UNIVERSIDAD DE QUINTANA ROO
DIVISIÓN DE CIENCIAS E INGENIERÍA

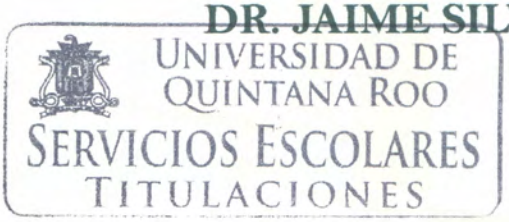
ANÁLISIS DE CONFIABILIDAD DE PUNTOS DE ACCESO INALÁMBRICOS DOMÉSTICOS EN LA CIUDAD DE CHETUMAL, QUINTANA ROO

TESIS
PARA OBTENER EL GRADO DE
INGENIERO EN REDES

PRESENTA
FRED MARTIN FAJARDO DURAN

DIRECTOR DE TESIS
MTI. VLADIMIR VENIAMIN CABAÑAS VICTORIA

ASESORES
DR. JAVIER VÁZQUEZ CASTILLO
MTI. MELISSA BLANQUETO ESTRADA
MSI. RUBÉN ENRIQUE GONZÁLEZ ELIXAVIDE
DR. JAIME SILVERIO ORTEGÓN AGUILAR



CHETUMAL QUINTANA ROO, MÉXICO, MAYO DE 2016

UNIVERSIDAD DE QUINTANA ROO
DIVISIÓN DE CIENCIAS E INGENIERÍA

TRABAJO DE TESIS ELABORADO BAJO SUPERVISIÓN DEL COMITÉ DE ASESORÍA Y APROBADO COMO REQUISITO PARCIAL PARA OBTENER EL GRADO DE:

INGENIERO EN REDES

COMITÉ DE TESIS

DIRECTOR:

MTI. VLADIMIR VENIAMIN CABAÑAS VICTORIA

ASESOR:

DR. JAVIER VÁZQUEZ CASTILLO

ASESOR:

MTI. MELISSA BLANQUETO ESTRADA

Universidad de Quintana Roo
DCI DIVISIÓN DE CIENCIAS E INGENIERÍA

UNIVERSIDAD DE QUINTANA ROO
SERVICIOS ESCOLARES
TITULACIONES

CHETUMAL QUINTANA ROO, MÉXICO, MAYO DE 2016

Dedicatoria

Con este trabajo el cual es la culminación de mi carrera profesional y la apertura hacia nuevos proyectos he finalizado uno de los objetivos de mi vida y quiero dar las gracias a todas personas que me apoyaron durante todo este tiempo, sin más que decir este logro se lo dedico:

A mis padres, Fred Martin Fajardo May y María Candelaria Duran Cardeña, quienes me brindaron su apoyo incondicional y los recursos necesarios para llegar hasta acá, gracias a ellos logre llegar hasta este punto.

A toda mi familia y amigos que me estuvieron apoyando durante toda mi estadía en la Universidad de Quintana Roo.

A mis profesores, quienes confiaron en mí y me brindaron su apoyo consejos y motivación día a día

Agradecimientos

Agradezco a mis padres que me apoyaron y motivaron durante toda mi formación académica, les doy las gracias por siempre confiar en mí.

Al M.T.I. Vladimir Veniamin Cabañas Victoria quien fue mi director de tesis, gracias por guía y asesoramiento durante la realización de este trabajo

Al MSI. Rubén Enrique Gonzales Elixavide por ser mi tutor, gracias por todos sus consejos y el apoyo que me brindo.

A mis asesores de tesis Dr. Javier Vázquez Castillo, Melissa Blanqueto Estrada, Ing. Rubén Enrique González Elixavide y Dr. Jaime Silverio Ortegón Aguilar.

A la Lic. Jade Ixchel Mahogany Pech Rivero.

A todos mis profesores que durante toda mi carrera profesional me brindaron apoyo y gracias por todas sus enseñanzas.

Resumen

En el presente trabajo se analizan algunos de los parámetros básicos (pero importantes en materia de seguridad) de los puntos de accesos inalámbricos domésticos basados en el protocolo 802.11 con el fin de poder obtener información del estado en el que se encuentran los Ap´s (Puntos de acceso por sus siglas en inglés) de la ciudad de Chetumal Quintana Roo y generar recomendaciones que ayuden a mitigar las deficiencias de confiabilidad que se presentan actualmente.

Este análisis se basó en la recolección *in situ* (en algunos cuadros de la ciudad de Chetumal) de los siguientes parámetros: marca del fabricante, SSID, canal y tipo de cifrado. Asimismo, la metodología empleada es OWISAM (*Open Wireless Security Assessment Methodology*) que permite observar controles de seguridad en las comunicaciones inalámbricas para identificar riesgos, minimizar impacto de ataques informáticos y aumentar la confiabilidad de infraestructuras *Wireless*.

Analizando los datos obtenidos durante la etapa de recolección se pudo determinar de manera general la confiabilidad de los accesos de puntos inalámbricos, lo cual permitió generar información estadística para saber con mayor precisión el estado en el que se encuentran los Ap´s en diversos puntos de la ciudad de Chetumal, Quintana Roo.

Con ello en mente, el resultado debe ser una opción que ayude a aumentar y mejorar el grado de confiabilidad de los puntos de acceso evitando que los usuarios caseros estén expuestos a amenazas por parte de hackers, piratas cibernéticos o cualquier otra persona malintencionada.

A través de la identificación de las vulnerabilidades y amenazas hacia los Ap´s domésticos de la ciudad de Chetumal, Quintana Roo se pretende mitigar sus efectos mediante una serie de recomendaciones basadas en el análisis de los 3 principales fabricantes de AP que tienen la mayor presencia en la zona.

Las recomendaciones finales se enfocaron de manera particular hacia las deficiencias que presentan cada uno de los fabricantes líderes de puntos de acceso.

Tabla de contenido

Índice de Ilustraciones y tablas

CAPÍTULO I Introducción

1.1 Definición del problema

Las redes inalámbricas del tipo doméstico en la ciudad de Chetumal Quintana Roo, han observado un gran crecimiento tanto por la demanda de conectividad, diminución de los costos y a la creciente oferta de los diversos proveedores de servicios de internet en el estado y en el país en general.

Los proveedores de servicios de internet que ofrecen equipos de conexión con capacidades inalámbricas habitualmente entregan los dispositivos con las configuraciones por defecto, es decir, presentan características que están ampliamente documentadas en internet la cual es fácil de obtener. Obviamente esto conlleva un riesgo importante en materia de seguridad informática.

1.2 Justificación

La configuración por default de los dispositivos de conectividad inalámbrica representa un riesgo en la integridad, privacidad y confidencialidad de la información de los usuarios de las redes domésticas. Por ello este trabajo pretende realizar un análisis de las principales características de los puntos de acceso domésticos como la marca del fabricante, modelo del dispositivo, *ssid (service set identifier)*, canal utilizado, la potencia de la señal y el tipo de cifrado utilizado.

1.3 Objetivos

Objetivo General

El objetivo de esta investigación es analizar la variedad de redes inalámbricas 802.11 que se encuentran en determinados puntos de la ciudad de Chetumal Quintana Roo, para identificar las principales características de los puntos de acceso y poder generar información útil y eficaz para mitigar de manera considerable los riesgos inherentes a las configuraciones por default y también las configuraciones deficientes y con ello aumentar la confiabilidad de las redes inalámbricas.

Objetivos específicos

- Realizar un monitoreo in situ de diferentes puntos de acceso inalámbrico para identificar sus principales características como: Marca del fabricante, modelo del dispositivo, ssid, canal utilizado, potencia de la señal y tipo de cifrado utilizado.

- Realizar un reporte de la información obtenida durante el monitoreo.
- Analizar la información generada en el reporte.
- Generar las recomendaciones pertinentes para aumentar la confiabilidad de los principales modelos de puntos de acceso encontrados.

1.4 Alcance

El alcance de este proyecto de investigación se centrará en la ciudad de Chetumal, Quintana Roo tomando como muestras las zonas denominadas AGEB (Área geoestadística básica). Específicamente las zonas 2300400010759 y 2300400010392 las cuales muestran un mayor índice de población; y servirán para la realización de las estadísticas correspondientes a este estudio.

Figura 1 AGEB 2300400010759

Figura 2 AGEB 2300400010392

1.5 Metodología

1.5.1 Tipo de metodología

En el análisis de esta investigación se optó por OWISAM (Metodología de evaluación de seguridad de Wireless abierta), que consiste en una metodología con 10 categorías de controles de seguridad, que corresponden a verificaciones que se deben llevar a cabo para realizar con éxito análisis de seguridad sobre una infraestructura inalámbrica.

El principal objetivo de esta metodología es la de mantener una metodología ágil y utilizable que ayude a realizar con éxito un análisis de seguridad sobre las redes WiFi, dicho análisis cubre todos los aspectos de seguridad relacionados a las redes inalámbricas, todo esto gracias a que OWISAM cuenta con 63 controles técnicos de seguridad agrupados en 10 categorías, las cuales son (Tarlogic, 2013):

- OWISAM-DI: Descubrimiento de dispositivos.
- OWISAM-FP: Fingerprinting.(Recopilación de información para identificación).
- OWISAM-AU: Pruebas sobre la autenticación.
- OWISAM-CP: Cifrado de las comunicaciones.
- OWISAM-CF: Configuración de la plataforma.
- OWISAM-IF: Pruebas de infraestructura.
- OWISAM-DS: Pruebas de denegación de servicio.
- OWISAM-GD: Pruebas sobre directivas y normativas.
- OWISAM-CT: Pruebas sobre los clientes inalámbricos.
- OWISAM-HS: Pruebas sobre host spots y portales cautivos.

En el presente trabajo se utilizó el análisis de *caja negra*, que es un tipo de análisis contemplado dentro de la metodología, puesto que la investigación se inició de un completo desconocimiento en la seguridad de los puntos de acceso, como su cifrado, canal, SSID y modelo del dispositivo del área geográfica a analizar, ya que al no contar con ninguna referencia en materia de seguridad inalámbrica empezó a recabar información que ayudara a realizar un análisis concreto, permitiendo de esta manera obtener un conocimiento más global y así mismo poder generar modelos estadísticos y porcentuales que contribuyeron a desarrollar reportes y recomendaciones que aumenten la confiabilidad de los Ap´s.

Así mismo se establecieron ciertas restricciones como lo son el área geográfica específica que consistió en dos AGEB y la ventana horaria la cual tuvo un margen entre las 11 AM y las 15:00 PM. (Tarlogic, 2013)

CAPÍTULO II Marco de Referencia

2.1 Componentes de las redes inalámbricas

2.1.1 Puntos de Acceso

Se considera un punto principal de emisión y recepción. Este punto se concentra en la señal de los nodos inalámbricos y centraliza el reparto de la información de toda la red local. También realiza el vínculo entre los nodos inalámbricos y la red cableada; por este se lo suele llamar **puente.**

Figura 3.-Típico AP (Access Point) que podemos encontrar en el mercado

Cuando conectamos varios AP (**sincronizados**) entre sí, podemos formar una gran red sin utilizar cables. Una mejor idea para poder entender el concepto de punto de acceso, es el situarse del lado del cliente (notebook, por ejemplo) y pensar que el **punto de acceso** provee un cable virtual entre cada cliente asociado a él. Así, este cable inalámbrico nos conecta a la red cableada como a cada uno de los demás usuarios de la red inalámbrica. (Claudio Alejandro Peña Millahual, 2012).

2.1.2 Router Inalámbrico

Es muy común confundir el término Access Point con un router inalámbrico. Este último es una Access Point combinado con un router y puede realizar tareas más difíciles que las del AP. Un router inalámbrico es como un **puente** (que une la red cableada y la no cableada) y un **direccionador** (que selecciona el destino según el enrutamiento del protocolo IP).

Figura 4 Router inalámbrico

Si se tiene una conexión ADSL que nos da acceso a internet a través de la línea telefónica, este dispositivo será el encargado de conectarnos. Pero no es la única función ya que, además, permite distribuir internet mediante cables y de forma inalámbrica mediante el punto de acceso que tiene integrado. (Salvetti, 2011)

También realiza las restricciones de acceso, por usuarios, servicios y horarios, entre otras opciones, y puede controlar el ancho de banda y las prioridades de acceso por cliente conectado o servicio (Claudio Alejandro Peña Millahual, 2012)

Figura 5 Algunos modelos de routers inalámbricos con antenas externas

2.2 Modo de operación

El modo de operación inalámbrica se refiere a los **estándares 802.11** que se define en dos modos fundamentales: **ad hoc** e **infraestructura.**

2.2.1 Modo ad hoc

Este modo es el más sencillo para configurar. Los únicos elementos necesarios para conformar una red en **modo ad hoc** son los dispositivos móviles que poseen placas de red inalámbricas.

También se le conoce con el nombre de punto a punto, ya que permite establecer comunicación directa entre los usuarios sin necesidad de involucrar un punto de acceso central que realice un vínculo.

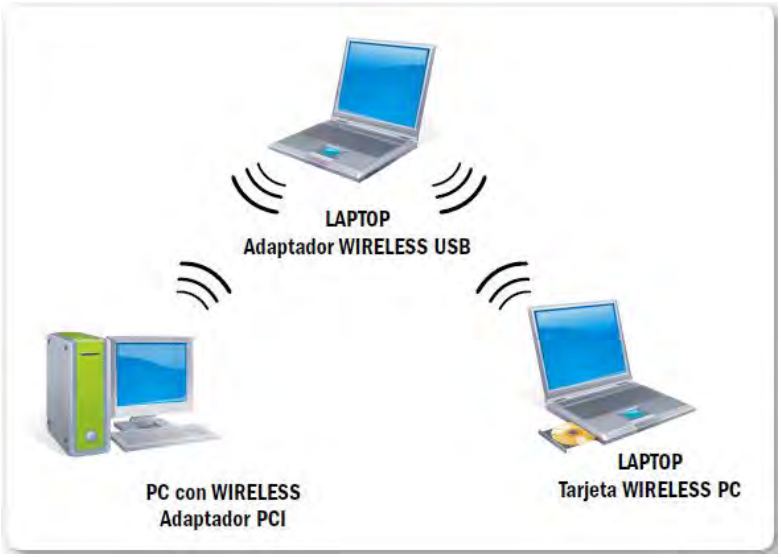


Figura 6 Ejemplo de una red ad hoc conformada por dispositivos comunes en cualquier hogar.

En pocas palabras, todos los nodos de una red ad hoc se pueden comunicar directamente con otros dispositivos y no es necesario ningún tipo de gestión administrativa de la red (punto de acceso).

Este tipo de red es común entre usuarios que desean compartir contenidos sin necesidad de conectar sus computadoras a redes habilitadas, ya que supone una configuración rápida y sencilla, para lo cual, en sistemas Microsoft Windows ®, solo hay que seguir un asistente de configuración. (Claudio Alejandro Peña Millahual, 2012).

2.2.2 Modo infraestructura

En las configuraciones en modo infraestructura se usa el concepto de **celda**, similar al implementado en la red de telefonía celular.

Se entiende por celda al área en la cual una señal radioeléctrica es efectiva. Así, una red inalámbrica puede tener una celda de tamaño reducido y, por medio de varios puntos de emisión, es posible combinar celdas y tener un área mayor.

Se logra esto utilizando los famosos puntos de acceso, que funcionan como **receptores** y, por eso, pueden duplicar el alcance de la red, ya que, en este caso, la distancia máxima no es entre estaciones, si no entre una estación y un punto de acceso. Estos dispositivos capaces de extender una red son colocados en lugares estratégicos, en general, altos y, además, realizan la coordinación del funcionamiento entre usuarios. Con solo un punto de acceso se puede soportar un grupo acotado de usuarios, el rango será de entre 30 metros y varios cientos más. Si se quiere

conectar varios puntos de acceso y usuarios, todos deben configurar el mismo SSID. (Salvetti, 2011)

Figura 7 Punto de acceso comunicando diferentes dispositivos en modo infraestructura.

2.4 Tipos de cifrado

2.4.1 Cifrado WEP (*Wired Equivalent Privacy*)

El sistema de cifrado WEP fue el primero que apareció para solucionar los problemas generados por las redes abiertas. Se trata de un sistema de cifrado que funciona mediante la autenticación del usuario con contraseña. De esta forma el tráfico viaja cifrado, y aquel usuario que se encuentre escuchando el tráfico sólo leerá caracteres sin sentido alguno, a no ser que tenga la clave del cifrado.

Este sistema de cifrado está basado en el algoritmo de cifrado RC4, utilizado para ello las claves de 64 o de 128 bits. Cada clave consta de dos partes, una de ellas la tiene que configurar el usuario en cada uno de los puntos de acceso de la red, mientras que la otra se genera

automáticamente y se denomina vector de inicialización, cuyo objetivo es obtener claves distintas para cada trama que se mueve en la red.

Inicialmente se creía que se trataba de un cifrado muy seguro, pero pronto se descubrió que no era así, demostrando que ofrece muchas vulnerabilidades.

Entre las principales vulnerabilidades de este sistema está que las claves permanecen siempre estáticas, y por otro lado los 24 bits del vector inicialización son insuficientes, además de trasmitirse sin cifrar.

Hoy en día es considerado un sistema poco seguro y no se aconseja su utilización en las redes inalámbricas, ya que se puede llegar a romper su seguridad mediante distintos sistemas como fuerza bruta o el ataque FMS (SAT, 2014).

2.4.2 Cifrado WPA (*WiFi Protected Access*)

Este sistema de cifrado surgió para solucionar los problemas de seguridad que ofrecía el sistema WEP.

Para ello hace uso de TKIP, un protocolo para gestionar las claves dinámicas, que resuelve muchos de los problemas que tenía WEP tales como la longitud de la clave, el cambio de la clave de estática a dinámica y la multidifusión.

WPA adopta la autenticación de usuarios mediante el uso de un servidor, donde se almacenan las credenciales y contraseñas de los usuarios de la red. Para no obligar al uso de tal servidor para el despliegue de redes, WPA permite la autenticación mediante una clave pre compartida, que de un modo similar al WEP, requiere introducir la misma clave en todos los equipos de la red.

WPA permite diferentes sistemas de control de acceso incluyendo la validación del usuario, como puede ser contraseña, certificado digital o simplemente hacer uso de una contraseña compartida para identificarse. (Lopez, 2008)

2.4.3 Cifrado WPA-PSK

Se trata del sistema de control de acceso más simple tras WEP y consiste en un sistema de clave compartida, clave formada entre 8 y 63 caracteres. Es un sistema fácil de utilizar y configurar y el más recomendable para entornos familiares y pequeñas empresas. Cualquier equipo que tenga esta clave podrá conectarse a la red.

Este sistema de acceso tiene el problema de que, al basarse en el uso de claves, esta se puede identificar por medio del uso de la fuerza bruta, es decir, ir comprobando distintas claves hasta dar con la correcta, de ahí que se fundamentan claves complejas alfanuméricas. (SAT, 2014), (Lopez, 2008)

2.4.4 Cifrado WPA2

En junio de 2004, fue adoptado el estándar IEEE 802.11i con la intención de responder a las preocupaciones empresariales ante la seguridad inalámbrica. El estándar 802.11i, también llamado WPA2, introdujo varios cambios fundamentales, como la separación de la autentificación de usuarios de la integridad y privacidad de los mensajes proporcionando una arquitectura segura para las redes inalámbricas.

WPA2 utiliza una nueva arquitectura para las redes Wireless llamada *Robust Security Network (RSN)* y utiliza la autentificación 802.11x, distribución de claves robustas y nuevos mecanismos de integridad y privacidad. Para el cifrado de datos utiliza el algoritmo de cifrado por bloques AES (*Advance Encryption Standart*).

Hasta el momento el algoritmo de cifrado WPA2 es el algoritmo más seguro y se aconseja su utilización frente a otros algoritmos que ya han sido “rotos”, como es el caso de WEP o WPA. (Salvetti, 2011).

2.4.5 WPA PSK

Lo más habitual en una red WiFi doméstica es que la autenticación se base en PSK, que son las siglas de Pre Shared Key (clave compartida previamente), es decir, la seguridad de la red WiFi se basa en un secreto compartido (la contraseña de la red WiFi), que conocen los usuarios y el punto de acceso.

Para simplificarlo, una red WiFi **WPA-PSK** dispone de una contraseña conocida por todos y cada uno de los usuarios que se conectan a la red.

Es la configuración de red más utilizada en los routers WiFi que los ISPs facilitan con sus conexiones de ADSL/Cable/Fibra óptica. (WiFi, 2014)

2.4.6 Red WiFi con WPA2 PSK

WPA2 es el nuevo estándar de seguridad WiFi que incorpora algunas mejoras para hacerlo más resistente a algunos ataques conocidos. con WPA2 las contraseñas se pueden seguir intercambiando cómo un secreto compartido (PSK) en las redes domésticas. (WiFi, 2014),

2.4.7 Red WiFi con seguridad TKIP

Tras la aparición de WPA como sustituto de WEP, el algoritmo de cifrado TKIP (Temporal Key Integrity Protocol) surge como un nuevo mecanismo de cifrado para proteger las comunicaciones inalámbricas.

En la actualidad se considera obsoleto, ya que fue sustituido por CCMP en el año 2009, pero **TKIP** sigue siendo una de las configuraciones más habituales (**WPA-TKIP** o también representado por **WPA-PSK-TKIP**). (WiFi, 2014)

2.4.8 Red WiFi con WPA CCMP y WPA2 CCMP

Son las siglas Counter Mode CBC-MAC Protocol . **CCMP**, también conocido como **AES CCMP**,y es el mecanismo de cifrado actual que sustituye a **TKIP** y el estándar definido para su uso con WPA2. Las especificaciones dicen que las redes WPA2 deben usar CCMP por defecto con **WPA2-CCMP** (**WPA2-PSK-CCMP**), aunque también puede ser utilizado con WPA para darle una mayor seguridad (**WPA-CCMP** / **WPA-PSK-CCMP**). (WiFi, 2014)

2.4.9 Red WiFi WPA MGT o WPA2 MGT

Si has visto redes WiFi con estas características, debes saber que cuando una red es **WPA MGT** o **WPA2 MGT** significa que la contraseña no es una clave pre compartida. En su lugar, la red WiFi está conectada a un sistema o servicio de autenticación, habitualmente un servicio radius, para verificar el usuario y la contraseña de la persona que se intenta conectar. Dado que las redes WiFi MGT (Management) necesitan una infraestructura algo más compleja, son las usadas en entornos profesionales y en empresas. (WiFi, 2014)

2.4.10 TKIP *vs* CCMP

Muchas redes pueden soportar simultáneamente WPA y WPA2, y cada uno de estos mecanismos de autenticación pueden soportar **TKIP** o **CCMP**.

Aunque el estándar no lo recomienda, el uso de TKIP con WPA2 PSK (**WPA2-PSK-TKIP**) se soporta por si es necesario dar compatibilidad a dispositivos antiguos. Salvo que este sea el caso, lo ideal es **desactivar la seguridad WPA** en la red WiFi, dejando únicamente activado la seguridad WPA2.
También se debe desactivar TKIP, dejando sólo las opciones CCMP. Las redes WiFi que disponen únicamente del mecanismo WPA2-CCMP (WPA**2-PSK-CCMP**) son las redes WiFi más seguras. (WiFi, 2014)

2.5 Canales

El IEEE 802.11 establece que los dispositivos pueden utilizar las bandas 2.4 GHz, 3.6 GHz y 5 GHz para la retransmisión inalámbrica. Cada banda esta subdividida en canales, que están separados por una frecuencia mínima de 5 MHz. La variedad de canales que pueden utilizar varia con la región, en Norte América se puede usar del 1 a 11, y en Japón del 1 a 14, pero en Europa, los routers que ofrecen las compañías tienen capacidad para operar con 14 canales son los siguientes:

Radio	Canal	Dominio Regulatorio
2.4 GHz radio	Canal 1-2412	Américas, EMEA, Japón y China
	Canal 2-2417	Américas, EMEA, Japón y China
	Canal 3-2422	Américas, EMEA, Japón, Israel y China
	Canal 4-2427	Américas, EMEA, Japón, Israel y China
	Canal 5-2432	Américas, EMEA, Japón, Israel y China

	Canal 6-2437	Américas, EMEA, Japón, Israel y China
	Canal 7-2442	Américas, EMEA, Japón, Israel y China
	Canal 8-2447	Américas, EMEA, Japón, Israel y China
	Canal 9-2452	Américas, EMEA, Japón, Israel y China
	Canal 10-2457	Américas, EMEA, Japón, y China
	Canal 11-2462	Américas, EMEA, Japón, y China
	Canal 12-2467	EMEA y solo Japón
	Canal 13-2472	EMEA y solo Japón
	Canal 14-2484	Solo Japón
5 GHz radio	Canal 34-5170	Solo Japón
	Canal 36-5180	Japón y Singapur
	Canal 38-5190	Solo Japón
	Canal 40-5200	Japón y Singapur
	Canal 42-5210	Solo Japón
	Canal 44-5220	Japón y Singapur
	Canal 46-5230	Solo Japón
	Canal 48-5240	Japón y Singapur
	Canal 52-5260	Américas y Taiwán
	Canal 56-5280	Américas y Taiwán
	Canal 60-5300	Américas y Taiwán
	Canal 64-5320	Américas y Taiwán

Tabla 1 Compañías con 14 canales de operación. (Reid, 2004), (Academy, 2006)

2.6 SSID (*Service Set Identifier*)

El **SSID** es el nombre que asignamos a nuestra red inalámbrica, el cual también se incluye en todos los paquetes **baliza** (**beacon** en inglés) que envía el punto de acceso. Una baliza es un paquete de información que se manda desde un dispositivo conectado a todos los demás, para anunciar su disponibilidad. Un intervalo de baliza es el periodo de tiempo (enviado con baliza) que debe transcurrir antes de que se vuelva a enviar la baliza. El intervalo de baliza puede ajustarse en términos de milisegundos (ms). (Reid, 2004), (Vieites, 2003)

2.7 Filtrado MAC

La dirección **MAC** (**Media Access Control**) es un identificador de 48 bits que está grabado en las placas de red (en todas) y que identifica físicamente a nuestra placa. Este valor viene establecido de fábrica, y cada dirección **MAC** es diferente según el fabricante. (Carballar Falcón, 2005)

De esta forma el filtrado MAC significa que solo un grupo limitado en direcciones MAC conocidas por nosotros pueden conectarse al punto de acceso. Es una medida de seguridad bastante débil, pero se puede usar combinada con otras un poco más avanzadas.

El filtrado MAC utiliza una lista de direcciones MAC. Tomando en cuenta dicha lista, hay dos modos en los que se puede configurar:

- **Permitiendo la conexión a los dispositivos añadidos a la lista de direcciones MAC,** quedando cualquier otro sin posibilidad de conectarse a la red. Esto es bastante útil cuando se quiere que solo unos determinados dispositivos puedan conectarse al Wi-Fi.
- **Denegando la conexión a los dispositivos que aparecen en la lista de direcciones MAC,** circunstancia en la que cualquier otro dispositivo podrá conectarse. Esta forma seria adecuada para no permitir la conexión a un determinado dispositivo del que se conoce la dirección MAC. (Andrew A. Vladimirov, 2005)

CAPÍTULO III Desarrollo

3.1 Recursos utilizados

1. Mapa Digital: Mapa obtenido del *Instituto Nacional de Estadística y Geografía* (INEGI, INEGI, 2015) en el cual se encuentran marcadas las zonas denominadas AGEB las cuales se usarán para realizar el análisis.
2. Software: *Acrylic WiFi Profesional* es un analizador que identifica los puntos de acceso y canales WiFi, identifica y resuelve incidencias en redes WiFi 802.11al alcance en tiempo real.
3. Equipo: Ultrabook Lanix Neuron UX, Intel Core i3 3217u a 1.8 GHz Windows 8, disco duro de 500 Gb, memoria RAM 4 GB
4. Dispositivo Inalámbrico: Adaptador USB inalámbrico TP-LINK de alta ganancia de 150 Mbps y 4 dBi.

Las AGEB como su nombre lo indica es un área geográfica ocupada por un conjunto de manzanas perfectamente delimitadas por calles, avenidas, andadores o cualquier rasgo de fácil identificación en el terreno cuyo uso del suelo es principalmente habitacional, industrial, de servicios, comercial, etc. y solo son asignadas al interior de localidades urbanas. (INEGI, 2010)

3.2 Técnica del análisis

Para llevar a cabo la investigación se optó por realizar una técnica estadística llamada *muestreo intencional o de conveniencia*. Esta técnica de muestreo se caracteriza por un esfuerzo deliberado de obtener muestras “representativas” mediante la inclusión en la muestra de grupos supuestamente típicos. (Villarce, s.f.)

Se seleccionó intencionalmente los AGEB 2300400010759 y 2300400010392, ya que al contar con la mayor cantidad de habitantes se espera poder encontrar suficientes puntos de acceso de inalámbricos y así poder obtener los resultados necesarios para el análisis.

3.3 Software para el análisis de los puntos de acceso (Ap´s)

Una vez determinado las AGEB con la mayor concentración de población en la ciudad y la técnica a emplear para obtener las muestras necesarias, se dispuso a elegir la herramienta con la que se realizara el escaneo de los puntos de acceso.

Durante la selección del software se probaron varias herramientas con las cuales la gran mayoría no se llegó a lo que se esperaba, ya que no contaban con una base de datos lo suficientemente amplia de fabricantes de puntos de acceso y en muchos casos simplemente el apartado de fabricantes se quedaba en blanco al no poder identificarlo.

Acrylic WiFi profesional a pesar de ser nuevo en el mercado cuenta con una amplia base de datos sobre fabricantes, que es uno de los puntos fuertes del análisis, *Acrylic WiFi profesional* también brinda la facilidad de exportar los resultados obtenidos a diferentes formatos como html, jpg y xls.

3.4 Ejecución del análisis

Para la ejecución primero se procedió a plantear un horario en el que se realizaría el recorrido por las AGEB mencionadas con anterioridad, el horario que se escogió fue entre las 11 y las 15 horas, ya que se pensó que sería una hora en que los que más hagan uso de los puntos de acceso estén en sus hogares en este caso los estudiantes y estos AP’s no se encuentren apagados.

3.4.1 Recorrido día 1

Para el primero día se recorrió la AGEB 2300400010759 esta primera AGEB se dividió en tres partes para facilitar el recorrido, la primera parte abarca de manera horizontal desde la Av. Insurgentes hasta la Av. Erick Paolo Martínez y de manera vertical de la calle Faisán hasta la Av. Javier Rojo Gómez.

Figura 8 Recorrido día 1 primera parte

En el primer día se encontró un total de *629 puntos de acceso inalámbricos*.

SSID	Mac Address	Rssi	Snr	Chan	Wide	802.11	Max Rate	WEP	WPA	WPA2	WPS	Password	WPS PIN	Vendor
CablemasC9C5	68:94:23:5D:CA:EC	-100	0	11	20	b,g,n	144.4			PSK-(TKIP|CCMP)				Hon Hai Precisi
HITRON-CF60	78:8D:F7:90:CF:68	-100	0	1	20	b,g,n	300		PSK-CCMP	PSK-CCMP	1.0			Hitron Technol
CablemasB3C7	F4:B7:E2:B1:53:69	-100	0	11	20	b,g,n	144.4			PSK-(TKIP|CCMP)				Hon Hai Precisi
INFINITUMa958	40:CB:A8:32:79:6C	-97	48	6	20	b,g,n	130		PSK-(TKIP|CCMP)	PSK-(TKIP|CCMP)	1.0			Huawei Techn
HITRON-A9F0	78:8D:F7:9A:A9:F8	-95	52	11	20	b,g,n	300		PSK-CCMP	PSK-CCMP	1.0			Hitron Technol
wlCORONA	20:AA:4B:50:1A:49	-94	54	11	20	b,g,n	144.4		PSK-(TKIP|CCMP)	PSK-(TKIP|CCMP)				Cisco-Linksys, I
TETE	F4:EC:38:F2:1F:D8	-100	0	1	20	b,g	54		PSK-(TKIP|CCMP)	PSK-(TKIP|CCMP)				TP-LINK TECH
wifi-seq	00:20:A6:EC:5A:10	-100	0	1	20	b,g	54		PSK-TKIP					Proxim Wireless
wlVisitantes	00:25:68:B8:26:1C	-98	46	1	20	b,g	54		PSK-TKIP	PSK-TKIP				Shenzhen Hua
wifi-seq	00:20:A6:5B:98:48	-100	0	1	20	b,g	54		PSK-TKIP					Proxim Wireless
INFINITUM525a	64:16:F0:D5:C3:34	-100	0	1	20	b,g	54	SharedKey						Shehzhen Hua
[Hidden]	00:A0:F8:6D:D1:EF	-100	0	9	20	b	11			PSK-CCMP				Zebra Technol
[Hidden]	00:A0:F8:6D:D1:EE	-100	0	9	20	b	11		PSK-TKIP	PSK-TKIP				Zebra Technol
[Hidden]	00:A0:F8:6D:5A:B6	-100	0	11	20	b	11		PSK-TKIP	PSK-TKIP				Zebra Technol
[Hidden]	00:A0:F8:6D:5A:B4	-100	0	11	20	b	11		PSK-TKIP	PSK-TKIP				Zebra Technol

Figura 9 Muestras del día 1

3.4.2 Recorrido día 2

En el segundo día se recorrió la segunda parte que abarca de manera horizontal desde la Av. Insurgentes hasta la Av. Erick Paolo Martínez y de forma vertical desde la Av. Javier Rojo Gómez hasta la calle Tzisauche.

Figura 10 Recorrido día 2 segunda parte

En el segundo día se encontraron un total de *335 puntos de acceso* inalámbricos.

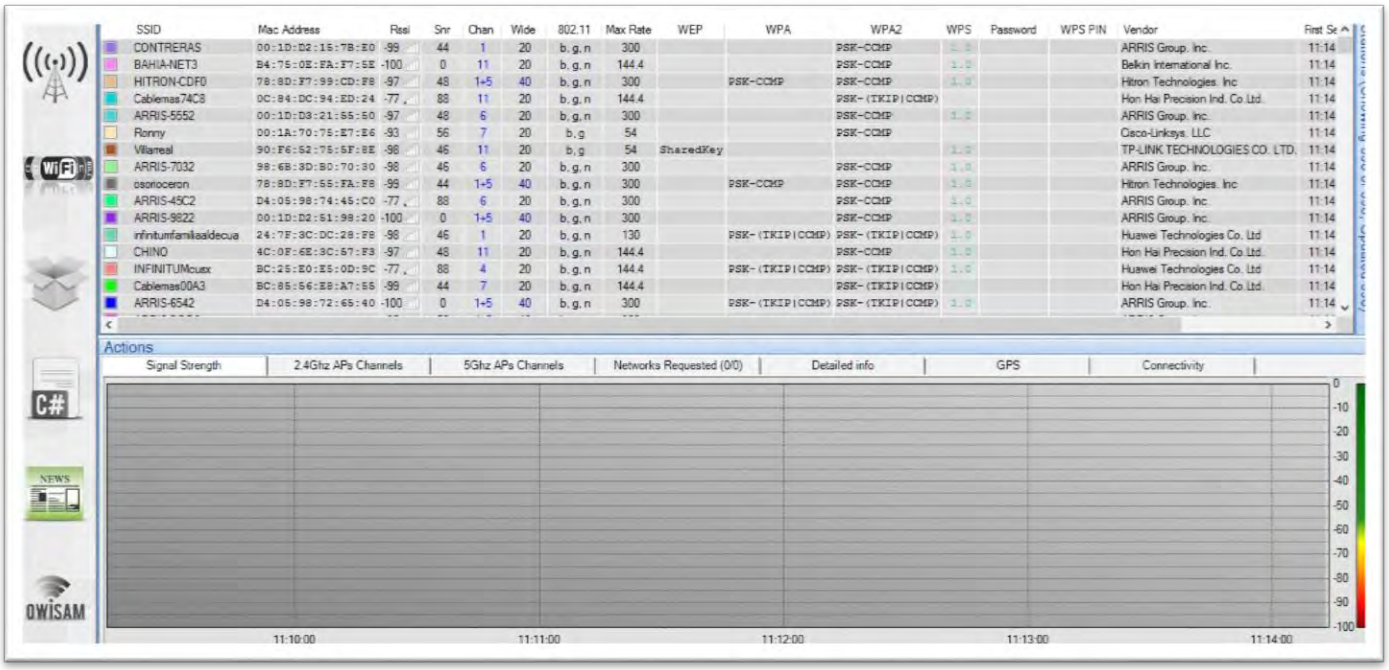


Figura 11 Muestras del segundo día

3.4.3 Recorrido día 3

El último recorrido de la primera AGEB se realizó entre las Av. Insurgentes y Erick Paolo Martínez de manera horizontal y de manera vertical entre las calles Tzisauche y Aarón Merino

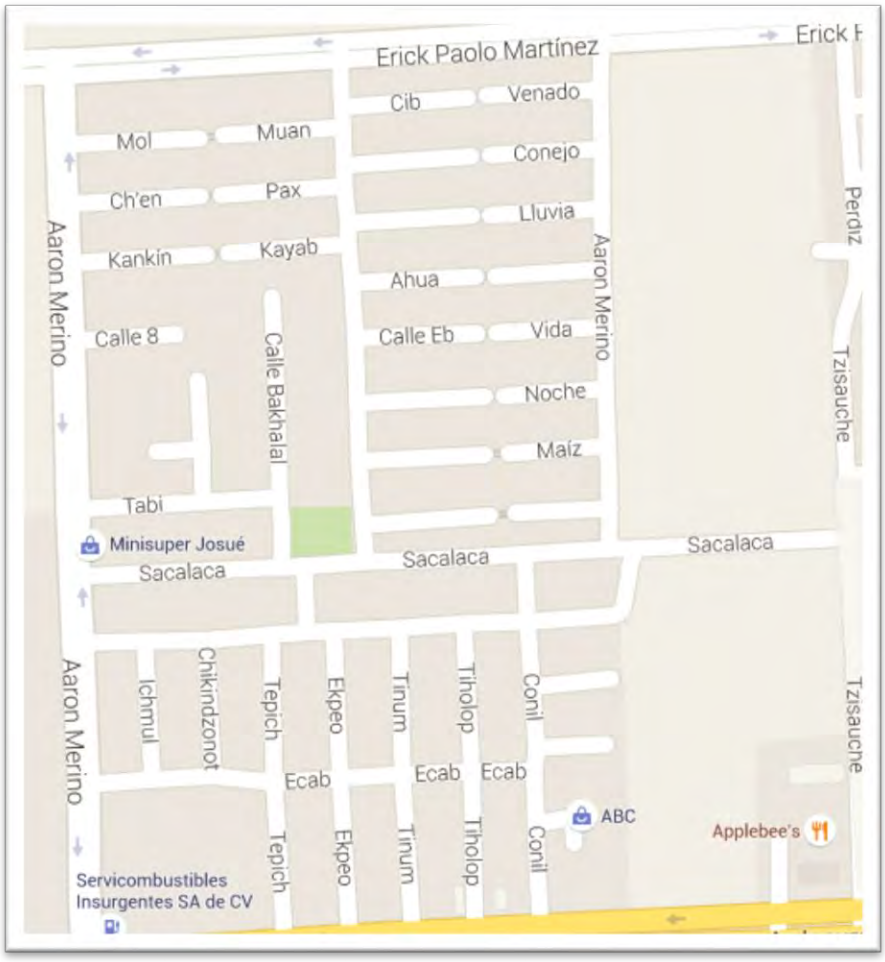


Figura 12 Recorrido día 3 tercera parte

En el cual se encontraron un total de *818 puntos de acceso* inalámbricos.

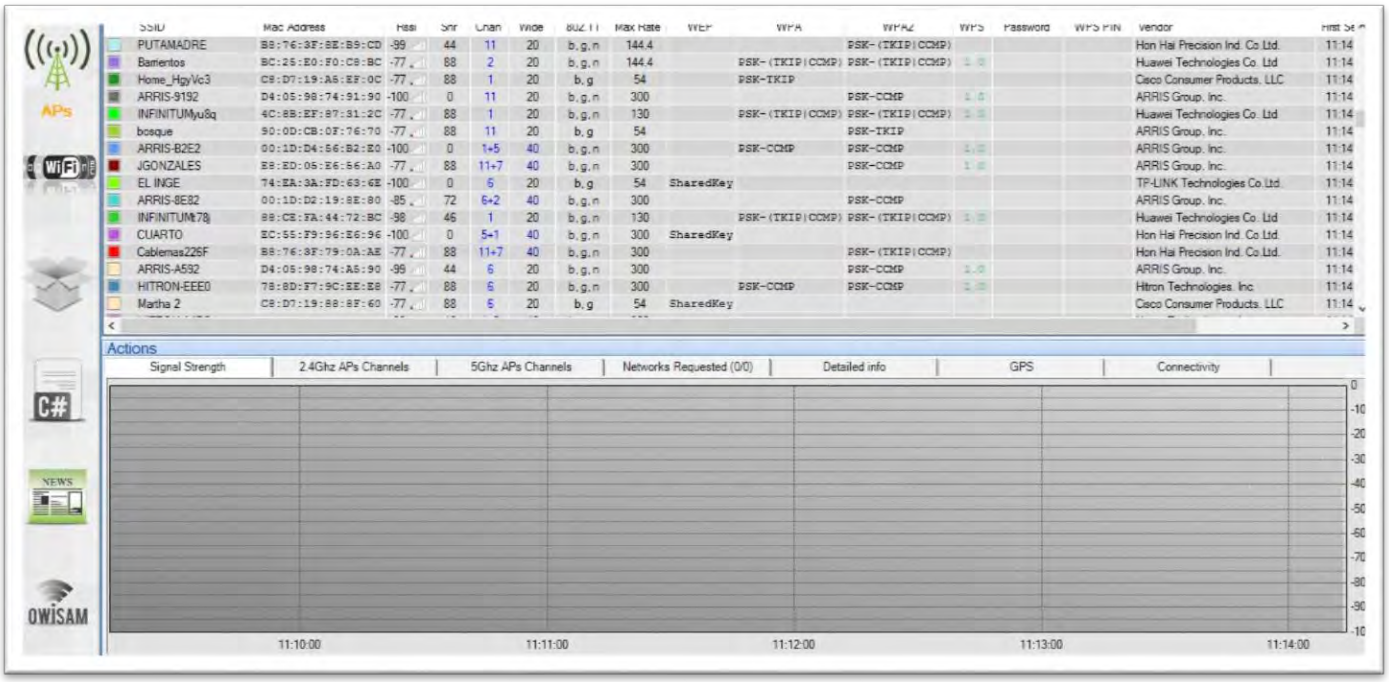


Figura 13 Muestras del tercer día

3.4.4 Recorrido día 4

El cuarto día ya empieza abarcar lo que es la segunda AGEB que es la 2300400010392 la cual abarca la colonia del Bosque, esta zona se dividió en dos partes la primera parte abarca verticalmente desde la Av. Universidad hasta la calle Francisco J. Mujica y horizontalmente desde la calle Ignacio Comonfort hasta la calle Pucté.

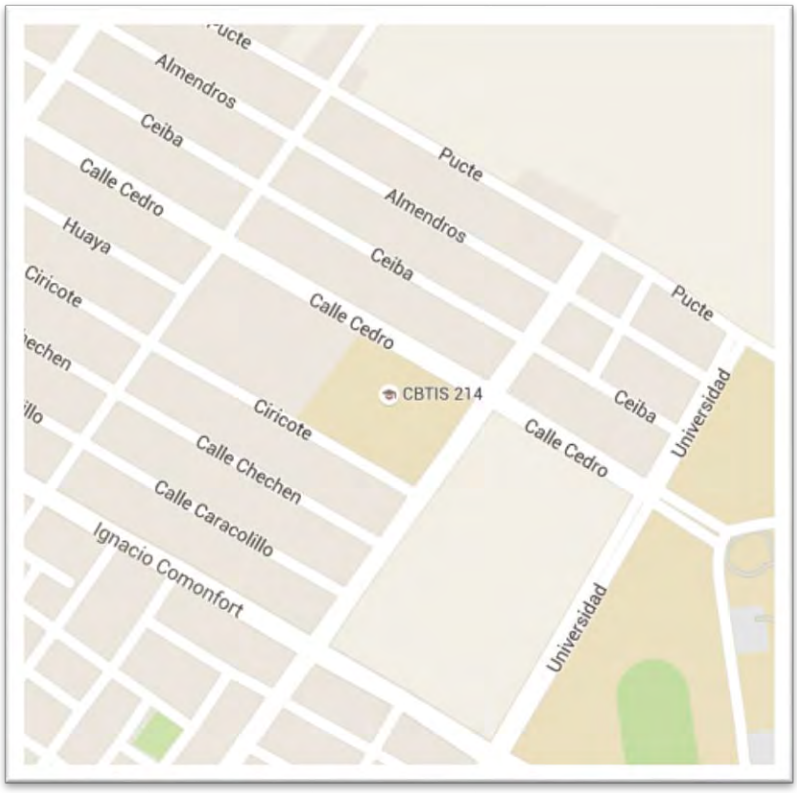


Figura 14 Recorrido día 4 parte 1

En esta primera parte del recorrido de la segunda AGEB se encontraron un total de *397 puntos de accesos inalámbricos.*

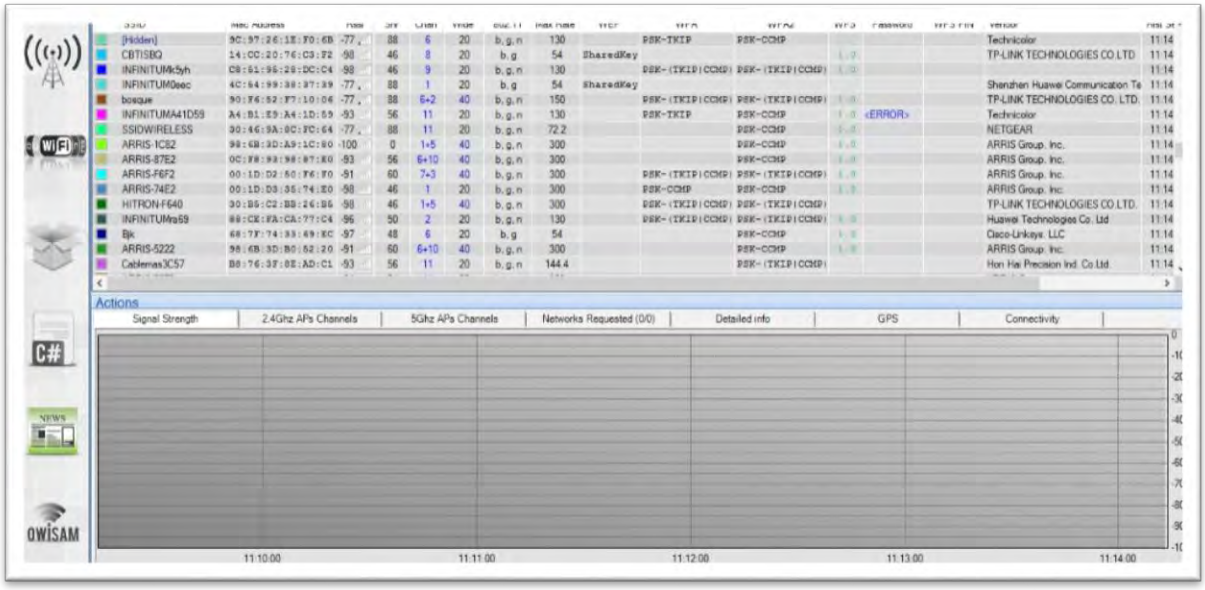


Figura 15 Muestras del cuarto día

3.4.5 Recorrido día 5

El último del recorrido de la segunda AGEB abarco de manera horizontal de la calle Ignacio Comonfort hasta la calle Pucté y Flamboyanes y de forma vertical de la calle Francisco J. Mujica hasta la Av. Belice

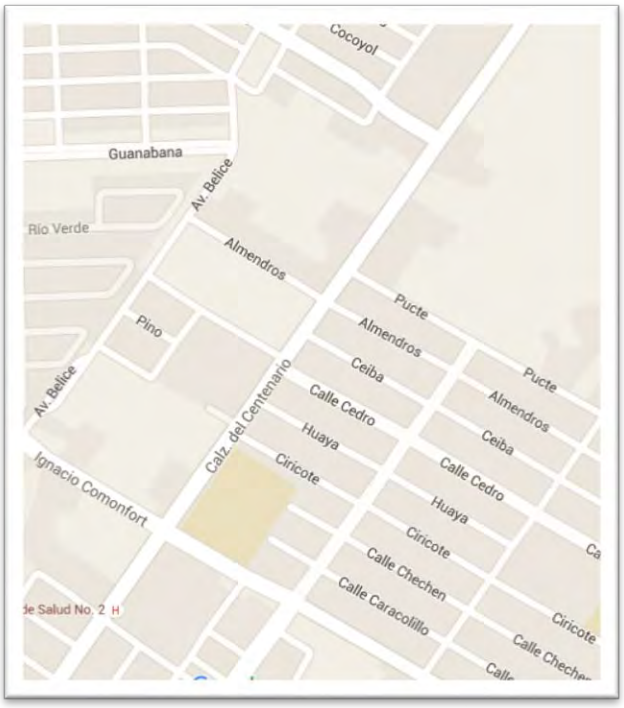


Figura 16 Recorrido día 5 parte 2

Para este último día se lograron encontrar un total de *561 puntos de acceso inalámbrico*.

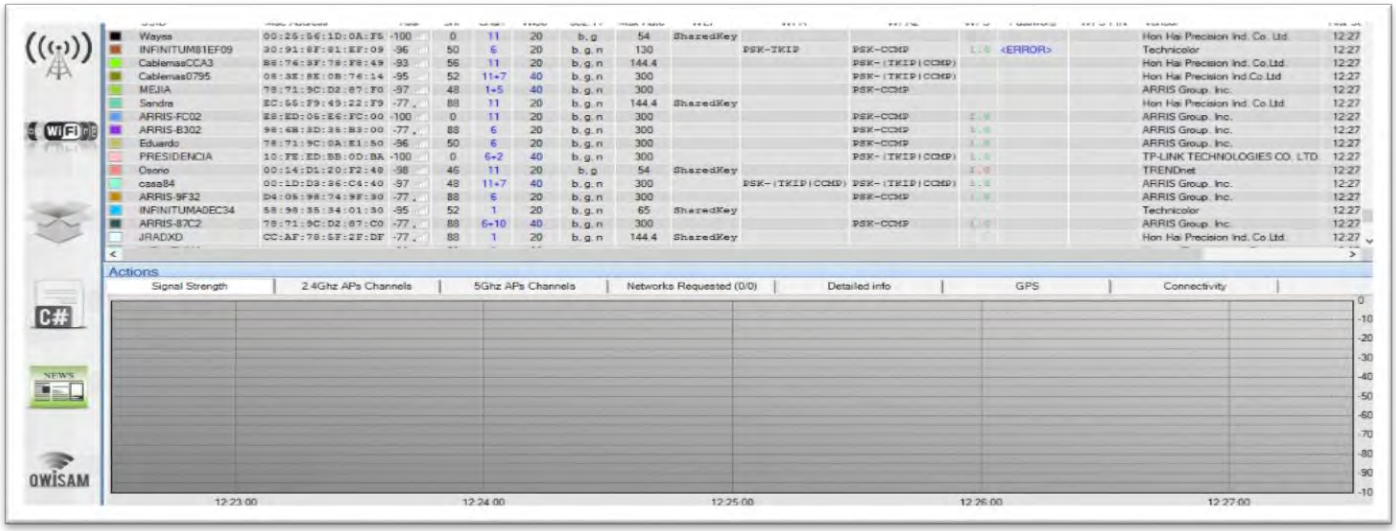


Figura 17 Muestras del último día

3.5 Datos obtenidos

Tras finalizar los días de recorrido por las AGEB, se obtuvieron un total de 2,740 puntos de acceso inalámbrico, de los cuales al examinarlos detalladamente se tuvo que realizar una limpieza de Ap´s ya que algunos de estos puntos no cumplían con los requerimientos de puntos de acceso inalámbricos caseros, por ejemplo, algunos puntos se encontraban repetidos, otros eran redes compartidas mediante dispositivos móviles, también se encontraron señales de impresoras inalámbricas, ciber-parques y escuelas hoteles y centros comerciales.

Una vez hecho la limpieza de puntos de accesos inalámbricos se vio en la necesidad de eliminar 450 Ap´s ya que no cumplían con el interés principal al no ser Ap´s caseros, quedando un total de 2290 Ap´s.-2290

Otro factor sobresaliente que se observó a la hora de analizar los datos obtenidos, fue que el cifrado de los Ap´s en la gran mayoría se mostraba que contaba con un cifrado WPA y WPA2 al mismo tiempo y lo que esto representa es que el Ap´s cuenta con una configuración para que algunos dispositivos que no soporten WPA2 como cifrado, puedan conectarse mediante WPA.

Numero de recorrido	***AP's encontrados***	***AP's Domesticos***
Recorrido # 1	629	530
Recorrido # 2	335	273
Recorrido # 3	818	664
Recorrido # 4	397	350
Recorrido # 5	561	473
Total	2740	2290

Tabla 2: Resumen de los AP's domésticos encontrados

Capitulo IV Resultados y recomendaciones

4.1 Tipo de cifrado más utilizado

De acuerdo a los resultados obtenidos la mayoría de los puntos de acceso inalámbricos en la ciudad de Chetumal, Quintana Roo, presentan el cifrado más confiable actualmente en el mercado el cual es *WPA2.*

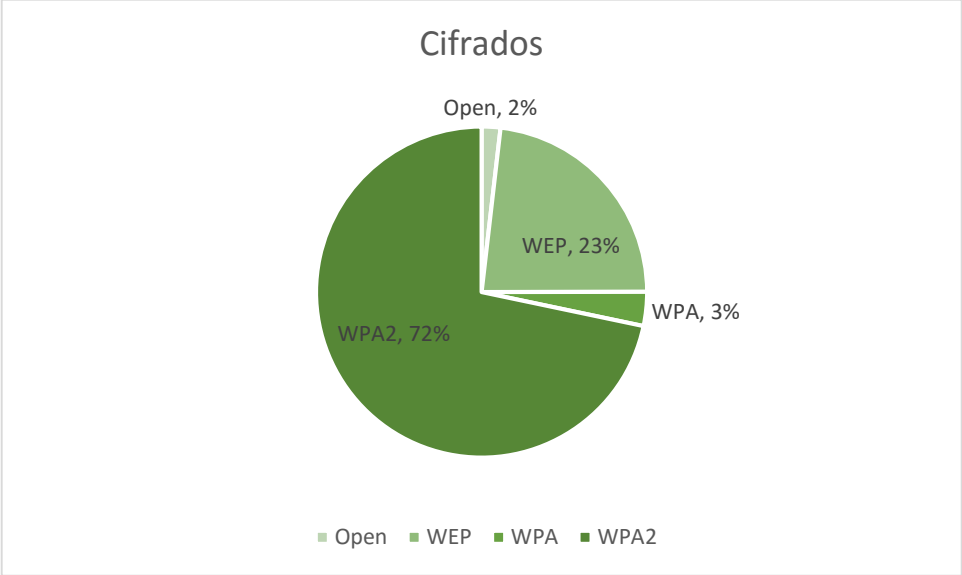


Figura 18 Porcentaje de cifrados

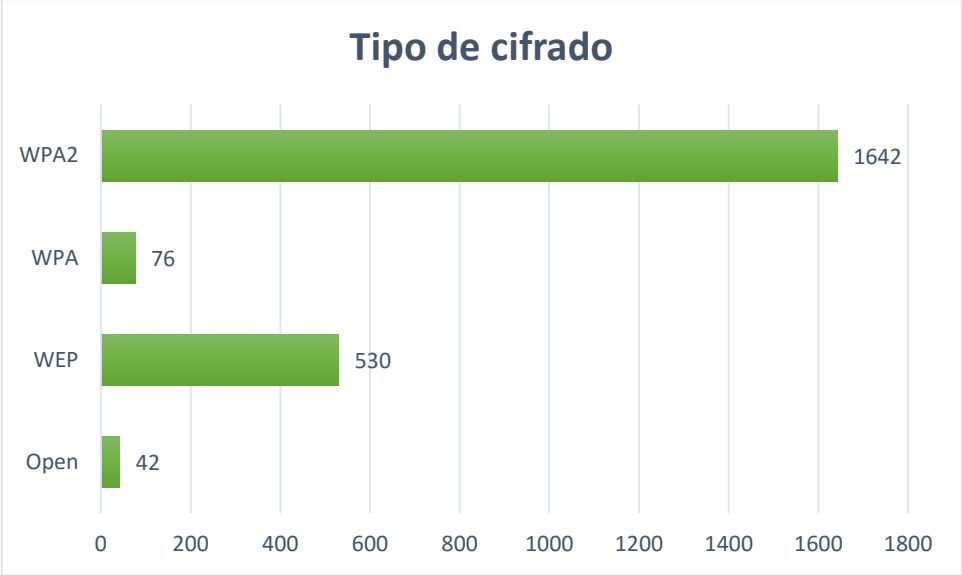


Figura 19 Grafica de total de cifrados

A pesar de que WPA2 es el cifrado que más predomina con un total de 1642 Ap´s que hacen uso de éste, lo preocupante es que el segundo cifrado más utilizado es WEP con un total de 530 Ap´s manteniendo una presencia significativa, lo que significa que los puntos de acceso inalámbrico aún se encuentran potencialmente en peligro al hacer uso de un cifrado obsoleto.

4.2 Fabricantes más populares

El fabricante más utilizado en la ciudad de Chetumal, Quintana Roo, es *Huawei Technologies* que alcanza un total de 488 Ap´s, y con prácticamente nada de diferencia le sigue *Hon Hai Precision* con 439, después en tercer lugar está el fabricante *Technicolor* con 322 Ap´s.

Figura 20 Grafica de fabricantes más populares

4.3 Uso de canales en la banda 2.4 GHz

Los canales más populares en la banda 2.4 GHz resultaron ser 3, los cuales son el canal 11 con un 30%, el canal 1 con un 21$ y el canal 6 con un 18%, los otros 10 canales no tienen una gran presencia ya que estos están entre 0% y el 6% de uso.

Al ser estos tres canales los más comúnmente utilizados en la zona, representan un problema más para funcionalidad que para seguridad, ya que al tener tantos Ap´s en un mismo canal saturan el espectro de radiofrecuencia llevando a la problemática conocida como *solapación de canales.*

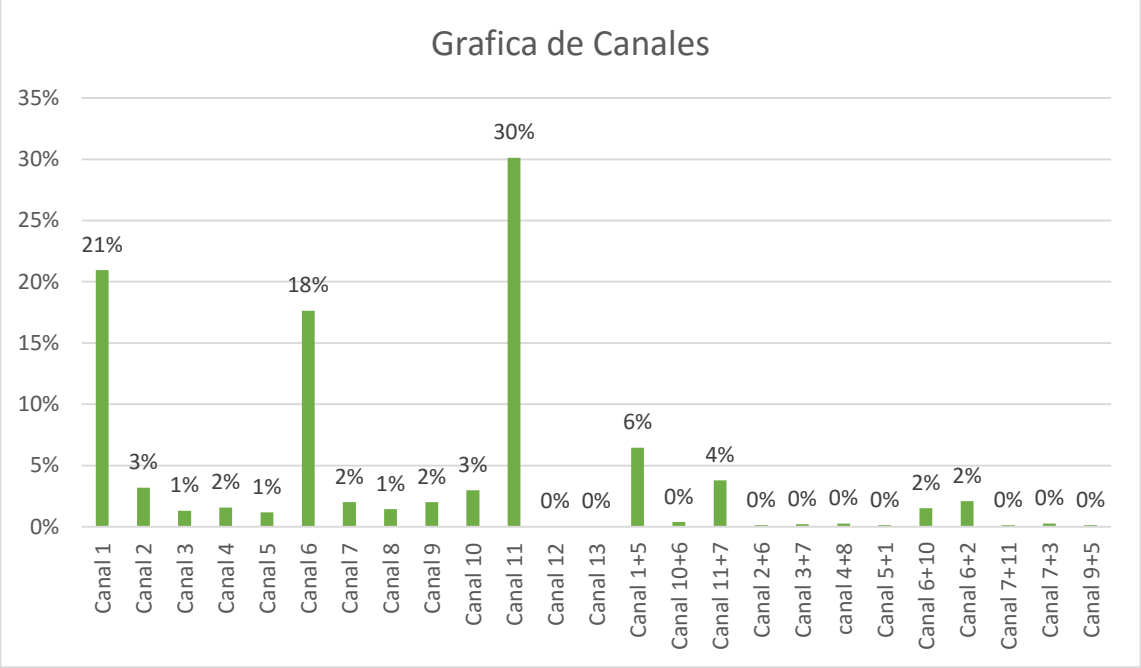


Figura 21 Uso de canales más populares

4.4 Análisis de fabricante Huawei Technologies

Por número de dispositivos analizados, Huawei Technologies es el fabricante de Ap´s más popular en la ciudad de Chetumal, Quintana Roo, por lo que el estado en que se encuentran actualmente es algo preocupante por los factores que a continuación se mencionan:

De los 488 Ap´s Huawei, 431 aún conservan su SSID por defecto el cual es INFINITUMXXXX, al dejar el SSID por defecto se facilita a hackers, cyberpiratas y cualquier intruso potencial acceder a la red inalámbrica WiFi, ya que existen páginas Web donde se pueden encontrar las claves por defecto de estos Ap´s.

Otro factor preocupante fue que el 38% de los Ap´s Huawei hacen uso del cifrado WEP lo que es aún más alarmante dado que WEP es un cifrado obsoleto y la seguridad puede ser violada en menos de 5 minutos incluso con dispositivos inteligentes como lo son los celulares actuales.

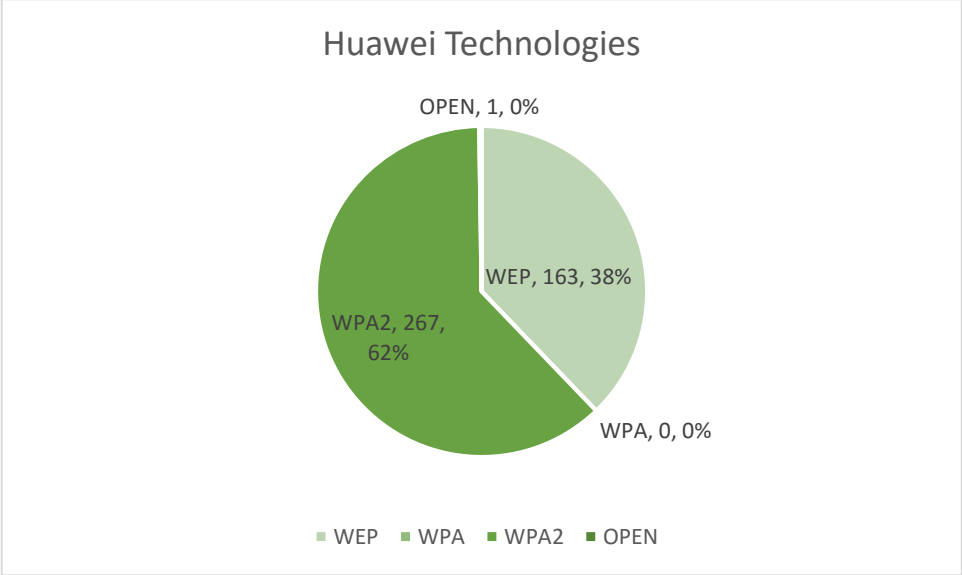


Figura 22 Estado del Cifrado del Ap´s más popular.

4.5 Análisis del fabricante *Hon Hai Precision*

El estado del segundo fabricante más popular en la ciudad de Chetumal, Quintana Roo ya no es tan preocupante como el del primero, pero eso no quiere decir que no se encuentre expuesto.

Con un total de 439 Ap´s *Hon Hai Precision*, el 59% mantienen su SSID por defecto los cuales son CABLEMASXXXX y UBEE y como se mencionó con anterioridad el conservar un SSID por defecto pone a la red inalámbrica WiFi potencialmente en peligro ya que las claves para acceder al Ap´s se encuentran documentadas en internet.

Por otro lado, el cifrado WPA2 que es usado por estos Ap´s es el más confiable hasta el momento, con un uso del 99%, sin embargo, si el 59% mantiene su SSID por defecto entonces es muy probable que la contraseña sea la que el AP trae por defecto, dejando vulnerable la confiabilidad del AP.

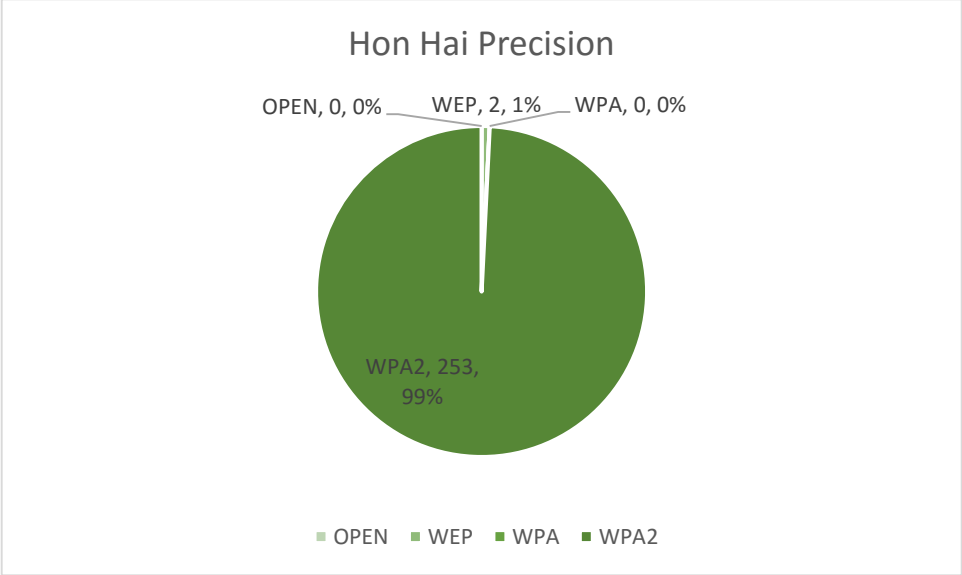


Figura 23 Estado del cifrado del Ap´s Hon Hai

4.6 Análisis del fabricante Technicolor

El estado del tercer fabricante más popular en cuanto a mantener un SSID por defecto es muy similar al primero dado que ambos son del mismo proveedor de servicios de internet: *TELMEX,* con un total de 322 Ap´s. El 85% (275 AP's) conserva su SSID por defecto y como se viene mencionando en los dos casos anteriores no cambiar el SSID pone en peligro a la red inalámbrica de ser atacada por personas mal intencionadas, por otro lado el cifrado que predomina es WPA2, un cifrado seguro y confiable con un 88%, pero WEP aún está presente con un 11%.

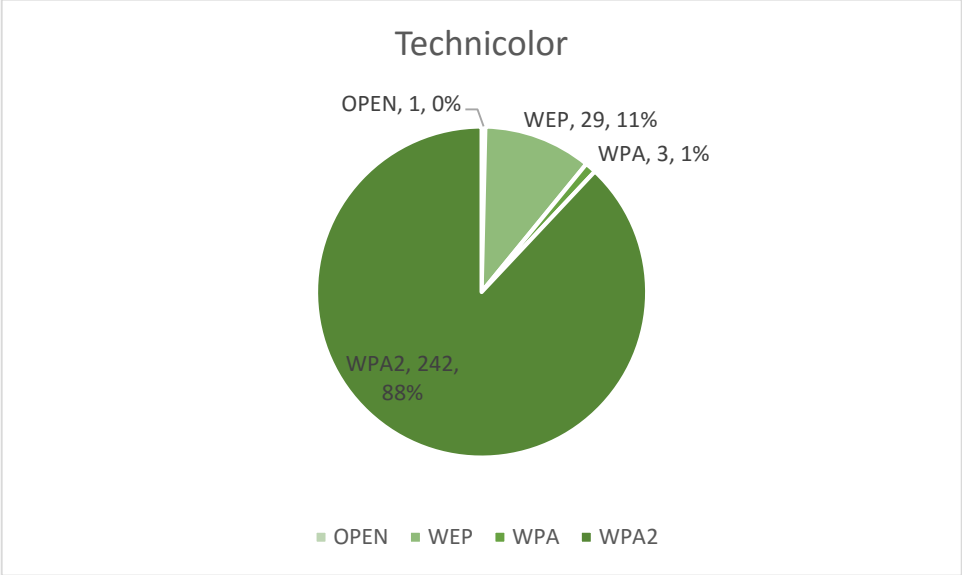


Figura 24 Estado del cifrado del Ap´s Technicolor

4.7 Aplicar medidas de seguridad

A continuación, se muestra un ejemplo de los pasos a seguir para aplicar medidas de seguridad a los AP's que son entregados por el proveedor de servicios de internet, en este caso por parte de Telmex:

4.7.1 Acceder al AP's

Como primer paso debemos entrar al navegador web e ingresar en la barra de direcciones 192.168.1.254 para poder entrar a la configuración del AP's, inmediatamente solicitara un usuario y contraseña,

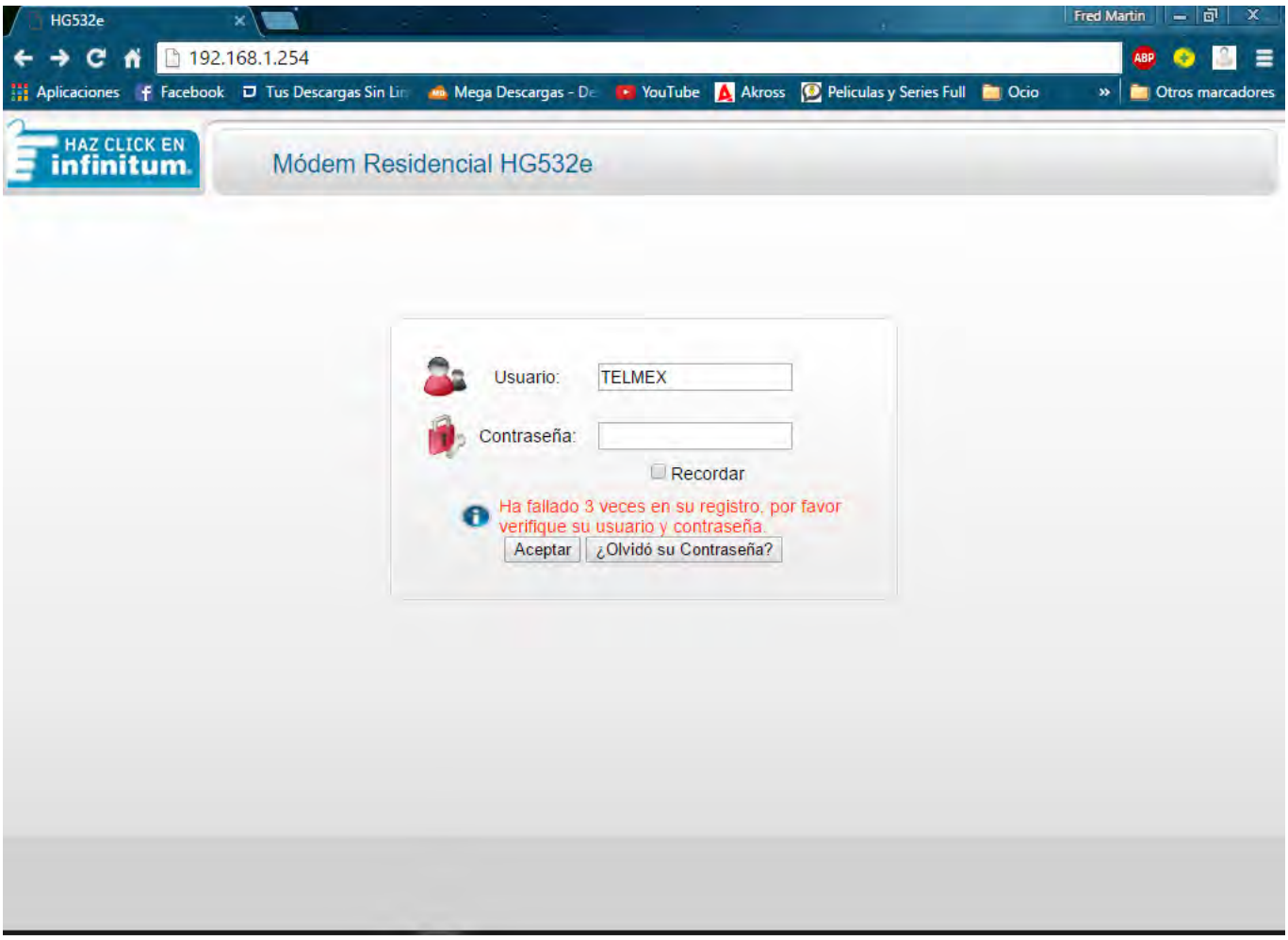


Ilustración 25 Usuario y contraseña del AP's

4.7.2 Modificar y ocultar SSID

Como primera medida de seguridad hay que modificar el SSID que trae por defecto el AP's, para ellos una vez dentro de la página principal del AP's de lado izquierdo se muestra una serie de opciones: Estado, Básico, Avanzado y Mantenimiento. Seleccionar opción de Básico, se desplegarán 4 opciones más las cuales son WAN, LAN, WLAN, y DSL, seleccionar la opción de WLAN el cual mostrara una serie de opciones entre las cuales está el SSID.

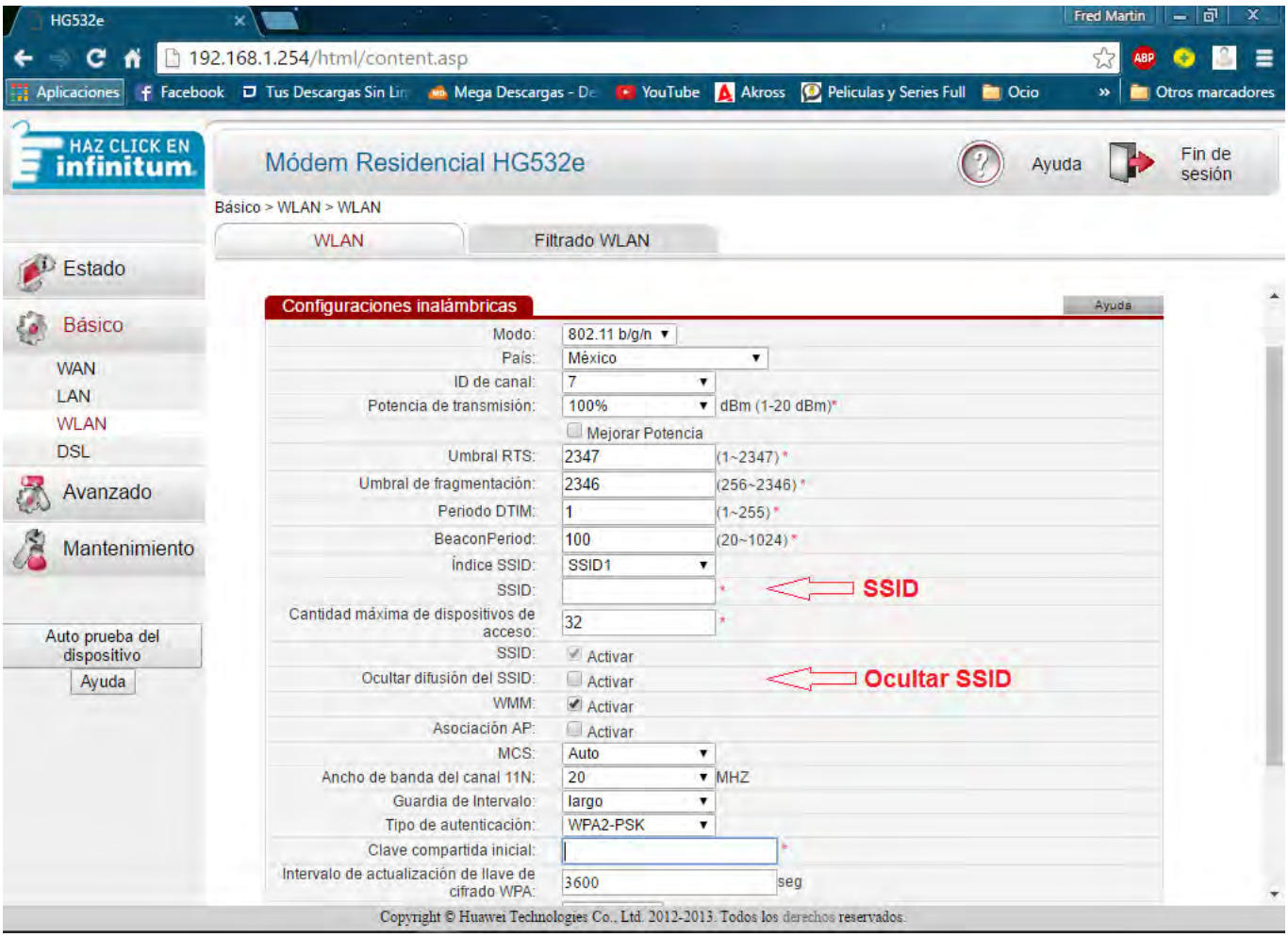


Ilustración 26 Modificar y ocultar SSID

4.7.3 Cifrado

Continuando en el mismo apartado se puede seleccionar el cifrado confiable y modificar la contraseña que trae por defecto el AP's

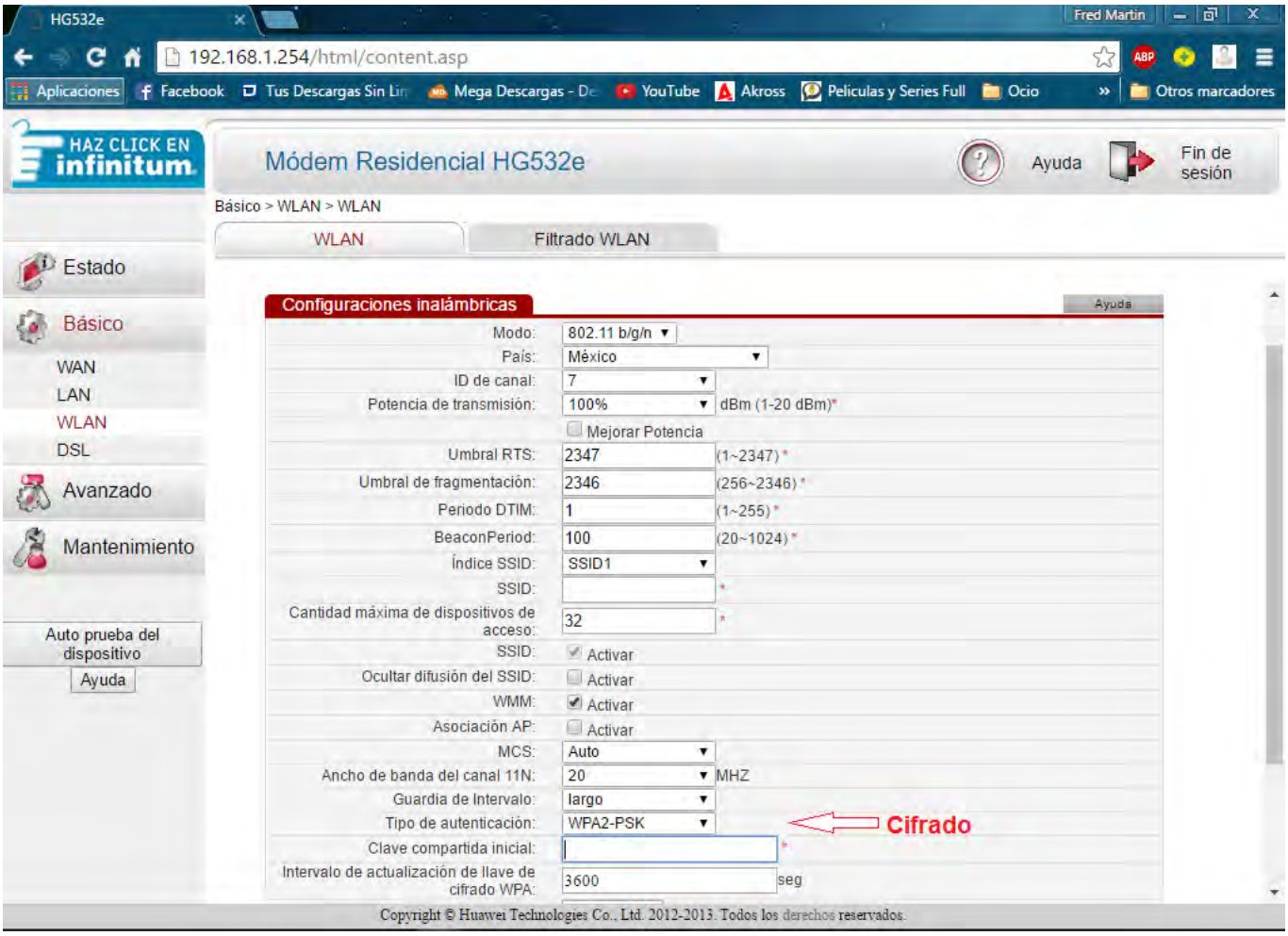


Ilustración 27 Cifrado

4.7.3 Canal

De igual forma en el mismo apartado se puede seleccionar el canal de entre los 11 disponibles a utilizar procurando no usar el mismo canal que un AP's adyacente.

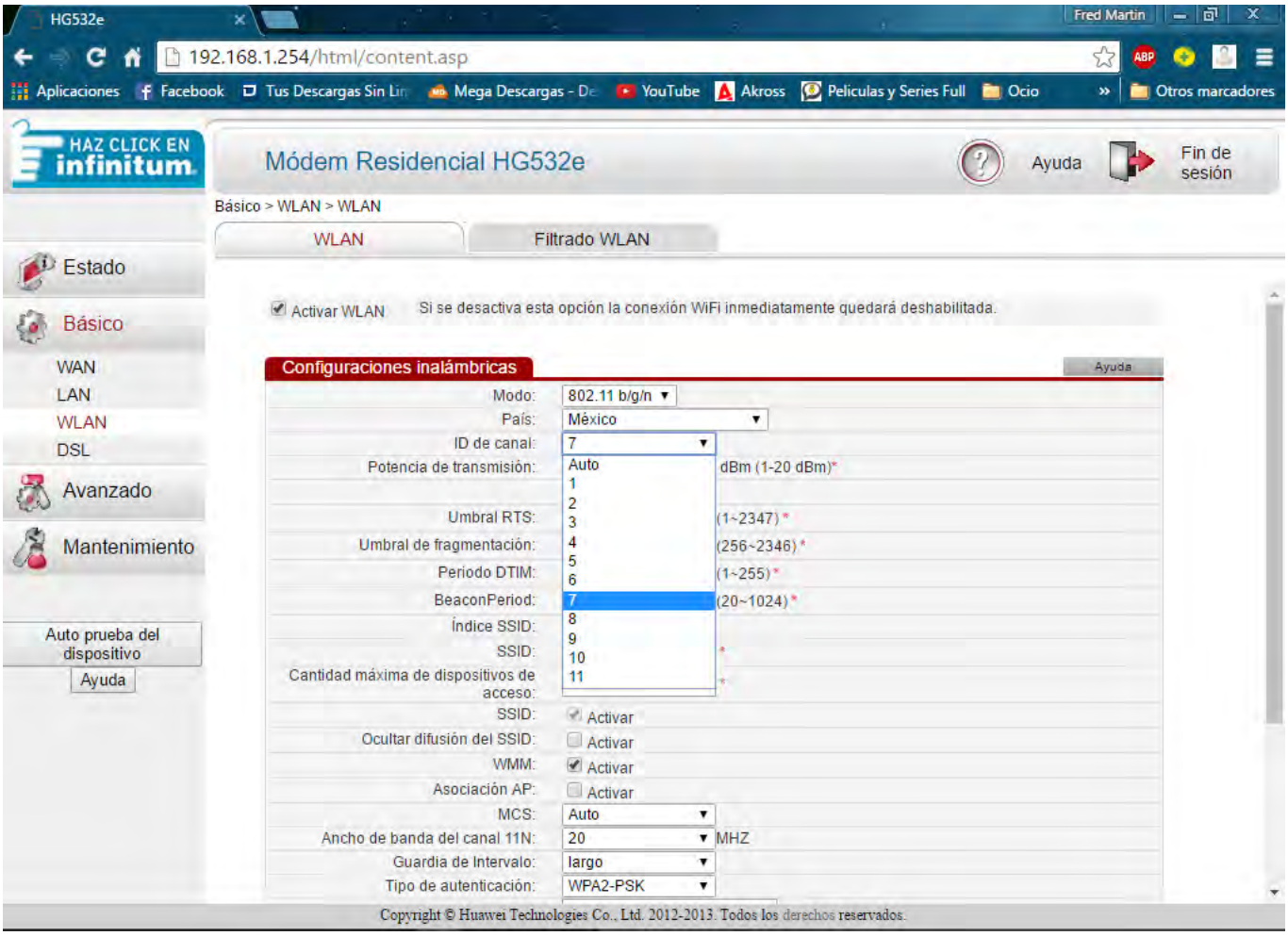


Ilustración 28 Canal

4.7.5 Filtrado MAC

En el mismo apartado del SSID se encuentra una pestaña extra la cual es filtrado WLAN en el cual se puede seleccionar entre los dos tipos de filtrado ya sea lista negra o lista blanca, es decir, permitir o denegar dispositivos al AP's

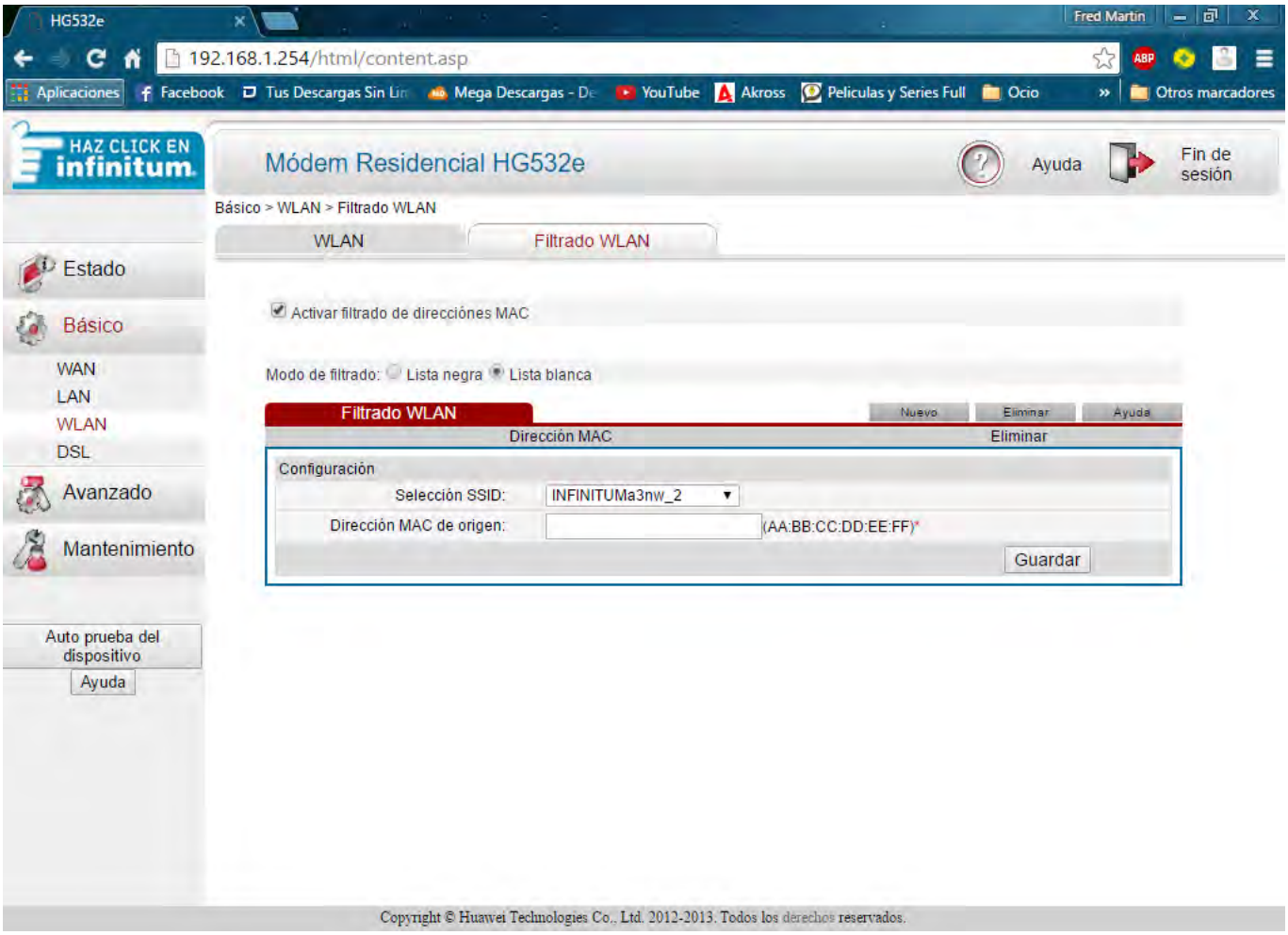


Ilustración 29 Filtrado MAC

4.8 Recomendaciones

De acuerdo a los datos obtenidos del análisis de confiabilidad de los Ap´s en la ciudad de Chetumal, Quintana Roo se proponen las siguientes recomendaciones para el estado en el que se encuentran éstos.

1. Uno de los factores más sobresalientes en el tema de confiabilidad de los Ap´s es el SSID, ya que los usuarios caseros no suelen tomar ninguna medida de seguridad al elegirlo; un porcentaje considerable le asignan nombres propios, de la familia o datos que indican de donde proviene la señal o incluso algo peor: mantienen el SSID por defecto. La manera de evitar errores de confiabilidad en los SSID es que éste no incluya datos que asocien al propietario con el AP, lo ideal sería que el SSID se componga de letras y números sin ningún significado especial. Es una tarea no muy complicada y mejora la confiabilidad del Ap´s.
2. Desactivar el broadcast del SSID, el SSID es importante y necesario que este sea conocido por los usuarios que se quieran conectar a la red, pero no se tiene ninguna ventaja que sea conocido por todos en el vecindario, si se evita que el SSID sea público los usuarios aun podrán conectarse al AP ya que sus equipos están configurados con ese SSID
3. Otro factor que pone en riesgo la confiabilidad de los Ap´s son los equipos visitantes, ya que estos pueden contener virus informáticos, spyware, keyloggers, virus troyanos o cualquier otro software malicioso. Por lo tanto, se tiene que evitar que dispositivos terceros se conecten al Ap´s mediante un filtrado MAC y si no es posible, limitar su utilización y asegurarse de que estén bajo control generando redes inalámbricas alternas para que estos dispositivos se conecten.
4. Otro punto importante para mantener una buena confiabilidad es el cifrado, aunque durante la recolección de Ap´s se confirmó que WPA2 el cifrado más confiable hasta el momento en el mercado es que el que domina, WEP siendo cifrado inseguro y obsoleto aún tiene una presencia muy significativa siendo el segundo más usado. Para mantener una buena confiabilidad hay que hacer uso del cifrado WPA2, no hacer uso de palabras del diccionario, por lo más conveniente sería que esté compuesta de letras, números, caracteres sin ningún significado especial y de ser posible incluir el espacio.

5. Lo que se observó con relación a los canales es que al ser el 1, 6, 11 los más utilizados, generan un problema muy común en las redes WiFi el cual es el solapamiento de canales.

   La mejor manera de evitar el solapamiento de canales es que una red este separado de la otra por una diferencia de 5 canales, y en dado caso de que esa separación no sea posible, una solución sería la de utilizar el canal más alejado de la señal más débil. (Salvetti, 2011)

Capítulo V Conclusiones

De acuerdo al estudio realizado mediante el *muestreo intencional o de conveniencia,* se obtuvieron datos que respaldan ampliamente la idea de que la gran mayoría de estos puntos de acceso inalámbricos usan el cifrado más seguro hasta el momento, el cual es WPA2 con un porcentaje de 72% equivalente a 1642 Ap´s de 2290 existentes, sin embargo, a pesar de este resultado, en general el estado es preocupante ya que el segundo cifrado más popular es WEP con un porcentaje de 23% equivalente a 530 Ap´s de 2290 el cual se considera un obsoleto e inseguro

Por lo que denota que a pesar de existir una gran diferencia de uso con respecto a WPA2, una gran población se encuentra en un estado vulnerable y expuesta a ser atacadas por hackers, piratas cibernéticos o cualquier otra persona malintencionada y todo esto gracias al hacer uso de un cifrado obsoleto que no brinda ningún tipo de confiabilidad como lo es WEP.

Así mismo los resultados con relación a los fabricantes de Ap´s dejan en claro que el fabricante que predomina en la ciudad de Chetumal, Quintana Roo es *Huawei Technologies y* entre los tres fabricantes más populares ocupa el 39% con un total de 488 puntos de acceso, con esto se concluye que claramente este es el AP que está más propenso a recibir ataques por personas mal intencionadas ya que debido a que este tipo de Ap´s generalmente se encuentran documentadas en internet exhibiendo todas las vulnerabilidades y métodos sobre como violar la "*Seguridad*" mediante guías y manuales, para ello hay fortalecer lo más que se pueda siguiendo las recomendaciones y hacer uso de las medidas de seguridad mencionadas con anterioridad.

Haciendo uso de las medidas de seguridad, los usuarios caseros pueden mejorar la confiabilidad considerablemente de sus redes inalámbricas, así mismo tienen la ventaja que se puede acceder a métodos de confiabilidad más avanzados, a través de las medidas de seguridad y recomendaciones mencionadas anteriormente se puede realizar la creación de nuevas redes inalámbricas o simplemente la capacidad para poder segmentar la red, con esto se puede tener una mejor administración de los dispositivos conectados al AP, decidiendo quienes pueden tener acceso a la red mediante un filtrado MAC, por otra parte con la creación de una red alterna permite separar a los dispositivos que se encuentra en el hogar de los dispositivos invitados, impidiendo riesgos innecesarios tanto para el AP como para los dispositivos hogareños, al mismo

tiempo separando estos dispositivos se evita el acceso a información privada o cualquier otro tipo de información a la que no queremos que terceras personas tengan acceso y no solo se evita el acceso sino que también no se arriesgan los datos.

Otro punto importante que se observó a la hora de realizar este proyecto fue que los usuarios se empeñan en mantener la configuración de fábrica de los Ap´s que les son entregados por su proveedor de internet, se llegó a esta conclusión a la hora de analizar los SSID ya que estos en su gran mayoría sostienen el SSID por defecto, teniendo 88% de los Ap´s *Huawei*, 51% de *Hon Hai* y 85% de los *Technicolor*; y si el identificador de la red inalámbrica es el de fábrica, hay una gran probabilidad que la contraseña para acceder a ella de igual forma sigua siendo la de fábrica.

Con respecto a los canales más utilizados en la ciudad de Chetumal, Quintana Roo, son el 1, 6 y 11, el problema reside en que, con el enorme crecimiento de los Ap´s, routers, portátiles y Smartphone el espectro de radiofrecuencia empieza a estar realmente saturado, en consecuencia, esto perjudica seriamente al rendimiento de las redes inalámbricas, puesto que con la gran demanda de las tecnologías WiFi fácilmente se puede caer en el *Solapamiento de canales,* es decir, que los canales se superponen; ya que al estar separados por 5 MHz y que cada canal necesite 22 MHz lleva a la problemática mencionada con anterioridad.

Lamentablemente, aunque se han mencionado maneras de minimizar los problemas a causa del *solapamiento de canales,* la sobrepoblación de redes inalámbricas no es lo único que ocasiona conflictos ya que las interferencias de igual forma se pueden producir por otros dispositivos que emiten radiofrecuencias al mismo tiempo: como lo son microondas dispositivos móviles o celulares, mouses inalámbricos, dispositivos bluetooth, etc. Para estos casos, siempre se puede optar por un nuevo cambio de canal, no obstante localizar la fuente de interferencia y llevar a cabo una óptima solución resulta no ser tan sencillo.

La asistencia de un técnico especializado en redes inalámbricas, aunque en principio podría considerarse como un costo extra, evitaría en gran medida los inconvenientes y problemas descritos en el presente trabajo.

Capítulo VI Referencias

Academy, C. N. (2006). *Cisco Networking Academy Program: Fundamentals of Wireless LANs Companion Guide.* Boston: Boston, MA.

Andrew A. Vladimirov, K. V. (2005). *Hacking wireless: seguridad de redes inalámbricas.* Madrid: Madrid : Anaya Multimedia.

Carballar Falcón, J. A. (2005). *Wi-Fi: Como construir una red inalámbrica* . México, D.F: Alfaomega ; Madrid : Ra-Ma, 2005.

Cisco. (2002). *Academia de networking de Cisco Systmes: guia del segundo año.* Indianapolis: Cisco Press.

Claudio Alejandro Peña Millahual. (2012). Redes Wifi en Entornos de Windows. *USERS*, 192.

INEGI. (2010). *INEGI*. Obtenido de INEGI: http://www.inegi.org.mx/sistemas/consulta_resultados/ageb_urb2010.aspx?c=28111

INEGI. (7 de 04 de 2015). *INEGI*. Obtenido de http://www.inegi.org.mx/

Lopez, J. G. (2008). *Guia de campo Wi-Fi.* México: AlfaOmega.

Reid, N. P. (2004). *Manual de redes inalámbricas* . Mexico: México: McGraw-Hill, 2004.

Salvetti, D. (2011). Redes Wireless. *Users*, 320.

SAT. (10 de 09 de 2014). Obtenido de SAT: http://www.fundacionctic.org/sat/articulo-medidas-de-seguridad-basicas-iii-seguridad-en-redes-wifi

Tarlogic. (08 de 03 de 2013). *OWISAM*. Obtenido de https://www.owisam.org

Vieites, Á. G. (2003). *Redes de ordenadores e Internet: Funcionamiento, servicios ofrecidos y alternativas de conexión.* Alfaomega.

Villarce, J. Á. (s.f.). *Tecnicas No-Probabilisticas* . Obtenido de Tecnicas No-Probabilisticas : https://tecnicas-no-probabilisticas.wikispaces.com/Jos%C3%A9+%C3%81ngel+Rojas+Villarce

WiFi, A. (14 de 12 de 2014). *Acrylic Wifi*. Obtenido de Acrylic Wifi: https://www.acrylicwifi.com/blog/que-es-wpa-psk-tkip-ccmp/