Redes inalámbricas en Puerto Vallarta y Bahía de Banderas

Héctor Gerardo Núñez
Universidad Tecnológica de Bahía de Banderas
hcgerardo@utbb.edu.mx

José César Ávila Hernández
Universidad Tecnológica de Bahía de Banderas
javila@utbb.edu.mx

Amparo Jazmín Meza Gutiérrez
Universidad Tecnológica de Bahía de Banderas
ajmeza@utbb.edu.mx

Héctor Salvador García Romo
Universidad Tecnológica de Bahía de Banderas
hgarciar@utbb.edu.mx

Resumen

En esta investigación se estudia la seguridad de las redes inalámbricas de internet en sitios públicos de Puerto Vallarta y Bahía de Banderas. Por medio de un software específico, se podrán observar las diferentes redes inalámbricas que existen en la región geográfica mencionada, su protocolo de seguridad, canal en el que trasmiten, frecuencia y dispositivo a través del cual se brinda el servicio de red. La información recabada se analizará y comparará para verificar si cumple con los criterios de integridad, confidencialidad y disponibilidad que forman parte de la seguridad de la información.

Abstract

This research studies the security of wireless internet networks in public places in Puerto Vallarta and Bahía de Banderas region. Using a specialized software, you can observe the different wireless networks in the referred geographic region, its security protocol, its transmission channel, frequency and device name through which the network service is provided. The gathered information will be analyzed and compared to see if it meets the criteria of integrity, confidentiality and availability as part of information security.

Palabras clave / Keywords: red inalámbrica, seguridad de la información, punto de acceso, internet, Bahía de Banderas. wireless network, information security, access point, internet, Bahía de Banderas.

Introducción

En este documento se presenta lo relacionado a la seguridad de redes inalámbricas de internet en el área de Bahía de Banderas, un aspecto que en la actualidad es de suma relevancia en el ámbito informático para saber si cumplen con los criterios integridad, confidencialidad y disponibilidad que forman parte de la seguridad de la información. Con la información recabada se pretende conocer cuántos usuarios de un servicio de red cambian la configuración inicial del dispositivo, analizando de esta manera la frecuencia con la cual se utilizan los hotspots y qué tan viable es su implementación en el área de Bahía de Banderas.

Objetivo

Obtener un resultado cuantitativo de la seguridad en las redes inalámbricas de internet en la región de Bahía de Banderas.

Justificación

Debido al crecimiento exponencial que han tenido las redes inalámbricas de internet es de suma importancia saber cuán vulnerables son. Por esta razón se realizó esta investigación, cuyos resultados arrojados ayudarán a concientizar a los usuarios sobre la importancia de cambiar los niveles de seguridad en los dispositivos que proveen el servicio de red e incluso a pensar en la implementación de un hotspot como medida alterna de seguridad. Cabe mencionar que la investigación se llevó a cabo en los lugares más concurridos de la región de Bahía de Banderas que son los centros comerciales y el malecón de Puerto Vallarta.

Preguntas de investigación

1. ¿Qué tan seguras son las redes inalámbricas de internet en el área de Bahía de Banderas?
2. ¿Qué tan viable es la implementación de *hotspots* en las redes inalámbricas de internet?
3. ¿En qué casos es viable la implementación de *hotspots*?
4. ¿Cuáles son los fabricantes de routers o access points más utilizados?
5. ¿Por qué la gran mayoría de las redes transmiten en la frecuencia de 2.4 GHz?
6. ¿Cuál es el criterio de elección de un canal para la transmisión de una red de internet inalámbrica?

Desarrollo

Las redes de internet inalámbricas son redes de telecomunicaciones en donde la interconexión entre nodos es implementada sin utilizar cables. Este tipo de redes son generalmente implementados con algún tipo de sistema de transmisión de información como las ondas de radio. La principal ventaja de las redes inalámbricas es que se eliminan metros y metros de cables, pero su seguridad debe ser más robusta.

La palabra Modem significa MOdulador-DEModulador y se refiere a un periférico de entrada/salida, que puede ser interno o externo a una computadora, y sirve para conectar una línea telefónica con la computadora. Se utiliza para acceder a internet u otras redes, realizar llamadas, etc. Los datos transferidos

desde una línea de teléfono llegan de forma analógica. El módem se encarga de "demodular" para convertir esos datos en digitales. Los módems también deben hacer el proceso inverso, "modular" los datos digitales hacia analógicos, para poder ser transferidos por la línea telefónica.

Uno de los problemas más graves a los cuales se enfrenta actualmente la tecnología Wi-Fi es la seguridad. Un muy elevado porcentaje de redes inalámbricas de internet son instaladas por su simplicidad de implementación sin tener en consideración la seguridad y, por tanto, convirtiendo sus redes en redes abiertas, sin proteger la información que por ellas circulan. Existen varias alternativas para garantizar la seguridad de estas redes. Las más comunes son la utilización de protocolos de seguridad de datos específicos para los protocolos Wi-Fi como el WEP, WPA, WPA2, WPA + WPS Y WPA2 +WPS que se encargan de autenticación, integridad y confidencialidad, proporcionados por los propios dispositivos inalámbricos, o IPSEC (túneles IP) y el conjunto de protocolos IEEE 802.1X, proporcionados por otros dispositivos de la red de datos y de reconocida eficacia a lo largo de años de experiencia.

Protocolos de seguridad

Protocolo WEP (Wired Equivalent Privacy).

Es un protocolo que tiene diversas funciones, entre ellas evita el acceso no autorizado a una red inalámbrica; esta función no es un objetivo explícito en la norma 802.11, pero se considera con frecuencia para ser una característica de WEP. Además WEP utiliza el algoritmo de encriptación RC4 que se conoce como un cifrado de flujo. Un cifrado de flujo opera mediante la ampliación de una clave corta en una corriente de clave seudoaleatoria infinito. El remitente XOR del flujo de clave con el texto plano para producir el texto cifrado. El receptor tiene una copia de la misma clave, y la utiliza para generar flujo de clave idéntica. XORing la corriente dominante con el texto cifrado se obtiene el texto normal.

Protocolo WPA (Wi-Fi Protected Access).

WPA, abreviatura de Wi-Fi Protected Access, es una especificación de codificación de data para un LAN inalámbrica. Mejora con la función de seguridad de WEP utilizando Extensible Authentication Protocol

(EAP) a un acceso de network seguro y un método de codificación para asegurar la transmisión de datos. WPA está diseñado para ser utilizado con servidor de autenticación 802.1X Basada en servidores de autentificación (normalmente servidores Radius (Remote Authentication Dial-In User Server)), en la que es el servidor de autenticación es el que distribuye diferentes llaves para cada usuario. No obstante también puede ser utilizado en un modo menos seguro llamado "Pre-Shared Key (PSK)" mode. PSK está diseñado para uso doméstico y networks de oficinas pequeñas en las cuales cada usuario posee la misma contraseña. WPA-PSK también es llamado WPA-Personal.

Protocolo WPA2,

En junio de 2004, la edición final del estándar 802.11i fue adoptada y recibió el nombre comercial WPA2 por parte de la alianza Wi-Fi. El estándar IEEE 802.11i introdujo varios cambios fundamentales, como la separación de la autenticación de usuario de la integridad y privacidad de los mensajes, proporcionando una arquitectura robusta y escalable, que sirve igualmente para las redes locales domésticas como para los grandes entornos de red corporativos. La nueva arquitectura para las redes wireless se llama Robust Security Network (RSN) y utiliza autenticación 802.1X, distribución de claves robustas y nuevos mecanismos de integridad y privacidad. Además de tener una arquitectura más compleja, RSN proporciona soluciones seguras y escalables para la comunicación inalámbrica. Una RSN sólo aceptará máquinas con capacidades RSN, pero IEEE 802.11i también define una red transicional de seguridad – Transitional Security Network (TSN), arquitectura en la que pueden participar sistemas RSN y WEP, permitiendo a los usuarios actualizar su equipo en el futuro.

Protocolo 802.11x

LAN inalámbrica 802.11 es un estándar IEEE que define cómo se utiliza la radiofrecuencia (RF) en las bandas sin licencia de frecuencia médica, científica e industrial (ISM) para la Capa física y la sub-capa MAC de enlaces inalámbricos. Cuando el 802.11 se emitió por primera vez, prescribía tasas de datos de 1 - 2 Mb/s en la banda de 2,4 GHz. En ese momento, las LAN conectadas por cable operaban a 10 Mb/s, de modo que la nueva tecnología inalámbrica no se adoptó con entusiasmo. A partir de entonces, los

estándares de LAN inalámbricas mejoraron continuamente con la edición de IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, y el borrador 802.11n. La elección típica sobre qué estándar WLAN utilizar se basa en las tasas de datos. Por ejemplo: 802.11a y g pueden admitir hasta 54 Mb/s, mientras que 802.11b admite hasta un máximo de 11 Mb/s, lo que implica que 802.11b es un estándar "lento" y que 802.11 a y g son los preferidos. Un cuarto borrador WLAN, 802.11n, excede las tasas de datos disponibles en la actualidad. El IEEE 802.11n fue ratificado en septiembre de 2008. La figura compara los estándares IEEE 802.11a, b y g . Las tasas de datos de los diferentes estándares de LAN inalámbrica están afectadas por algo llamado técnica de modulación. Las dos técnicas de modulación comprendidas en este curso son: Espectro de dispersión de secuencia directa (DSSS) y Multiplexación por división de frecuencias octagonales (OFDM). No necesita saber cómo trabajan estas técnicas para este curso , pero debe saber que cuando un estándar utilice OFDM, tendrá tasas de datos más veloces. Además, el DSSS es más simple que el OFDM, de modo que su implementación es más económica.

Estándar 802.11a.

Los dispositivos 802.11a que operan en la banda de 5 GHz tienen menos probabilidades de sufrir interferencia que los dispositivos que operan en la banda de 2,4 GHz porque existen menos dispositivos comerciales que utilizan la banda de 5 GHz. Además, las frecuencias más altas permiten la utilización de antenas más pequeñas. El IEEE 802.11a adoptó la técnica de modulación OFDM y utiliza la banda de 5 GHz. Existen algunas desventajas importantes al utilizar la banda de 5 GHz. La primera es que, a frecuencia de radio más alta, mayor es el índice de absorción por parte de obstáculos tales como paredes, y esto puede ocasionar un rendimiento pobre del 802.11a debido a las obstrucciones. El segundo es que esta banda de frecuencia alta tiene un rango más acotado que el 802.11b o el g. Además, algunos países, incluida Rusia, no permiten la utilización de la banda de 5 GHz, lo que puede restringir más su implementación.

Estándar 802.11b y 802.11g.

802.11b especificó las tasas de datos de 1; 2; 5,5 y 11 Mb/s en la banda de 2,4 GHz ISM que utiliza DSSS. 802.11g logra tasas de datos superiores en esa banda mediante la técnica de modulación OFDM. IEEE

802.11g también especifica la utilización de DSSS para la compatibilidad retrospectiva de los sistemas IEEE 802.11b. El DSSS admite tasas de datos de 1; 2; 5,5 y 11 Mb/s, como también las tasas de datos OFDM de 6; 9; 12; 18; 24; 48 y 54 Mb/s. Existen ventajas en la utilización de la banda de 2,4 GHz. Los dispositivos en la banda de 2,4 GHz tendrán mejor alcance que aquellos en la banda de 5 GHz. Además, las transmisiones en esta banda no se obstruyen fácilmente como en 802.11a. Hay una desventaja importante al utilizar la banda de 2,4 GHz. Muchos dispositivos de clientes también utilizan la banda de 2,4 GHz y provocan que los dispositivos 802.11b y g tiendan a tener interferencia.

Estándar 802.11n.

El borrador del estándar IEEE 802.11n fue pensado para mejorar las tasas de datos y el alcance de la WLAN sin requerir energía adicional o asignación de la banda RF. 802.11n utiliza radios y antenas múltiples en los puntos finales, y cada uno transmiten la misma frecuencia para establecer streams múltiples. La tecnología de entrada múltiple/salida múltiple (MIMO) divide un stream rápido de tasa de datos en múltiples streams de menor tasa y los transmite simultáneamente por las radios y antenas disponibles. Esto permite una tasa de datos teórica máxima de 248 Mb/s por medio de dos streams. Importante: el sector de comunicaciones de la Unión internacional de telecomunicaciones (ITU-R) asigna las bandas RF. La ITU-R designa las frecuencias de banda de 900 MHz, 2,4 GHz, y 5 GHz como sin licencia para las comunidades ISM. A pesar de que las bandas ISM no tienen licencia a nivel global, sí están sujetas a regulaciones locales. La FCC administra la utilización de estas bandas en los EE. UU., y la ETSI hace lo propio en Europa.

Metodología

Se recopiló información relacionada con los diversos protocolos de seguridad llamados: WEP, WPA, WPA2, WPA + WPS, WPA2 + WPS, TK y PSK. El protocolo de redes inalámbricas 802.11x que establece parámetros como la frecuencia de transmisión, las tasas de velocidad de transmisión de los datos y canal en el que emiten. Se definieron términos técnicos tales como: *hotspot*, red inalámbrica de internet, modem, frecuencia y canal de transmisión. Además se buscaron manuales referentes al uso del software a operar.

Formulación de hipótesis

Se formuló la siguiente hipótesis: “Las redes inalámbricas de internet en el área de Bahía de Banderas son inseguras”.

Generación de objetivos

Una vez establecida la hipótesis y teniendo como respaldo la fundamentación teórica recopilada, se buscó demostrar la veracidad de la hipótesis de una manera cuantitativa.

Experimentación (Prácticas de Campo)

Se decidió utilizar el software Backtrack5 en conjunto con InSSIDer como instrumento para poder examinar las redes inalámbricas de internet, visitando los lugares más concurridos del área de Bahía de Banderas que son el malecón de Puerto Vallarta y los centros comerciales (Plaza Marina, Paradise Village, Plaza Caracol, Macroplaza, Galerías Vallarta, Plaza Lago Real y Plaza Península), recopilando los siguientes datos: Nombre de la red (BSSID), dirección MAC, fabricante de modem, canal en el que transmite y frecuencia de transmisión. La recopilación de los datos se llevó a cabo mediante el software OpenOffice.Calc.

Análisis de Resultados

Se realizó el procesamiento de datos con la ayuda de la hoja de cálculo, obteniendo los siguientes tipos de gráficas: Porcentaje de redes inalámbricas de internet Infinitum vs redes inalámbricas de internet con nombre asignado (Figura 1), Cantidad de fabricantes de modem utilizados en las redes inalámbricas de internet (Figura 2), Porcentaje de los diferentes niveles de seguridad de las redes inalámbricas de internet (Figura 3), Porcentaje de uso de los diferentes canales de transmisión de las redes inalámbricas de internet (Figura 4) y Cantidad de redes inalámbricas de internet que utilizan la frecuencia 2.4 GHz y las que usan la de 5 GHz (Figura 5).

Figura 1. Porcentaje de redes inalámbricas de internet Infinitum vs redes inalámbricas de internet con nombre asignado.

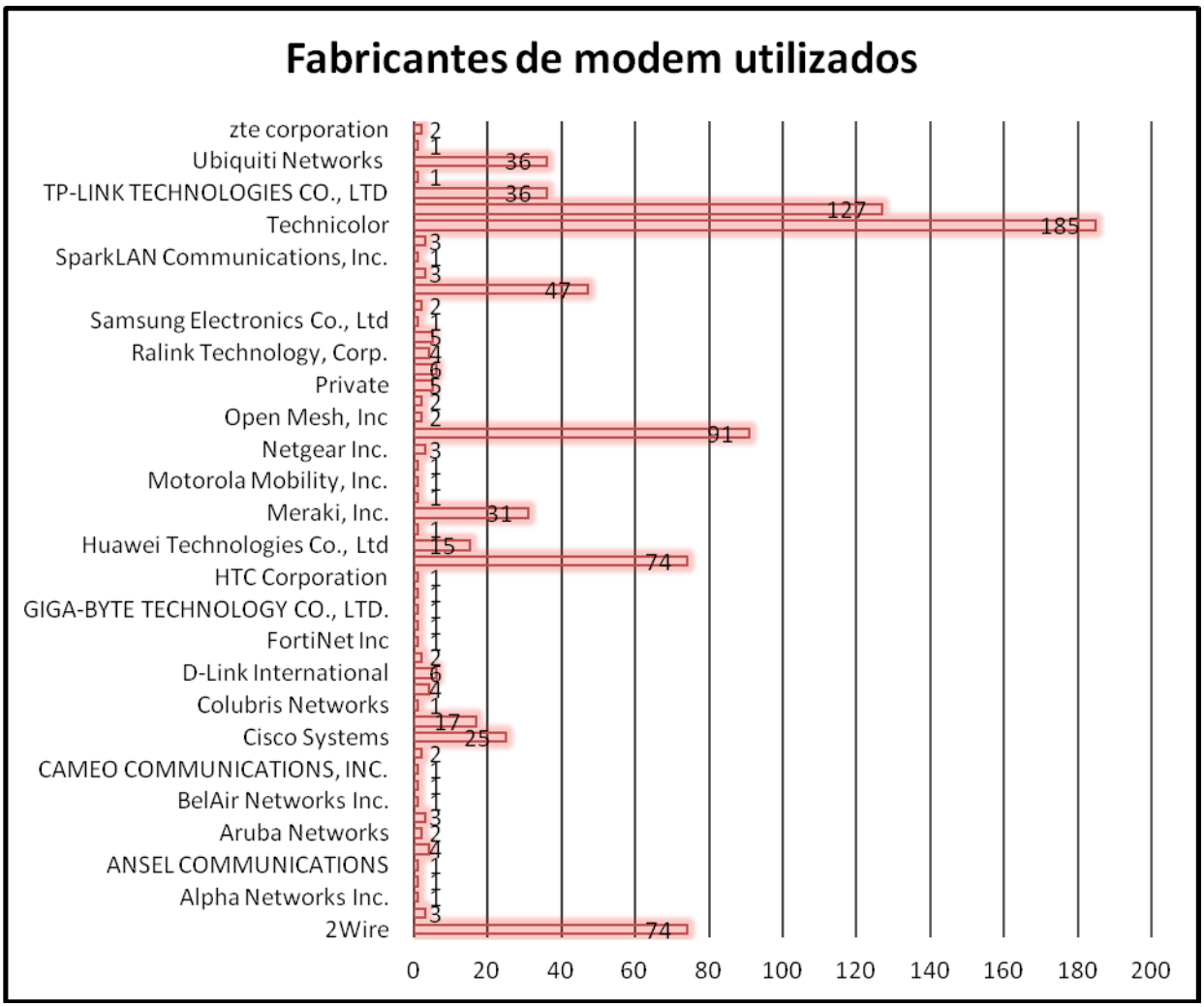

Figura 2. Cantidad de fabricantes de modem utilizados en las redes inalámbricas de internet.

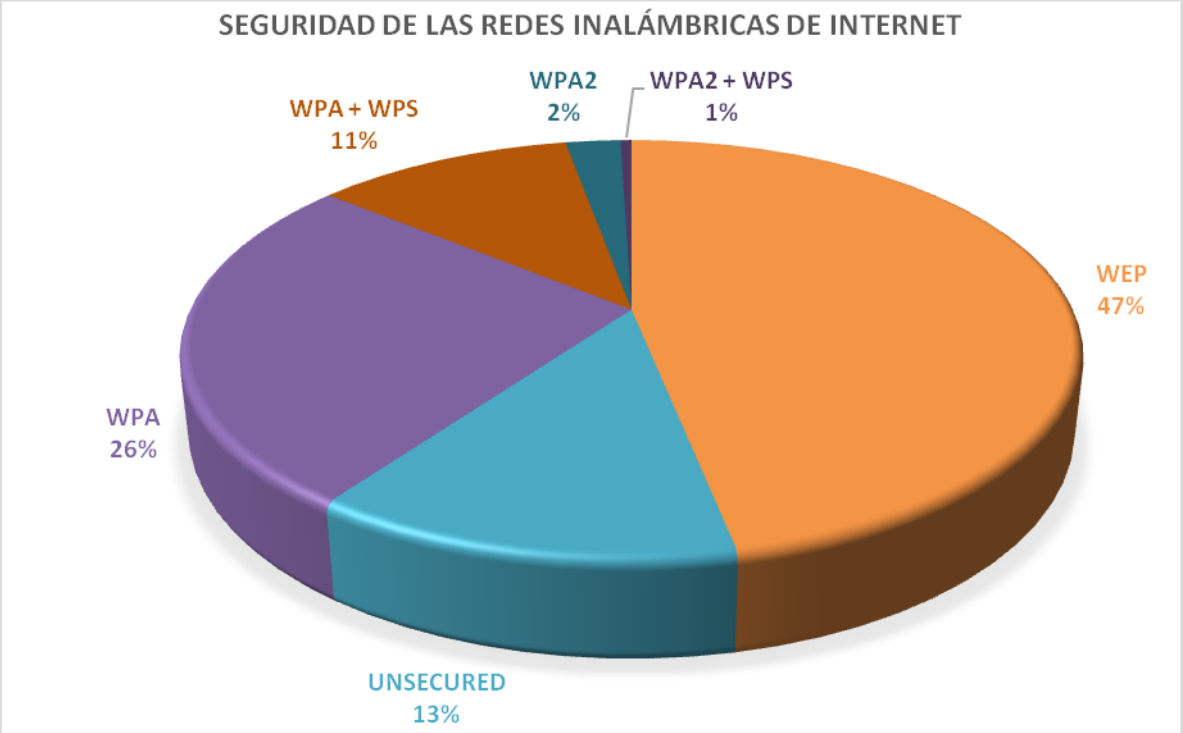

Figura 3. Porcentaje de los diferentes niveles de seguridad de las redes inalámbricas de internet.

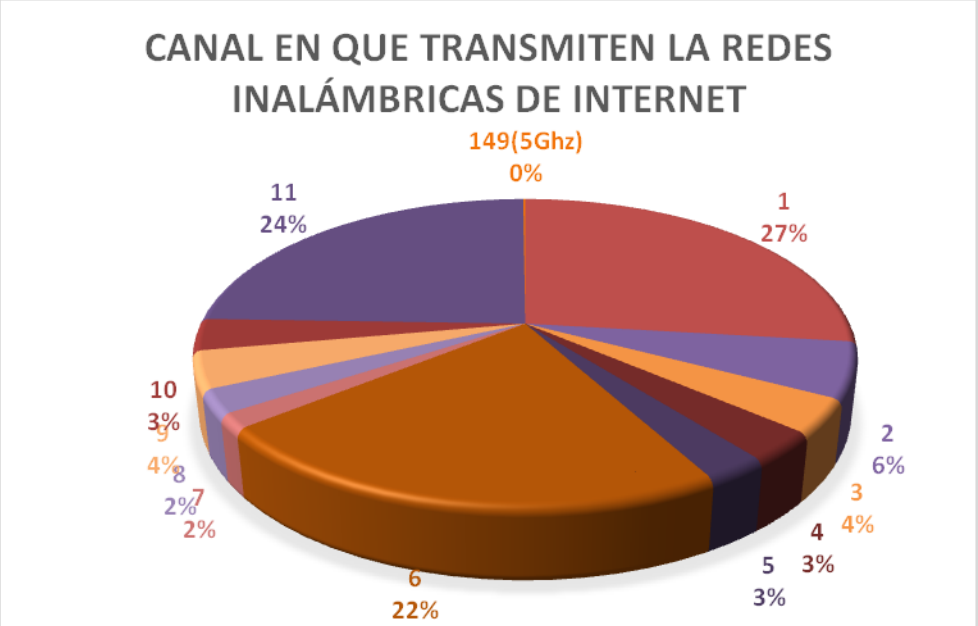

Figura 4. Porcentaje de uso de los diferentes canales de transmisión de las redes inalámbricas de internet.

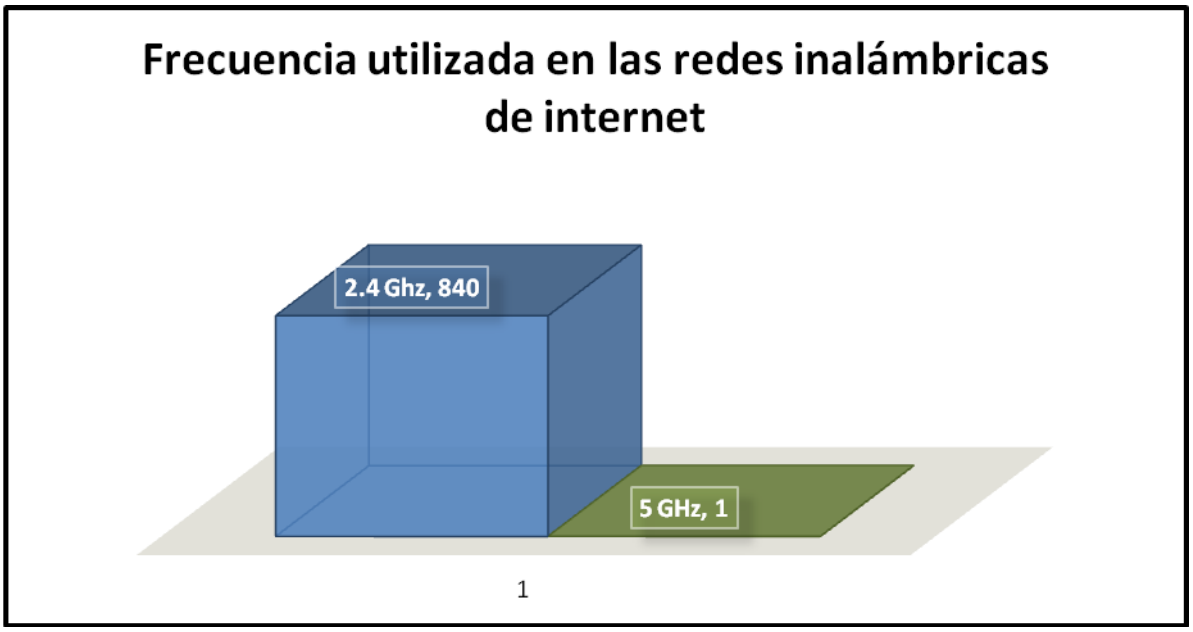

Figura 5. Cantidad de redes inalámbricas de internet que utilizan la frecuencia 2.4 GHz y las que usan la de 5 GHz.

Conclusión

Los resultados obtenidos del procesamiento de datos muestran los siguientes porcentajes, siendo el 46.85% correspondiente a redes inalámbricas de internet que cuentan con seguridad WEP el cual es el protocolo de seguridad más vulnerable por lo cual no se considera seguro.

Por otro lado tenemos que el 13.08% representan a las redes inalámbricas de internet sin seguridad aparente, pero que al conectarse a ellas cuentan con un punto de acceso (Hotspot) el cual se considera seguro, el 26.04% se refiere al porcentaje de redes que utilizan el protocolo WPA que es vulnerable pero requiere una mayor complejidad al momento de romper el algoritmo de encriptación, por tanto es considerado seguro de la misma manera que su última versión WPA2 que cuenta con el 11.18%. Las combinaciones de seguridad WPA+WPS y WPA2+WPS representan el 2.38%, 0.48% respectivamente, también consideradas seguras.

El conjunto de todas las redes consideradas seguras suman un total de 53.15%, contra un 46.85% inseguro lo cual demuestra que la hipótesis planteada al principio de la investigación es falsa, es decir las redes inalámbricas de internet en el área de bahía de banderas son seguras.

Pese a que la hipótesis fue rechazada es necesario concientizar a los usuarios debido a que el porcentaje de redes a las cuales no se les ha cambiado la seguridad sigue siendo muy alto. Para todas estas redes las cuales no se ha modificado su protocolo de seguridad, existe la alternativa de implementar un *hotspot*.

Bibliografía

- Chen, J. C., & Wang, Y. P. (2005). Extensible authentication protocol (EAP) and IEEE 802.1 x: tutorial and empirical experience. IEEE Communications Magazine, 43(12), 26-32.
- Ding, P., Holliday, J., & Celik, A. (2004, January). Improving the security of Wireless LANs by managing 802.1 X Disassociation. In Consumer Communications and Networking Conference, 2004. CCNC 2004. First IEEE (pp. 53-58). IEEE.
- Pack, S., & Choi, Y. (2003). Pre-authenticated fast handoff in a public wireless LAN based on IEEE 802.1 x Model. In Mobile and Wireless Communications (pp. 175-182). Springer US.

- Potter, B. (2006). Wireless hotspots: petri dish of wireless security. Communications of the ACM, 49(6), 50-56.
- Seguridad de la información. (2014, 24 de noviembre). Wikipedia, La enciclopedia libre. Recuperado el 6 de diciembre de 2014 desde http://es.wikipedia.org/w/index.php?title=Seguridad_de_la_informaci%C3%B3n&oldid=78341429.
- Tewson, K., Riley Steve. (2008). *Security Watch. A guide to Wireless Security*. TechNet Magazine. Recuperado el 6 de diciembre de 2014 desde http://technet.microsoft.com/es-es/magazine/2005.11.securitywatch(en-us).aspx
- Wireless security. (2014, December 6). In Wikipedia, The Free Encyclopedia. Recuperado el 6 de diciembre de 2014 desde http://en.wikipedia.org/w/index.php?title=Wireless_security&oldid=636856273