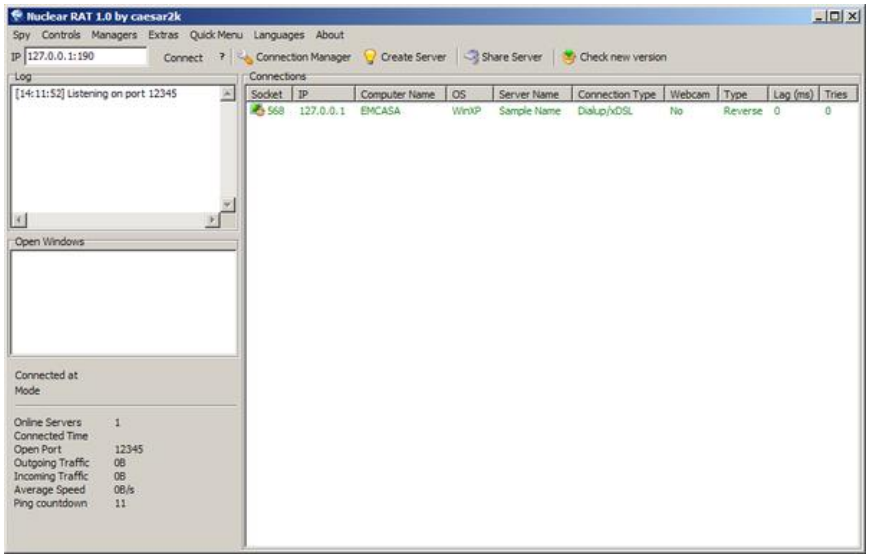

Figura 3.13 Captura de pantalla del troyano Nuclear RAT **Fuente**: Trojaniest

Otros tipos por distintas características son los que se relacionan a continuación:

Virus residentes:

La característica principal de estos virus es que se ocultan en la memoria RAM de forma permanente o residente. De este modo, pueden controlar e interceptar todas las operaciones llevadas a cabo por el sistema operativo, infectando todos aquellos ficheros y/o programas que sean ejecutados, abiertos, cerrados, renombrados, copiados. Algunos ejemplos de este tipo de virus son: Randex, CMJ, Meve, MrKlunky.

Virus de acción directa:

Al contrario que los residentes, estos virus no permanecen en memoria. Por tanto, su objetivo prioritario es reproducirse y actuar en el mismo momento de ser ejecutados. Al cumplirse una determinada condición, se activan y buscan los ficheros ubicados dentro de su mismo directorio para contagiarlos.

Virus de sobreescritura:

Estos virus se caracterizan por destruir la información contenida en los ficheros que infectan. Cuando infectan un fichero, escriben dentro de su contenido, haciendo que queden total o parcialmente inservibles.

Virus de boot (bot_kill) o de arranque:

Los términos boot o sector de arranque hacen referencia a una sección muy importante de un disco o unidad de almacenamiento CD, DVD, memorias USB, etc. En ella se guarda la información esencial sobre las características del disco y se encuentra un programa que permite arrancar el ordenador. Este tipo de virus no infecta ficheros, sino los discos que los contienen. Actúan infectando en primer lugar el sector de arranque de los dispositivos de almacenamiento. Cuando un ordenador se pone en marcha con un dispositivo de almacenamiento, el virus de boot infectará a su vez el disco duro.

Los virus de boot no pueden afectar al ordenador mientras no se intente poner en marcha a este último con un disco infectado. Por tanto, el mejor modo de

defenderse contra ellos es proteger los dispositivos de almacenamiento contra escritura y no arrancar nunca el ordenador con uno de estos dispositivos desconocido en el ordenador.

Virus de enlace o directorio:

Los ficheros se ubican en determinadas direcciones (compuestas básicamente por unidad de disco y directorio), que el sistema operativo conoce para poder localizarlos y trabajar con ellos.

Los virus de enlace o directorio alteran las direcciones que indican donde se almacenan los ficheros. De este modo, al intentar ejecutar un programa (fichero con extensión EXE o COM) infectado por un virus de enlace, lo que se hace en realidad es ejecutar el virus, ya que éste habrá modificado la dirección donde se encontraba originalmente el programa, colocándose en su lugar.
Una vez producida la infección, resulta imposible localizar y trabajar con los ficheros originales.

Virus cifrados:

Más que un tipo de virus se trata de una técnica utilizada por algunos de ellos, que a su vez pueden pertenecer a otras clasificaciones. Estos virus se cifran a sí mismos para no ser detectados por los programas antivirus. Para realizar sus actividades, el virus se descifra a sí mismo y, cuando ha finalizado, se vuelve a cifrar.

Virus polimórficos:

Son virus que en cada infección que realizan se cifran de una forma distinta (utilizando diferentes algoritmos y claves de cifrado). De esta forma, generan una elevada cantidad de copias de sí mismos e impiden que los antivirus los localicen a través de la búsqueda de cadenas o firmas, por lo que suelen ser los virus más costosos de detectar.

Virus multipartitos:

Virus muy avanzados, que pueden realizar múltiples infecciones, combinando diferentes técnicas para ello. Su objetivo es cualquier elemento que pueda ser infectado: archivos, programas, macros, discos, etc.

Virus del fichero:

Infectan programas o ficheros ejecutables (ficheros con extensiones EXE y COM). Al ejecutarse el programa infectado, el virus se activa, produciendo varios efectos.

Virus de FAT:

La tabla de asignación de ficheros o FAT (del inglés File Allocation Table) es la sección de un disco utilizado para enlazar la información contenida en éste. Se trata de un elemento fundamental en el sistema. Los virus que atacan a este elemento son especialmente peligrosos, ya que impedirán el acceso a ciertas

partes del disco, donde se almacenan los ficheros críticos para el normal funcionamiento del ordenador.

Virus hijackers:

Son programas que secuestran navegadores de internet principalmente el explorer. Los hijackers alteran las páginas iniciales del navegador e impide que el usuario pueda cambiarla, muestra publicidad en pops ups. Instala nuevas herramientas en la barra del navegador y a veces impiden al usuario acceder a ciertas páginas web. Un ejemplo puede ser no poder acceder a una página de antivirus.

Virus Zombie:

Son programas que secuestran computadoras de forma que es controlada por terceros. Se utiliza para diseminar virus, keyloggers y procedimientos invasivos en general. Esto puede ocurrir cuando la computadora tiene el firewall y su sistema operativo desactualizado.

Virus Keylogger:

Este virus se encarga de registrar cada tecla que sea pulsada, en algunos casos también registran los clics. Son virus que quedan escondidos en el sistema operativo de manera que la víctima no tiene cómo saber que está siendo monitorizada. Los keyloggers se utilizan usualmente para robar contraseñas de

cuentas bancarias, obtener contraseñas personales como las del E-mail, Facebook, etc.

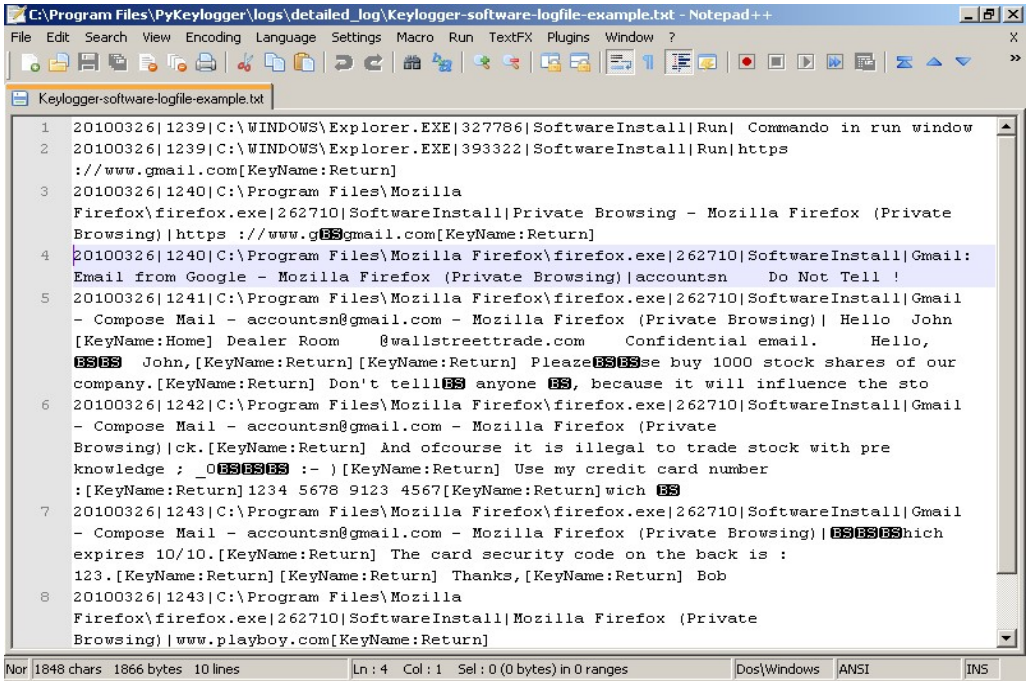

Figura 3.14 Un archivo de registro de un keylogger basado en software **Fuente**: PyKeylogger

3.4.5 Cifrados

En criptografía, el cifrado es un procedimiento que utiliza un algoritmo de cifrado con cierta clave (clave de cifrado) para transformar un mensaje, sin atender a su estructura lingüística o significado, de tal forma que sea incomprensible o, al menos, difícil de comprender a toda persona que no tenga la clave secreta (clave de descifrado) del algoritmo. Las claves de cifrado y de descifrado pueden ser iguales (criptografía simétrica), distintas (criptografía asimétrica) o de ambos tipos (criptografía híbrida).

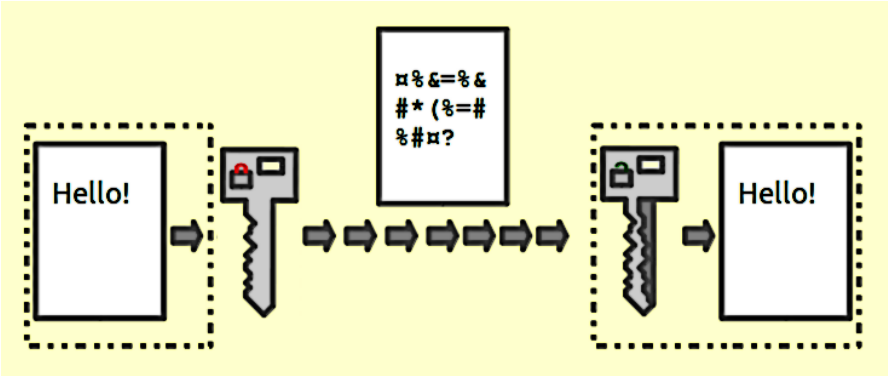

Figura 3.15 Ilustración de cómo se usa el cifrado dentro de los servidores **Fuente**: Johannes Landin

Hay dos tipos principales de datos que deben estar protegidos: los datos quietos y los datos en movimiento. Estos dos tipos de datos están protegidos en formas similares mediante una tecnología similar, aunque la implementación puede ser completamente diferente. Ninguna implementación protectora puede evitar todos los métodos posibles de compromiso ya que la misma información puede estar quieta o en movimiento en diferentes momentos.

Datos quietos:

Datos quietos son los datos almacenados en el disco duro, cinta, CD, DVD, disco, u otro medio. La mayor amenaza informática surge del robo físico. Portátiles en aeropuertos, CD que se envían por correo y cintas de seguridad que se dejan en lugares errados son todos los ejemplos de eventos en los que los datos pueden verse comprometidos por robo. Si los datos estaban cifrados en los medios entonces no habría por qué preocuparse tanto de que la información pueda comprometerse.

Datos en movimiento:

Los datos en movimiento son los datos que se están transmitiendo en la red. La mayor amenaza para los datos en movimiento es la interceptación y su alteración. Su nombre de usuario y contraseña nunca se deben transmitir por la red sin protección, ya que puede ser interceptada y utilizada por alguien que se haga pasar por usted o pueda acceder a información confidencial. La información privada como la información de una cuenta bancaria se debe también proteger cuando se transmite por la red. Si la sesión de la red estaba cifrada entonces no tendrá que preocuparse tanto sobre que los datos se hayan visto comprometidos cuando se transmitían.

Los datos en movimiento son particularmente vulnerables porque el atacante no tiene que estar cerca del computador en el cual están los datos que se están almacenando, solamente necesita estar en alguna parte de la ruta. Los túneles de cifrado pueden proteger los datos junto con la ruta de comunicaciones.

Las Redes virtuales privadas (VPN) proporcionan túneles cifrados entre computadores y redes de computadores a través de todos los puertos. Con VPN en su sitio, todo el tráfico de redes desde el cliente es reenviado al servidor a través del túnel cifrado. Es decir, que el cliente está lógicamente en la misma red a la que el servidor está conectado vía VPN. Las VPN son muy comunes, fáciles de usar y de configurar.

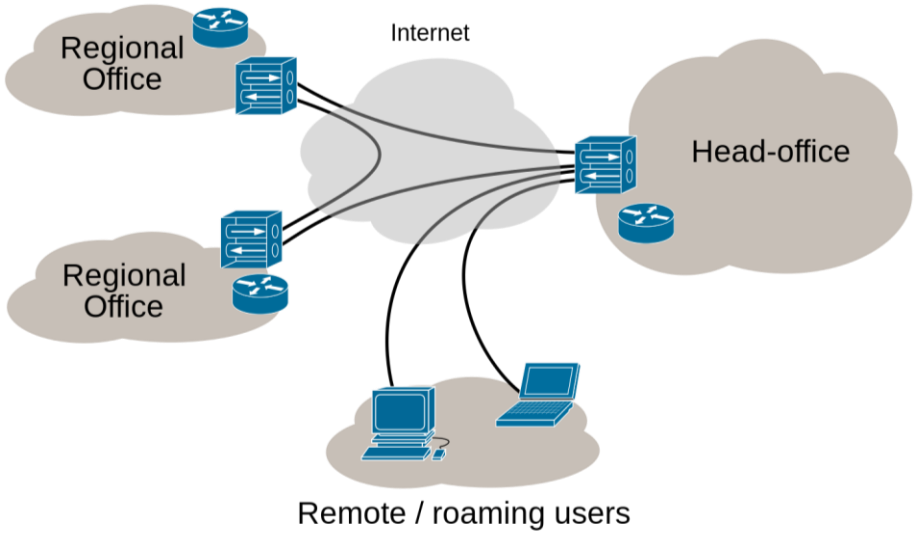

Figura 3.16 Descripción general de conectividad VPN **Fuente**: Ludovic Ferre

Shell segura (SSH) es un protocolo de redes poderoso que sirve para comunicarse con otro sistema en un canal seguro. Las transmisiones mediante SSH están cifradas y protegidas de interceptaciones. El registro criptográfico también puede utilizarse para proporcionar un mejor método de autenticación que los nombres de usuarios y contraseñas tradicionales.

SSH es muy fácil de activar. Simplemente inicie el servicio sshd y el sistema comenzará a aceptar conexiones cuando se proporcione un nombre de usuario y contraseña correctos durante el proceso de conexión. El puerto TCP estándar para el servicio SSH es 22, sin embargo puede cambiarse si modifica el archivo de configuración /etc/ssh/sshd_config y reinicia el servicio. Este archivo contiene otras opciones de configuración para SSH.

La shell segura (SSH) también proporciona túneles cifrados entre computadores pero solo mediante un puerto único. El reenvío de puerto puede hacerse en un túnel SSHy el tráfico será cifrado cuando pase por ese túnel aunque mediante reenvío de puerto no es tan fluido como un VPN.

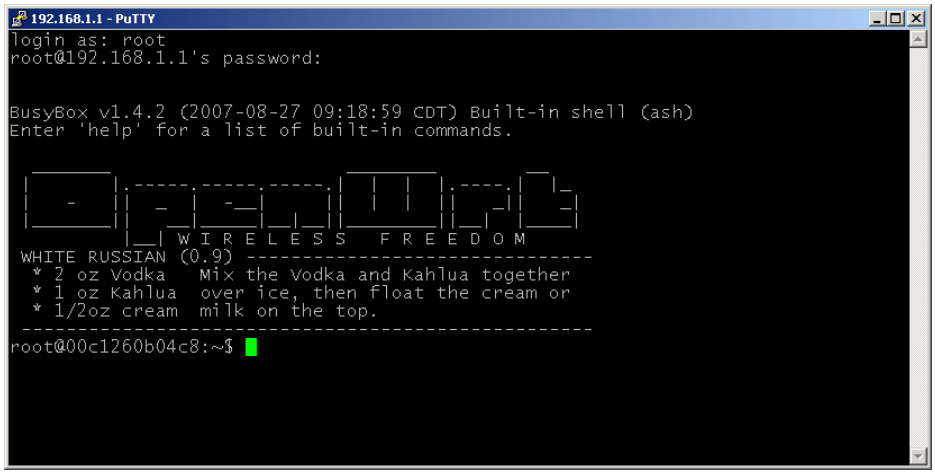

Figura 3.17 Iniciando sesión en OpenWrt a través de SSH usando PuTTY corriendo en Windows. **Fuente**: Wikimedia

CAPÍTULO IV.

PROPUESTA DE UN SISTEMA DE GESTIÓN DE PARQUEOS EN ÁGORA MALL

4.1 Situación actual de la empresa

El centro comercial Ágora Mall está ubicado en la intersección de las avenidas Abraham Lincoln con John F. Kennedy en la ciudad de Santo Domingo, Distrito Nacional, capital de la República Dominicana.

La obra de Ágora Mall es una estructura de hormigón armado de 130,000 m2 de construcción, dividida en tres edificios separados por juntas de construcción y consta de un edificio de estacionamiento de once niveles (tres soterrados).

Figura 4.1 Vista del Mapa Ágora Mall. **Fuente:** Google Maps

Ágora Mall dispone de un total de 1,800 estacionamientos (1,100 soterrados; 700 en torre) con accesos directos a cada uno de sus niveles. Los visitantes acceden a más de 180 establecimientos comerciales a través de 10 ascensores y 20 escaleras eléctricas.

Figura 4.2 Vista aérea entre la intersección Av. Abraham Lincoln y Av. John F. Kennedy. **Fuente:** IDA.do

Por su ubicación Ágora Mall posee un gran flujo de visitas, dicha cantidad se ve incrementado en temporadas especiales o fechas específicas como son Día de las Madres, Black Friday y/o Navidad. Debido al aumento de los visitantes en estas fechas han tenido que disponer de los parqueos de la Dirección General de Aduanas (DGA) ubicados en la Av. Abraham Lincoln al lado del centro comercial. Además de los parqueos del Centro de Atención Empresarial de Claro en la Av. John F. Kennedy con transporte incluido sin ningún costo.

El sistema de parqueo que poseen actualmente, esta basado en sensores instalados por medio de cableado, los cuales conectados a una central, actualizan una seria de señalizaciones instaladas en el primer nivel, las cuales informan o señalan a los visitantes al momento de llegar a la plaza la disponibilidad existente por niveles.

Niveles	Parqueos	Reservados
Sótano 1	360	8
Sótano 2	360	6
Sótano 3	360	6
Nivel 1	0	0
Nivel 1M	62	8
Nivel 2	66	4
Nivel 2M	62	8
Nivel 3	66	4
Nivel 3M	62	8
Nivel 4	66	4
Nivel 4M	62	8
Nivel 5	130	10

Tabla 4.1 Distribución de parqueos por niveles. **Fuente**: Autores

4.2 Propuesta de un sistema de gestión de parqueos en Ágora Mall

La propuesta de un sistema para el control de disponibilidad de los estacionamientos mediante el uso de tecnología de redes inalámbricas y radares tiene como finalidad o propósito el de reducir de manera significativa los problemas de duración para obtener un espacio disponible en los estacionamientos de los centros comerciales de la ciudad de Santo Domingo. Dicho problema no solo afecta el tránsito dentro de los estacionamientos de los centros comerciales sino que también las calles o avenidas que dan accesos a estos, debido a que llega un punto en el que la fila de vehículo por espera de disponibilidad se acumula hasta salir del centro comercial sobre todo en horas pico.

Figura 4.3 Horarios y vías de accesos a Ágora Mall. **Fuente:** myguidedominicanrepublic.com

El uso de esta tecnología de redes inalámbricas junto al sistema a desarrollar representa una solución tanto para estacionamientos techados como también para aquellos que se encuentran en espacios abiertos, ya que con el uso de herramientas inalámbricas no estaríamos limitados a los problemas que pueden ser presentados cuando no sea posible la instalación de una estructura cableada por limitaciones del área.

La propuesta está basada en un sistema el cual consta de un diseño de red inalámbrica la cual está compuesta de radares y puntos de accesos (Access Point) desarrollados por Siemens los cuales ofrecen la detección confiable de vehículos sin la necesidad de conductos extensos. Estos utilizan magnetómetros pequeños alimentados por batería, incrustados en la superficie del pavimento, para detectar vehículos y comunicar eventos de detección a un controlador de host. El sensor del magnetómetro es un dispositivo equivalente a un bucle que utiliza perturbaciones en el campo magnético de la tierra para detectar vehículos que pasan y/o se estacionan.

Toda la información es almacenada en un servidor el cual tendrá un servicio web (Web Service) tipo REST el cual será consumido tanto por la aplicación móvil como también la aplicación web para la actualización de las mismas.

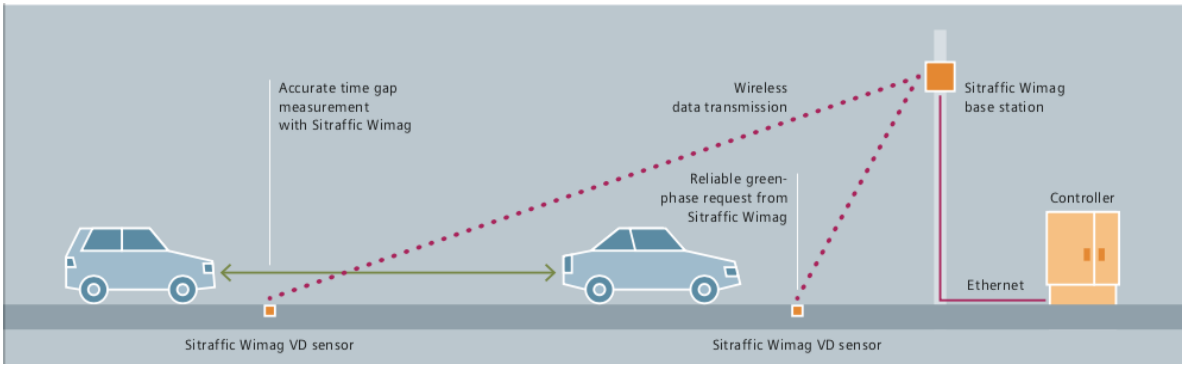

Figura 4.4 Los sensores permiten medir la distancia entre los vehículos **Fuente**: Siemens

Los sensores tienen un transmisor/receptor inalámbrico de baja potencia incorporado y una batería dedicada de larga duración para transmitir datos de detección a un punto de acceso o repetidor asociado. El punto de acceso es una puerta de enlace inalámbrica que mantiene enlaces inalámbricos bidireccionales a sensores y repetidores dentro del sistema. El punto de acceso de Siemens tiene una conexión de Ethernet con cable para transmitir los datos de detección del sensor del magnetómetro a un controlador de tráfico en el camino a través de una tarjeta de interfaz. Se pueden usar múltiples puntos de acceso si es necesario para proporcionar conectividad a muchos magnetómetros.

El atractivo de esta propuesta es que a diferencia del sistema que se utiliza actualmente, este nuevo les facilitará a los usuarios o visitantes información no importando el lugar en donde se encuentre ya sea lugar de trabajo, casa, universidad o incluso en las calles.

4.3 Diseño del sistema de control de parqueos

4.3.1 Definición del Funcionamiento

El usuario contará con dos aplicaciones por la cual podrá consultar la disponibilidad de los parqueos de los centros comerciales, por medio de una pagina web, así también como un aplicativo instalado en su dispositivo móvil.

Esta aplicación le permitirá ver en tiempo real el estado actual de los cupos en los distintos estacionamientos. Cuales están libres, ocupado, reservados y un tiempo promedio de espera. Al poseer esta información al usuario se le permite poder tomar una decisión previa y así poder evitar largas horas de espera y ahorro de combustible.

Para la detección se estará utilizando tecnología inalámbrica y sensores de radar desarrollados por Siemens. Los componentes que no son necesarios no implicarán ni instalación ni mantenimiento esfuerzos y costos. Con estos equipos, no se requiere trabajo de cableado porque la operación del detector es completamente inalámbrica. El dispositivo posee dimensiones notablemente compactas (7,5 × 7,5 × 5,0 cm) lo que permiten una instalación rápida. Otra ventaja es la total libertad en la elección de la posición del sensor: se puede instalar a cualquier distancia del controlador de intersección y en cualquier tipo de pavimento. El sitio puede ser seleccionado basado puramente en criterios de ingeniería de tráfico, sin restricciones por consideraciones de costo.

Figura 4.5 Componentes y proceso de instalación de los sensores. **Fuente:** Siemens

Los sensores pueden establecer su rango es decir puede detectar con precisión diferentes alturas y tipos de vehículos. Al momento de que un vehículo es estacionado la estación base deja de recibir la señal emitida por el sensor colocado en el pavimento, la estación a su vez procesa la información y la transmite al controlador de tráfico el cual recopila información altamente precisa sobre los volúmenes de tráfico actuales y cada estación base o punto de acceso permite la conexión de un máximo de 380 sensores.

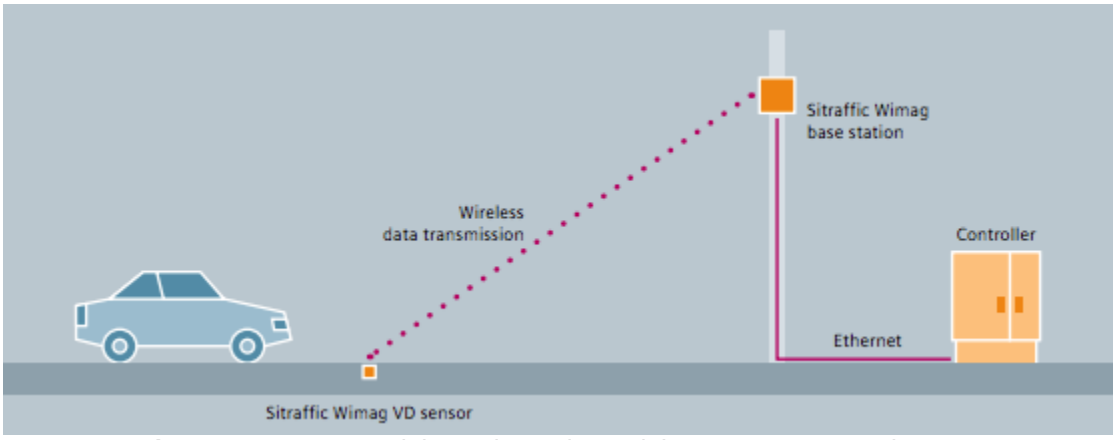

Figura 4.6 Esquema del Funcionamiento del sensor. **Fuente:** Siemens

4.3.2 Especificaciones Técnicas

Detección de vehículo WiMag:

• Detección: detección de campo magnético de 3 ejes

• Dimensiones: 74 mm x 74 mm x 49 mm

• Fuente de alimentación: Li-SOCl2 primaria no reemplazable 3.6V

paquete de baterías

• Rango: típicamente hasta 30 m hasta el repetidor / punto de acceso

• Temperatura de funcionamiento: -40 ° C + 85 ° C

• Peso: 0.3kg

• Banda de frecuencia: 2400 a 2483.5 MHz

• Tamaño del núcleo de instalación: Ø100 mm x 57 mm de profundidad

• Compuesto de instalación: sellador de poliurea de silicona en dos partes

• Calificación de protección de entrada: IP68

Figura 4.7 Sensor Wimag PD. **Fuente:** Siemens

Punto de acceso:

• Rango: típicamente hasta 300 m hasta el punto de acceso (estándar) o hasta 600 m al punto de acceso (repetidor repetidor)

• Las tarjetas se pueden conectar juntas para aumentar la capacidad

• Interfaces:

- A / desde detectores o unidades repetidoras a través de 802.15.4 PHY radio

- A / desde dispositivo de configuración (PC) a través de TCP / IP sobre 10Base T Ethernet

- Para el controlador de tráfico ST950 a través del estándar WiMag tarjeta de interfaz (hasta 20 detectores por tarjeta)

- Para los controladores a través de la tarjeta de reemplazo del detector de bucle WiMag (hasta 4 detectores por tarjeta)

• Banda de frecuencia: 2400 a 2483.5 MHz

• Fuente de alimentación: 36 - 58V DC (48V DC nominal) forma WiMag Rack o WiMag Loop Detector Replacement card

• Consumo de energía: 2W

• Dimensiones: 159 mm x 159 mm x 89 mm

• Peso (incluido el kit de montaje): 1,4 kg

• Calificación de protección de entrada: IP67

• Temperatura de funcionamiento: -40ºC a + 80ºC

Repetidor:

• Rango: por lo general, hasta 300 m hasta el punto de acceso (estándar) o hasta 600 m al punto de acceso (repetidor repetidor)

• Las tarjetas se pueden conectar juntas para aumentar la capacidad

• Interfaces: a / desde detectores, punto de acceso y otros unidades repetidoras

• Banda de frecuencia: 2400 a 2483.5 MHz

• Canales de frecuencia: 16

• Fuente de alimentación: primario reemplazable por el usuario Li-SOCI2 3.6v paquete de baterías

• Duración de la batería: aproximadamente 2 años (estándar), 8 años (extendido) modelo disponible

• Dimensiones: 197 mm x 166 mm x 137 mm

• Peso (incluido el kit de montaje): 2,25 kg

• Calificación de protección de entrada: IP65

• Temperatura de funcionamiento: -40ºC a + 80ºC

4.3.3 Base de Datos

Se puede definir una base de datos como una colección de información organizada de tal modo que sea fácilmente accesible, gestionada y actualizada. Dependiendo cómo se organizan los datos se pueden observar distintos tipos de gestores de base de datos. Las bases de datos a veces se clasifican de acuerdo con su enfoque organizativo.

El enfoque más frecuente es la base de datos relacional, una base de datos tabular en la que los datos se definen de manera que puede ser reorganizada y se accede en un número de maneras diferentes. Una base de datos distribuida es una que puede ser dispersada o replicada entre diferentes puntos de una red.

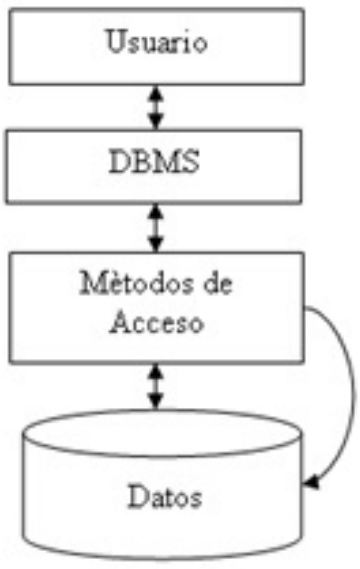

Figura 4.8 Componentes de una base de datos. **Fuente:** Wikimedia

Entre los distintos tipos se encuentran las bases de datos espaciales, en la cual se manipulan objetos espaciales de la misma manera en que se manipula cualquier otro tipo de objeto en la base de datos. Los datos espaciales representan información sobre la ubicación física y la forma de objetos geométricos.

Estos objetos pueden ser ubicaciones de punto u objetos más complejos como ciudades, avenidas o lugares.

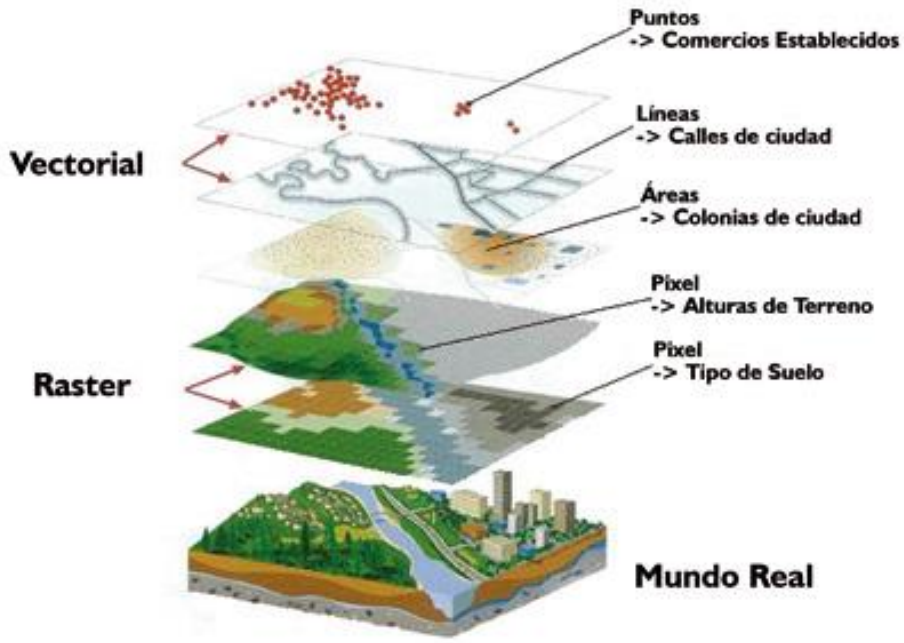

Figura 4.9 Niveles o capas de objetos. **Fuente:** Aulati.net

En la implementación de una base de datos espacial se suelen encontrar los siguientes elementos:

● Tipos de datos espaciales: representan formas geométricas como puntos, líneas y polígonos.
● Índices espaciales: se utilizan índices multidimensionales para procesar de manera eficiente operaciones espaciales.
● Funciones espaciales: algoritmos para realizar consultas sobre datos espaciales.

Debido a que la información de disponibilidad va relacionadas al espacio/ubicación de los estacionamientos de los centros comerciales, se propone la implementación de una base de datos espacial para almacenar la información. PostGIS añade a PostgreSQL soporte para los tres elementos claves de una base de datos relacional: tipos espaciales, índices espaciales y funciones espaciales. PostgreSQL es un poderoso sistema gestor de base de datos objeto-relacional.

Utiliza el tipo de licencias BSD, siendo un software libre y código abierto. PostGIS.

convierte a PostgreSQL en una de las bases de datos preferidas para implementar.

Sistemas de Información Geográfica (GIS).

4.3.4 Aplicación Móvil

Una aplicación móvil es una solución informática diseñada para ser ejecutada en teléfonos inteligentes, tabletas y otros dispositivos móviles y que permite al usuario efectuar una tarea concreta de cualquier tipo: profesional, de ocio, educativas, de acceso a servicios, etc., facilitando las gestiones o actividades a desarrollar.

Debido a que el hardware sobre el cual se ejecuta la aplicación no está atado a una ubicación física, las aplicaciones móviles pueden ser utilizadas en cualquier lugar, razón por la cual constituyen una plataforma idónea para la consulta de la disponibilidad de parqueos no importando el lugar en que se encuentre.

Para el desarrollo de las aplicaciones móviles existen distintas herramientas, entre ellas Xamarin las cual es la elegida para este sistema.

Los desarrolladores de software pueden usar Xamarin para escribir aplicaciones móviles nativas para Android, iOS y Windows, y compartir código a través de múltiples plataformas, incluyendo Windows y macOS.

Figura 4.10 Logo de Xamarin. **Fuente:** Xamarin

Pantallas Interfaz Gráfica

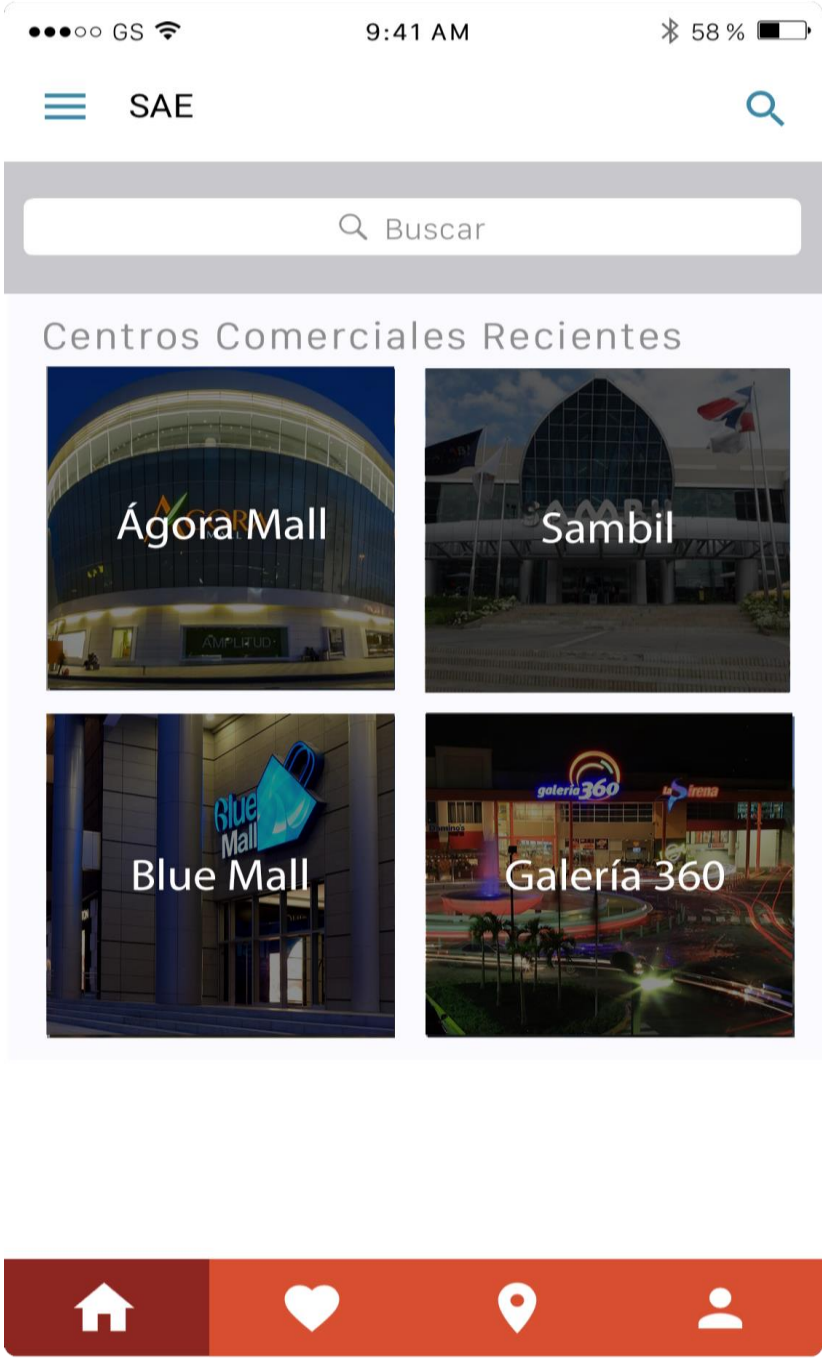

Figura 4.11 Pantalla de Inicio. **Fuente:** Autores

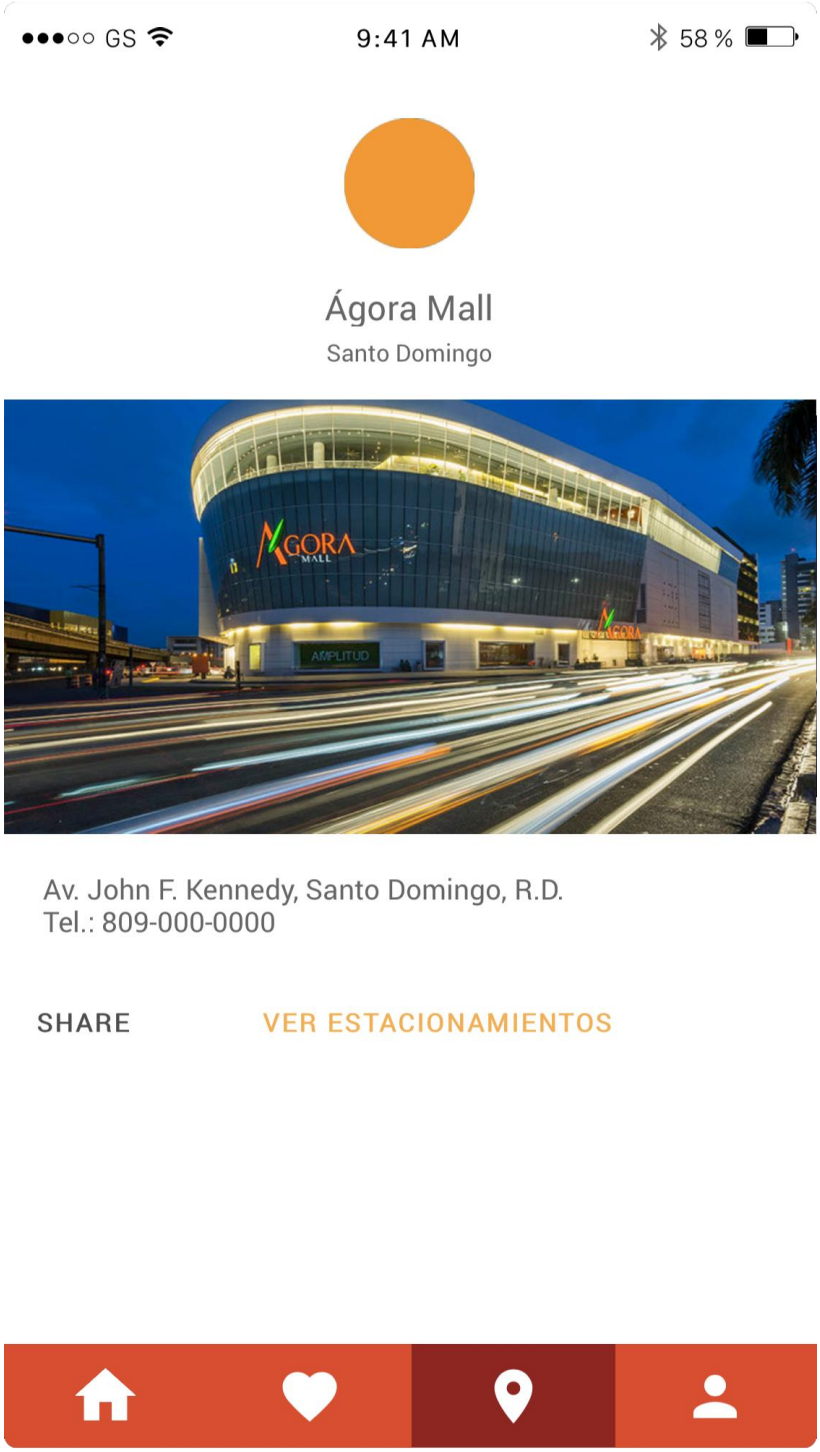

Figura 4.12 Pantalla Informativa del Centro Comercial. **Fuente:** Autores

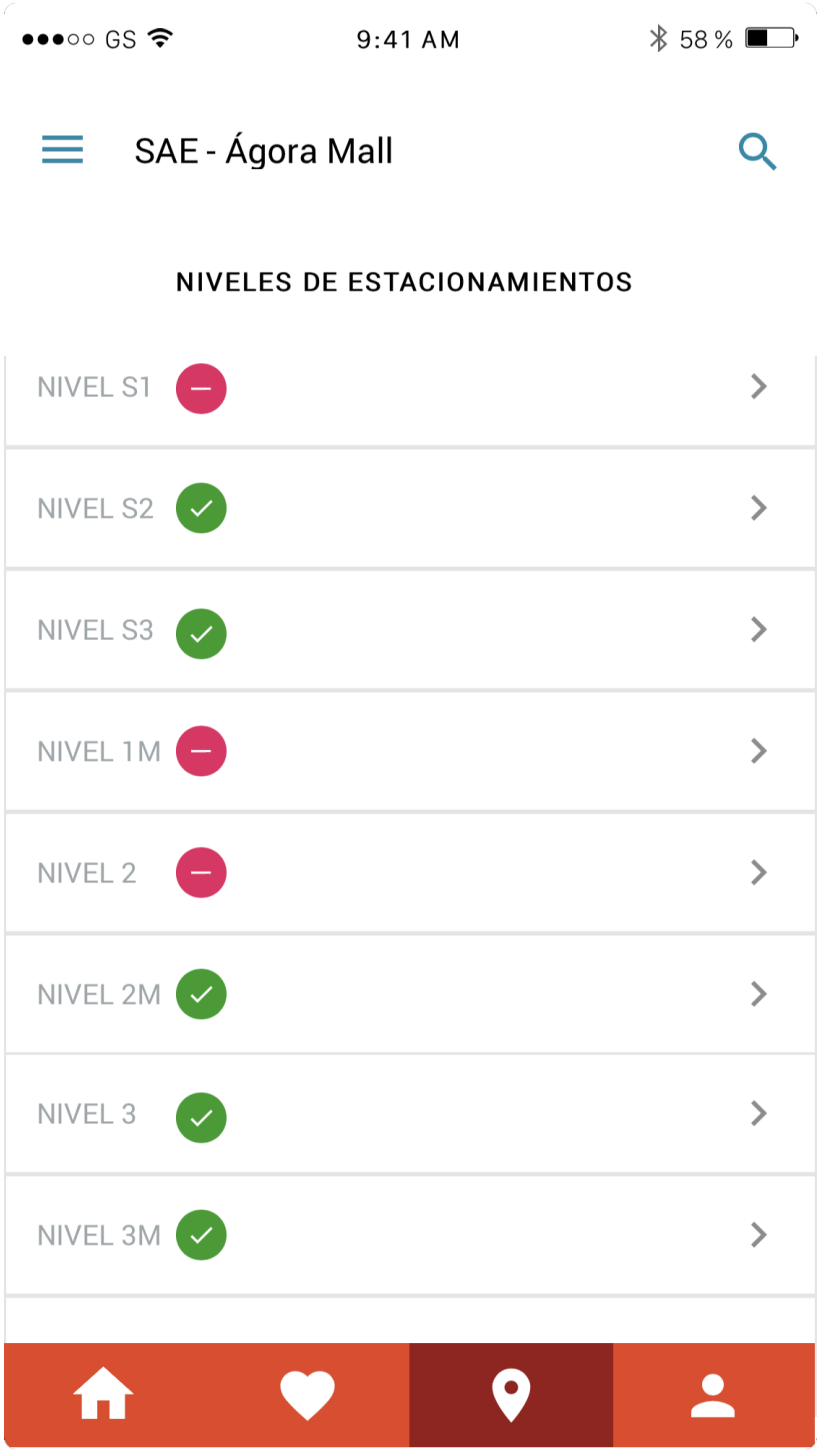

Figura 4.13 Pantalla de los Niveles de Estacionamiento. **Fuente:** Autores

Figura 4.14 Pantalla de Estacionamiento por Nivel. **Fuente:** Autores

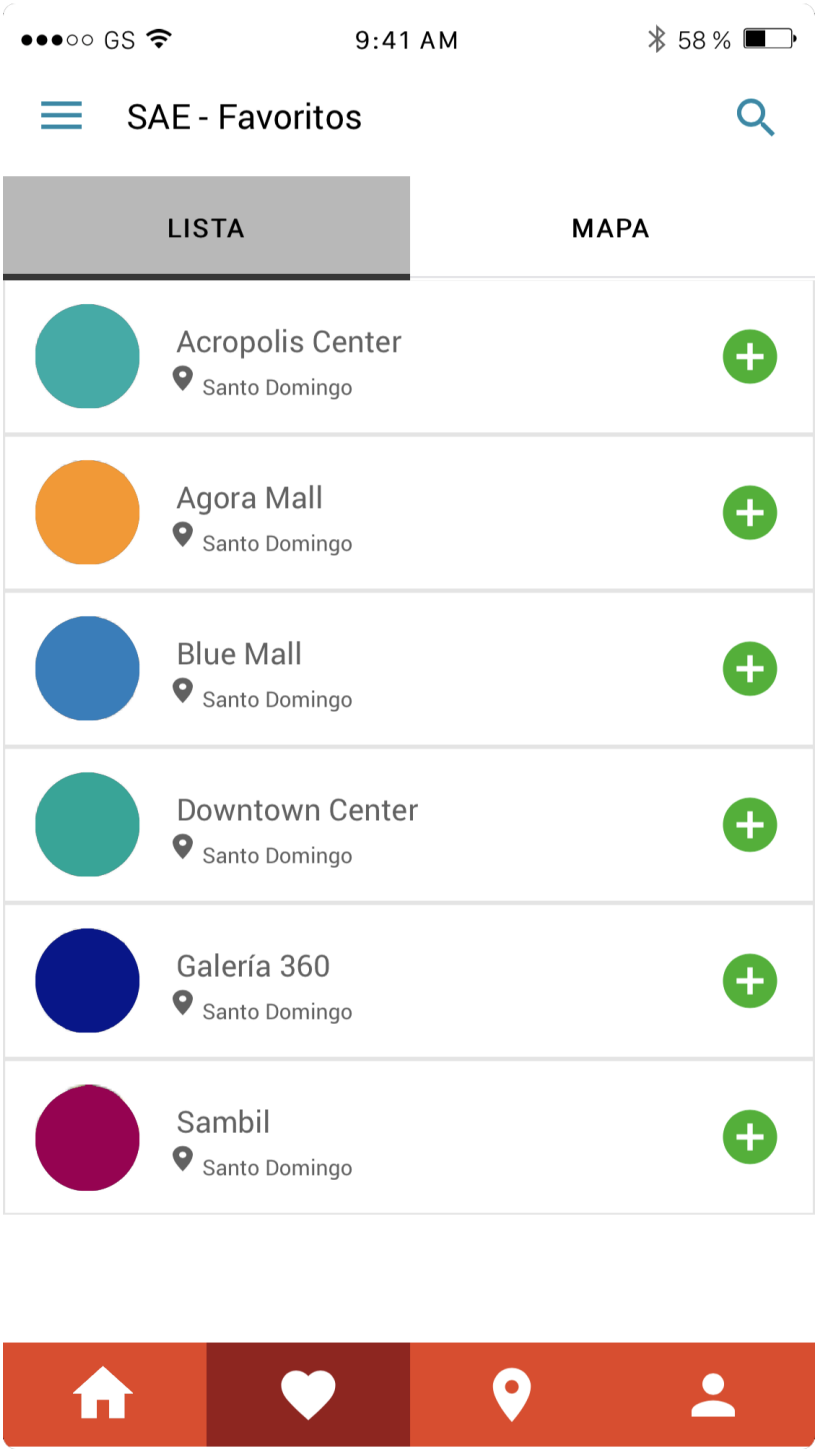

Figura 4.15 Pantalla Centro Comerciales Favoritos. **Fuente:** Autores

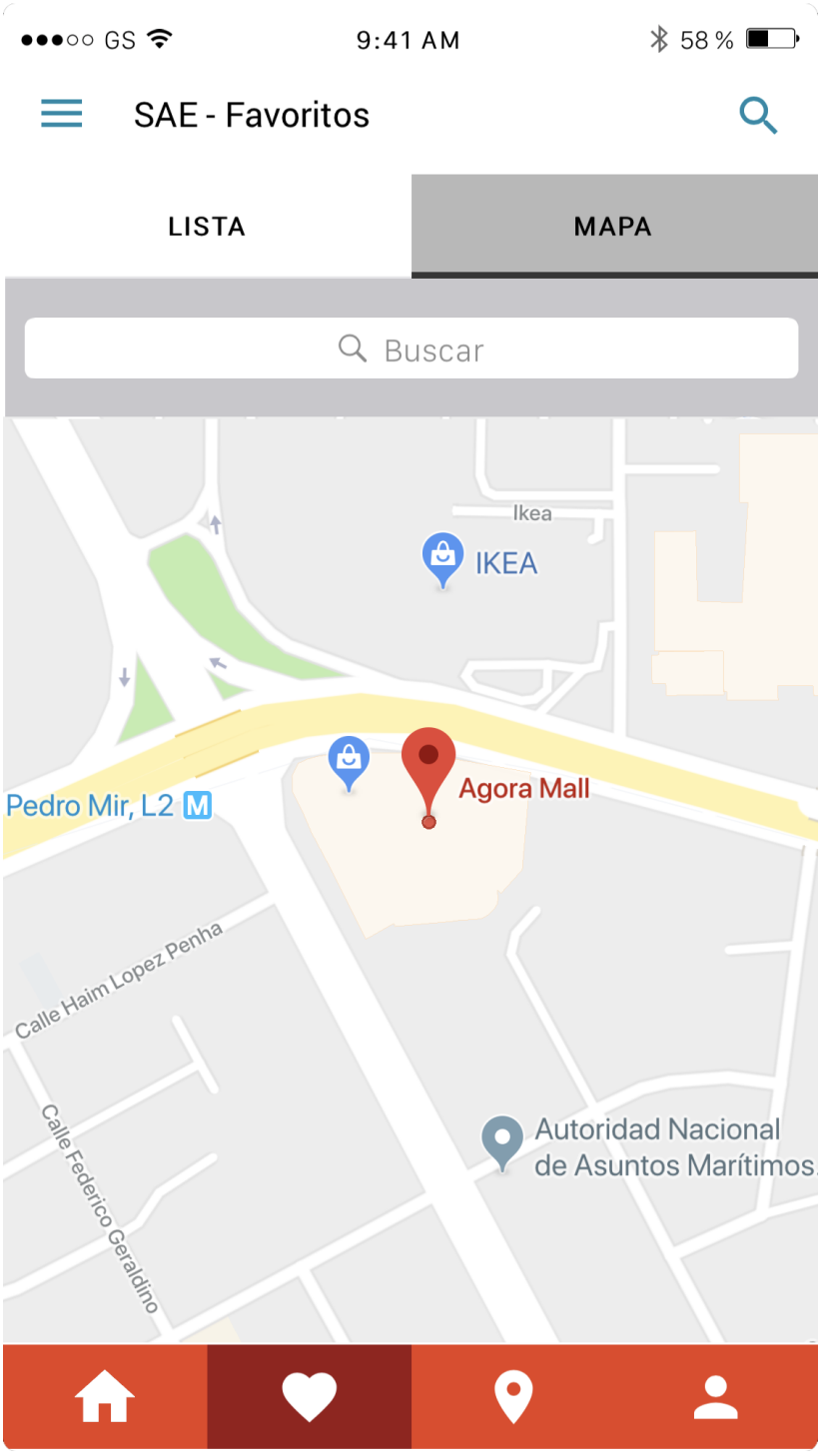

Figura 4.16 Pantalla Búsqueda en Mapa. **Fuente:** Autores

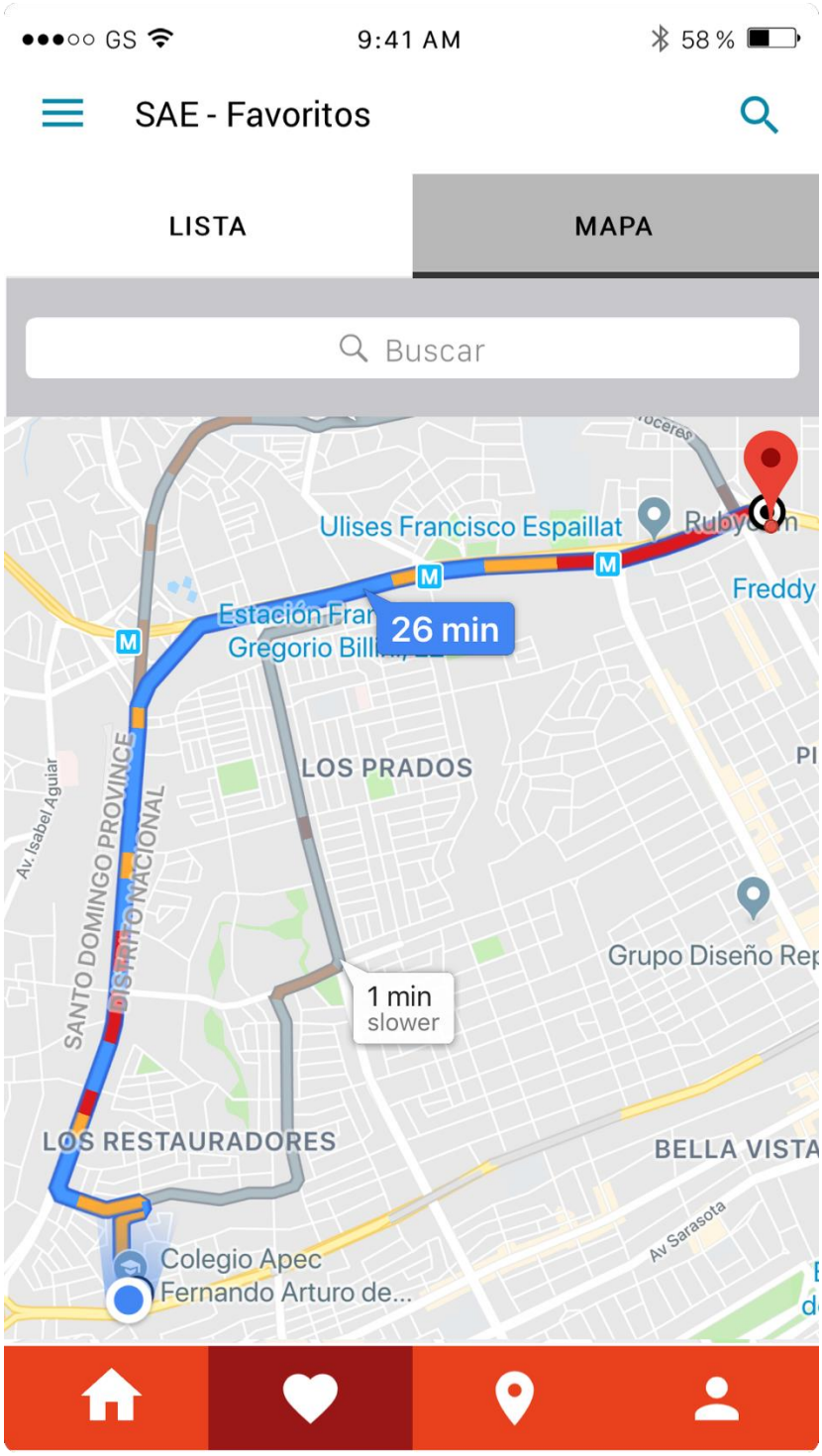

Figura 4.17 Pantalla Búsqueda en Mapa indicado Rutas. **Fuente: Autores**

4.3.5 Aplicación Web

Para aquellos usuarios a los cuales se les limita el uso de equipos móviles ya se porque el lugar donde se encuentran actualmente no esta permitido los mismos, pondrán contar con una versión Web del sistema el cual tendrá las mismas funcionalidades que la aplicación móvil.

Esta versión web también servirá a través de un acceso para un ambiente backend para el manejo, configuración y control de las funciones administrativas de la aplicación móvil y la base de datos.

Dicha aplicación web será desarrollada bajo el lenguaje de programación PHP 7 dado que es un lenguaje de programación bastante estándar en la web y puede cumplir con los requerimientos actuales y futuros del proyecto. Se estará utilizando como web framework la herramienta de Codeigniter en su versión 3.1.9 basado en los términos rigurosos de seguridad que implica este tipo de aplicación y la facilidad de adaptar nuevas necesidades al proyecto. Este framework es uno de los más robustos existentes.

Por medio de la aplicación web se podrá realizar las siguientes tareas administrativas:

- Creación y modificación de Centro Comercial: Según vayan construyendo nuevos centros comerciales la aplicación irá creciendo por lo que no estará limitada los existentes actualmente, permitiendo agregar

información relacionada como dirección, teléfono e imágenes de los centros.

- Creación y modificación de Niveles y Estacionamientos.
- Creación y edición de Usuario.
- Generación de Reportes Estadísticos para los centros comerciales.

4.4 Análisis FODA

El análisis FODA o análisis DAFO, es una técnica o herramienta utilizada en empresas, instituciones y proyectos, con el fin de estudiar una situación en particular. En las misma se plantean características internas (Debilidades y Fortalezas) y la situación externa del sujeto en sí (Amenazas y Oportunidades).

En la tabla 4.2, se presenta una matriz FODA, la misma se realizó con el fin de presentar las características internas y la situación externa, también llamados factores internos y externos, que son los que afectan directamente el proyecto. A cada uno de estos factores se les realizó un levantamiento de información con el fin de obtener toda la ventaja posible de las oportunidades y de reducir al mínimo las amenazas que puedan afectar al proyecto. Consta de estrategias que se definen como maxi-maxi (enfocadas en aprovechar oportunidades), mini-maxi (disminuyen las debilidades a partir de oportunidades), maxi-mini (disminuyen el impacto de las amenazas) y mini-mini (neutralizar cualquier tipo de amenazas).

Factores Internos / Factores externos	Fortalezas	Debilidades
	F1: Automatización y alto control. F2: Alta tecnología e innovación. F3: Seguridad y organización. F4: Ahorro en el tiempo y combustible F5: Valor agregado para los usuarios. F6: Operable las 24 horas del día. F7: Alta disponibilidad	D1: Alta dependencia de redes inalámbricas TCP/IP. D2: Sensores expuestos D3: Alto costo del mantenimiento D4: Fácil acceso a los componentes físicos. D5: El clima puede distorsionar la comunicación.
Oportunidades O1: Expansión a futuras instalaciones de estacionamientos. O2: Calidad de servicio para los usuarios O3: Escalabilidad O4: Garantizar la seguridad con nuevas tecnologías. O5: Aumento de usuarios por las facilidades de estacionarse.	**FO(Maxi-Maxi)** FO1: Realizar revisiones y/o mantenimientos con el fin de mejorar la calidad y mantener el buen funcionamiento de las redes inalámbricas. F2, O2 FO2: Apoyarse de la escalabilidad con el fin de extender este sistema y sus buenas prácticas para adquirir la total satisfacción de los usuarios. F5, O3	**DO(Mini-Maxi)** DO1: Utilizar tecnologías que aporten alta seguridad y que puedan disminuir los riesgos provocados por el clima. D2, D4, D5, O4. DO2: Mitigar las dependencias de las redes inalámbricas con el fin de proporcionar un sistema con alta disponibilidad. D1, D2, D4, O5.
Amenazas A1: Variaciones del Clima A2: El tiempo de vida la batería de los sensores. A3: El mal entendimiento de los usuarios. A4: Mala configuración o recepción de los componentes y sensores. A5: Ataques a las vulnerabilidades de los nodos.	**FA(Maxi-Mini)** FA1: Proteger con alternativas de seguridad los sensores para la conservación de estos. F1, F2, A1, A2. FA2: Monitorear constantemente los sistemas y realizar los mantenimientos a lugar, con el fin de preservar la disponibilidad y de prevenir fallos. F5, F6, F7, A4, A5.	**DA(Mini-Mini)** DA1: Utilizar diferentes alternativas, como la redundancia, con el fin de no depender siempre de la misma red inalámbrica. D1, A4, A5. DA2: Restringir el acceso a los componentes, utilizando seguridad biométrica y/o contraseñas para abrir la ubicación de los sensores. D2, D4, A5.

Tabla 4.2 Matriz FODA. **Fuente:** Autores

4.5 Resultados de la Investigación

En el transcurso de la investigación se utilizó como técnica de recopilación de información, la encuesta, la cual abarcaba un sin número de puntos que sirven como punto de partida y de análisis para la investigación. Dicha encuesta, enfocada en un grupo focal, consta de 10 preguntas y para expresar el resultado de esta, se utilizaron 36 personas para realizar las estadísticas.

Resultados estadísticos de la encuesta por pregunta:

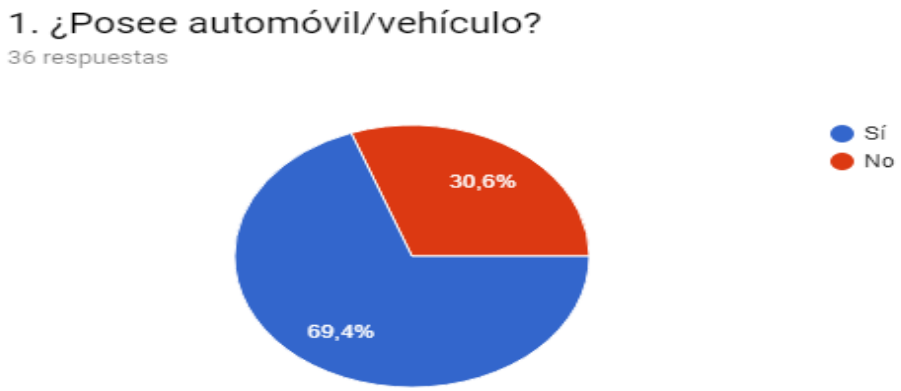

Figura 4.18 – Porcentaje de usuarios que poseen automóvil. **Fuente**: Autores

El objetivo de esta pregunta es identificar la cantidad de personas que poseen un automóvil o vehículo ya sea laboral, familiar o personal.

Según la figura un 69,4% de los encuestados posee un vehículo/automóvil para desplazarse, por lo que las experiencias en cuanto a estacionamientos son bastante altas.

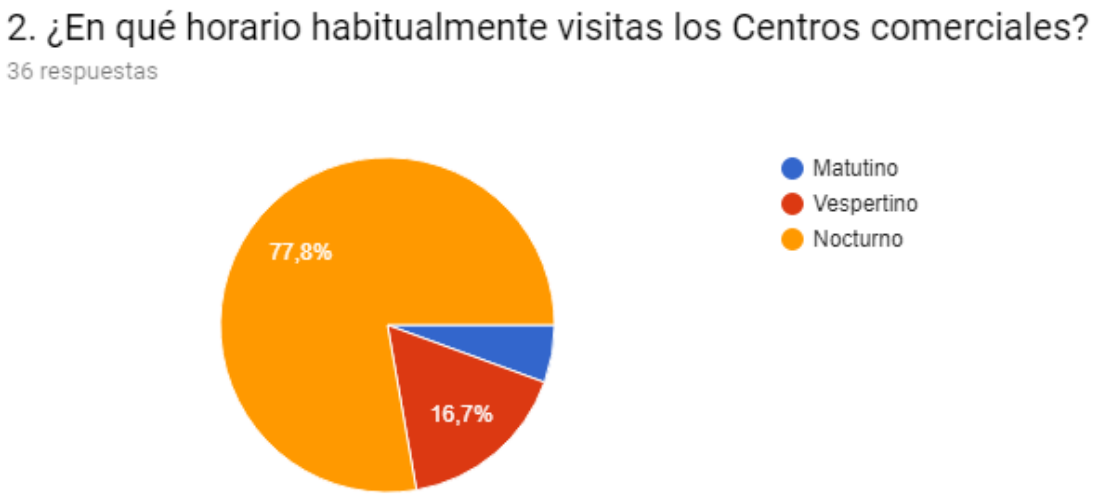

Figura 4.19 – Porcentaje de horarios en que los usuarios visitan los centros comerciales. **Fuente**: Autores

El objetivo de esta pregunta es identificar en qué horario los encuestados van a los centros comerciales, de modo que se pueda identificar donde debe de haber una mayor organización en los estacionamientos.

Según la figura el 77,8% de los encuestados prefiere ir en horario nocturno a los centros comerciales, de modo que por la noche se hace más difícil encontrar donde estacionarse.

Figura 4.20 – Nivel de importancia de los métodos de estacionamiento para los usuarios. **Fuente**: Autores.

El objetivo de esta pregunta es identificar la importancia de los métodos que utilizan los centros comerciales para identificar la disponibilidad de los estacionamientos.

Según la figura el 88,9% optó por responder con un “Sí”, ya que ayudará a ahorrar tiempo y combustible.

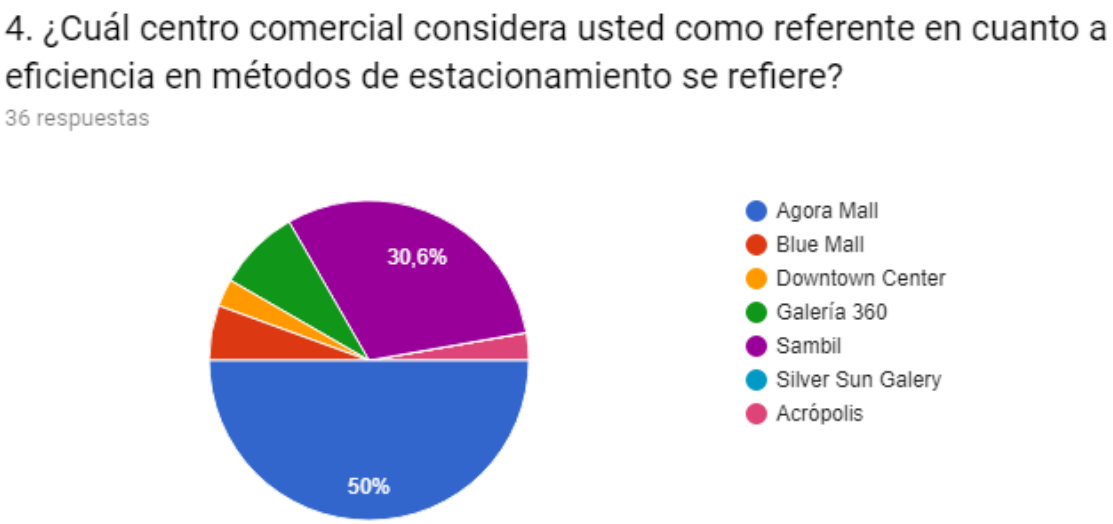

Figura 4.21 – Centros comerciales con mayor eficiencia en sus métodos de estacionamiento. **Fuente**: Autores.

El objetivo de esta pregunta es identificar cuál centro comercial es el preferido por los encuestados por sus métodos de estacionamientos.

Según la figura, el 50% de los encuestados eligieron Ágora Mall como uno de los centros comerciales en donde estacionarse requiere de menos tiempo y combustible.

Figura 4.22 - Nivel de aceptación de los usuarios de utilizar una aplicación que les permita ver la disponibilidad de los estacionamientos. **Fuente**: Autores.

El objetivo de esta pregunta es identificar si los encuestados prefieren utilizar un aplicativo móvil, con el fin de identificar la disponibilidad de los estacionamientos en un centro comercial.

Según la figura, el 86,1% estuvo de acuerdo en utilizar una aplicación móvil para visualizar la disponibilidad de los estacionamientos, ya que simplifica este proceso y aportaría un valor agregado al usuario.

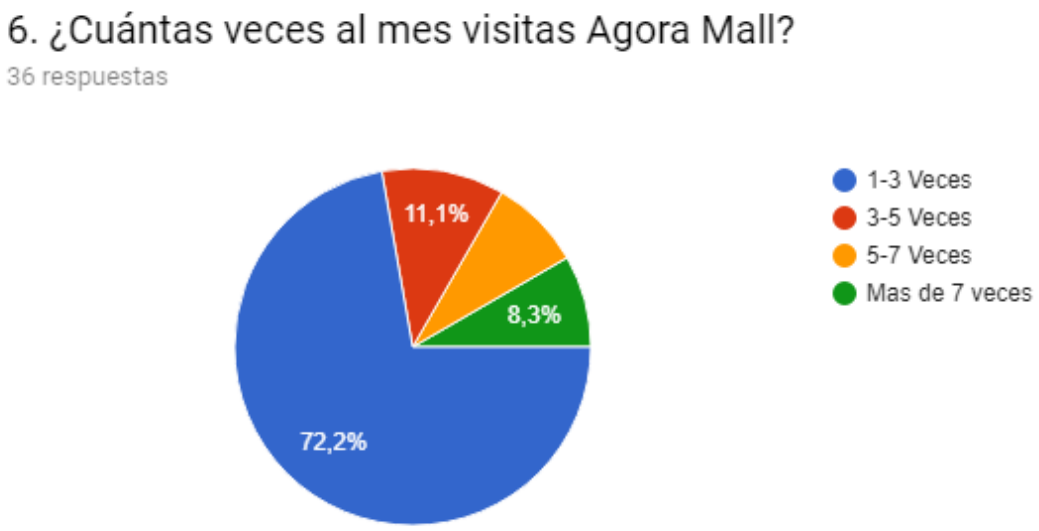

Figura 4.23 – Nivel de frecuencia con la cual los usuarios visitan Ágora Mall. **Fuente**: Autores.

El objetivo de esta pregunta es identificar la concurrencia con la que los encuestados visitan el centro comercial Ágora Mall.

Según la figura, el 72,2% visita mensualmente Ágora Mall entre una a tres veces.

Figura 4.24 – Porcentaje de duración para estacionarse en Ágora Mall. **Fuente**: Autores.

El objetivo de esta pregunta es identificar qué tiempo tardan los encuestados en encontrar un estacionamiento disponible en el centro comercial Ágora Mall.

Según la figura, el 41,7% duran entre tres y cinco minutos para estacionarse, mientras que el 25% duran entre cinco y siete minutos.

Figura 4.25 – Nivel de satisfacción con el tiempo de espera de estacionamientos. **Fuente**: Autores.

El objetivo de esta pregunta es identificar el nivel de satisfacción de los encuestados en cuanto al tiempo que les dura estacionarse en el centro comercial Ágora Mall.

Según la figura, el 37, 1% de los encuestados se encuentran pocos satisfechos con el tiempo que deben de esperar para poder conseguir un estacionamiento, otro 17,1% se encuentran insatisfechos debido a que pierden mucho el tiempo consiguiendo donde estacionarse.

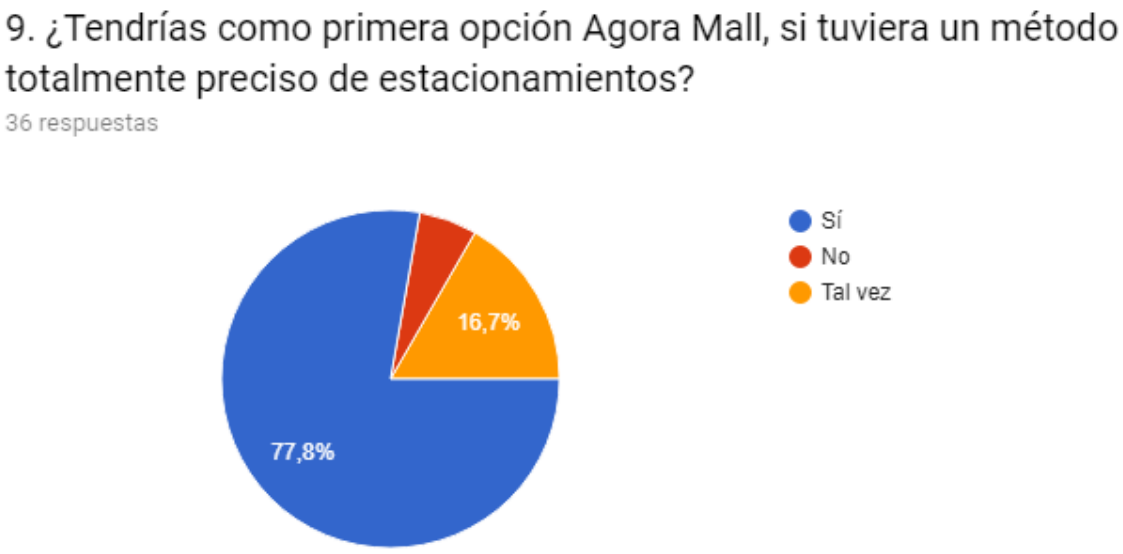

Figura 4.26 – Nivel de aceptación en caso de poseer un método de estacionamiento preciso. **Fuente**: Autores.

El objetivo de la pregunta es confirmar que mediante el uso de un método totalmente preciso de estacionamientos, los encuestados elegirían siempre Ágora Mall como centro comercial.

Según la figura, el 77,8% de los encuestados optó por poner como primera opción a Ágora Mall si sus métodos de estacionamientos fueran totalmente. Un 16,7% optó por tal vez.

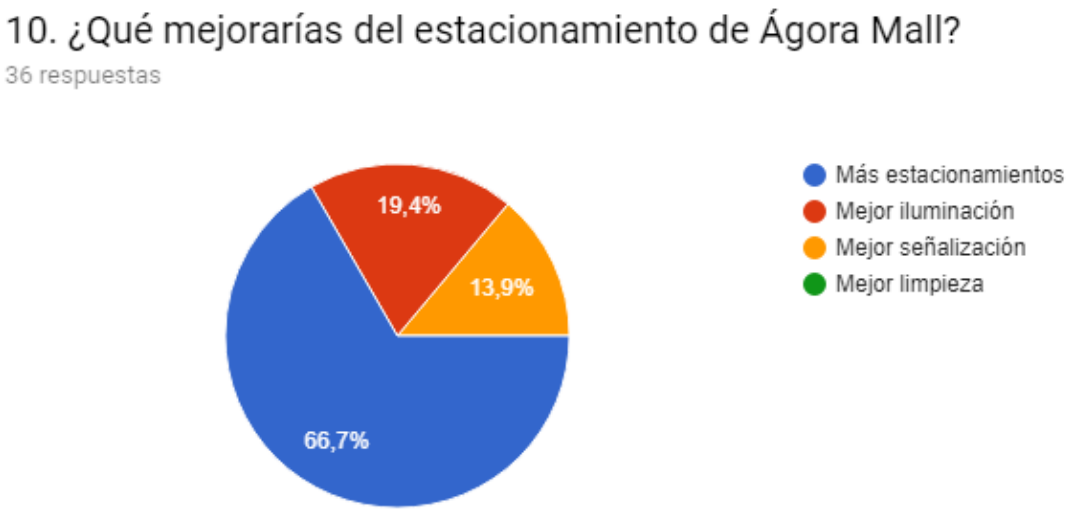

Figura 4.27 – Opciones de mejoras recomendadas por los usuarios para los estacionamientos. **Fuente**: Autores.

El objetivo de esta pregunta es identificar los puntos de mejoras que ayudarían a el centro comercial Ágora Mall a posicionarse como el centro comercial de preferencia de los encuestados.

Según la figura, el 66,7% de los encuestados mejoraría la cantidad de los estacionamientos, el 19,4% sugiere una mejor iluminación en los estacionamientos, mientras que un 13,9% optó por utilizar una mejor señalización en los estacionamientos.

4.6 ROI

Como parte de un uso eficiente de los parqueos de Ágora Mall, una mejora en la experiencia del usuario, ahorro en tiempo y combustible sin mencionar la disminución de dióxido de carbono (CO2) emitido por los vehículos al estar encendidos por menos tiempo, se procederá al cobro por descarga de la aplicación.

(ingresos) 30 mil visitas diarias a Ágora Mall, de las cuales de acuerdo con la encuesta realizada un 68 % son realizadas en automóviles (aproximadamente 20,400 visitas en vehículo). Partiendo de que solo el 5 % de la población que visita diariamente Ágora Mall en vehículo descargue la aplicación se obtienen 1,020 descargas diarias o 372,300 descargas al año.

NRO. ITEM	SUB ITEM	PARTIDA	MEDIDA	CÁLCULO TOTAL
1		**Aportes**		
	1.1	Costo por descarga de la aplicación (RD$5)	Diaria	RD$5,100.00
		SUB-TOTAL INGRESOS		RD$1,861,500
		TOTAL		**RD$1,861,500**

Tabla 4.3 Detalle del ROI **Fuente:** Autores

Tomando en cuenta los valores de ingresos y egresos obtenidos en el análisis financiero y en la figura anterior, se calculó el retorno de inversión de la solución propuesta, considerando los siguientes parámetros:

Retorno de Inversión del Producto (ROI)	
Inversión Inicial (Egresos)	RD$ 1,026,110
Monto Devuelto (Ingresos)	RD$1,861,500 (1 año)
Ganancia o Pérdida	RD$ 835,390
% de Ganancia o Pérdida	81.41%

Tabla 4.4 ROI **Fuente:** Autores

El cálculo del ROI se realizó de la siguiente manera:

ROI = (retorno de la inversión - inversión inicial) / inversión inicial

Sustituyendo por los valores de esta propuesta sería

ROI = (1,861,500 - 1,026,110) / 1,026,110 = 0.8141 ó 81.41 %

De acuerdo con los resultados arrojados por el ROI, la inversión realizada se recupera luego de haber transcurrido un año de la inversión inicial de acuerdo con el retorno anual de RD$1,861,500 lo que representa un margen de ganancia de RD$835,390 sobre la inversión inicial.

Figura 4.28 Calculadora ROI **Fuente:** Pine Grove Software

A partir de los resultados obtenidos se concluye que la propuesta realizada es rentable para Ágora Mall, ya que en tan solo un año dicho centro comercial comenzará a percibir ganancias respecto a la inversión realizada.

4.7 Análisis Económico

A continuación se presentarán los resultados de los diferentes análisis realizados para evaluar la factibilidad general de la propuesta realizada en el presente trabajo de grado. El objetivo de estos diferentes análisis es diagnosticar desde diferentes aristas la situación actual presentada y tomar decisiones en el momento oportuno.

4.7.1 Análisis Financiero

En el siguiente cuadro se desglosan los artículos y costos para desplegar la propuesta realizada en esta tesis con las funcionalidades descritas a lo largo de la misma.

Egresos	Cálculo en el transcurso del año 2018				
No. Item	**Sub-item**	**Partida**	**Precio**	**Medida**	**Costo**
1		**Compra de Equipos**			
	1.1	Sensor de Parqueos Wimag PD	$450.00	1800	$810,000.00
	1.2	Recopilador de Información	$1,800.00	11	$19,800.00
	1.3	Router Inalámbrico	$5,000.00	3	$15,000.00
	1.4	Pantallas LED (Entrada a los Parqueos)	$10,000.00	11	$110,000.00
	1.5	Gastos Aduanales			$30,000.00
		Sub-Total Compra de Equipos			**DOP 984,800.00**
2		**Compra de Equipos de Potencia Eléctrica**			
	2.1	APC 600VA UPS Battery Backup & Surge Protector with USB Charging Port, APC UPS Back-UPS (BE600M1)	$3,500.00	2	$7,000.00
		Subtotal Implementación			**DOP 7,000.00**
3		**Servicios de Azure**			
				Años	
	3.1	SQL Server Principal		1	$0.00
	3.2	Base de Datos SQL Principal	$5,500.00	1	$5,500.00
	3.3	SQL Server Replicación	$3,500.00	1	$3,500.00
	3.4	Base de Datos SQL Replicación	$5,500.00	1	$5,500.00
	3.5	Maquina Virtual	$5,000.00	1	$5,000.00
	3.6	Servicio en la nube	$3,000.00	1	$3,000.00
		Subtotal Implementación			**DOP 24,500.00**
4		**Entrenamiento**		**9 meses**	
	4.1	Material Multimedia Explicativo			DOP 2,500.00
	4.2	Guía de Usuario			DOP 2,250.00
	4.3	Documentación Técnica			DOP 5,060.00
		Subtotal Implementación			**DOP 9,810.00**
		Total Presupuesto			**DOP 1,026,110.00**

Tabla 4.5 Detalle del Análisis Financiero **Fuente:** Autores

4.7.2 Análisis de Riesgo

Para el Análisis de Riesgo se tomaron en consideración los siguientes agentes de riesgo:

- **Personal:**
    - Gerente de Infraestructura;
    - Analistas de Soporte Técnico;
    - Encargado de Cyberseguridad

- **Infraestructura Tecnológica:**
    - Servidores;
    - Puntos de Acceso;
    - Enrutadores;
    - Sensores

- **Sistemas:**
    - Aplicación móvil;
    - Sistemas sensores;
    - Aplicación servidor

- **Otros:**
    - Servicios de Comunicación

Al realizar este análisis se identificaron riesgos generales para los agentes evaluados, a saber:

- Accidentes laborales que pongan en peligro la integridad física de los empleados;
- Catástrofes naturales que pongan en peligro la integridad física del edificio, como incendios, inundaciones, terremotos, etc.
- Desperfecto en los dispositivos;
- Fallas técnicas en los servicios de internet y redes LAN;
- Malware, virus, gusanos, spyware y otros tipos de amenazas;
- Fallas de carácter eléctrico;
- Término de la vida útil de los equipos;
- Bugs en el software;
- Robos.

Entre los controles definidos para reducir los riesgos anteriormente citados se encuentran los siguientes:

- Personal de vigilancia diurna/nocturna y cámaras de vigilancia;
- Antivirus y cortafuegos;
- Respaldo de energía eléctrica (UPS o planta eléctrica);
- Redundancia del ISP;
- Desagües pluviales;

- Extintores y alarmas contra incendio;
- Mantenimiento y rotación periódica del hardware;
- Actualizaciones de software;

En lo que resta de este subtema se trabajará con la matriz de riesgos que identifica los peligros más inherentes asociados a este proyecto de manera que la misma pueda servir como instrumento válido para mejorar la seguridad general.

En dicha matriz se señalan los riesgos a los que están expuestos los activos, con el propósito de asignar un valor numérico al nivel de amenaza al que se encuentra expuesto cada componente.

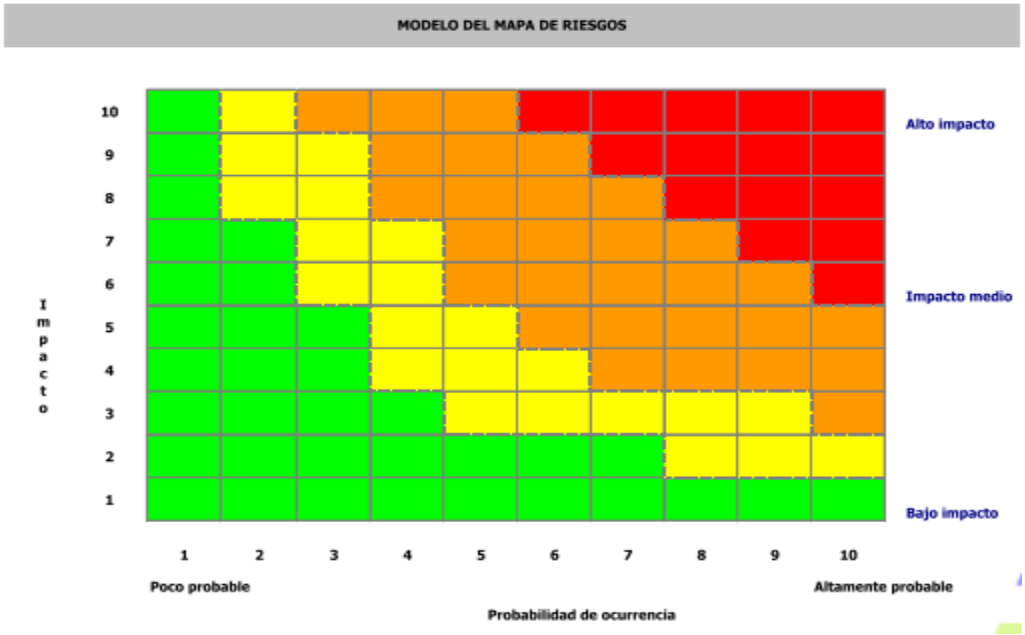

Figura 4.29 Modelo del Mapa de Riesgos **Fuente**: Cemla.org

En esta escala de 10 niveles se logra una mayor amplitud en los cuadrantes de riesgo y se tiene la posibilidad de manejar cuadrantes de riesgo Bajo, Alto, Medio y Crítico. El riesgo de los factores se determinará por su probabilidad de impacto y de ocurrencia.

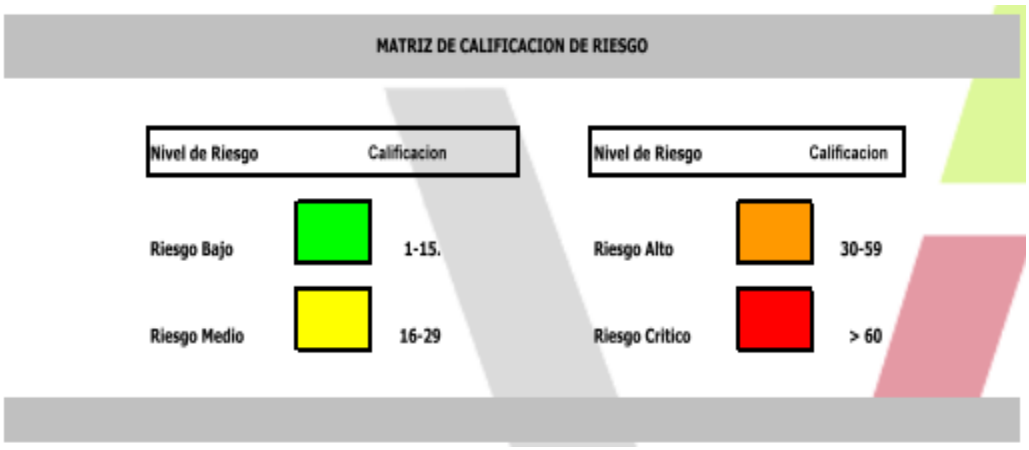

Figura 4.30 Matriz de Clasificación de Riesgos **Fuente**: Cemla.org

Matriz de Análisis de Riesgos										
Activo	Amenazas	Accidentes Laborales	Catástrofes Naturales	Desperfectos	Fallas técnicas en servicios de redes	Virus	Fallas Eléctricas	Término vida útil equipos	Bugs	Robos
Gerente de Infraestructura	Impacto	5	4	0	0	0	0	0	0	0
	Probabilidad	2	2	0	0	0	0	0	0	0
	Riesgo	10	8	0	0	0	0	0	0	0
Analistas de Soporte Técnico	Impacto	4	4	0	0	0	0	0	0	0
	Probabilidad	3		0	0	0	0	0	0	0
	Riesgo	12	0	0	0	0	0	0	0	0
Encargado de Cyberseguridad	Impacto	5	1	0	0	0	0	0	0	0
	Probabilidad	3	2	0	0	0	0	0	0	0
	Riesgo	15	2	0	0	0	0	0	0	0
Servidores	Impacto	1	8	3	5	4	5	4	2	3
	Probabilidad	1	3	3	2	3	4	3	2	9
	Riesgo	1	24	9	10	12	20	12	4	27
Puntos de Acceso	Impacto	1	6	6	3	3	4	2	5	4
	Probabilidad	2	3	3	3	3	3	3	1	4
	Riesgo	2	18	18	9	9	12	6	5	16
Enrutadores	Impacto	1	5	5	3	2	4	2	3	1
	Probabilidad	1	2	2	2	3	2	2	3	1
	Riesgo	1	10	10	6	6	8	4	9	1
Sensores	Impacto	1	5	5	2	4	3	5	2	5
	Probabilidad	1	2	2	3	3	3	4	3	1
	Riesgo	1	10	10	6	12	9	20	6	5
Aplicación móvil	Impacto	0	0	0	4	0	0	0	4	0
	Probabilidad	0	0	0	5	0	0	0	3	0
	Riesgo	0	0	0	20	0	0	0	12	0
Sistemas sensores	Impacto	2	1							
	Probabilidad	2	3							
	Riesgo	4	3	0	0	0	0	0	0	0
Aplicación servidor	Impacto	2	2	2	1	2	2	1	1	2
	Probabilidad	2	3	2	4	3	1	1	2	1
	Riesgo	4	6	4	4	6	2	1	2	2
Servicios de comunicación	Impacto	2	1	4	5	1	3	4	1	3
	Probabilidad	2	3	2	3	1	3	2	1	2
	Riesgo	4	3	8	15	1	9	8	1	6

Figura 4.31 Matriz de Riesgos **Fuente**: Autores

4.8 Cronograma de actividades

En la siguiente figura se muestra de manera general las actividades necesarias para la exitosa implementación de la propuesta planteada. En el nivel de detalle se incluyen fechas tentativas para la realización de las actividades, así como el nivel de precedencia y dependencia entre las mismas.

ID	Task Name	Duration	Start	Finish	Predecessors	Resource Names
1	**Proyecto**	**102 days**	**7/20/18 8:00 AM**	**12/10/18 5:00 PM**		
2	Inicio	0 days	7/20/18 8:00 AM	7/20/18 8:00 AM		
3	**Fase 1**	**7 days**	**7/20/18 8:00 AM**	**7/30/18 5:00 PM**		
4	Búsqueda de los equipos	3 days	7/20/18 8:00 AM	7/24/18 5:00 PM	2	
5	Selección de equipos	1 day	7/25/18 8:00 AM	7/25/18 5:00 PM	4	
6	Cotización de los equipos	3 days	7/26/18 8:00 AM	7/30/18 5:00 PM	5	
7	Cotización de la aplicación	1 day	7/20/18 8:00 AM	7/20/18 5:00 PM		
8	**Fase 2**	**61 days**	**7/20/18 8:00 AM**	**10/12/18 5:00 PM**		
9	Compra de los equipos	1 day	7/20/18 8:00 AM	7/20/18 5:00 PM		
10	Llegada de los equipos	30 days	7/23/18 8:00 AM	8/31/18 5:00 PM	9	
11	**Fase 2.1**	**51 days**	**7/23/18 8:00 AM**	**10/1/18 5:00 PM**		
12	Análisis de la aplicación	20 days	9/3/18 8:00 AM	9/28/18 5:00 PM	10	
13	Señalamientos de los parqueos	3 days	7/23/18 8:00 AM	7/25/18 5:00 PM	9	
14	Enumeración de los parqueos	3 days	7/26/18 8:00 AM	7/30/18 5:00 PM	13	
15	Instalación de los equipos	21 days	9/3/18 8:00 AM	10/1/18 5:00 PM	10	
16	**Fase 2.2**	**30 days**	**9/3/18 8:00 AM**	**10/12/18 5:00 PM**		
17	Desarrollo de Aplicación Móvil	10 days	10/1/18 8:00 AM	10/12/18 5:00 PM	12	
18	Desarrollo de Aplicación Web	10 days	9/3/18 8:00 AM	9/14/18 5:00 PM	10	
19	**Fase 3**	**61 days**	**9/17/18 8:00 AM**	**12/10/18 5:00 PM**		
20	Prueba de Aplicación	15 days	9/17/18 8:00 AM	10/5/18 5:00 PM	18	
21	Prueba de Equipos	15 days	10/8/18 8:00 AM	10/26/18 5:00 PM	20	
22	**Prueba del Funcionamiento**	**30 days**	**10/29/18 8:00 AM**	**12/7/18 5:00 PM**		
23	Prueba de Humo	2 wks	10/29/18 8:00 AM	11/9/18 5:00 PM	21	
24	Prueba de Regresión	2 wks	11/12/18 8:00 AM	11/23/18 5:00 PM	23	
25	Pruebas de Aceptación	2 wks	11/26/18 8:00 AM	12/7/18 5:00 PM	24	
26	Publicación de la aplicación	1 day	12/10/18 8:00 AM	12/10/18 5:00 PM	25	
27	Fin	0 days	12/10/18 5:00 PM	12/10/18 5:00 PM	26	

Figura 4.32 Cronograma de Trabajo **Fuente:** Autores

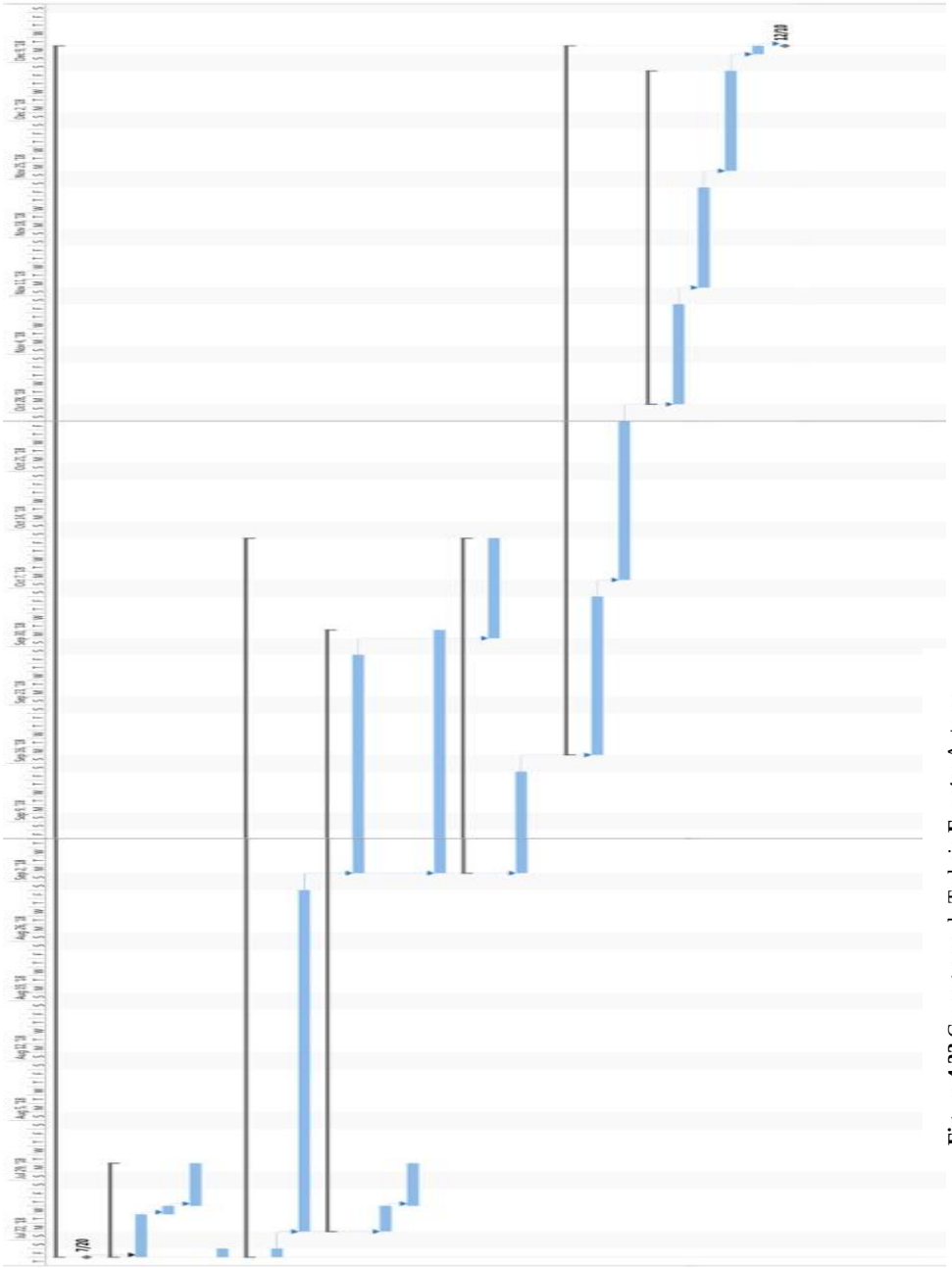

Figura 4.33 Cronograma de Trabajo **Fuente:** Autores

CONCLUSIÓN

Al terminar con el proceso de investigación y la elaboración de la propuesta, se considera que el sistema es factible, ya que podría solucionar la problemática actual que existe en los métodos de estacionamientos del centro comercial Ágora Mall, donde el sistema hace referencia a una solución efectiva y precisa. Dicha solución ofrece ayuda tanto a los visitantes que se estacionan, como al personal de seguridad a la hora de supervisar y dirigir todo el proceso.

De implementarse el sistema, se determinó que los resultados serían positivos y de forma inmediata, donde los mismos se traducirían en ganancia en el tiempo, debido a que los visitantes se dirigirán, de manera rápida, directamente a los estacionamientos disponibles que identifique el sistema, así como la disminución de los embotellamientos, tanto en el centro comercial como en calles aledañas. Estas ventajas hacen posible que el sistema pueda expandirse y ser utilizado por otros centros comerciales.

Mediante los resultados del análisis financiero y el ROI, se pudo obtener que la implementación del sistema en el centro comercial Ágora Mall, hace la inversión totalmente factible, la cual se obtendrá en un periodo de corto plazo debido a los beneficios obtenidos por la organización de los estacionamientos que conlleva implementar este sistema.

RECOMENDACIONES

- El centro comercial Ágora Mall debe invertir en una aplicación para la gestión de parqueos, en vista que de acuerdo con el análisis financiero realizado en la presente propuesta a partir del primer año se percibirán ganancias.

- Una vez implementada la aplicación, el equipo de Tecnología de Ágora Mall deberá mantenerse monitoreando la cantidad de usuarios y actuar proactivamente para asegurarse que no se exceda la capacidad de los recursos tecnológicos y que la gestión de la demanda se realice de manera efectiva.

- Ágora Mall debe crear un instructivo que indique cómo deben estacionarse los usuarios (orientación y posicionamiento del vehículo) de manera que los sensores puedan arrojar lecturas más precisas.

- Ágora Mall deberá contratar personal especializado en el área de Ciberseguridad para garantizar la integridad, confidencialidad y disponibilidad de la información recogida por los sensores IoT sobre los usuarios y sus vehículos.

- El Departamento de Tecnología de Ágora Mall debe crear un SSID que cuente con acceso encriptado para el intercambio de información. Como medida de seguridad las contraseñas a utilizar deben contener caracteres en minúscula y mayúscula, así como números y caracteres especiales.

- Ágora Mall deberá de dar publicidad a la App para móviles, con el fin de que los visitantes sepan que existe un sistema que le ayudará a obtener estacionamiento de una manera mas rápida, además de agregar valor al centro comercial al diferenciarlo del resto y colocarlo entre los líderes tecnológicos del país.

- Ágora Mall deberá realizar un video tutorial sobre cómo debe ser utilizado el aplicativo móvil, con el fin de que los visitantes entiendan cómo funciona el sistema y la transición al método del aplicativo móvil sea lo más transparente posible.

GLOSARIO DE TÉRMINOS

Broadcast: es una forma de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea, sin necesidad de reproducir la misma transmisión nodo por nodo.

Codeigniter: es un framework para aplicaciones web de código abierto para crear sitios web dinámicos con PHP.

Código QR: Es un módulo para almacenar información en una matriz de puntos o en un código de barras bidimensional.

Computación ubicua (ubicomp): es un concepto en ingeniería de software y las ciencias de la computación. Es entendida como la integración de la informática en el entorno de la persona, de forma que los ordenadores no se perciban como objetos diferenciados, apareciendo en cualquier lugar y en cualquier momento.

CSMA/CA: es un protocolo de control de acceso a redes de bajo nivel que permite que múltiples estaciones utilicen un mismo medio de transmisión.

Duplexor: es un dispositivo electrónico que permite la comunicación bidireccional (duplex) sobre una misma línea de transmisión.

Electromagnetismo: es una rama de la física que estudia y unifica los fenómenos eléctricos y magnéticos en una sola teoría.

Firewalls: es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

Framework: es un conjunto estandarizado de conceptos, prácticas y criterios para enfocar un tipo de problemática particular que sirve como referencia, para enfrentar y resolver nuevos problemas de índole similar.

Hacker: persona experta en el manejo de computadoras, que se ocupa de la seguridad de los sistemas y de desarrollar técnicas de mejora.

IEEE: Institute of Electrical and Electronics Engineers, es una asociación mundial de ingenieros dedicada a la estandarización y el desarrollo en áreas técnicas.

IrDA: Asociación de Datos Infra-rojos, define un estándar físico en la forma de transmisión y recepción de datos por rayos infrarrojos.

Magnetómetro: dispositivos que sirven para cuantificar en fuerza o dirección la señal magnética de una muestra.

M2M (machine to machine, 'máquina a máquina') es un concepto genérico que se refiere al intercambio de información o comunicación en formato de datos entre dos máquinas remotas.

MIMO: Múltiple entrada múltiple salida, se refiere específicamente a la forma como son manejadas las ondas de transmisión y recepción en antenas para dispositivos inalámbricos como enrutadores.

Osciloscopio: es un instrumento de visualización electrónico para la representación gráfica de señales eléctricas que pueden variar en el tiempo.

PHP: es un lenguaje de programación de propósito general de código del lado del servidor originalmente diseñado para el desarrollo web de contenido dinámico.

Radar: es un sistema que usa ondas electromagnéticas para medir distancias, altitudes, direcciones y velocidades de objetos estáticos o móviles.

RFC: serie de publicaciones del grupo de trabajo de ingeniería de internet que describen diversos aspectos del funcionamiento de Internet y otras redes de computadoras, como protocolos, procedimientos, etc.

RFID o identificación por radiofrecuencia (del inglés Radio Frequency Identification) es un sistema de almacenamiento y recuperación de datos remoto que usa dispositivos denominados etiquetas, tarjetas o transpondedores RFID.

SSH: nombre de un protocolo y del programa que lo implementa, y sirve para acceder servidores privados a través de una puerta trasera.

TKIP: es también llamado hashing de clave WEP WPA, incluye mecanismos del estándar emergente 802.11i para mejorar el cifrado de datos inalámbricos.

UDP: es un protocolo del nivel de transporte basado en el intercambio de datagramas.

Wearable: es aquel dispositivo electrónico que se lleva sobre, debajo o incluido en la ropa. Otras de sus características es que permite la multitarea por lo que no requiere dejar de hacer otra cosa para ser usado y puede actuar como extensión del cuerpo o mente del usuario.

Web Service: es una tecnología que utiliza un conjunto de protocolos y estándares que sirven para intercambiar datos entre aplicaciones.

Widget: es una pequeña aplicación o programa, usualmente presentado en archivos o ficheros pequeños que son ejecutados por un motor de widgets o Widget Engine.

ZigBee: es el nombre de la especificación de un conjunto de protocolos de alto nivel de comunicación inalámbrica para su utilización con radiodifusión digital de bajo consumo

BIBLIOGRAFÍA

Libros:

- Aguilera, P. (2010). Seguridad informática. Editorial Editex. 1era Edición. España

- Chen, L., Ji, J., Zhang, Z. (2013) Wireless Network Security. Springer. 2da Edición. USA.

- Garbarino, Jimena. (2012) Protocolos para redes inalámbricas de sensores. EAE. 1era Edición. España.

- Greengard, Samuel. (2015) The Internet of Things. MIT. 1era Edición. USA.

- Kendall, Kenneth; Kendall, Julie. (2005) Análisis y Diseño de Sistemas. Pearson Educación. 6ta Edición. México.

- Kingsley, Simon; Quegan, Shaun. (1999) Understanding Radar Systems. McGraw-Hill. 1era Edición. USA.

- Mazumder, Sudip K. (2010) Wireless Networking Based Control. Springer. 1era Edición. USA.

- McEwen, Adrian. Cassimally Hakim. (2014) Internet de las cosas: la tecnología revolucionaria que todo lo conecta. Anaya Multimedia. 1era Edición. España.

- McWherter, Jeff; Gowell, Scott. (2012) Professional Mobile Application Development. Wrox. 1era Edición. USA.

Digital:

- ARQUITEXTO, (2013, enero). Ágora Mall. Recuperado de https://arquitexto.com/2013/01/agora-mall/

- Business Insider, (2015. febrero). The corporate 'Internet of Things' will encompass more devices than the smartphone and tablet markets combined. Recuperado de http://www.businessinsider.com/the-enterprise-internet-of-things-market-2014-12

- CEMLA.org, (2010, mayo). Matriz de Riesgo Operacional. Recuperado de http://www.cemla.org/actividades/2010/2010-05-EducacionFinanciera/MatrizRiesgo-BrunoBV28.pdf

- Conectate.com.do, (2016, noviembre). Ágora Mall Santo Domingo, todo en un solo lugar. Recuperado de http://www.conectate.com.do/articulo/agora-mall-santo-domingo/

- CISCO, (2013, julio). Connections Counter: The internet of everything in motion. Recuperado de https://www.newsroom.cisco.com/feature-content?type=webcontent&articleId=1208342

- CISCO. What is a Smart City? Recuperado de https://www.cisco.com/c/en/us/solutions/industries/smart-connected-communities/what-is-a-smart-city.html

- Coherent Chronicle, (2018, mayo). Machine to Machine (M2M) Connections Market is expected to show significant growth over the forecast period. Recuperado de http://www.coherentchronicle.com/machine-to-machine-m2m-connections-market-is-expected-to-show-significant-growth-over-the-forecast-period/

- IEEE Standards Association. INTERNET OF THINGS RELATED STANDARDS. Recuperado de http://standards.ieee.org/innovate/iot/stds.html

- I-Scoop. What is the Internet of Things? Internet of Things definitions. Recuperado de https://www.i-scoop.eu/internet-of-things

- I-Scoop. The Internet of Things (IoT) – essential IoT business guide. Recuperado de https://www.i-scoop.eu/internet-of-things-guide/

- Information Security Buzz, (2016, febrero). Smart City Security and Cyber Attacks. Recuperado de

https://www.informationsecuritybuzz.com/articles/smart-city-security-and-cyber-attacks/

- Linkedin, (2015, febrero). Pros & Cons of Internet Of Things (IOT). Recuperado de https://www.linkedin.com/pulse/pros-cons-internet-things-iot-bhaskara-reddy-sannapureddy/

- DGII.com, (2017). Parque Vehicular. Recuperado de http://www.dgii.gov.do/informacionTributaria/estadisticas/parqueVehicular/Documents/ParqueVehicular2013.pdf

- DiarioLibre.com.do, (2015, noviembre). Ágora Mall, primer centro comercial con certificación “Green Building” en Centroamérica y el Caribe. Recuperado de https://www.diariolibre.com/economia/empresas/agora-mall-primer-centro-comercial-con-certificacion-green-building-en-centroamerica-y-el-caribe-BM1853056

- Financial-Calculators.com, Retorno de la Inversión Calculadora. Recuperado de https://financial-calculators.com/es/calculadora-de-ROI

- Listindiario.com, (2017). LEY 63-17 - Medina promulga ley de transporte terrestre. Recuperado de http://www.listindiario.com/la-republica/2017/02/22/455032/medina-promulga-ley-de-transporte-terrestre

- Hernández, C. (2001, junio). Hackers: Los piratas del Chip y de Internet. Recuperado de http://www.tugurium.com/docs/Hackers2_LosPiratasDelChipYDeInternet_ClaudioHernandez.pdf

- Outsourcing Automation, (2017, octubre). CÓMO MAXIMIZAR LA SEGURIDAD DE LOS DISPOSITIVOS IOT. Recuperado de https://oasys-sw.com/maximizar-seguridad-dispositivos-iot/

- Red Hat (2017). VULNERABILIDADES Y ATAQUES COMUNES, Recuperado de https://access.redhat.com/documentation/es-es/red_hat_enterprise_linux/6/html/security_guide/sect-security_guide-common_exploits_and_attacks

- Siemens, (2016). Intelligent Traffic Systems. Recuperado de https://www.siemens.co.uk/traffic/en/

- Siemens, (2017). Sitraffic SmartDetection, Recuperado de https://www.siemens.com/global/en/home/products/mobility/road-solutions/traffic-management/on-the-road/smart-detection.html

- Wikipedia. Internet of things. Recuperado de https://en.wikipedia.org/wiki/Internet_of_things

ANEXOS

UNAPEC
UNIVERSIDAD APEC

Decanato:
Ingeniería e Informática (Escuela de Informática)

Anteproyecto de Trabajo de Grado

Tema

Análisis y diseño de un sistema web y móvil para el control de disponibilidad de estacionamientos apoyado en el internet de las cosas, en los centros comerciales de la ciudad de Santo Domingo durante el periodo mayo-agosto 2018 (caso de estudio Ágora Mall).

Asesor
Freddy Jiménez

Sustentantes

Randol Mariano Frías Taveras	2014-2499
Smiley Rafael Mariñez Mota	2014-2052
Brayler Sánchez Peguero	2014-2571

07 de febrero, 2018

Santo Domingo, D.N.

República Dominicana

DEPARTAMENTO DE SOCIALES
PROYECTO DE TRABAJO DE GRADO
APROBADO
FIRMA
FECHA 22/3/18

1. Título del tema:

Análisis y diseño de un sistema web y móvil para el control de disponibilidad de estacionamientos apoyado en el internet de las cosas, en los centros comerciales de la ciudad de Santo Domingo durante el periodo mayo-agosto 2018. (caso de estudio Ágora Mall)

2. Introducción:

En los últimos años el aumento vehicular ha provocado un sin número de embotellamientos y dificultades a la hora de estacionarse en lugares públicos o privados, como son los centros comerciales. Cada una de estas dificultades han causado que las personas se vean obligadas a invertir tiempo valioso en la búsqueda de estacionamientos debido a la falta de un sistema de monitoreo que contabilice los mismos.

Dicha contabilización puede ser lograda mediante el uso de tecnologías que detectan la entrada y/o salida de vehículos de cualquiera de estos lugares, cómo son los radares y las redes inalámbricas. Las redes inalámbricas se han vuelto muy populares debido a la facilidad de uso y de movilidad que tienen las personas cuando la utilizan, mientras que los radares no son más que aquellos sistemas que utilizan ondas electromagnéticas con el fin de realizar mediciones de distancia, dirección, altitud y velocidad de objetos que se encuentran de forma estática o en movilización.

La utilización de las dos tecnologías mencionadas anteriormente y de otras más, no menos importantes, han llevado a esta investigación a enfocarse en el diseño de un sistema de control de parqueos en los centros comerciales de Santo Domingo, que hará posible solventar las dificultades y/o problemáticas que tienen los ciudadanos al estacionarse en centros comerciales.

Dicho sistema tendrá como propósito principal llevar a cabo la contabilización de los parqueos de manera automática, con el fin de realizar una mejor gestión y de notificar a los dueños de vehículos la disponibilidad de los parqueos, dando como resultado una mayor facilidad para la obtención de los mismos y menos pérdida de tiempo a la hora de estacionarse.

3. Justificación:

En la actualidad, existe la problemática de que al momento de visitar los distintos centros comerciales de la ciudad de Santo Domingo, se desconoce la cantidad de parqueos libres que disponen en los mismos, dando como resultado largas horas de espera al momento de estacionarse.

La presente investigación propone un sistema web y móvil para la gestión de parqueos en los centros comerciales, tomando como referencia el caso Ágora Mall. Esto resulta útil especialmente en la época en la que vivimos en la que el índice de adquisición de vehículos aumenta con cada año que pasa; sin embargo, la cantidad de parqueos disponibles permanece invariante. Alrededor del 30% del mercado automotriz de la República Dominicana se concentra en el Distrito Nacional, por lo que es preciso implementar medidas que ayuden a mejorar el manejo de parqueos en Santo Domingo.

Ágora Mall dispone de 1,800 parqueos (1,400 propios y 400 de la Dirección General de Aduanas disponibles en horario no laborables de la entidad oficial) distribuidos en sus 8 niveles, de los cuales 6 son en una torre y 2 son soterrados. Este centro comercial cuenta con más de 180 establecimientos comerciales que atraen a un promedio de 30 mil visitas diarias. Alojar esta enorme cantidad de personas al día resulta un reto para cualquier institución.

Con el sistema propuesto en esta investigación se dotará de información de valor tanto al centro comercial como al visitante, de manera que ambos puedan tomar las mejores

decisiones en lo que respecta a los parqueos de Ágora Mall, ya que entre las facilidades que ofrece el sistema se encuentra poder realizar estudios o análisis de reportes basados en los datos generados, tanto por la entrada y salida de vehículos lo que significa que se logrará medir de manera eficiente en el caso de entidades comerciales como plazas o tiendas, cuáles son los horarios o días en los que reciben mayor o menor cantidad de visitas. Del lado del conductor o usuario, este le permitirá ver la disponibilidad de parqueos, tanto cantidad como ubicación de los mismos.

Entre los beneficios principales del sistema se encuentran:

· Rápida ubicación de parqueos disponibles, lo que se traduce en menor tráfico de vehículos dentro de la plaza y por tanto menores embotellamientos;

· Mejor experiencia de usuario a nivel general al no ser necesario invertir tiempo adicional localizando plazas de parqueos;

· Reducción del dióxido de carbono (CO_2) emitidos por los vehículos dentro de la plaza, lo que representa un impacto positivo en el medio ambiente.

4. Delimitación del tema y planteamiento del problema de investigación.

Delimitación del tema.

El tema abordará la situación de los parqueos en base a la problemática de la ciudad de Santo Domingo. Además de que se centra en el estudio y mejora del proceso de parqueo en lugares de mucha concurrencia específicamente los centros comerciales y se estará agotando el periodo mayo - agosto 2018.

Planteamiento del problema.

El aumento de vehículos en República Dominicana siempre ha estado presente a un ritmo acelerado. Según el último boletín de la Dirección General de impuestos internos (DGII) en 2016 el parque vehicular reportó más de 240 mil vehículos de nuevo ingreso para un total de más de 3.5 Millones de unidades concentrándose mayormente en el Distrito Nacional y la provincia Santo Domingo con un 41.9%. Por esto, y la pobre zonificación de nuestra ciudad, la cual radica en que las zonas de trabajo están muy cerca de las zonas residenciales y al centro de la ciudad, han causado que el tránsito se congestione gravemente sobre todo en las horas pico.

En el caso de los parqueos que es nuestro objeto de estudio hay una situación que se torna inaguantable debido a que en las horas pico los establecimientos e instituciones no disponen de la cantidad de parqueo necesaria, lo que conlleva a la pérdida de tiempo y de combustible, no solamente está la situación de durar una gran cantidad de horas perdidas en largas filas de tapones, sino que se le suma la de no encontrar o tener que esperar más tiempo para la espera de disponibilidad de un parqueo.

5. Objetivos generales y específicos.

Objetivo general

- Diseñar un Sistema de Control de Parqueos para los centros comerciales de la ciudad de Santo Domingo.

Objetivos específicos

- Diagnosticar los sistemas de parqueo actuales en los centros comerciales de Santo Domingo.

- Identificar las debilidades y deficiencias de los sistemas de parqueos actuales.

- Determinar el tipo de aplicativo electrónico que podría utilizarse para el control de la disponibilidad de los parqueos en base a las deficiencias y debilidades encontradas.

- Especificar la capacidad que tendrá el aplicativo móvil para el control de los parqueos.

- Determinar las facilidades que ofrece tanto para el cliente (Entidades públicas y privadas) como el usuario (Conductores de vehículos) el uso de un dispositivo móvil para el acceso a la disponibilidad de parqueos.

6. Marco teórico referencial.

Marco teórico

Según Ramiro Alberto Ríos y Vera Lucia Vicentini (2013) en un informe para el Banco Interamericano de Desarrollo, es importante detallar sobre cómo actuar para disminuir la congestión generada por la motorización, la falta de planificación urbana adecuada y las políticas regresivas de transporte. Esto se ha denominado, en términos generales, Gestión de la Demanda. El tema de la Gestión de la Demanda del Transporte –GDT (o TDM, por sus siglas en inglés)– es relativamente nuevo para las ciudades y sus gobernantes. La gestión de la demanda tiene como principal objetivo tratar de solucionar los crecientes problemas de la congestión y los asociados a ella, pero no a través de una mayor oferta vial, sino a través de la administración eficiente de los viajes, así como la de los modos de transporte disponibles en la ciudad.

ITDP (Institute for Transportation and Development Policy) define la gestión de la demanda de la siguiente manera: “el conjunto de estrategias encaminadas a cambiar el comportamiento de viaje de las personas (cómo, cuándo y dónde viaja la gente) con el fin de aumentar la eficiencia de los sistemas de transporte y lograr objetivos específicos de política pública encaminados al desarrollo sostenible. Las estrategias de gestión de la movilidad priorizan el movimiento de personas y bienes por encima de vehículos, es decir, a modos eficientes de transporte, como caminar, usar la bicicleta, transporte público, trabajar desde casa, compartir el automóvil, etc.” (Medina, ITDP México, et al. 2012).

En la planificación actual de sistemas de transporte sostenible se ha utilizado frecuentemente una categorización introducida por Dalkmann y Branningan (2007), donde se plantea que la implementación de políticas que mejoren las condiciones para el transporte sostenible debe integrar medidas de planeación, regulación, económicas, de información y tecnológicas.

“En las calles de la República Dominicana circulan 3,398,304 vehículos de dos y cuatro ruedas, de los que el 43%, circulan en el Distrito Nacional y la provincia Santo Domingo, según datos de la Dirección General de Impuestos Internos en 2015. De ese total el 27% operan en el Distrito Nacional, y el 16% – en la provincia de Santo Domingo, mientras que, en Santiago se registra el 8.5% del parque de vehículos del país.” (DGII, 2017).

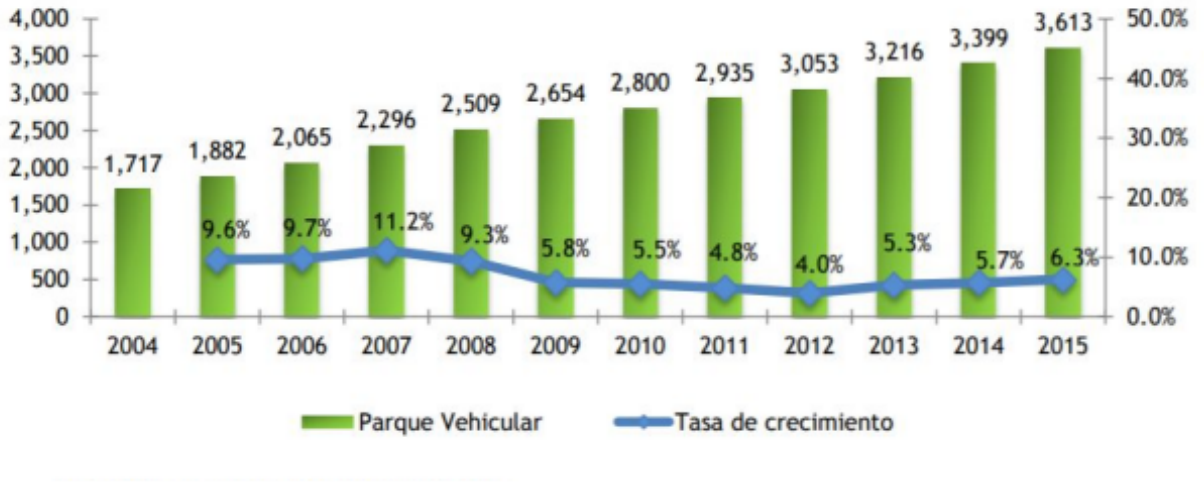

Figura 1 – Evolución del parque vehicular 2004-2015, en miles de unidades.
(*Fuente: DGII.GOV.DO*)

“La ciudad de Santo Domingo contará a partir de este año con parqueos públicos como parte del proyecto de mejorar el tránsito y movilidad. El proyecto ya ha sido aprobado y además se habilitarán estacionamientos en las cercanías de las estaciones del Metro de Santo Domingo con el fin de que los pasajeros dejen sus vehículos y aborden el tren.” (Danilo Medina en su rendición de cuentas correspondiente al año 2017).

“Las tecnologías de la información y la comunicación no son ninguna panacea ni fórmula mágica, pero pueden mejorar la vida de todos los habitantes del planeta. Se dispone de herramientas para llegar a los Objetivos de Desarrollo del Milenio, de instrumentos que harán avanzar la causa de la libertad y la democracia y de los medios necesarios para propagar los conocimientos y facilitar la comprensión mutua. “(Kofi Annan, discurso inaugural de la primera fase de la WSIS en Ginebra, 2003).

Marco conceptual:

Aplicativo Móvil: “Es una aplicación informática diseñada para ser ejecutada en teléfonos inteligentes, tabletas y otros dispositivos móviles y que permite al usuario efectuar una tarea concreta de cualquier tipo —profesional, de ocio, educativas, de acceso a servicios, etc., facilitando las gestiones o actividades a desarrollar.” (Santiago, Raúl, et al., 2015).

Figura 2 - Aplicativo móvil Google Maps.
(*Fuente: Icons8.com)*

WiMag: “Es una tecnología de detección alternativo que utiliza magnetómetros pequeños alimentados por batería, incrustados en la superficie de la carretera, para detectar vehículos y comunicar eventos de detección a un controlador de host, sin la necesidad de un extenso cableado o ductos.” (Siemens, 2013).

Figura 3 - Equipo WiMag de la marca Siemens.
(Fuente: Siemens.com)

Parking Bay Sensor: “Es un detector de radar de microondas de potencia ultra-baja. La tecnología integrada en el sensor se usa para detectar vehículos estacionados, midiendo el inicio y el final del estacionamiento. Los sensores se encuentran debajo del pavimento, y cada uno contiene un transmisor/receptor inalámbrico incorporado con una batería dedicada que transmite datos de detección a un punto de acceso asociado que lo envía al sistema de gestión de tráfico para su análisis.” (Siemens, 2016).

Figura 4 - Parking Bay Sensor de la marca Siemens.
(Fuente: Siemens.com)

Internet de las Cosas (IoT): En la actualidad no existe una definición única sobre el Internet de las Cosas. IoT es una infraestructura global para la sociedad de la información, lo que permite servicios avanzados mediante la interconexión de las cosas tanto físicas como virtuales en base a cosas existentes y evolución de las tecnologías de la información y comunicación interoperables. (Unión Internacional de Telecomunicaciones, 2012)

Figura 5 - Red con equipos conectados a internet.
(Fuente: AyudaWP.com)

Infraestructura Tecnológica: "Se entiende por infraestructura tecnológica al conjunto de todos los elementos tecnológicos hardware y software: servidores, computadores, portátiles, impresoras, switches, routers, firewall, escáneres, cableado estructurado, cpu's, software informático, equipos de comunicación, internet, red LAN."

(Gómez, 2011, pág. 3).

Figura 6 – Modelo de infraestructura tecnológica.
(Fuente: SIDDE.CO)

7. Diseño metodológico: metodología y técnicas de investigación cuantitativa y/o cualitativa.

En base al grado de profundidad con que se abordará este tema se estará implementado y/o realizando un tipo de estudio o investigación descriptiva. Además, se trabajará aplicando el Método de Análisis, utilizando la Encuesta como técnica para la recolección de la información, con un enfoque cualitativo para la investigación.

7.1 Tipo de Estudio Mixto de orden:

Descriptivo, de este modo se dará a conocer la información que actualmente existe sobre el tema de los parqueos, identificar las debilidades de los actuales procesos y desarrollar las acciones necesarias que eficientizarían el problema, utilizando distintas fuentes para recolectar las informaciones necesarias para poder detallar de forma precisa los componentes del diseño a desarrollar.

Exploratorio, de manera que se pueda tener una visión general de tipo aproximativo sobre la realidad de los parqueos de Ágora Mall, se puedan identificar tendencias de horarios de embotellamientos y relaciones potenciales entre las variables involucradas en la causa de la congestión.

Documental, para recopilar adecuadamente datos e información sobre la problemática a analizar mediante el uso de documentos impresos, electrónicos o gráficos, compararlos y llegar a una conclusión que respalde o no la hipótesis planteada.

7.2 Método de Investigación:

Análisis, mediante este método o proceso se identificarán cada una de las partes que conforman el tema presentado y sus respectivas características. Para de esa forma establecer una relación de causa y efecto entre los elementos que componen dicho caso.

7.3 Técnica:

Focus Group (Grupo de enfoque), será el instrumento que se utilizará para la recolección de información que se necesita para la investigación. Con dicha técnica se busca conseguir la opinión de los usuarios en cuanto a su conformidad con los parqueos en los distintos centros comerciales de Santo Domingo.

Además, se estarán utilizado como fuentes secundarias las encuestas y artículos de la web enfocados en la situación de los parqueos.

8. Fuentes de documentación (fuentes bibliográficas primordiales sobre el tema).

Libros:

- Aguilera, P. (2010). Seguridad informática. Editorial Editex. 1era Edición. España

- Chen, L., Ji, J., Zhang, Z. (2013) Wireless Network Security. Springer. 2da Edición. USA.

- Formoso, A., Mazzilli, A. (2014). ParkIt – Plataforma inteligente de estacionamiento público. Memoria Investigaciones en Ingeniería, 12, 85-91.

- Garbarino, Jimena. (2012) Protocolos para redes inalámbricas de sensores. EAE. 1era Edición. España.

- Greengard, Samuel. (2015) The Internet of Things. MIT. 1era Edición. USA.

- Kendall, Kenneth; Kendall, Julie. (2005) Análisis y Diseño de Sistemas. Pearson Educación. 6ta Edición. México.

- Kingsley, Simon; Quegan, Shaun. (1999) Understanding Radar Systems. McGraw-Hill. 1era Edición. USA.

- Mazumder, Sudip K. (2010) Wireless Networking Based Control. Springer. 1era Edición. USA.

- McEwen, Adrian. Cassimally Hakim. (2014) Internet de las cosas: la tecnología revolucionaria que todo lo conecta. Anaya Multimedia. 1era Edición. España.

- McWherter, Jeff; Gowell, Scott. (2012) Professional Mobile Application Development. Wrox. 1era Edición. USA.

Referencias digitales:

- CISCO, (2013, julio). Connections Counter: The internet of everything in motion. Recuperado de https://www.newsroom.cisco.com/feature-content?type=webcontent&articleId=1208342

- DGII.com, (2017). Parque Vehicular. Recuperado de http://www.dgii.gov.do/informacionTributaria/estadisticas/parqueVehicular/Documents/ParqueVehicular2013.pdf

- Listindiario.com, (2017). LEY 63-17 - Medina promulga ley de transporte terrestre. Recuperado de http://www.listindiario.com/la-republica/2017/02/22/455032/medina-promulga-ley-de-transporte-terrestre

- Hernández, C. (2001, junio). Hackers: Los piratas del Chip y de Internet. Recuperado de http://www.tugurium.com/docs/Hackers2_LosPiratasDelChipYDeInternet_ClaudioHernandez.pdf

- Siemens, (2016). Intelligent Traffic Systems. Recuperado de https://www.siemens.co.uk/traffic/en/

- Siemens, (2017). Sitraffic SmartDetection, Recuperado de https://www.siemens.com/global/en/home/products/mobility/road-solutions/traffic-management/on-the-road/smart-detection.html

- Red Hat (2017). VULNERABILIDADES Y ATAQUES COMUNES, Recuperado de https://access.redhat.com/documentation/es-es/red_hat_enterprise_linux/6/html/security_guide/sect-security_guide-common_exploits_and_attacks

9. Esquema preliminar de contenido del Trabajo de Grado.

Agradecimientos

Dedicatorias

Introducción

Resumen Ejecutivo

Metodología

Capítulo I: Antecedentes históricos de Ágora Mall

1.1. Historia
1.2. Misión
1.3. Visión
1.4. Valores
1.5. Filosofía Institucional
1.6. Objetivos
1.7. Organigrama Institucional

Capítulo II: Internet de las cosas (IoT)

2.1. Historia
2.2. Definición
2.3. Aplicaciones
    2.3.1 Consumidor
    2.3.2 Empresas
    2.3.3 Infraestructura
2.4. Tendencias
    2.4.1 Inteligencia
    2.4.2 Arquitectura
    2.4.3 Estándares
2.5. Privacidad y seguridad

Capítulo III: Tecnologías de detección inalámbrica o radar

- 3.1 Radar
  - 3.1.1 Historia
  - 3.1.2 Principios
  - 3.1.3 Diseño
  - 3.1.4 Clasificación
- 3.2 Redes Inalámbricas
  - 3.2.1 Conceptos
  - 3.2.2 Tipos de Redes
    - 3.2.2.1 Redes WAN
    - 3.2.2.2 Redes MAN
    - 3.2.2.3 Redes LAN
  - 3.2.3 Estándares
    - 3.2.3.1 IEEE 802.11a
    - 3.2.3.2 IEEE 802.11b
    - 3.2.3.3 IEEE 802.11g
    - 3.2.3.4 IEEE 802.11n
  - 3.2.4 Seguridad
    - 3.2.4.1 WPA
    - 3.2.4.2 WPA2
    - 3.2.4.3 WEP
    - 3.2.4.4 EAP
- 3.3 Tecnología WiMag
  - 3.3.1 Definición
  - 3.3.2 Aplicaciones

Capítulo 4: Propuesta de un sistema de gestión de parqueos en Ágora Mall

- 4.1 Propuesta
- 4.2 Situación actual de la empresa
- 4.3 Diseño del sistema de control de parqueos
- 4.4 Análisis FODA