Riesgos con las redes Wi-Fi públicas del centro de Medellín, Colombia

Roberto Carlos Guevara Calume

FONDO EDITORIAL
CORPORACIÓN UNIVERSITARIA REMINGTON

Guevara Calume, Roberto Carlos

Riesgos con las redes Wi-Fi públicas del centro de Medellín, Colombia / Roberto Carlos Guevara Calume.
Medellín: Corporación Universitaria Remington, 2017
71 p.; 16,5x23 cm
Incluye bibliografía.

ISBN: 978-958-56132-0-1 (Internet-PDF)
DOI: https://doi.org/10.22209/9789585613201

1. Wi-Fi, 2. WEP, 3.WPA, 4. WPA2, 5. Distribución de protocolos, 6. Medellín comuna 10, 7. mapas georreferenciados. 8. Usuarios de internet. 9. Corporación Universitaria Remington.

CDD: 005.8 G939

Primera edición, febrero de 2017

Diseño, diagramación y portada
Cristina Yepes Pérez

Corrector de estilo
Juan David Villa Rodríguez

Fondo Editorial Remington
Lina Maria Yassin Noreña, editora en jefe
fondo.editorial@uniremington.edu.co
Calle 51 # 51-27, Edificio Uniremington
Telefax: (57) (4) 3221000, extensión 3001 – 3008
Medellín, Colombia

Autor

Roberto Carlos Guevara Calume

Docente investigador, Coordinador del Grupo Ingeniar, Facultad de Ciencias Básicas e Ingeniería, Corporación Universitaria Remington. Ingeniero de Sistemas de la Universidad San Buenaventura, Medellín. Especialista en Redes Corporativas en Integración de Tecnologías. MSc Automatización y Control Industrial. Candidato a Doctor en proyectos.

Agradecimientos

A los coinvestigadores:
Giovanny Alberto Flórez y Álvaro de Jesús Laverde.

A los profesores colaboradores:
Carlos Guillermo Londoño, Jorge Mauricio Sepúlveda
y Porfirio de Jesús Álvarez.

A los Estudiantes colaboradores Semillero Semcei,
adscrito al grupo de investigación Ingeniar
Nelson Jair Mosquera Palacio, Alex Ferney Collazos Patiño,
Johan Steven Bolívar Uribe y Víctor Alonso Granada Mesa.

A Jorge Mario Puerta Soto, Director Ejecutivo de Corpocentro
y Andrea Velásquez Mesa, Comunicadora Corpocentro.

Tabla de Contenido

Lista de Tablas

Lista de Figuras

Prólogo

Como decano de la Facultad de Ciencias Básicas e Ingeniería de la Corporación Universitaria Remington (Uniremington), tengo el agrado de presentar este libro resultado de investigación, el cual es fruto de la dedicación del autor y del crecimiento continuo del grupo de investigación Ingeniar.

Esta es una investigación que permite conocer la realidad de las redes Wi-Fi en sitios céntricos y en la cual se ha tomado como caso de estudio a la comuna 10 de la ciudad de Medellín, Colombia. En el libro se cuantifican variables como el solapamiento de canales y la seguridad usada, y se muestra cómo estas pueden afectar la comunicación en este tipo de tecnologías inalámbricas.

Además de la publicación de este libro como mecanismo de divulgación, vale resaltar la labor realizada por el autor para el acercamiento entre la academia, la comunidad y la empresa a través de la Corporación Cívica Centro de Medellín, Corpocentro, entidad que dio su apoyo para hacer las mediciones de campo y con la cual se han venido realizando convenios tendientes a culturizar a los comerciantes del centro de Medellín en el uso adecuado y la protección de sus redes Wi-Fi.

Jorge Mauricio Sepúlveda Castaño
Decano de la Facultad de Ciencias
Básicas e Ingeniería, Uniremington

Introducción

Este libro es el resultado de las investigaciones realizadas en la Corporación Universitaria Remington, Uniremington, por profesores del grupo de investigación Ingeniar y de la colaboración de estudiantes del semillero de investigación SemCEI, adscritos a la Facultad de Ciencias Básicas e Ingeniería de la Uniremington, con el fin de obtener datos precisos acerca de factores como la interferencia y la seguridad de las redes Wi-Fi en la comuna 10 de Medellín; para la obtención de estos datos se contó con el apoyo de la Corporación Cívica del Centro de Medellín, Corpocentro, a través de un convenio marco.

Resumen

El acceso a internet a través de redes inalámbricas Wi-Fi es cada vez más cotidiano; su bajo costo, sumado a la ventaja de no requerir cables, le ha traído gran popularidad no obstante la vulnerabilidad inherente ante accesos no autorizados. En Medellín, principalmente en el centro de la ciudad, se encuentran muchos sitios que ofrecen internet a través de redes Wi-Fi; además, muchas pymes también las usan para la comunicación interna entre sus computadores.

En este documento se muestran los resultados del análisis de solapamiento de canales y problemas de interferencia que afectan la velocidad de transferencia en los puntos de acceso libre a internet que emplean tecnología Wi-Fi, suministrados por entidades públicas y privadas en el área de estudio, a través de la georreferenciación de planos digitales. Por último, se realiza una encuesta para identificar el uso que se da a las redes Wi-Fi.

Se analizarán y mostrarán los resultados sobre el grado de seguridad de la red en las empresas localizadas cerca de estos puntos de acceso libre a internet para alertar y mejorar la seguridad ante intrusos que intenten acceder sin ser autorizados.

Palabras clave. Wi-Fi, WEP, WPA, WPA2, distribución de protocolos, Medellín comuna 10, mapas georreferenciados.

Justificación

Tecnologías inalámbricas como Wi-Fi tienen gran aceptación en comunicación de computadores y acceso a internet. La revista Tendencias de la Telecomunicaciones del 17 de marzo de 2010 (Paul, 2010) revela un estudio realizado por AT&T donde se muestra que el 65 % de las pequeñas y medianas empresas no sobrevivirían sin redes inalámbricas; además muestra cómo día a día las tecnologías inalámbricas están adquiriendo un mayor protagonismo en el sector empresarial y se han convertido en herramientas indispensables para

su supervivencia; así, para un 49 % de las empresas que participaron en la encuesta, la tecnología inalámbrica es la clave para mantener su competitividad y un 74 % de aquellas espera aumentar su uso en los próximos dos años. Esta afirmación casi triplica la respuesta de los encuestados de un estudio similar en 2007, donde solo el 16 % consideraba a las tecnologías inalámbricas como un factor clave de competitividad.

El auge y los bajos costos asociados a tecnologías inalámbricas específicas, como Wi-Fi, han hecho de estas un sustituto de las redes de cableados de transmisión de datos. Wi-Fi en especial es para muchos un medio ideal de transmisión inalámbrica, fiable para cubrir las necesidades de transmisión de datos a bajo costo.

Sin embargo, el uso de diferentes redes en la misma área de cobertura geográfica lleva a plantear interrogantes asociados a la interferencia que pueden causar entre sí y su real incidencia sobre parámetros de desempeño del sistema.

En Medellín, principalmente en el centro, hay muchos sitios que ofrecen internet a través de redes Wi-Fi. Asimismo, muchas empresas usan Wi-Fi para la comunicación entre sus computadores y como una herramienta económica de acceso a internet de forma privada, lo que trae consigo que diferentes redes que empleen el mismo canal de comunicación se solapen entre sí. Lo anterior causa lentitud e incluso pérdida del servicio.

Planteamiento del problema

Existe una gran cantidad de redes Wi-Fi, lo cual trae consigo problemas tales como:

- La gran cantidad de redes Wi-Fi en la misma zona hace que redes geográficamente cercanas se interfieran entre sí, lo que aumenta la demora en la descarga de archivos y la navegación.
- El bajo costo hace posible que existan organizaciones que proporcionen acceso a internet libre, pero se desconoce su ubicación exacta.

- La facilidad de implementación lleva a que personal no capacitado instale redes Wi-Fi sin una adecuada seguridad, lo que aumenta el riesgo de accesos no autorizados.

El estudio de estos problemas en una zona de la comuna 10 permitirá:

- Evitar en lo posible que redes geográficamente cercanas se interfieran, de tal manera que haya un uso óptimo de los canales y del ancho de banda y un aumento de la velocidad de descarga de archivos y de navegación.
- Establecer dónde se encuentran los puntos de libre acceso a internet en una zona de la comuna 10.
- Aumentar la seguridad de las redes Wi-Fi privadas en una zona de la comuna 10 a través del uso de protocolos confiables.

Las redes inalámbricas 802.11 son inseguras y además pueden ser interferidas por una gran cantidad de dispositivos de comunicación que funcionan en la frecuencia de 2.4 GHz o 5 GHz, tales como teléfonos inalámbricos, microondas, Bluetooth, ZigBee, entre otros; estas interferencias pueden afectar la velocidad de transmisión, (Gómez López, 2008).

Las bajas velocidades de transferencia pueden ser causadas por varios factores como la modulación, el encapsulamiento producido en los protocolos de comunicación, la sintonización fina de la tarjeta de red y el *router* inalámbrico, los protocolos de encriptación usados, la distancia al *router* o *Access Point* (AP); sin embargo, el factor más relevante es el solapamiento de los canales empleados (Moreno & Fernandez, 2007). Vale la pena resaltar que en la actualidad no existe ningún estudio realizado en la comuna 10 que dimensione el problema.

En cuanto a los sitios de libre acceso a internet en dicha comuna, si bien se tiene información sobre la existencia de zonas Wi-Fi libres, no hay un estudio que divulgue su ubicación de una forma sistemática

empleando la georreferenciación, lo que sería de suma utilidad para los visitantes y los habitantes del centro de la ciudad.

Objetivo general

Documentar a través de mapas de cobertura el uso de las redes Wi-Fi en la banda de 2.4 GHz, de libre acceso en puntos críticos de la comuna 10, para proponer una metodología que permita trazar estos mapas; además de aumentar los niveles de seguridad capacitando a las empresas en principios básicos de seguridad que protegen la información y el acceso no autorizado a las redes Wi-Fi de empresas geográficamente cercanas.

Objetivos específicos

Generar mapas georreferenciados de la localización de las redes Wi-Fi de libre acceso y de la utilización de los canales, lo cual exige definir el lugar de estudio y proponer una metodología.

Analizar los protocolos de seguridad empleados por las empresas geográficamente cercanas al lugar de estudio con el fin de generar informes estadísticos y sugerir cómo proteger la información y evitar el acceso no autorizado a sus redes Wi-Fi 2.4 GHz.

Cuantificar experimentalmente la vulnerabilidad de protocolos de seguridad tales como WEP, WPA, WPA2, empleados en las redes Wi-Fi, para hacer recomendaciones sobre los que deben y no deben utilizarse.

Organización del documento. Con la intención de facilitar el conocimiento y comprensión de la temática, este libro se ha organizado en cuatro capítulos:

- En el primer capítulo se hace una revisión del marco conceptual requerido para el solapamiento de canales, la seguridad en Wi-Fi y la creación de mapas georreferenciados, así como la descripción del estudio realizado.

- En el segundo capítulo se describe el diseño del marco experimental, donde se explica la metodología de medición de las interferencias y la toma de muestras para la construcción de los mapas georreferenciados y la situación de la seguridad Wi-Fi en la comuna 10.
- El tercer capítulo lo conforman el marco experimental y la toma de datos donde se desarrollan las mediciones.
- El cuarto y último capítulo presenta la discusión de resultados, seguida de las conclusiones generales de la investigación.

Tecnologías Wi-Fi

Es muy común el uso simultaneo de varias redes Wi-Fi en espacios como residencias, campus universitarios, empresas y sitios públicos; estas pueden producir interferencias entre sí cuando están localizadas en la misma zona. Es frecuente encontrar problemas de bajas velocidades en la transferencia de archivos, incluso con pocos PC conectados a la red Wi-Fi. Este estudio puede ser útil para comprender cómo es afectada la tasa de transferencia de datos en redes Wi-Fi, pero en un aspecto más amplio puede aplicarse a procesos industriales que sean monitoreados o controlados usando tecnologías como ZigBee, la cual podría ser interferida por la red de datos Wi-Fi corporativa.

Dispositivos inalámbricos ZigBee, Bluetooth y Wi-Fi trabajan en la frecuencia ISM (Industrial, Scientific and Medical) de 2.4 GHz, bandas reservadas internacionalmente para uso no comercial y aplicaciones científicas y médicas; la **Tabla 1** hace una comparación de las principales tecnologías que usan esta banda no licenciada de 2.4 GHz.

Tabla 1. Comparación entre tecnologías ZigBee, Bluetooth y Wi-Fi.

	Wi-Fi	Bluetooth	ZigBee
Bandas de frecuencias	2.4 GHz	2.4 GHz	2.4 GHz, 868 / 915 MHz
Tamaño de pila	~ 1 Mb	~ 1 Mb	~ 20 kb
Tasa de transferencia	11 Mbps	1 Mbps	250 kbps (2.4 GHz) 40 kbps (915 MHz) 20 kbps (868 MHz)
Números de canales	11-14	79	16 (2.4 GHz) 10 (915 MHz) 1 (868 MHz)
Tipos de datos	Digital	Digital, audio	Digital (texto)
Rango de nodos internos	100 m	10 m–100 m	10 m–100 m
Números de dispositivos	32	8	255 / 65535

Continúa en la próxima página.

Continuación de la Tabla 1. Comparación entre tecnologías ZigBee, Bluetooth y Wi-Fi.

	Wi-Fi	Bluetooth	ZigBee
Requisitos de alimentación	Media alta - horas de batería	Media - días de batería	Muy baja - años de batería
Introducción al mercado	Alta	Media	Baja
Arquitecturas	Estrella	Estrella	Estrella, árbol, punto a punto y malla
Mejores aplicaciones	Edificio con internet adentro	Computadoras y teléfonos	Control de bajo costo y monitoreo
Consumo de potencia	400 ma transmitiendo, 20 ma en reposo	40 ma transmitiendo, 0.2 ma en reposo	30 ma transmitiendo, 3 ma en reposo
Precio	Costoso	Accesible	Bajo
Complejidad	Complejo	Complejo	Simple

Tomada y modificada de: http://webdelcire.com/wordpress/archives/1714.

Comunicación en modo infraestructura. Como puede verse en la **Figura 1,** en las redes configuradas en modo infraestructura, los computadores se comunican a través de un equipo de comunicaciones inalámbricas, típicamente un *router* inalámbrico o *access point* (Cisco Press, 2006).

La configuración formada por el punto de acceso y las estaciones ubicadas dentro del área de cobertura se llama conjunto de servicio básico en ingles *Basic Service Set* (BSS). En el modo infraestructura cada una de las redes Wi-Fi tiene un identificador llamado SSID, de 48 bits, que corresponde a la MAC del *access point* (Jin-a, Park, Park & Cho, 2002).

Es posible vincular varios puntos de acceso o BSS con una conexión llamada sistema de distribución SD (ByongGi & Sunghyun, 2008), formando así un conjunto de servicio extendido llamado ESS, generalmente a través de un *router* inalámbrico; cada SSID es decir cada nombre de red asociado a una red Wi-Fi debe ser ubicado en un canal diferente para evitar interferencias.

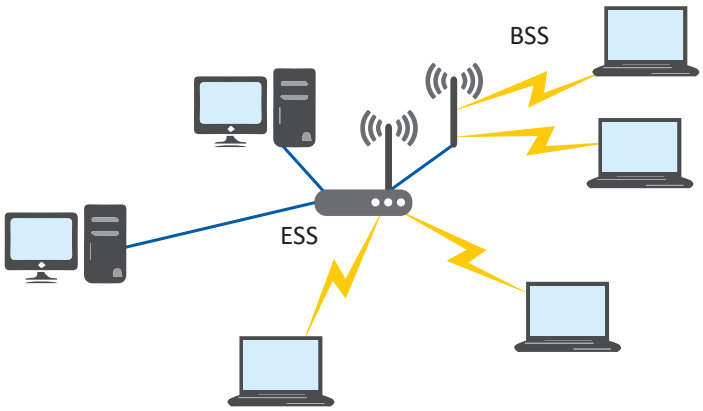


Figura 1. Modo infraestructura con *access point*.

Canales empleados en las redes Wi-Fi. La comunicación Wi-Fi se establece en la banda de 2.4 GHz con 14 canales disponibles; cada uno ocupa 22 MHz de ancho de banda (Jin-a, Park, Park & Cho, 2002). Estos canales con sus respectivas frecuencias se listan en la **Tabla 2.**

Tabla 2. Canales IEEE 802.11 b/gWi-Fi.

Banda	Frecuencia	Canal
2.4 GHz	2412.0 MHz	1
2.4 GHz	2417.0 MHz	2
2.4 GHz	2422.0 MHz	3
2.4 GHz	2427.0 MHz	4
2.4 GHz	2432.0 MHz	5
2.4 GHz	2437.0 MHz	6
2.4 GHz	2442.0 MHz	7
2.4 GHz	2447.0 MHz	8
2.4 GHz	2452.0 MHz	9
2.4 GHz	2457.0 MHz	10
2.4 GHz	2462.0 MHz	11
2.4 GHz	2467.0 MHz	12
2.4 GHz	2472.0 MHz	13
2.4 GHz	2484.0 MHz	14

El estándar IEEE 802.11 b/g permite solo tres canales (canal 1, canal 6 y canal 11) no interferentes, espaciados por 3 MHz (ByongGi & Sunghyun, 2008), como se observa en la **Figura 2.**

Canal 1= 2.412 GHz
Canal 6= 2.437 GHz
Canal 11= 2.462 GHz

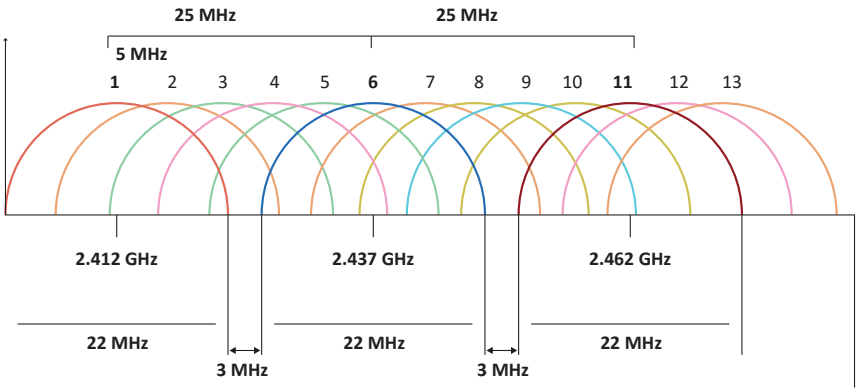


Figura 2. Canales para Wi-Fi no interferibles y anchos de banda. Adaptada por el autor.

De la **Figura 2** se deduce que los canales 2, 3, 4 y 5 interfieren en mayor o menor grado con las comunicaciones del canal 1; así mismo, el canal 6 es interferido por los canales 2, 3, 4, 5, 7, 8, 9 y 10; de igual forma, el canal 11 es interferido por los canales 7, 8, 9, 10, 12, 13 y 14.

Protocolos y seguridad en Wi-Fi

Las tecnologías inalámbricas facilitan el acceso a internet desde cualquier parte. Asimismo, permiten movilidad a los usuarios removiendo las conexiones físicas a las redes. Sin embargo, características propias de emisión en redes inalámbricas han causado preocupación sobre la seguridad, ya que la información es intercambiada en el espacio, donde la intercepción y uso malicioso de aquella se hace más fácil para cualquiera que tenga el equipo adecuado. Por lo tanto, es necesario

desarrollar servicios de seguridad proporcionados por protocolos (López, Alcocer, Barraza, Mendoza e Hinostroza, 2009).

Del estado del arte se concluye que los protocolos más frecuentemente utilizados en las redes Wi-Fi son:

Wired Equivalency Privacy. Este protocolo tiene la intención de suministrar el mismo nivel de privacidad de una red con cable. Es un protocolo de seguridad basado en el método de criptografía RC4, de 64 bits o 128 bits. Ambas utilizan un vector de inicialización de 24 bits. Sin embargo, la clave secreta tiene una extensión de 40 bits o de 104 bits. Todos los productos Wi-Fi soportan la criptografía de 64 bits, pero no todos soportan la criptografía de 128 bits. Además de la criptografía, utiliza un procedimiento de comprobación de redundancia cíclica en el patrón CRC-32, usado para verificar la integridad del paquete de datos. El WEP no protege la conexión por completo, sino solamente el paquete de datos. El protocolo WEP no es totalmente seguro, pues ya existen programas capaces de quebrar las claves de criptografía en el caso de que la red sea monitorizada durante un tiempo considerable, (Grupo Informática-Hoy, s. f.).

Wi-Fi Protected Access. Diseñado para proteger las versiones actuales y futuras de los dispositivos IEEE 802.11. WPA es un subconjunto de la especificación IEEE 802.11i y reemplaza a WEP con una nueva tecnología de encriptación llamada Protocolo de Integridad de Clave Temporal (TKIP) con Message Integrity Check (MIC). También proporciona un esquema de autenticación mutua utilizando protocolo IEEE 802.1X/ Extensible autenticación (EAP) o la clave precompartida (PSK) tecnología (Wi-Fi Alliance, 2005).

Fue elaborado para solucionar los problemas de seguridad del WEP. El WPA posee un protocolo denominado TKIP (Temporal Key Integrity Protocol), con un vector de inicialización de 48 bits y una criptografía de 128 bits. Con la utilización del TKIP la llave es alterada en cada paquete

y sincronizada entre el cliente y el *access point*; también hace uso de autenticación del usuario por un servidor central. (Wi-Fi Alliance, 2005).

WPA2. Es una mejoría de WPA que utiliza el algoritmo de encriptación denominado AES (Advanced Encryption Standard); WPA2 ofrece protección avanzada contra ataques de red inalámbrica. Utilizando AES, encriptación de nivel gubernamental y IEEE 802.1X/EAP, WPA2 proporciona fuerte autenticación mutua basada en estándares y cifrado avanzado para proteger la red Wi-Fi de una variedad de amenazas y ataques.

Ante la detección de la existencia de una brecha en la seguridad del protocolo utilizado por WPA versión 1, la Wi-Fi Alliance desarrolló una segunda versión que corrige dicho problema. Esta obliga a la implementación del protocolo de encriptación AES, que se usa por defecto en la norma WPA versión 2.

Mapas georreferenciados

Los mapas georreferenciados como el mostrado en la **Figura 3** están formados por un esquema de lugares o espacios selectivos identificados por medio de referencias dadas geográficamente, creadas por un dispositivo de localización GPS, sistema de posicionamiento global, para la obtención de información a través de un medio de comunicación; los servicios de información georreferenciados, útiles en entornos de movilidad, permiten localizar los sitios de interés geográfico y los contenidos georreferenciados que crean los usuarios con conocimientos sobre un entorno físico para compartir información (Solórzano, 2007).

La ubicación expresada como un texto es por lo general la dirección de una calle, ciudad, comuna, código postal, etc. Una ubicación espacial puede ser expresada en términos de coordenadas geográficas usando latitud-longitud-altitud, esta última opcional; la latitud se expresa en grados de 0-90 al norte o sur del Ecuador, la longitud en grados de 0-180

al este u oeste del meridiano de Greenwich, y la altitud en metros sobre el nivel del mar (Bertuzzi, 2007).

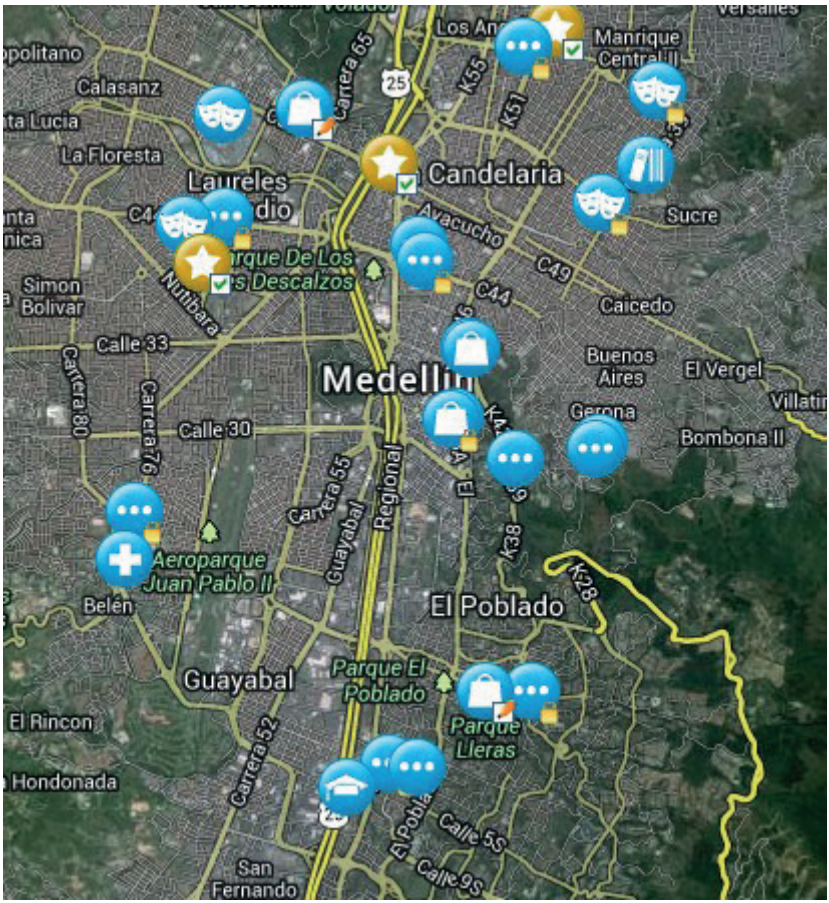


Figura 3. Mapa georreferenciado de Medellín. Tomada de: http://www.wefi.com/maps/

Existen sistemas interactivos para la gestión de documentos georreferenciados basados en identificación por radiofrecuencia (RFID, Radio Frequency IDentification), que se relacionan con la selección de varias zonas para la creación de un mapa que permita compartir la

información obtenida entre varios usuarios a través de GPS por medio de la comunicación Wi-Fi (Romero, Tesoriero, Gallud & Penichet, 2004).

Penetración y uso público del Wi-Fi

La penetración del Wi-Fi es sustancialmente superior a las de tecnologías que también vienen en crecimiento como 3G; en muchas plazas y parques alrededor del mundo se instalan nuevas redes para Wi-Fi con libre acceso a internet.

La iniciativa del Ministerio TIC busca acercar a todos los habitantes de Colombia al uso del internet Wi-Fi en plazas de mercado, terminales de transporte, parques principales y sitios emblemáticos (MinTic, 2014). Venezuela quiere modernizarse en lo que respecta al acceso a internet y para lograrlo, en los próximos meses abrirán nuevos puntos de acceso a internet vía Wi-Fi, que estarán ubicados en las zonas públicas de las ciudades más importantes del país (Siliconweek, 2014). En Perú se busca dotar de manera gratuita con conexión a internet a través de la red "Wi-Fi sin costo" a centros comerciales, parques, playas y espacios deportivos y de entretenimiento en Lima. Se espera contar con más de 200 puntos de acceso en diferentes lugares de la ciudad; esta señal Wi-Fi ya es utilizada por más de 20.000 usuarios (Perú 21, 2014). En Ecuador se planea conectar a 1.171 instituciones educativas. Solo en Guayaquil se proyecta conectar, en el primer cuatrimestre del 2014, a 40 de estas (El ciudadano, 2014). En chile, el actual programa de zonas Wi-Fi ChileGob beneficiará en total a 153 localidades en seis regiones del país. La implementación de la primera fase comenzó en julio 2014 con 196 puntos de acceso; la segunda etapa del programa se iniciará en septiembre de 2014, para finalizar el próximo año con 416 puntos de acceso (Subtel, 2014). Por su parte, Bolivia tiene planes de socializar un proyecto de ley sobre la instalación de internet Wi-Fi gratuito que fue aprobado en la Cámara de Diputados y que está corriendo trámite en el Senado (WIFIBolivia, 2015). En Argentina, desde el 2013 el sistema Metrobús 9 de Julio de Buenos Aires cuenta con Wi-Fi; en esta ciudad existen más de 150 puntos de acceso, entre parques, plazas, espacios

públicos, sedes comunales, hospitales y centros de salud, bibliotecas y museos (Buenos Aires Ciudad, 2014).

Sin embargo, sobre el uso de Wi-Fi con acceso gratis a internet, las empresas F-secure y el Instituto de Investigaciones Cyber Security Research Institute y SyyS realizaron un experimento en el cual se puso un punto de acceso inalámbrico Wi-Fi; el objetivo de esta investigación fue demostrar que los puntos de acceso público son inseguros. Luego observaron cómo la gente se conectaba sin importarles que su actividad en internet fuera espiada. En un periodo de 30 minutos, 250 dispositivos se conectaron al punto de acceso; probablemente muchos de ellos de manera automática y sin que sus dueños se dieran cuenta. 33 personas activaron el tráfico de internet por medio de la realización de búsquedas en la web y envío de datos y *mails*. 32 MB de tráfico fueron capturados y destruidos rápidamente para cuidar la privacidad (Safe&Savvy, 2014).

Según Sean Sullivan, asesor de seguridad de F-Secure, comenta: "A todos nos gusta usar Wi-Fi gratis para ahorrar datos o las tarifas de *roaming*; es demasiado fácil para cualquiera que cree un punto de acceso darle un nombre que parece creíble y espiar la actividad de internet de los usuarios" (Noticias Palermonline, 2014).

Marco metodológico

Definir el lugar geográfico de estudio dentro de la comuna 10

El estudio se determinó teniendo en cuenta los centros comerciales, bulevares, los sitios concurridos como la plaza Botero, y los hoteles, así como la cercanía a la Uniremington, de tal manera que los resultados impacten a nuestros vecinos; por lo anterior se estableció la zona comprendida entre Carabobo (carrera 52) hasta la avenida Oriental, y desde la calle 53 hasta Colombia (calle 50). Esta delimitación se muestra en la **Figura 4.**

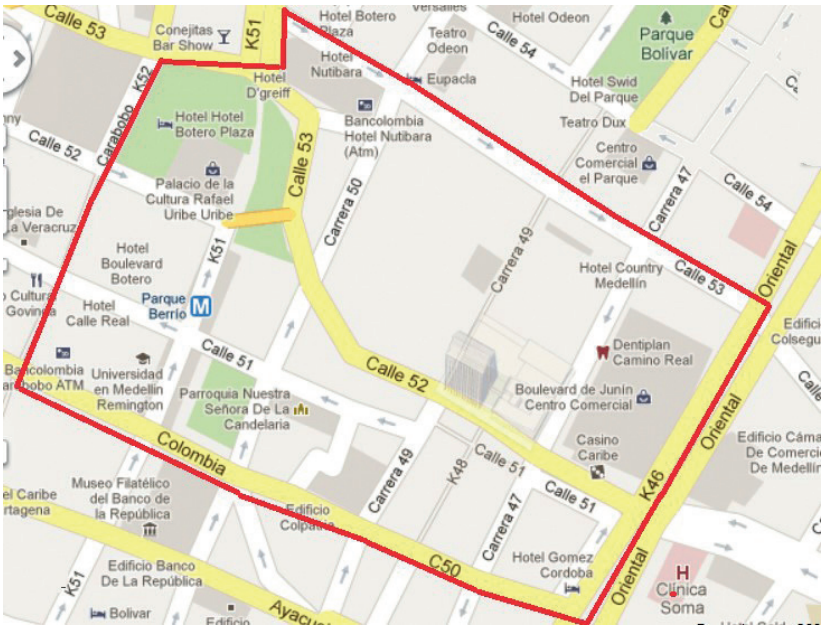


Figura 4. Delimitación del área de estudio. Tomada de: Google Maps.

Protocolo de medición

Se realizaron varios tipos de Mediciones Preliminares (MP) llamadas MPWS (Medición Preliminar Wi-Fi Solapamiento), que permiten cuantificar la degradación de la transferencia de datos por solapamiento

de canales; en segundo lugar se desarrollan las pruebas MPWV (Medición Preliminar Wi-Fi Vulnerabilidades), que permite conocer las vulnerabilidades de los protocolos de seguridad empleados en las redes Wi-Fi. En tercer lugar se realiza la búsqueda de redes de uso libre en el área de estudio, llamadas CWZL (Pruebas Campo Wi-Fi Zonas Libres); por último se realizan las pruebas de campo y la caracterización del uso de protocolos de seguridad de las redes Wi-Fi, llamadas PCWPS (Pruebas Campo Wi-Fi Protocolos de Seguridad).

El estudio se centra en la comuna 10, específicamente en el aérea comprendida entre la calle 50 (Colombia)-carrera 46 (avenida Oriental)-Calle 53 (Maracaibo)-Carrera 52 (Carabobo), **(Figura 4).** Se dividió el área de estudio en 24 zonas y se realizó un primer recorrido exploratorio de toma de muestras seleccionando diferentes zonas reconocidas como de mayor influencia comercial: centros comerciales, hoteles, hospitales, etc., con el propósito de determinar inicialmente cuántas subdivisiones son necesarias para la prueba general (la división final de zonas se muestra en la **Figura 5**).

En el proceso se determinó que es necesario solicitar permisos a las instituciones y lugares acordados para realizar la toma de pruebas y acceder a la información requerida.

Además, es necesario realizar recorridos exploratorios de toma de muestras con dispositivos más pequeños, como teléfonos con *software*, que permitan hacer cálculos de la cantidad de redes Wi-Fi que pueden encontrarse y la densidad de estas, y tomar decisiones sobre cómo hacer el escaneo. Dado que las redes cambian por la potencia relativa, se toman tiempos superiores a 10 minutos para "estabilizar" la toma de muestras.

Metodológicamente, el proceso se puede resumir como lo muestra la **Figura 6** para cada una de las 24 zonas.

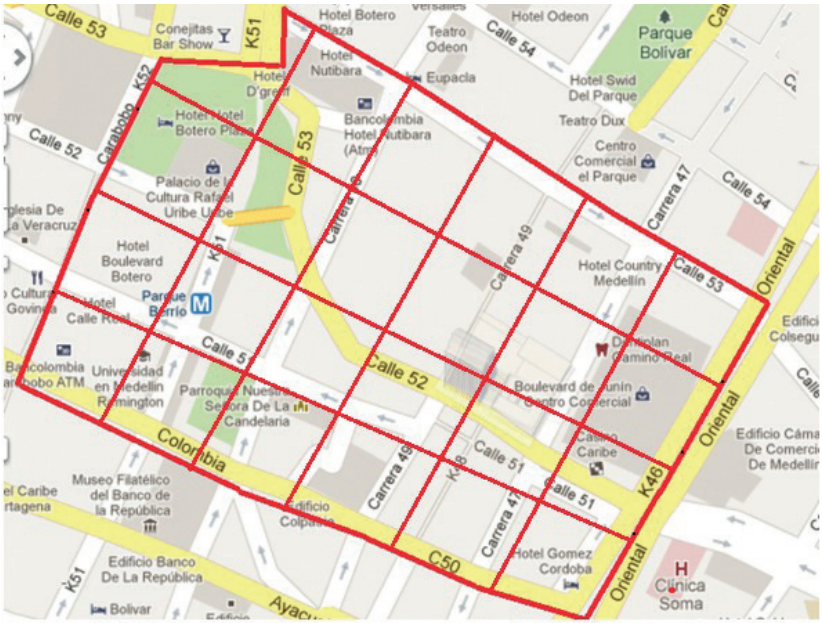


Figura 5. División en zonas del área de estudio. Tomada de: Google Maps.

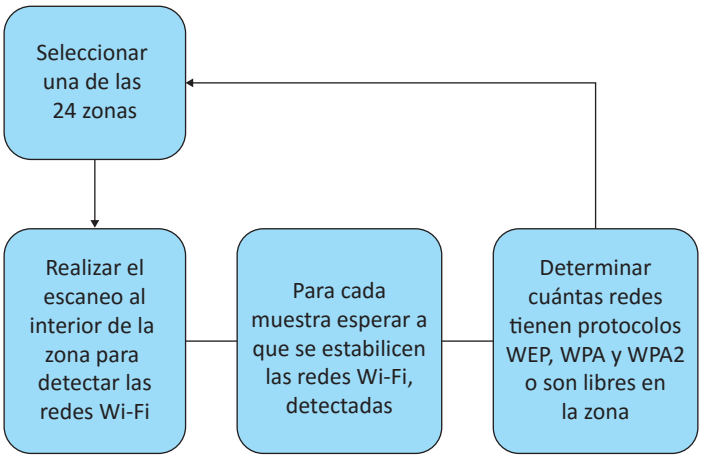


Figura 6. Representación metodológica empleada.

Dado que fueron requeridos varios tipos de pruebas y mediciones en campo, se detallaron en la **Tabla 3** para mayor claridad del lector.

Tabla 3. Descripción detallada de pruebas experimentales realizadas en la investigación.

Pruebas experimentales	
MP	**MPWS.** Pruebas preliminares de tipo experimental que permiten cuantificar la degradación de la transferencia de datos por solapamiento de canales; así se cuantifica el problema.
	MPWV. La prueba permite descifrar claves en redes Wi-Fi configuradas con protocolo de seguridad WEP para demostrar su vulnerabilidad.
PC	**PCWZL.** Este tipo de pruebas tiene como finalidad crear un mapa con los puntos de conexión Wi-Fi de libre acceso obtenidos en cada una de las zonas de estudio.
	PCWPS. Estas pruebas de campo tienen como objetivo realizar la caracterización del uso de protocolos de seguridad de las redes Wi-Fi en la comuna 10.

Un mapa conceptual completo de los tipos de experimentos involucrados se detalla en la **Figura 7.**

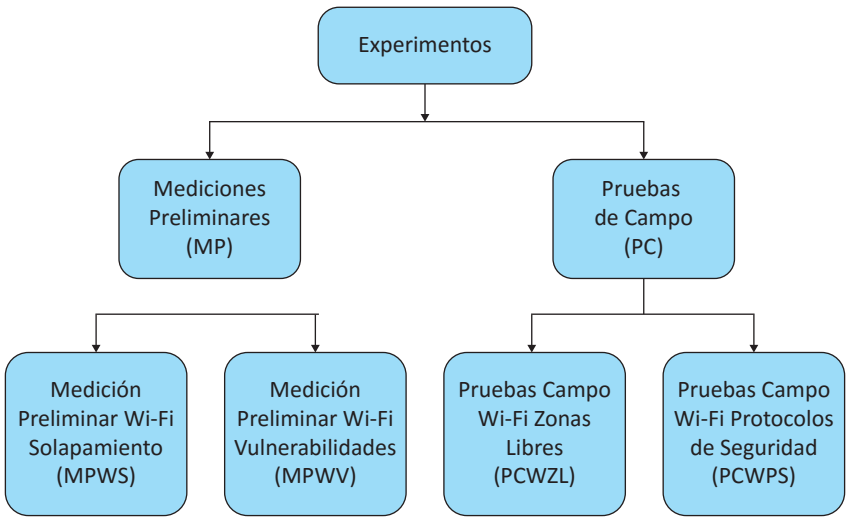


Figura 7. Mapa conceptual de las pruebas experimentales.

Las pruebas experimentales, además de las siglas empleadas, serán diferenciadas por un número consecutivo de dos dígitos.

La **Tabla 4** muestra un resumen de los protocolos empleados para cada una de las pruebas experimentales.

Tabla 4. Resumen del protocolo de medición de las pruebas experimentales.

Pruebas experimentales	
MP	**MPWS** 1. Se busca un canal que esté usado por otra transmisión Wi-Fi. 2. Se toman muestras de las tasas promedio de transferencia de datos enviando un archivo de 1.2 GB en 15 ocasiones diferentes. 3. Se toman promedios por cada uno de los envíos; se calcula la media y el promedio. 4. Se busca un canal libre de interferencias y se realizan los pasos 2 y 3.
	MPWV 1. Se obtiene un listado de las redes Wi-Fi del entorno: SSID, canal, protocolo de seguridad. 2. Se eligen las redes con seguridad WEP y buena señal (por encima del 50 % de fuerza). 3. Se capturan aproximadamente 25 paquetes y se guardan en un archivo. 4. Utilizando el archivo anterior, se procede a descifrar la clave de la señal que se está atacando. 5. Al final se obtiene una clave que normalmente estará en formato hexadecimal; las pruebas realizadas tienen un 100 % de éxito y no demoran más de 30 minutos.
PC	**PCWZL** 1. La zona seleccionada de la comuna 10 tendrá 24 subdivisiones de campo para efectuar cuatro mediciones de prueba de acceso libre a redes Wi-Fi en distintos espacios de tiempo, los cuales permitirán tomar 96 muestras para realizar los análisis de resultados. 2. Los lugares escogidos serán los centros comerciales con mayor cantidad de locales. 3. Se hace la verificación y registro de la coordenada de los puntos de conexión libre. 4. Con las coordenadas se hace un mapa georreferenciado de la zona **(Figura 4).** 5. Se registra el número de conexiones libres por cada sector; se identifican las que presentan solapamiento, y se marca por cada sector la ubicación georreferenciada de los puntos libres encontrados para visualizar el mapa. Las pruebas entregarán información para los siguientes aspectos: 1. **Nombre de conexión SSID:** el nombre del usuario con el proveedor del servicio Wi-Fi.

Continúa en la próxima página.

Continuación de la Tabla 4. Resumen de protocolo de medición de las pruebas experimentales.

Pruebas experimentales	
PC	2. **Tipo de radio:** establece el alcance y nivel de la señal 802.11X con X = a, b, g, n. 3. **Tipo de seguridad:** determina la clase de protocolo de seguridad (WPA, WPA2, TKIP, WEP, 802.1x etc.). 4. **Coordenada geográfica GPS (latitud, longitud, altitud):** son valores que se referencian indicando el punto de conexión de libre acceso marcado en el mapa (de forma manual o usando un *software* de computadora). 5. **Conexión de libre acceso:** no identifica ningún protocolo de seguridad.
	PCWPS 1. En cada uno de los sectores (24 en total) se realiza un escaneo para la búsqueda de redes Wi-Fi. 2. Se determina cuántas redes Wi-Fi no tienen protocolos de seguridad (libres) y cuántas no. 3. Se determina cuáles son las redes que tienen protocolos de seguridad (WEP, WPA y WPA2).

Nota: la **Tabla 3** muestra una descripción de las pruebas y convenciones usadas en esta investigación.

Encuesta

¿Qué resultados se buscan? Se realizará una encuesta para determinar el grado de conocimiento de las personas ubicadas en centros comerciales, hoteles, bulevares y sitios concurridos en la zona de la comuna 10 (definida en la **Figura 1**) acerca de los factores que afectan la conexión a internet, tales como: interferencia, seguridad y solapamiento de canales en sitios de libre acceso cuando se emplean redes Wi-Fi.

Aspectos éticos. La información suministrada por las personas ubicadas en sus respectivos negocios en la zona ya descrita no será publicada ni divulgada y solo será utilizada por quienes participan en el proyecto.

Descripción de la unidad de análisis. Ficha técnica.

- **Objeto de estudio.** Se desea conocer qué saben acerca de la caracterización y documentación georreferenciada de la interferencia, la seguridad y el solapamiento de canales en sitios de libre acceso a internet para redes Wi-Fi.

- **Población.** La encuesta se hará en los centros comerciales, bulevares, sitios concurridos como la plaza Botero, hoteles y otros espacios cercanos a la Corporación Universitaria Remingtonque cuenten con conexión Wi-Fi gratis (acceso libre).

- **Muestra.** Se les aplicará la encuesta a los empleados o encargados de la red de los locales que tengan el servicio, según lo mencionado en la población.

- **Variable.** Es una característica del objeto de estudio. Existen principalmente dos tipos de variables: cualitativas y cuantitativas.

- **Escala de medición.** Mide el comportamiento de la variable. Existen principalmente cuatro tipos de escala de medición, que son: nominal, ordinal, intervalar y proporcional.

- **Recolección de la información.** El personal se desplazará hasta el lugar determinado para realizar la encuesta, conformada por 12 preguntas.

- **Tipos de muestreo.** Se utilizarán dos tipos de muestreo; el primero es aleatorio simple, un proceso probabilístico que permite determinar al azar qué negocios o personas se deben encuestar. Como apoyo se utilizará en la investigación de campo un muestreo no probabilístico porque se desconoce la precisión de la muestra. El investigador seleccionará los casos que contengan la mayor cantidad de información acerca del objeto de estudio. La **Tabla 5** muestra las preguntas, el tipo de variable y las escalas de medición empleada.

Tabla 5. Preguntas variables y escalas de medición.

Pregunta	Variable	Escala de medición
¿Usted cree que su nivel de conocimiento acerca de Wi-Fi es?	Cuantitativa discreta	Ordinal
¿Qué tanto cree usted que Wi-Fi es seguro?	Cuantitativa discreta	Ordinal
¿Ha utilizado conexiones Wi-Fi para realizar transacciones comerciales?	Cualitativa	Nominal
¿Considera usted que las conexiones Wi-Fi son más rápidas que las conexiones cableadas?	Cualitativa	Nominal
¿Cuál de estas conexiones es la que más utiliza?	Cualitativa	Nominal
¿A través de qué dispositivo se conecta en mayor medida a redes Wi-Fi?	Cualitativa	Nominal
¿Cuál es su proveedor de servicios (ISP) de banda ancha (internet)?	Cualitativa	Nominal

Continúa en la próxima página.

Continuación de la Tabla 5. Preguntas variables y escalas de medición.

Pregunta	Variable	Escala de medición
¿De cuántos *megabytes* es la conexión de banda ancha que tiene contratada?	Cuantitativa continua	Intervalar
¿Cuál es la frecuencia de uso de Wi-Fi?	Cuantitativa continua	Intervalar
¿Qué tan seguro se siente al utilizar redes Wi-Fi de libre acceso?	Cuantitativa discreta	Ordinal
¿Conoce usted sitios de libre acceso en el centro de la ciudad?	Cualitativa	Nominal
¿Ha utilizado conexiones Wi-Fi sin autorización?	Cualitativa	Nominal

Marco experimental

Mediciones Preliminares (MP)

Medición Preliminar Wi-Fi Solapamiento (MPWS). Para cuantificar la magnitud de la interferencia se optó por una prueba experimental, la cual consistió en el montaje de una red donde se pudieran tomar algunas mediciones; para la construcción de esta red se requirieron algunos elementos de *software* y *hardware*.

***Software*:** existen analizadores de espectro y *software* que permiten ver el comportamiento de los canales empleados; para la elaboración de las pruebas se usó *software*; entre varias opciones disponibles se escogió la herramienta InSSIDer[1], que es un programa de escaneo que realiza un análisis en tiempo real del espectro en la banda de 2,4 GHz y 5 GHz.

El *software* InSSIDer es de uso libre y permite ver los ESSID de las redes inalámbricas que se encuentren en la zona, así como el canal usado de un modo gráfico; también muestra la intensidad de trasmisión de los ESS (Metageek, 2011).

***Hardware*:** las pruebas se realizaron en un computador portátil HP TX2 2010 con tarjeta *wireless* LAN 802.11a/b/g/n y tecnología Bluetooth. Otras especificaciones técnicas de la HP TouchSmart tx2 son:

1. Procesador AMD Turion™ X2 RM-77 Dual-Core.
2. Memoria de 3072 MB DDR2 a 800 MHz.
3. Disco duro de 320 GB SATA a 7200 RPM.
4. El *router* usado fue un NetGear WGT624.
5. Internet/WAN 10/100 Mbps (auto-sensing) Ethernet, RJ-45.

1 http://www.metageek.net/products/inssider, open-source Wi-Fi scanner software, inSSIDer actually works with Windows Vista, Windows 7, and 64-bit PCs.

6. LAN: 4 ports 10/100 Mbps (auto-sensing) Ethernet, RJ-45.
7. *Wireless*: -Network Speeds 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, & 54 Mbps (auto-rate capable) 108 Mbps (Static and Dynamic).
8. Modulation Type: OFDM with BPSK, QPSK, 16QAM, 64QAM, DBPSK, DQPSK. CCK Frequency Band: 2.4 GHz, Standards Capability: 802.11 g and 802.11 b - Antenna: 2 dBi attached.

La prueba experimental MPWS permitirá cuantificar qué tan real es el problema de las interferencias en las redes Wi-Fi para poder proyectar esta interferencia a procesos de comunicación en redes industriales ZigBee que trabajan en la misma frecuencia ISM 2.4 GHz de uso no comercial. Dada la alta utilización de las redes Wi-Fi en escenarios diversos, es muy común encontrar bajas velocidades en la transferencia de archivos en una configuración de infraestructura, incluso si en la red solo hay dos computadores conectados inalámbricamente.

Para MPWS se decidió usar un escenario totalmente real, típico de muchos sitios residenciales donde existen varias redes Wi-Fi, cada una con su propio ESSID, convergiendo en un mismo sitio geográfico e interfiriendo entre sí. Se instaló una red de tipo infraestructura entre el portátil y el *router*, como se muestra en la **Figura 8,** usando el ESSID RCGCalume; y se transmitió en un canal interferido y luego en otro que no lo estuviera. Para conocer los canales usados por las diferentes ESS se realiza un escaneo previo con inSSider.

Al *router* se conectaron 2 PC: uno inalámbrico y otro al puerto LAN por cable; este último comparte un archivo para transferir.

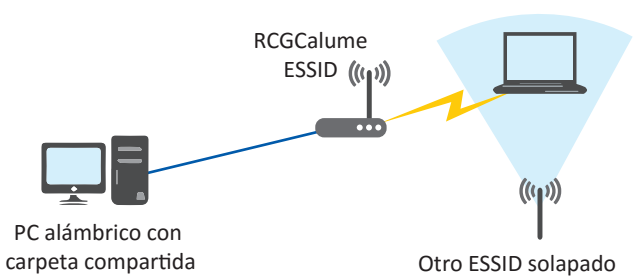


Figura 8. Infraestructura empleada.

Se realiza una transmisión de un archivo de tipo AVI; se escoge este tipo de archivo por ser de gran tamaño (aproximadamente 1.2 GB) y que además tiene un radio de compresión alto que no permite ser nuevamente comprimido durante la transmisión. Esta se realizó primero con un canal libre no interferido y luego se hizo la prueba en otro canal donde hubiese solapamiento con otro ESS cercano; con estos valores promedio se contrastó la tasa de transferencia para cada caso.

Toma de muestras: la distribución de potencia de señal medida en dBm[2]; el cálculo del valor de un nivel de potencia P en dBm viene dado por la **Ecuación 1.**

$$P(\text{dBm}) = 10 \text{ x } \log \frac{P(w)}{1 \text{ mW}} \quad (1)$$

Debe tenerse en cuenta que si se quieren realizar operaciones más complejas con estos niveles de potencia, por ejemplo, sacar un promedio de los datos, estos deben ser transformados a potencia en watts, sacar el promedio y luego transformar el resultado de vuelta a dBm con la **Ecuación 2.**

$$\text{dBm}_{\text{promedio}} = 10 \text{ x } \log \left(\frac{\Sigma_{i=1}^{n} P_n}{n * 1\text{mW}} \right) \quad (2)$$

Las **Ecuaciones 1 y 2** deben emplearse para calcular y promediar los resultados obtenidos, lo cual es entregado en forma gráfica por el inSSIDer. En la **Figura 9** se muestra el comportamiento de varias redes Wi-Fi, cada una representada por un color diferente; se observa que la potencia de las señales cambia en el tiempo.

2 El dBm es una unidad de medida utilizada, principalmente, en telecomunicación para expresar la potencia absoluta mediante una relación logarítmica. El dBm se define como el nivel de potencia en decibelios en relación con un nivel de referencia de 1 mW.

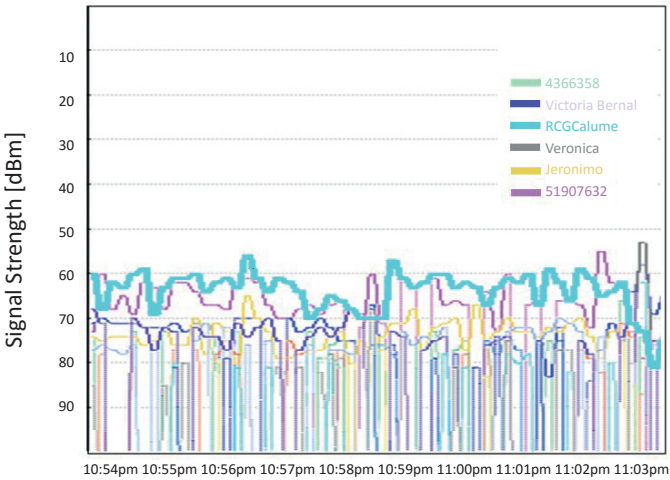


Figura 9. Distribución de potencia en tiempo dado en dBm.
El autor utilizó el programa InSSider.

La **Figura 10** muestra el resultado del escaneo realizado con el *software* inSSIDer; aquí se ilustran las situaciones actuales de la distribución de las redes (ESSID) cercanas, así como los canales que usan para el escenario de prueba.

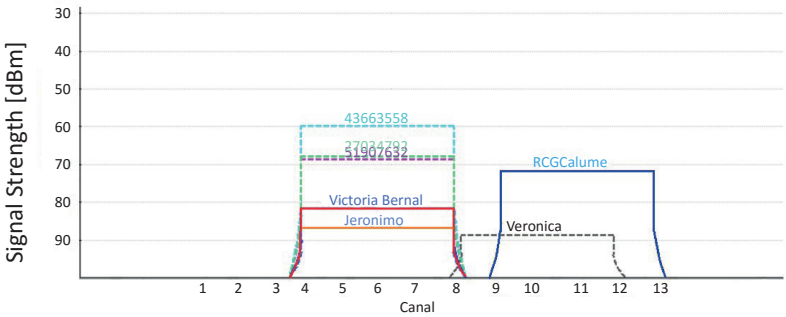


Figura 10. Distribución en los canales de las redes cercanas.
El autor utilizó el programa InSSider.

Para la prueba experimental EPPW01 se configuró la red "RCGCalume" para transmisión en el canal 11, como se observa en la **Figura 10,** que se solapa con la red "Veronica".

Se realizan una serie de pruebas en las que se toman muestras de las tasas promedio de transferencias de datos (se envía el archivo de 1.2 GB 15 veces y se toman promedios por cada uno de los envíos). Los resultados se consignan en la **Tabla 6** y se analizan en el próximo capítulo.

Tabla 6. Resultados de envío de archivo en canal con interferencia.

Número de prueba	Promedio en Kbps
1	369
2	368
3	310
4	378
5	439
6	345
7	407
8	422
9	380
10	441
11	391
12	326
13	340
14	435
15	409
Promedio	384
Mediana	380

Se calcula la mediana porque esta proporciona la tendencia central de los datos obtenidos; se encuentra en el intervalo donde la frecuencia acumulada llega hasta la mitad de la suma de las frecuencias absolutas; la mediana de una serie de datos viene dada por la **Ecuación 3:**

$$Me = L_i + \frac{\frac{N}{2} - F_{i-1}}{f_i} . a_i \quad (3)$$

Luego del escaneo de frecuencias se observa que el canal 1 está libre, por lo que se ubica el *router* en este; se envía nuevamente el mismo archivo y se promedia la velocidad de transferencia en 15 transmisiones independientes.

Para este nuevo escenario se hace el escaneo y se repite el mismo proceso con el canal libre. Los resultados se consignan en la **Tabla 7** y se analizan en el próximo capítulo (también se muestran en la **Figura 11**).

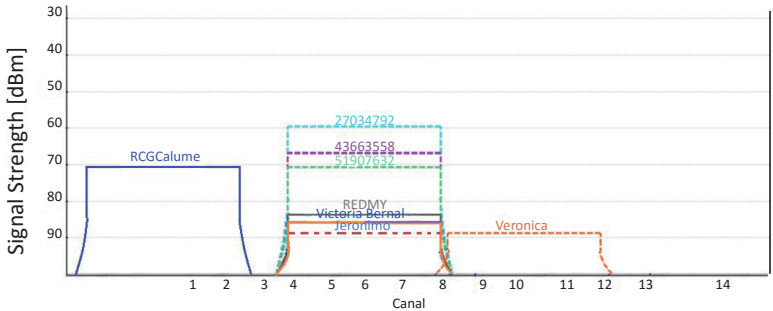


Figura 11. Distribución en los canales de las redes cercanas luego del cambio. El autor utilizó el programa InSSider.

Tabla 7. Canal libre interferencia MPWS.

Número de prueba	Promedio en Kbps
1	1950
2	1975
3	1890
4	1940
5	1875
6	1920
7	1988

Continúa en la próxima página.

Continuación de la Tabla 7. Canal libre interferencia MPWS.

Número de prueba	Promedio en Kbps
8	1834
9	1990
10	1810
11	1984
12	1960
13	1920
14	1984
15	1930
Promedio	1930
Mediana	1940

Medición Preliminar Wi-Fi Vulnerabilidades (MPWV). Para descifrar la clave de una red Wi-Fi con protocolo WEP primero se configuró un *router* con estas especificaciones; luego se asignó una clave de 64 bits y se conectó un equipo de escritorio a internet a través de este *router*, con un tráfico que principalmente consistía en videos de YouTube.

Luego de tener éxito con esta prueba se realizó el mismo procedimiento con una señal proveniente de una red vecina, a la cual estaban conectados tres dispositivos, lo que generaba un buen tráfico, suficiente para acumular la cantidad de paquetes requeridos en poco tiempo.

***Software*:** para las pruebas de penetración y auditoría en temas de seguridad informática se utilizó una distribución Linux en formato Live CD llamada BackTrack 5 r3.

De la distribución fueron usadas las siguientes herramientas:

- **Airmon-ng:** parar o iniciar los servicios de la tarjeta de red.
- **Macchanger:** cambiar la dirección MAC de la tarjeta de red.
- **Airodump-ng:** detectar las redes inalámbricas disponibles y capturar paquetes.

- **Aireplay-ng:** inyectar tráfico en la red.
- **Aircrack-ng:** obtener la clave WEP con base en los paquetes capturados.

***Hardware*:** la prueba fue realizada con los siguientes elementos de *hardware*.

- *Router* inalámbrico TP LINK modelo TL-WR1043ND con velocidad de 300 Mbps, tres antenas de 5 dBi, velocidad de señal 11 ngb y frecuencia 2.4 - 2.4835 GHz.
- PC de escritorio con procesador Intel Core 2 Duo de 2.33 GHz, 4 GB de memoria RAM y 500 Gb en disco duro con capacidad de conexión Wi-Fi.
- Un computador portátil con procesador Core i7 de 2.3 GHz, 8 GB de memoria RAM y disco duro de 1024 GB con capacidad de conexión Wi-Fi.

Toma de muestras MPWV: la prueba MPWV permite verificar que es posible descifrar la clave de las redes Wi-Fi configuradas con protocolos WEP, lo cual se constituye en un problema de seguridad.

La prueba se realiza en dos contextos: primero se dispone una pequeña red conformada por un *router*, configurada con seguridad WEP y una clave de 64 bits, un computador de mesa para generar tráfico y uno portátil para realizar el ataque.

En el segundo contexto, y para verificar la eficacia de la prueba, se repite el proceso haciendo un ataque experimental a una red vecina, para lo cual solo se utilizan el portátil y el *software* de penetración.

Queda fuera del alcance de este documento instruir o documentar la forma en la cual se puede vulnerar una red Wi-Fi; sin embargo, se realizaron pruebas con el *software* CDLive de Backtrack 5. El procedimiento en su totalidad no deberá tardar más de 30 minutos si se tiene la configuración adecuada.

En muchos casos, si la red atacada no tiene un tráfico significativo, es posible, para acelerar la captura de paquetes, inyectar tráfico en la señal de la red atacada siempre y cuando los *routers* lo permitan. Estas pruebas dan como resultado que es posible generar una clave que permita el uso no autorizado de la red Wi-Fi atacada; esto es ampliamente respaldado tanto en la literatura formal en bases de datos reconocidas como en la literatura gris encontrada.

Pruebas de campo

Mediciones de Campo Wi-Fi Zonas Libres (MCWZL). Estas pruebas de campo permitieron encontrar los puntos de conexión Wi-Fi de libre acceso en cada una de las 24 zonas de la comuna 10, como se muestra en la **Figura 5;** cada una de estas redes Wi-Fi de libre acceso se georreferenció empleando el siguiente *software* y *hardware*.

***Software*:** para hallar y analizar la ubicación de los puntos de acceso que no poseen seguridad en el área geográfica establecida se usaron Inssider y Wi-Spy; estos permiten hacer un escaneo de las redes Wi-Fi en las frecuencias de 2.4 y 5 GHz para ver en tiempo real el espectro completo de la señal; sin embargo, este estudio solo se focalizó en las frecuencias de 2.4 MHz, ya que es la más común. Se realizó un barrido en cada uno de los 14 canales para observar paramentos como el tipo de conexión, el tráfico, la potencia, la ocupación del canal y las interferencias por solapamiento. Para generar los mapas georreferenciados se obtuvo para cada una de las redes Wi-Fi la localización GPS; luego, estas coordenadas se geolocalizaron con ayuda de la herramienta de libre uso que facilita Google para este fin: InSSider.

InSSider: esta herramienta de *software* analiza la potencia de las redes Wi-Fi cercanas y el canal en el cual están trabajando; genera una imagen completa sobre cómo es la actividad e intensidad de la señal Wi-Fi. Esta

información permitiría en un momento dado localizar y diagnosticar problemas por solapamiento de canales.

Funcionamiento: el *software* inSSider muestra una imagen del espectro de la señal, que se interpreta con franjas de color que obedecen a la utilización del canal **(Figura 12).**

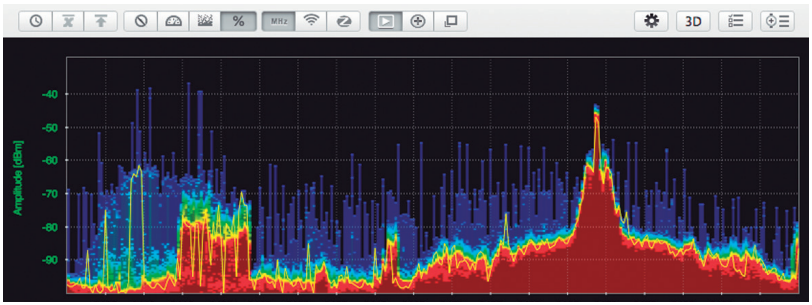


Figura 12. Espectro de una señal. Tomada de: http://www.metageek.net/products/wi-spy/ El autor utilizó el programa InSSider.

Wi-Spy: este es un analizador de espectro que sirve para ver los problemas y visualizar e interpretar características de las fallas de Wi-Fi, como la interferencia electrónica en el proceso de enlace de las señales, lo que facilita a los administradores de redes el análisis de espectro real para poder plantear mejoras en la gestión de red Wi-Fi. Con capacidad de hacer mediciones de señales, este *software* viene con una antena propia que se instala en el PC a través de un puerto USB.

Funcionamiento: cuando se instala Wi-Spy en el computador y se da inicio al programa, se pueden ver todas las señales de redes inalámbricas detectadas convertidas en gráficos y hojas de datos; muestra además las interferencias de radiofrecuencia. Cuando se mezcla con una interfaz de red inalámbrica, deja ver los puntos de acceso activos como se muestra en el espectro para determinar si se creó interferencia en la señal.

***Software* Google Maps:** es un servidor de Google que fue lanzado en febrero de 2005; funciona basado en el uso de código Java Script y ofrece imágenes satelitales de todo el planeta con los mapas de sus ciudades; por ser de programación abierta proporciona diversas utilidades desde distintos puntos en la web. *Funcionamiento:* Google Maps permite crear los mapas de una región geográfica y referenciarlos con marcación selectiva de un lugar específico con gran precisión para ser accedida desde la web en cualquier instante. Tiene la posibilidad de cargar datos por medio de la dirección o coordenada geográfica de un lugar de región representando un punto georreferenciado, marcado como imagen, el cual es buscado y señalado en el mapa de región. Un grupo de marcaciones sobre distintas coordenadas va formando el mapa georreferenciado con sus diferentes capas de zona referenciada, como se muestra en la **Figura 13.**

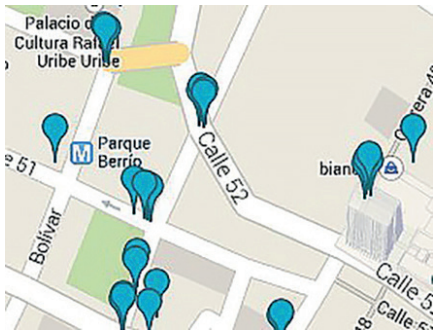


Figura 13. Ejemplo de mapa georreferenciado del estudio en la comuna 10 de Medellín. Tomada de: Google Maps.

Hardware: las pruebas de campo se realizaron con un computador portátil Lenovo G460 2007 con las siguientes características:

1. Procesador Intel® Core™ i3 CPU M 380 @ 2.53GHz, 2527 MHz RM-77.
2. Tarjeta de red *wireless* Broadcom 802.11n.
3. Memoria RAM de 2,934 MB.
4. Disco duro de 320 GB ST9320325AS ATA Device.

La interfaz de *hardware* usada corresponde al modelo Wi-Spy DBx con las siguientes características:

1. Rango de frecuencia 2.400 a 2.495 GHz, 5.150 a 5.850 GHz.
2. Resolución de amplitud 0.5 dBm, antena RP-SMA.
3. Rango de amplitud 100 dBmto -6.5 dBm.

La interfaz de *hardware* usada corresponde al modelo 14Wi-Spy DBx con las siguientes características:

1. Rango de frecuencia 2.400 a 2.495 GHz. 5.150 a 5.850 GHz.
2. Resolución de amplitud 0.5 dBm, antena RP-SMA.
3. Rango de amplitud 100 dBmto -6.5 dBm.

Toma de muestras: se realizaron pruebas de campo para saber el número de conexiones libres encontradas en cada una de las zonas del estudio.

En las 24 zonas en las que se dividió el área de estudio se realizó un escaneo para encontrar las redes Wi-Fi libres.

Se determinó la ubicación en coordenadas GPS de las redes Wi-Fi existentes que no tuvieran protocolos de seguridad (Wi-Fi de libre acceso).

Se tabularon los datos y los resultados de redes Wi-Fi de libre acceso en cada zona tal y como se muestra en la **Tabla 8.**

Tabla 8. Resultados de mediciones Wi-Fi de libre acceso.

Zona	Redes Wi-Fi sin seguridad (libres)
1	2
2	4
3	4
4	2
5	3

Continúa en la próxima página.

Continuación de la Tabla 8. Resultados de mediciones Wi-Fi de libre acceso.

Zona	Redes Wi-Fi sin seguridad (libres)
6	6
7	9
8	4
9	4
10	1
11	0
12	4
13	4
14	8
15	5
16	5
17	5
18	14
19	0
20	2
21	4
22	3
23	0
24	10
Total	103

Mediciones de Campo Wi-Fi con Protocolos de Seguridad (MCWPS). Estas pruebas de campo tienen como objetivo realizar la caracterización de los protocolos de seguridad empleados en las redes Wi-Fi en el área de estudio. Para ello se hicieron mediciones tendientes a encontrar las redes Wi-Fi y determinar el tipo de seguridad aplicada; se emplearon algunos elementos de *software* y *hardware*.

***Software*:** para determinar las redes Wi-Fi en un área geográfica se puede usar *software*; entre varias opciones disponibles para este estudio se

empleó el *software* Chanalyzer, que conjuntamente con Wi-Spy trabaja en las frecuencias de **2.4** y **5 GHz** mostrando en tiempo real el espectro completo, canales 1-14. Con este *software* se puede observar el tráfico, la ocupación, potencia y posibles interferencias de las señales recibidas en un punto en concreto; también muestra el protocolo de seguridad empleado en esa red.

***Hardware*:** las pruebas se realizaron en un computador portátil Lenovo G460 2007 con tarjeta *wireless* Broadcom 802.11n.
Otras especificaciones técnicas del Lenovo G460 son:

- Procesador Intel® Core™ i3 CPU M 380 @ 2.53 GHz, 2527 MHz RM-77.
- Memoria de 2934 MB.
- Disco duro de 320GB ST9320325AS ATA Device.

También se usó el Wi-Spy DBx **(Figura 14),** una herramienta económica de comunicación electrónica que se usa para la identificación de problemas e interferencias en Wi-Fi. Desde el año 2005, Wi-Spy ha servido de ayuda a los administradores de red al ofrecer un análisis de espectro fiable y asequible. Las redes inalámbricas presentan un conjunto de problemas de gestión y Wi-Spy es la alternativa rápida para la solución confiable de los mismos.

Se conecta Wi-Spy al computador, se inicia el *software* y se pueden observar las diferentes redes inalámbricas.

El *software* convierte los datos tomados por Wi-Spy en gráficos interactivos, hojas de datos; lo que permite a los usuarios visualizar las redes inalámbricas y detectar todas las interferencias RF que no se "ven" fácilmente, lo que puede generar problemas en las redes.

Cuando se combina con una tarjeta de red inalámbrica, el *software* también puede mostrar los puntos de acceso activos, tal como aparecen en el espectro, dando así una idea rápida para determinar la existencia o no de interferencias.

Figura 14. Wi-Spy DBx, elemento de *hardware* empleado.
Tomada de: http://www.wi-spy.eu/wi-spy-dbx/.

Otras especificaciones técnicas del Wi-Spy DBx son:

- Rango de frecuencia: 2.400 a 2.495 GHz, 5.150 a 5.850 GHz.
- Rango de amplitud: 100 dBm a -6.5 dBm.
- Resolución de amplitud: 0.5 dBm.
- Antena RP-SMA.

Toma de muestras: se realizaron mediciones tendientes a encontrar las redes Wi-Fi y determinar el tipo de seguridad aplicada.

1. En cada una de las zonas (24) en las que se dividió el área de estudio se realiza un escaneo para la búsqueda de redes Wi-Fi.
2. Se determina cuántas redes Wi-Fi hay sin protocolos de seguridad (libres) y cuántas con protocolos.
3. Se determina cuáles son las redes que tienen protocolos de seguridad: WEP, WPA y WPA2.

A continuación se presentan los resultados de las mediciones **(Tabla 9):**

Tabla 9. Resultados de mediciones por zonas.

Zona	Sin seguridad	Con seguridad			Total de redes Wi-Fi
		WEP	WPA	WPA2	
1	2	5	3	10	20
2	4	3	8	11	26
3	4	7	8	7	26
4	2	6	9	7	24
5	3	2	11	17	33
6	6	7	14	12	39
7	9	6	7	3	35
8	4	8	13	18	43
9	4	8	10	9	31
10	1	2	15	11	29
11	0	1	1	3	5
12	4	7	22	9	42
13	4	0	0	2	6
14	8	2	23	22	55
15	5	5	7	13	30
16	5	1	7	5	18
17	5	1	3	15	24
18	14	10	21	26	71
19	0	2	12	9	23
20	2	7	20	12	41
21	4	6	13	15	38
22	3	5	11	15	34
23	0	3	8	8	19
24	10	15	20	19	64

Las mediciones con redes sin seguridad y con seguridad WEP, WPA y WPA2 se muestran en la **Tabla 10.**

Tabla 10. Resumen de resultados de mediciones.

Redes Wi-Fi				
Sin seguridad	Con seguridad			Total de redes Wi-Fi
103	WEP	WPA	WPA2	766
	119	266	278	

Mapas

Distribución de las redes Wi-Fi de libre acceso. El mapa es una indicación geográfica marcada satelitalmente con coordenadas GPS para hacer notar un evento, en este caso la ubicación de las redes Wi-Fi en un momento dado **(Tabla 11).** Para construir los mapas georreferenciados de red Wi-Fi se requiere:

1. Un PC compatible con el *software* de detección seleccionado para determinar la existencia de la señal de red en tiempo real.
2. Realizar pruebas de campo con el *software* inSSider y ubicar la dirección de cada una de las zonas según la tabla obtenida.

Tabla 11. Distribución y ubicación de las redes Wi-Fi sin seguridad.

Zona	Redes Wi-Fi sin seguridad	Ubicación representativa
1	2	Edificio Corporación Universitaria Remington Navarro Ospina
2	4	Pasaje Comercial La Bolsa
3	4	Banco Popular
4	2	Centro Comercial Palacé Carrera 49 (Junín), calle 50 (Colombia)
5	3	La Anticuaria
6	6	Centro Comercial Beneficencia
7	9	Plaza Botero
8	4	Estación Metro Parque Berrío
9	4	Notaría 18
10	1	Centro Comercial Junín La Candelaria
11	0	Botica Junín
12	4	Avenida Oriental con La Playa
13	4	Casa de la Cultura
14	8	Hotel Nutibara
15	5	Pasaje Comercial Astoria
16	5	Centro Comercial Unión Plaza

Continúa en la próxima página.

Continuación de la Tabla 11. Distribución y ubicación de las redes Wi-Fi sin seguridad.

Zona	Redes Wi-Fi sin seguridad	Ubicación representativa
17	5	Bulevar de Junín
18	14	Centro Comercial Camino Real
19	0	Comfenalco
20	2	Centro Comercial Comunicaciones
21	4	Éxito de Junín
22	3	Pasaje Comercial El Paso
23	0	Clínica Medellín Centro
24	10	Colseguros

3. Identificar los puntos de las conexiones libres en cada zona seleccionada con la dirección de cada lugar. Ejemplo: carrera 50 n.º 51-04, Medellín, Antioquia, Colombia, la cual corresponde a una ubicación de zona y región específica.
4. Introducir las direcciones del grupo de lugares que indicarán los puntos libres en Google Maps para crear el mapa digitando el nombre del lugar por localizar en el buscador principal y hacer clic en la dirección encontrada; luego se hace clic en adicionar.
5. Posteriormente, al registrarse en Google Maps se debe efectuar el asistente de creación de mapas georreferenciados de la página web y seguir las instrucciones siguientes:
   - Seleccionar la capa de datos.
   - Clic en etiquetas.
   - Clic en menú desplegable.
   - Seleccionar el encabezado de la columna que se va a emplear para etiquetar los elementos que tendrá el mapa **(Figura 15).**
6. Pasar los datos de las pruebas de campo al portal de cada capa de creación de mapas teniendo en cuenta la selección del lugar correspondiente y verificando la existencia de la ubicación para evitar marcar el punto en la zona de una región equivocada.
   Se debe hacer clic en la ubicación del marcador en el mapa, tal como se muestra en la **Figura 16** en el campo resaltado.

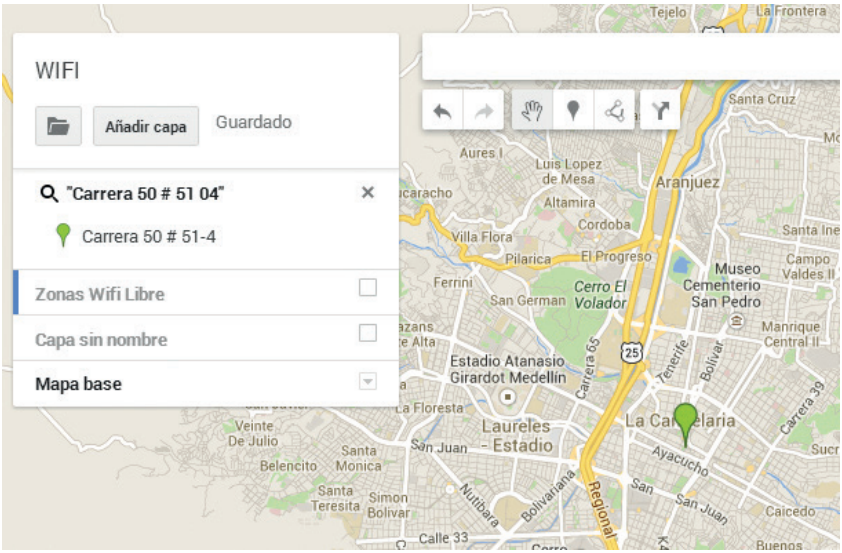


Figura 15. *Software* Google Maps. Tomado de: Google Maps.

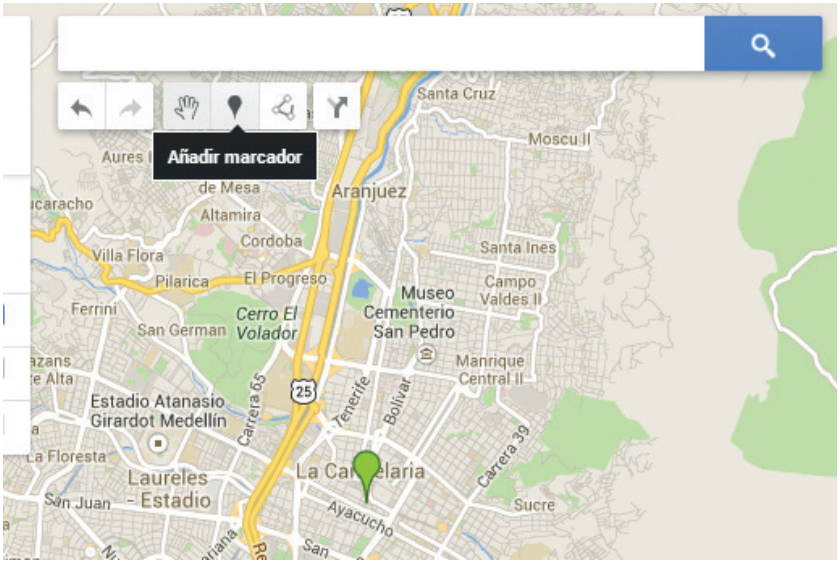


Figura 16. Insertando un marcador en Google Maps. Tomado de: Google Maps.

7. Publicar el mapa en la web para obtener el link haciendo clic en el campo compartir, marcado con color verde, y seleccionar del menú la opción requerida (publicación web privada o pública) **(Figura 17).**

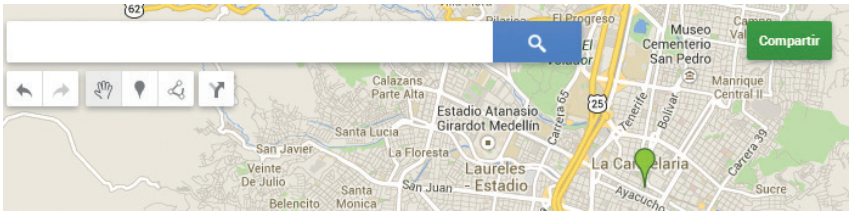


Figura 17. Compartir la información. Tomado de: Google Maps.

8. Visualizar el mapa georreferenciado usando el link publicado **(Figura 18).**

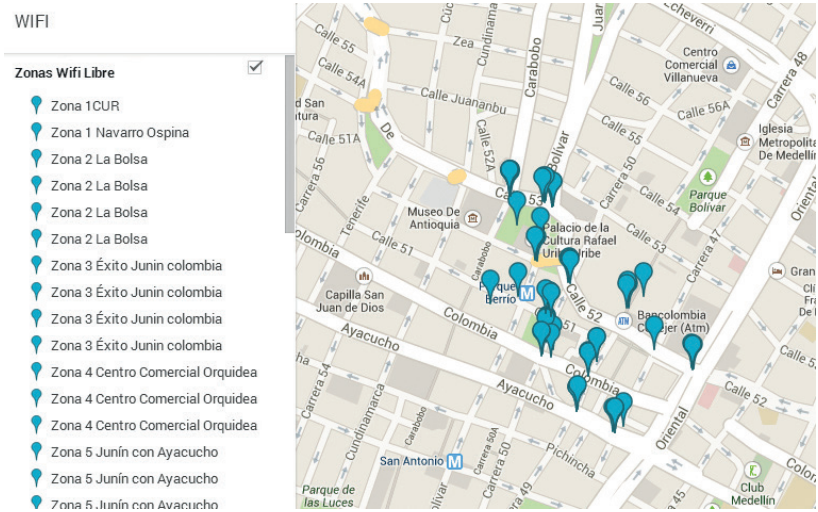
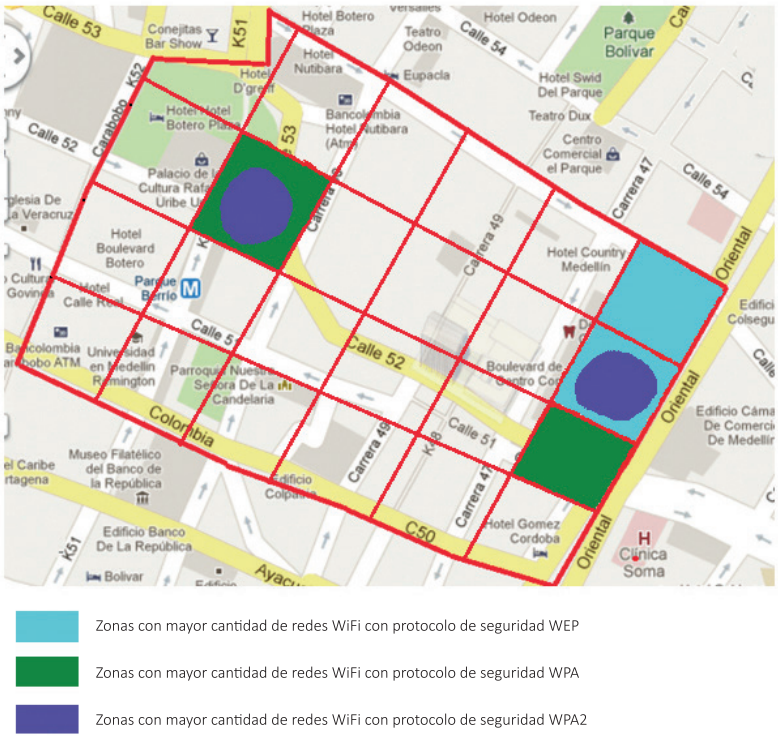


Figura 18. Mapa georreferenciado con las ubicaciones.
Tomado de: https://mapsengine.google.com/map/edit?mid=zN_usRAk6SEE.k--daEL8SJ88

Distribución de los protocolos de seguridad. La distribución de los protocolos de seguridad en el área de estudio es muy variada; sin

embargo, existen algunas zonas con una gran cantidad de redes con seguridad WEP, WPA, WPA2. Estas áreas se muestran en la **Figura 19.**



Zonas con mayor cantidad de redes WiFi con protocolo de seguridad WEP

Zonas con mayor cantidad de redes WiFi con protocolo de seguridad WPA

Zonas con mayor cantidad de redes WiFi con protocolo de seguridad WPA2

Figura 19. Concentración de redes según el tipo de seguridad. Tomada de: Google Maps.

Según la cantidad de redes Wi-Fi y el protocolo se encontró la siguiente distribución:

- Protocolo WEP; en las zonas donde más existe este tipo de protocolos hay de 10 a 15 redes WEP.
- Protocolo WPA se encontró que en las zonas de mayor influencia de este protocolo hay entre 22 y 23 redes WAP.
- Protocolo WPA2; se encontró que en las zonas de mayor influencia WPA2 hay entre 22 y 26 redes.

Resultados de la encuesta

Se mostrará el análisis de la encuesta realizada con el fin de cuantificar el grado de conocimiento y de utilización de la Wi-Fi en esta zona de la comuna 10.

A continuación se muestran los resultados obtenidos para las 12 preguntas de la encuesta.

1. ¿Usted cree que su nivel de conocimiento acerca de Wi-Fi es? **(Tabla 12 y Figura 20)**

Tabla 12. Respuesta encuesta pregunta 1.

Conocimiento	Encuestados	Porcentaje
Bueno	42	42,00 %
Malo	21	21,00 %
Muy bueno	10	10,00 %
Regular	27	27,00 %
Total	100	100,00 %

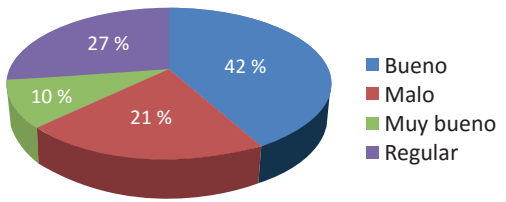


Figura 20. Diagrama circular encuesta pregunta 1 conocimiento.

2. ¿Qué tanto cree usted que Wi-Fi es seguro? **(Tabla 13 y Figura 21)**

Tabla 13. Respuesta encuesta pregunta 2.

Grado de seguridad	Encuestados	Porcentaje
Seguro	37	37,00 %
Inseguro	14	14,00 %
Muy seguro	3	3,00 %
Muy inseguro	5	5,00 %
Regular	41	41,00 %
Total	100	100,00 %

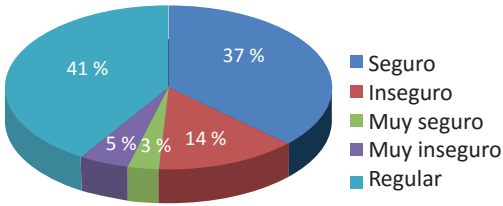


Figura 21. Diagrama circular pregunta 2, Wi-Fi.

3. ¿Ha utilizado conexiones Wi-Fi para realizar transacciones comerciales? **(Tabla 14 y Figura 22)**

Tabla 14. Respuesta encuesta pregunta 3.

Transacciones comerciales	Encuestados	Porcentaje
No	78	78,00 %
Sí	22	22,00 %
Total	100	100,00 %

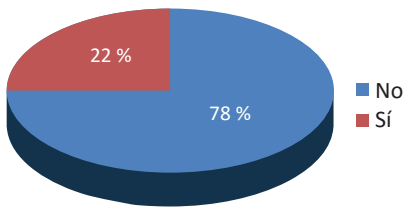


Figura 22. Diagrama circular pregunta 3, transacciones comerciales.

4. ¿Considera usted que las conexiones Wi-Fi son más rápidas que las conexiones cableadas? **(Tabla 15 y Figura 23)**

Tabla 15. Respuesta encuesta pregunta 4.

Rapidez	Encuestados	Porcentaje
No	64	64,00 %
NS / NR	11	11,00 %
Sí	25	25,00 %
Total	100	100,00 %

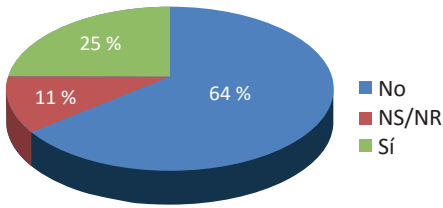


Figura 23. Diagrama circular pregunta 4, Wi-Fi.

5. ¿Cuál de estas conexiones es la que más utiliza? **(Tabla 16 y Figura 24)**

Tabla 16. Respuesta encuesta pregunta 5.

Conexiones	Encuestados	Porcentaje
Cableada	45	45,00 %
Otra	2	2,00 %
Wi-Fi	53	53,00 %
Total	100	100,00 %

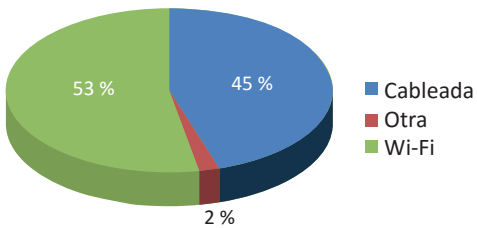


Figura 24. Diagrama circular pregunta 5, conexiones a internet más usadas.

6. ¿A través de qué dispositivo se conecta en mayor medida a redes Wi-Fi? **(Tabla 17)**

Tabla 17. Respuesta encuesta pregunta 6.

Dispositivos	Encuestados	Porcentaje
Principalmente PC escritorio	14	14,00 %
Principalmente teléfono o tableta electrónica	40	40,00 %
Principalmente portátil	43	45,00 %
Principalmente otros	3	3,00 %

7. ¿Cuál es su proveedor de servicios (ISP) de banda ancha (internet)? **(Tabla 18)**

Tabla 18. Respuesta encuesta pregunta 7.

Proveedor	Encuestados	Porcentaje
Claro	23	23,00 %
Movistar	1	1,00 %
Tigo	4	4,00 %
UNE	71	71,00 %
Virgin	1	1,00 %
No sabe	0	0 %
Total	100	100,00 %

8. ¿De cuántos megabytes es la conexión de banda ancha que tiene contratada? **(Tabla 19)**

Tabla 19. Respuesta encuesta pregunta 8.

Ancho banda	Encuestados	Porcentaje
1 o menos	7	7,00 %
1 a 2	22	22,00 %
2 a 4	52	52,00 %
4 a 10	17	17,00 %
Más de 10	2	2,00 %
Total	100	100,00 %

9. ¿Cuál es la frecuencia de uso de Wi-Fi? **(Tabla 20 y Figura 25)**

Tabla 20. Respuesta encuesta pregunta 9.

Frecuencia	Encuestados	Porcentaje
1 hora o menos por semana	16	16,00 %
1 a 3 horas por semana	14	14,00 %
3 a 10 horas por semana	19	19,00 %
10 a 24 horas por semana	10	10,00 %
Más de 24 horas por semana	41	41,00 %
Total	100	100,00 %

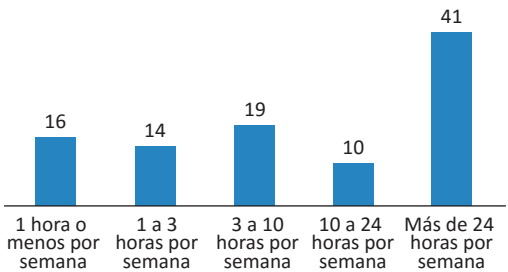


Figura 25. Histograma pregunta 9, frecuencia del uso del Wi-Fi.

10. ¿Qué tan seguro se siente al utilizar redes Wi-Fi de libre acceso? **(Tabla 21)**

Tabla 21. Respuesta encuesta pregunta 10.

Libre acceso	Encuestados	Porcentaje
Muy seguro	3	3,00 %
Seguro	32	32,00 %
Medianamente seguro	38	38,00 %
Inseguro	18	18,00 %
Muy inseguro	9	9,00 %
No sabe	0	0 %
Total	100	100,00 %

11. ¿Conoce usted sitios de libre acceso en el centro de la ciudad? **(Tabla 22 y Figura 26)**

Tabla 22. Respuesta encuesta pregunta 11.

Acceso	Encuestados	Porcentaje
No	57	57,00 %
Sí	43	43,00 %
Total	100	100,00 %

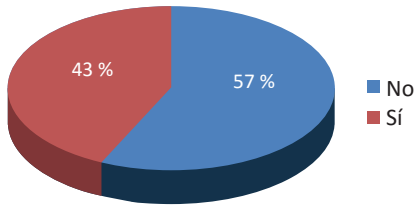


Figura 26. Diagrama circular pregunta 11, sitios de libre acceso a internet en el centro de la ciudad.

12. ¿Ha utilizado conexiones Wi-Fi sin autorización? **(Tabla 23 y Figura 27)**

Tabla 23. Respuesta encuesta pregunta 12.

Conexiones Wi-Fi sin autorización	Encuestados	Porcentaje
Nunca	49	49,00 %
Alguna vez	20	20,00 %
Pocas veces	12	12,00 %
Muchas veces	14	14,00 %
Siempre	5	5,00 %
Total	100	100 %

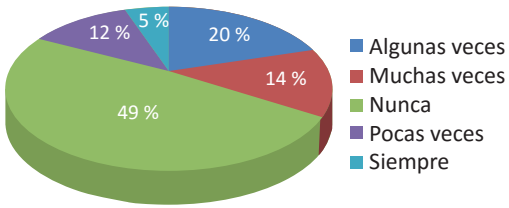


Figura 27. Diagrama circular pregunta 12, conexiones Wi-Fi sin autorización.

Discusión de resultados

Medición Preliminar Wi-Fi Solapamiento (MPWS). Para la transferencia de datos realizada en el canal 11 con interferencia de la red con ESSID "Veronica", **Figura 10,** luego de analizar los resultados de la **Tabla 5** se observa que la velocidad de envío del archivo es de 384 KB/segundo, promedio y media de 380 KB/segundo. Como la medida de transferencia se expresa en bps (bits por segundo), se realiza el cambio de unidades a **(Ecuaciones 4 y 5):**

$$384\ \text{Kbps} * 8 = 3072\ \text{Kbps} \quad (4)$$

$$\frac{3072\ \text{Kbps}}{1024} = \boxed{2.1942\ \text{Mbps}} \quad (5)$$

La **Tabla 7** muestra que la velocidad media de envío del archivo cuando no existe interferencia **(Figura 11)** fue calculada en 1,93 MB/segundo y el promedio en 1,94 MB/s, es decir, alrededor de cinco veces la velocidad alcanzada en la prueba anterior. A continuación se realizan nuevamente los cambios de unidades **(Ecuación 6):**

$$1{,}93\ \text{MBps} * 8 = \boxed{15.44\ \text{Mbps}} \quad (6)$$

El promedio de transferencias es de 15,44 Mbps con el canal libre y de solo 2,1942 Mbps con interferencia **(Tabla 24).**

Tabla 24. Resultados de transferencia con interferencia y sin esta entre los canales.

Canal usado	Promedio de envío	Estado
1	2.1942 Mbps	Interferido
11	15.44 Mbps	No interferido

De la prueba realizada se puede concluir que la velocidad de transferencia en una red inalámbrica con interferencia por solapamiento de canales puede disminuir al menos cinco veces si se compara con una transferencia libre de interferencia; con lo que queda establecido que la velocidad entre redes Wi-Fi es afectada por la interferencia de otras redes inalámbricas, como lo muestra la **Figura 28.**

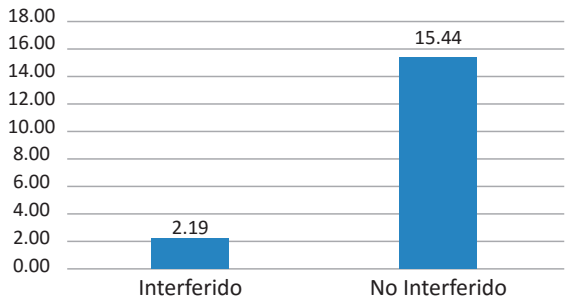


Figura 28. Comparación de envíos Wi-Fi con y sin interferencia de otras redes.

Se concluye que la interferencia causada entre redes Wi-Fi ocasiona una gran disminución en la transferencia de datos, lo que degrada el rendimiento; esto ocurre cuando estas redes se solapan o comparten el mismo canal de comunicaciones, incluso si existen pocos nodos Wi-Fi involucrados.

Medición Preliminar Wi-Fi Vulnerabilidades (MPWV). Más allá de las pruebas de campo realizadas, en las que se verifica la vulnerabilidad del protocolo de seguridad WEP, un sinnúmero de autores coinciden en indicar que las medidas que utiliza este protocolo son sustancialmente débiles; artículos como "Seguridad de WEP, WPA y WPA2" del 2006 muestran cómo vulnerar sistemas Wi-Fi (Lehembre, 2006). El artículo sostiene que el "crackeado" de WEP puede ser demostrado con facilidad utilizando herramientas como Aircrack (creado por el investigador francés en temas de seguridad Christopher Devine). Aircrack contiene tres utilidades principales, usadas en las tres fases del ataque necesario

para recuperar la clave; además indica que la meta principal del ataque es generar tráfico para capturar IV (vectores de inicialización), únicos utilizados entre el cliente y el *access point*.

Artículos como "Intercepting mobile communications: the insecurity of 802.11" (Borisov, Goldberg & Wagner, 2001), desde el 2001 recomiendan no usar este protocolo y sugieren que sea rediseñado; además, establecen las siguientes debilidades:

- Se usa la misma clave para cifrado y autenticación.
- Las claves son estáticas de 40 y 104 bits.
- Las claves pueden ser forjadas por estaciones no autorizadas.
- WEP no encripta ni las direcciones MAC de las estaciones ni el SSID.
- Una implementación débil del algoritmo de RC4.
- La secuencia del vector de inicialización (VI) es demasiado corta.

Pruebas de Campo Wi-Fi Zonas Libres (PCWZL). De los datos obtenidos al escanear las redes libres se puede determinar que no existe, como es de esperarse, una consistencia en el número de conexiones Wi-Fi libres; sin embargo, dada la cercanía geográfica de las redes de libre acceso, sin tener en cuenta otras redes con protocolos de seguridad, se puede inferir que zonas como la plaza Botero (7), el Hotel Nutibara (14) y Colseguros (24), por su alta concentración de Wi-Fi libres, presentan solapamiento de canales y por ende bajas velocidades. No obstante, son zonas en las que fácilmente se puede tener acceso a internet. Por el contrario, las zonas la Botica Junín (11), Comfenalco (19) y la Clínica Medellín Centro (23) no cuentan con redes de acceso libre.

La **Figura 29** muestra dentro de la zona de estudio la distribución de las redes Wi-Fi de libre acceso.

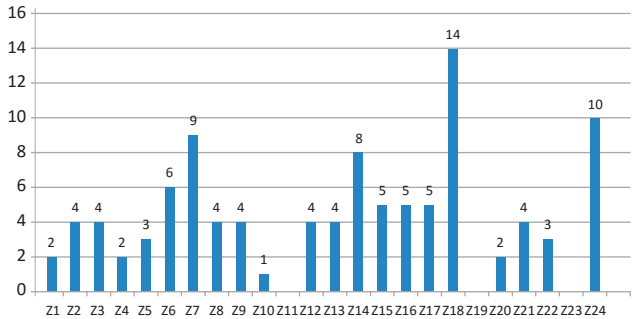


Figura 29. Número de redes de libre acceso por zona de estudio, red Wi-Fi.

La ubicación de estas redes puede verse en la **Tabla 10.** El estudio muestra que existen 103 redes Wi-Fi de libre acceso; sin embargo, hay zonas como la 11, la 19 y la 23 que no tienen; estas zonas corresponden al 12.5 % del área de estudio; el 87.5 % tiene al menos un punto de libre acceso, como lo muestra la **Figura 30.**

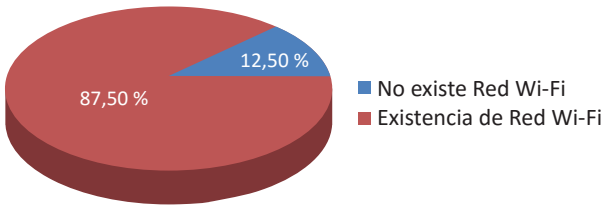


Figura 30. Distribución de redes Wi-Fi con libre acceso.

Pruebas de Campo Wi-Fi Protocolos de Seguridad (PCWPS). Algunas generalidades encontradas en el estudio indican que el porcentaje de usuarios del protocolo de seguridad WEP es menor que el de los que han adoptado los protocolos WPA y WPA2.

Existen 103 redes sin seguridad contra 663 que sí la tienen **(Figura 31);** esto significa que una de cada seis redes es insegura.

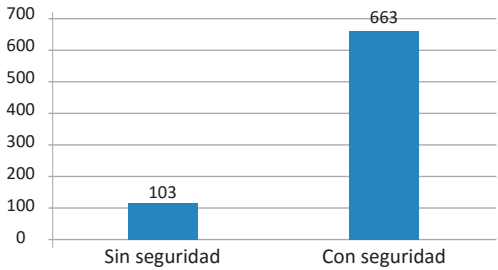


Figura 31. Redes Wi-Fi con algún tipo de seguridad *vs.*, redes Wi-Fi sin ningún tipo de seguridad.

Al realizar el análisis sobre los resultados de las mediciones con respecto a las redes Wi-Fi, se encontró que de un total de 766, el 86.55 % (663 redes) posee seguridad y el 13.45 % (103 redes) no.

Por otro lado, el protocolo predominante es el WPA2, con un 41.93 % (278 redes), seguido de WPA, con un 40.12 % (266 redes), y al final está el WEP, con un 17.95 % (119 redes), como lo muestra la **Figura 32.**

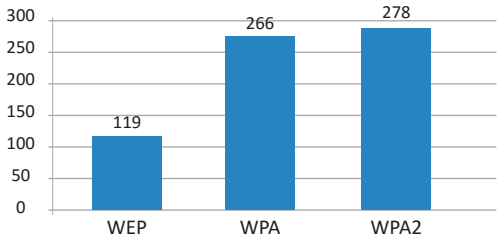


Figura 32. Distribución de los protocolos empleados en las redes Wi-Fi con algún tipo de seguridad.

Conclusiones y trabajos futuros

Como el Wi-Fi es una tecnología económica para conexión de equipos, actualmente se usa de forma masiva y satura los tres canales que se diseñaron para hacer transmisiones libres de interferencia.

En sitios de alta concentración de redes Wi-Fi, el problema puede realmente ser inmanejable y producir lentitud en la descarga y navegación, incluso si se tienen contratados grandes anchos de banda.

Gran cantidad de redes Wi-Fi en una misma área geográfica produce inevitablemente que las redes Wi-Fi se solapen entre sí, es decir, que transmitan en los mismos canales. Si bien se puede hacer una redistribución de canales usados, el conocimiento del público en general es muy escaso con respecto al manejo de herramientas como los analizadores de espectro; sin embargo, en zonas como la estudiada, donde hay una gran cantidad de redes usando la frecuencia de 2.4 GHz, no basta con reubicarlas. La **Tabla 25** muestra un resumen de los resultados de las Mediciones Preliminares, MP, MPWS, MPWV, y de las Pruebas de Campo, PC, (PCWZL y PCWPS), que están descritas en la **Tabla 1.**

En cuanto a la percepción de los encuestados, se puede ver que de los usuarios de redes Wi-Fi, el 10 % cree tener un nivel de conocimiento muy bueno, mientras que quienes creen que es regular o malo suman un 48 %; al respecto de la percepción de seguridad sobre las redes Wi-Fi, solo un 3 % de los usuarios cree que es muy buena, lo que indica que existe una gran cantidad de personas que desconfía; no obstante, un 78 % de los encuestados usa Wi-Fi para transacciones comerciales; es decir que las redes Wi-Fi se emplean aunque haya algún grado de desconfianza.

Aunque el empleo de redes Wi-Fi trae consigo bajas velocidades como se demostró en este mismo documento, un 25 % de los encuestados no lo considera así o no ve la disminución como un obstáculo.

Tabla 25. Resumen pruebas y estudio realizado.

Pruebas experimentales	
MP	**MPWS** • La velocidad de transferencia de los nodos Wi-Fi se ve afectada por las interferencias producidas por otras redes. • El solapamiento de canales Wi-Fi produce reducción de la tasa de transferencia, sin que existan errores de transmisión. • En un escenario como el estudiado en EPPW-01 se puede disminuir la velocidad de transferencia en al menos cinco veces si se compara con una transferencia libre de interferencia. • Se debe realizar un estudio *a priori* de las redes inalámbricas existentes en la zona para lograr una velocidad óptima. • Se propone realizar un estudio que caracterice y determine en forma detallada cómo afectan la potencia, distancia y solapamiento de canales la velocidad de transmisión en redes Wi-Fi, para así determinar cuál de estos factores es el más importante.
	MPWV • Las pruebas permitieron experimentar y validar que es posible conectarse a una red Wi-Fi con protocolo de seguridad WEP de una forma relativamente sencilla. • Existen programas de fácil descarga y manuales en internet que facilitan el proceso. • Se considera que no debe emplear seguridad WEP, ya que es altamente vulnerable a accesos no autorizados.
PC	**PCWZL** • El estudio muestra que existen 103 redes Wi-Fi de libre acceso en el área de estudio. • El 12.5 % del área de estudio no tiene redes Wi-Fi de libre acceso; el 87.5 % tiene al menos un punto de libre acceso. • El mapa georreferenciado generado en este estudio se puede encontrar en https://mapsengine.google.com/map/edit?mid=zN_usRAk6SEE.k--daEL-8SJ88
	PCWPS • Un número importante de usuarios desconoce la importancia de la seguridad en las redes de Wi-Fi, ya que utilizan el WEP. • El protocolo predominante es el WPA2, con un 41.93 % (278 redes), seguido de WPA, con un 40.12 % (266 redes), y al final está el WEP, con un 17.95 % (119 redes). • El porcentaje de usuarios que utiliza el protocolo de seguridad WEP para proteger su conexión es menor que el que ha adoptado los protocolos WPA y WPA2. • Se propone realizar un trabajo de campo en el cual se muestre a los usuarios de WEP cómo es de insegura su red, con el fin de que se apropien y tomen con responsabilidad el manejo de la información que poseen.

Es claro que las conexiones Wi-Fi son empleadas con mayor frecuencia que las cableadas: un 53 % usa Wi-Fi y un 45 %, cableadas. Además, se observa que, aunque son muy diversos los dispositivos utilizados para conectarse a redes Wi-Fi, se destacan el portátil y el teléfono.

Sobre el ISP que tienen los usuarios de la comuna 10, se destaca UNE con un 71 % y Claro con un 23 %; el ancho de banda más empleado, con un 51 %, está entre 2 y 4 Mbps; sobre la frecuencia de uso de internet, se muestra que el 41 % de los encuestados entra más de 24 horas por semana a la red. Por último, solo el 3 % de los usuarios de redes Wi-Fi se siente totalmente seguro, mientras el 65 % siente algún grado de inseguridad.

A pesar de que la comuna 10 tiene una gran cantidad de puntos Wi-Fi de libre acceso, un 43 % de los encuestados desconoce su ubicación. El 51 % manifiesta haberse conectado alguna vez a una red sin autorización y el 19 % se conecta sin autorización con alguna frecuencia.

La encuesta muestra claramente que elementos como teléfonos y *tablets* son muy usados para el acceso a internet (40 %), lo cual implica un alto uso de Wi-Fi; mientras que apenas el 14 % usa el PC para navegar en la red.

Bibliografía

- Buenos Aires Ciudad. (2014). *Buenos Aires Ciudad.* Obtenido de http://www.buenosaires.gob.ar/noticias/le-red-de-wifi-gratis-de-la-ciudad-llego-metrobus-9-de-julio
- Bertuzzi, R. (2007). Diseño e implementación de un servicio de localización y visualización de mapas utilizando J2ME para dispositivos móviles y herramientas de libre distribución. *R. C. Bertuzzi Síntesis Tecnológica, 3* (2), 39-57.
- Borisov, N., Goldberg, I. & Wagner, D. (2001). Intercepting mobile communications. *isaac.cs.berkeley.edu*
- ByongGi, L. & Sunghyun, C. (2008). Broadband wireless access and local networks: mobile WiMax and Wi-Fi artech house inc.
- Cisco Press. (2006). *Fundamentos de redes inalámbricas.* Mexico: Prentice Hall.
- El Ciudadano. (2014). Obtenido de http://www.elciudadano.gob.ec/gobierno-nacional-implementa-red-wi-fi-gratuito-alrededor-de-la-unidad-educativa-aguirre-abad/
- Garaizar, P. (s. f.). *Seguridad en redes*. Obtenido de http://www.e-ghost.deusto.es/docs/SeguridadWiFiInestable2005.pdf
- Gómez López, J. (2008). *Guía de campo de Wi-Fi.* Ciudad: Editorial Ra-Ma.
- Grupo Informática-Hoy. (s. f.). *Informática, tecnología e Internet*. Obtenido de http://www.informatica-hoy.com.ar/redes-inalambricas-wifi/Seguridad-en-redes-Wi-Fi.php
- - (s. f.). *Wefi*. Obtenido de http://www.wefi.com/maps/
- Jin-a, Park, S. K., Park, P. D. & Cho, K.R. (2002). Analysis of spectrum channel assingnment for IEEE 802.11b Wirelees LAN. *IEEE Explorer*.
- Lehembre, G. (2006). Seguridad Wi-Fi WEP,WPA y WPA2. *Hackin9*, 26.
- López, M., Alcocer, I., Barraza, A., Mendoza, A. e Hinostroza, V. (2009). Algoritmos de protocolos de seguridad en redes de computadoras

inalámbricas y el estudio paramétrico de su implementación. *Revista Espectro Tecnológico*, 4.

- Manfredi. (2008). Obtenido de *http://inta.gob.ar/documentos/realizacion-de-mapas-georeferenciados-de-malezas/*
- Metageek. (2011). *Metagreek*. Obtenido de http://www.metagreek.net/products/Insider
- MinTic. (2014). *MinTic Colombia*. Obtenido de http://www.mintic.gov.co/portal/604/w3-article-6655.html
- Moreno, J. & Fernández, D. (2007). *Informe técnico protocolo ZigBee IEEE 802.15.4.* No publicado.
- Noticias Palermonline. (2014). Obtenido de http://palermonline.com.ar/
- Perú 21. (2014). Obtenido de http://peru21.pe/tecnologia/instalan-redes-internet-wi-fi-gratuito-lima-2165993
- Romero, S., Tesoriero, R. V., Gallud, J. & Penichet, V. (2004).Obtenido de *http://www.sebastianromero.net/papers/rmaps.pdf*
- Safe&Savvy. (2014). Obtenido de http://safeandsavvy.f-secure.com/2014/09/29/danger-of-public-wifi/
- Siliconweek. (2014). Obtenido de http://www.siliconweek.com/actualidad/el-gobierno-venezolano-promete-wifi-gratis-en-las-principales-ciudades-del-pais-51321
- Solórzano, L. (2007). *Telefónica: investigación y desarrollo*. Obtenido de http://www.lacofa.es/index.php/tecnologias/futuro-de-internet/geoweb-contenidos-georeferenciado
- Subtel. (2014). Obtenido de http://www.subtel.gob.cl/component/search/?searchword=inauguracion%20de%20WIFi&searchphrase=all&Itemid=1146
- Wi-Fi Alliance. (2005). *WPA and WPA2, implementation white paper.*
- Wi-FiBolivia. (2015). Obtenido de http://wifibolivia.blogspot.com/2013/11/tarija-socializan-proyecto-de-ley-para.html

Este libro es el resultado de las investigaciones realizadas en la Corporación Universitaria Remington, Uniremington, por profesores del grupo de investigación Ingeniar y de la colaboración de estudiantes del semillero de investigación SemCEI, adscritos a la Facultad de Ciencias Básicas e Ingeniería de Uniremington, con el fin de obtener datos precisos acerca de factores como la interferencia y la seguridad de las redes Wi-Fi en la comuna 10 de Medellín; para la obtención de estos datos se contó con el apoyo de la Corporación Cívica del Centro de Medellín, Corpocentro, a través de un convenio marco.

UNIREMINGTON®
CORPORACIÓN UNIVERSITARIA REMINGTON
RES. 2661 MEN JUNIO 21 DE 1996

ISBN: 978-958-56132-0-1
9 789585 613201