Análisis de seguridad en redes inalámbricas de las MiPyME y propuesta de mejora

Security analysis in wireless networks of MiPyMEs and proposal for improvement

César Manuel Hernández Mendoza
Instituto Tecnológico Superior de Irapuato
cesar.hernandez@itesi.edu.mx

Luz María Rodríguez Vidal
Instituto Tecnológico Superior de Irapuato
luzrodriguez@itesi.edu.mx

Maricela Aguilar Almanza
Instituto Tecnológico Superior de Irapuato
maaguilar@itesi.edu.mx

Resumen

Hoy en día, al hablar de redes inalámbricas no sólo se habla de comunicación, sino también de una gran cantidad de características técnicas y operativas que difieren según la marca y fabricante del dispositivo emisor, tales como las configuraciones básicas de seguridad, sus prestaciones, su alcance e incluso la posición y ubicación del equipo en el área asignada; son características que un usuario común usualmente pasa por alto al momento de contratar el servicio de internet, pues aunque el proveedor puede proponer un lugar apropiado para la conexión y el equipo de red, el usuario prefiere dar prioridad a los aspectos de estética y espacio, aunque sacrifique un poco el rendimiento y el nivel de seguridad de la red. Se puede ser más certero aplicando un análisis de seguridad en el caso de las micro y pequeñas empresas comunes que podemos encontrar, por ejemplo, en los centros comerciales, donde la concentración de negocios es muy alta y cada una de ellas cuenta con una red inalámbrica, requerida para el proceso de ventas (e-commerce) o para brindar el servicio al cliente. Sin embargo, pueden presentarse problemas que aumentan en proporción al número de usuarios conectados al módem, propiciando varios factores, como la reducción de ancho de banda, las interferencias con otras redes vecinas, la atenuación de obstáculos

físicos y el problema general a resolver en este trabajo: “el nivel de vulnerabilidad que poseen”, el cual converge en accesos no autorizados a la red que ponen en riesgo información vital del negocio así como sus dispositivos. La investigación determina cuáles son las posibles mejoras que un usuario puede dar a sus equipos de red, con la finalidad de aumentar la seguridad y evitar este tipo de accesos no autorizados con sus consecuencias.

Palabras clave: seguridad informática, vulnerabilidad de red, nivel de confianza, red inalámbrica, tipos de cifrado.

Abstract

Nowadays, talking about wireless networks, It is not just talking about communication, It is making a mentioning about a lot of technical and operational characteristics, wich are different according to the brand and the transmitter device manufacturer, such as: basic security settings, Its features and its scope even the location of the equipment in a specific area; all of these are characteristics that a common user usually does not considered at the time of hiring the internet service, because although the service provider could propose a suitable place for the connection and network equipment, user prefers to prioritize aspects of aesthetics and space, although it sacrifices performance and the network security; You can be more accurate by applying a security analysis when we are talking about micro and small enterprises; for example, in shopping malls, where every store has a wireless network, which is necessary for the sales process (e-commerce) or to provide customer service, however, there could be problems that increase the amount of connected users to the modem, contributing to the reduction of bandwidth avoiding interference with other neighboring networks, attenuation with physical obstacles and the main problem which is describing in this paper: "security vulnerabilities of wireless networks", which put at risks the business information as well as its devices. This is how it begins with a research that determines what are possible improvements that a user can give to their network equipment, in order to increase security and avoid unauthorized access.

Key words: computer security, network vulnerability, trust level, wireless network, encryption types.

Fecha Recepción: Junio 2016 **Fecha Aceptación:** Diciembre 2016

Introducción

El rendimiento de una red inalámbrica con conexión a internet se determina por diversos factores, entre los más comunes podemos mencionar el servicio de ancho de banda que el usuario contrata con el proveedor, el cual a su vez determina la velocidad promedio o máxima con la que se podrá contar. En teoría, la velocidad óptima se alcanza si se cumplen ciertas condiciones en la infraestructura y conexión física, como equipos y dispositivos (emisores y receptores) acordes a las prestaciones del servicio; una transmisión cableada es casi inmune o vulnerable en menor medida a las interferencias y obstáculos que pueden presentarse en el proceso de comunicación, mientras que una buena transmisión inalámbrica depende de factores ajenos a su propio equipo, como la cantidad de usuarios conectados, la ubicación en el área destinada, los obstáculos físicos, e inclusive la propia presencia del usuario. Aunado a ello, el principal problema es el tipo de transmisión que se utiliza, en este caso la técnica Half-Duplex, por la cual se envía y recibe información, pero no simultáneamente como en el caso de la Full-Dúplex, implementada en medios cableados. Estas razones propician que el ancho de banda en una red WiFi disminuya hasta en 60 %, según estudios realizados a nivel mundial por el portal "*testdevelocidad.com"*.

Las micro y pequeñas empresas pueden evitar este problema de manera relativamente sencilla, basta con invertir un poco y conectar sus equipos con medios cableados; otro factor que impide un buen rendimiento en la red es el tipo de cifrado que se utiliza para conectar a los usuarios, pues actualmente existen diversos protocolos de seguridad para redes inalámbricas como el WEP, WPA y WPA2, de los cuales cabe señalar que el usuario promedio tiene poco conocimiento; puede desconocer cuáles son las ventajas que tal vez le reporte el contar con un cifrado más seguro, ya que en la práctica solo le preocupa contar con una clave de acceso (comúnmente por default), sin conocer cuál es el tipo de cifrado con el que cuenta el módem, acces-point o router. A partir de este punto comienza la participación maliciosa de usuarios externos que utilizan equipos móviles o dispositivos que requieren acceso a internet; es muy común que este tipo de usuarios se "cuelguen" del servicio con aplicaciones que obtienen las claves fácilmente y en cuestión de minutos, sobre

todo si el equipo proveedor no cuenta con las suficientes características de seguridad o blindaje requerido para evitar este problema, y aumenta si los equipos en red de la compañía comparten información entre los equipos conectados. Por tanto, podemos determinar: que la seguridad puede ser violada fácilmente, que la información puede llegar a ser vulnerable, el ancho de banda disminuir al dividirse entre el número de equipos conectados, que problemas físicos como la atenuación de señal o las interferencias se presentan, y que el servicio de internet puede ser ineficaz en días y horas pico para este tipo de negocios, por lo que evitar accesos no autorizados debe ser una prioridad para los administradores en caso de requerir señal inalámbrica para los servicios de la empresa. A partir de esta problemática se decidió realizar un estudio previo que determinara, a partir de una muestra, el nivel de vulnerabilidad de este tipo de negocios, las características con las que cuentan, las prestaciones del equipo de red; un estudio que permitiera demostrar cuáles son las mejoras técnicas y operativas que su pueden aplicar para reducir y evitar accesos no autorizados, propiciando un mayor rendimiento y seguridad de la red.

Metodología

Para comenzar debemos iniciar conociendo algunos aspectos básicos sobre las redes WiFi y su forma de operar. Toda red inalámbrica es, a fin de cuentas, un campo de energía que se transmite por ondas electromagnéticas (ondas portadoras de información) no visibles para el ojo humano, pero sí detectables para los dispositivos y sensores electrónicos, y donde cada onda posee una altura diferente a las demás (crestas), cierta distancia entre ellas y, por supuesto, una velocidad periódica, conocidas como periodo, amplitud y frecuencia, características técnicas que difieren en cada uno de los módems proveedores del servicio y lo que hace posible obtener una frecuencia diferente para cada una de las señales de cada negocio. Se ha comprobado que las ondas WiFi pueden llegar a medir de 7 a 12 cm desde su punto más alto al más bajo y dependiendo del tipo de modulación las crestas de las ondas se traducen en 1 y las depresiones en 0, lo que hace posible a partir de una conversión digital-analógica (muestreo Nyquist) comunicar equipos y dispositivos en leguaje binario, y traducir posteriormente a letras, números y lenguajes que forman contenidos multimedia como páginas web. En la figura 1 podemos observar cómo se verían los campos de energía electromagnéticos desde una altura considerable si fueran visibles en uno de los lugares más representativos de la ciudad de Washington, mientras que en la figura 2 se observan desde el nivel del piso.

Figura 1 *Campos de energía*
Nickolai L, 2013, "what-if-you-could-see-wifi", Recuperado de:
http://motherboard.vice.com/blog/this-is-what-wi-fi-would-look-like-if-we-could-see-it

En la figura 1 se observan ocho puntos de origen con esta señal, algunas características difieren como la distancia de cobertura, la atenuación o el nivel de intensidad en cada una. Existen algunos espacios en los que las señales inalámbricas se unen, provocando pérdida de señal o interferencias que impiden la correcta comunicación entre dispositivos, mientras que en la figura 2 se observa el campo electromagnético a nivel de piso, pudiendo detectar la altura de la señal y determinar que los campos electromagnéticos son esféricos, omnidireccionales. Según pruebas obtenidas por el doctor M Browning Vodel, se extienden entre 20 y 30 metros si son dispositivos comerciales y de bajo precio, mientras que algunos dispositivos emisores con mayores prestaciones llegan a alcanzar más de 90 metros de radio.

Figura 2 *Campos electromagnéticos esféricos.*
Nickolai L, 2013, "what-if-you-could-see-wifi", Recuperado de:
http://motherboard.vice.com/blog/this-is-what-wi-fi-would-look-like-if-we-could-see-it

Una vez conocidos algunos aspectos técnicos de las redes inalámbricas, continuamos con el análisis en el área de estudio donde se logró medir el nivel de vulnerabilidad, el cual es un centro comercial que alberga más de 120 negocios, de los cuales 105 cuentan con redes inalámbricas. Tras hacer una muestra estadística por medio de la técnica de chi cuadrada, obtenemos un total de 21 negocios que estarán dentro del margen de la muestra, de los cuales se determinó su nivel de seguridad, para lo cual se requirieron algunas aplicaciones como "WPS-PIN", con una base que genera PIN'S de seguridad, que tienen por defecto algunas marcas y modelos de Routers, además de la aplicación "JumpStart", un software portable y gratuito enfocado a la gestión de redes Wireless en Windows que incorpora varios métodos para mostrar y comprobar algunos fallos de seguridad, entre ellos la obtención de la clave WPA o WPA2. Sin embargo, existe una gran variedad de software y aplicaciones tanto para dispositivos móviles como de escritorio, destinadas al "hackeo" de estas claves. En la tabla 1 se muestran los más usuales y conocidos, así como sistemas operativos portables, con los que algunos usuarios, aun sin conocimientos sobre el área y paralelamente a los múltiples video-tutoriales existentes en internet, pueden infringir la seguridad de estas redes y con ello acceder a internet de forma gratuita e ilimitada. Basta con que el usuario escriba en la tienda de Windows o Play Store la palabra "WiFi" y estas aplicaciones aparecen inmediatamente, se descargan, instalan, se siguen las instrucciones y en menos de cinco minutos la clave se obtiene sin que el administrador de la red note algún cambio o por lo menos hasta que ocurren ciertos factores desfavorables, los cuales se mencionan más adelante.

Tabla 1 Aplicaciones de escritorio para vulnerar redes inalámbricas**.**

Sistemas y aplicaciones de escritorio		
Nombre	**Descripción**	**Sistema**
Netstumbler	No sólo obtiene clave de acceso, sino que muestra una buena cantidad de información al respecto.	Windows
Acrylic	Programa desarrollado por la empresa Tarlogic que permite monitorizar redes inalámbricas y comprobar su seguridad, obteniendo las contraseñas de forma automática.	Windows
Wifislax	Distribución que sirve para la auditoría de seguridad de redes inalámbricas. Con ella se puede comprobar la seguridad de nuestro Router y descifrar sus claves WiFi.	Linux
Backtrack	Distribución en formato Live CD pensada y diseñada para la auditoría de seguridad y relacionada con la seguridad informática en general.	GNU/Linux
JumpStart	Incorpora varios métodos para mostrar y comprobar algunos fallos de seguridad descubiertos tanto en el protocolo Wps, como en la obtención de la clave.	Windows
WiFi Auditor	Es una herramienta con la que se podrá comprobar la seguridad de las redes WiFi cercanas, lo que a efectos prácticos supondrá ver las contraseñas.	WiFi Auditor
WiFiWay	Wifiway es una distribución pensada y diseñada para la auditoría de seguridad de las redes WiFi, Bluetooth y RFID.	GNU/Linux
Pentoo	Pentoo es una distribución en Live-CD basada en Gentoo diseñada para pruebas de penetración y seguridad.	Linux
John the Ripper	Herramienta para cracking de contraseñas. Es una de las más conocidas y populares.	Linux/ Windows
Kali Linux	Distribución basada en Debian diseñada principalmente para la auditoría y seguridad informática en general.	GNU/Linux
Beini	Distribución enfocada a analizar la seguridad de las redes inalámbricas de tipo WEP/WPA/WPA2, basada en el tynicore.	Linux

En la tabla 2 se muestran las aplicaciones más conocidas para dispositivos móviles con el sistema operativo de Android y IOS.

Tabla 2. Aplicaciones de hackeo para dispositivos móviles.

Aplicaciones móviles		
Nombre	**Descripción**	**Sistema**
Router Keygen	Escanea automáticamente las redes WiFi para encontrar aquellas disponibles y tratar de calcular la contraseña.	Android
Angry IP Scanner	Escáner de red de código abierto y multiplataforma diseñado para ser rápido y fácil de usar.	IOS
WiFi Unlocker	Si la app marca la red WiFi como vulnerable, será capaz de obtenerla en alrededor de 2 minutos.	Android
WiFi Free	Programa para develar el cifrado público.	IOS

Como se observa, el acceso a la red puede ser desde ataques de denegación de servicios, captura de paquetes, infiltración en el módem, inclusive algunas técnicas para codificar y decodificar las contraseñas. Dado que la popularidad que están teniendo los dispositivos móviles sigue creciendo, el uso y manejo de estas herramientas es más común, desarrollando nuevas aplicaciones capaces de vulnerar estos sistemas inalámbricos aun cuando el usuario desconozca a ciencia cierta qué fue lo que realizó para tener acceso.

En cuanto a seguridad, existen diversos tipos de cifrados que pueden operar los dispositivos emisores de señales (módem, acces-point, router), cada uno con un nivel de seguridad y de variables características (tabla 3).

Tabla 3. Tipos de cifrado en redes inalámbricas

Cifrado	Características	Descripción	Seguridad
WEP Wired Equivalent Privacy	✓ Diseñado para garantizar comunicaciones seguras. ✓ Introducido en la primera versión del standard (802.11), pero mantenido sin cambios en las nuevas (802.11a, 802.11b). ✓ Compatibilidad entre distintos fabricantes. ✓ Los cifrados de 64 y 128 bits son dos niveles de seguridad WEP.	✓ WEP utiliza RC4 como algoritmo de cifrado. ✓ En WEP se usan claves de 64 o 128 bits (40+24 o 104+24). ✓ Cada paquete cifrado contiene un IV sin cifrar y el bloque de datos cifrado, el cual a su vez contiene un CRC32 (cifrado) para comprobar integridad.	Muy Bajo
WPA WiFi Protect Access	✓ Utiliza TKIP (Temporal Key Integrity Protocol). ✓ Utiliza claves dinámicas. ✓ Utiliza el algoritmo RC4 para generar un flujo de bits que se utilizan para cifrar con XOR.	Consiste en un mecanismo de control de acceso a una red inalámbrica, pensado con la idea de eliminar las debilidades de WEP.	Muy Bajo
WPA2	✓ Utiliza CCMP. ✓ Soportan el protocolo 802.1 ✓ Algoritmo utilizado para controlar la integridad del mensaje. ✓ Implementa una versión mejorada de MIC.	Sistema para proteger las redes inalámbricas (WiFi); creado para corregir las vulnerabilidades detectadas en WPA.	Bajo
WPA-PSK	✓ Sistema, actualmente, más adecuado para redes de pequeñas oficinas o domésticas. ✓ Su configuración es muy simple. ✓ Su seguridad es aceptable. ✓ Encriptación dinámica.	Usa una clave de acceso de una longitud entre 8 y 63 caracteres.	Intermedio
WPA2-PSK	✓ Autenticación mediante clave compartida (PSK). ✓ Utiliza CCMP basado en AES. ✓ La PSK proporciona una alternativa a la generación de 802.1X PMK (Pairwise Master Key) usando un	Protocolo de encriptación más robusto que WEP.	Alta

	servidor de autenticación.		
WPAWPA2-PSK	✓ Permite tanto WPA y WPA2. ✓ Gestión de claves: TKIP y CCMP/AES. ✓ Compatible de forma nativa tanto PSK y empresariales basadas mecanismos de Autenticación para Autenticación de gestión de claves de terceros ✓ Provee un mínimo de 256 bit de longitud de clave pre – compartida. ✓ Ofrece la posibilidad de un punto de acceso para ser autenticada por un cliente mediante el uso de certificados y RSN (Robust Security Network)	Máxima compatibilidad con todos los dispositivos antiguos que pueda tener, sino que también garantiza un atacante puede romper su red por descifrar el esquema de cifrado de mínimo común denominador.	Muy Alta

Si bien ya mencionamos el funcionamiento de una red inalámbrica, el área de estudio, las dificultades técnicas de una red WiFi, las aplicaciones maliciosas y la gran cantidad de información con la que cuenta un usuario para comprometer la seguridad de la red obteniendo acceso a internet, podemos hacer referencia finalmente a los principales problemas generados y encontrados a partir de accesos no autorizados:

- Interferencias: es tal vez uno de los problemas que difícilmente pueda solucionar un administrador de red, ya que por lo general está condicionado a depender de factores ajenos, pues cualquier obstáculo físico impide el paso de la señal, así como redes inalámbricas cercanas, señal satelital de teléfono celular (Smartphone), y señales de bluetooth, lo cual provoca una notable disminución en el alcance inalámbrico, una tasa de transferencia baja, pérdida completa o intermitente de la conexión y tal vez la más molesta de los usuarios: dificultades para conectar dispositivos durante la fase de detección de red, fenómeno que se presentó en cada uno de los negocios de la muestra analizada.
- Disminución de ancho de banda: posiblemente más de una vez hemos escuchado frases similares a: "se requiere aumentar el ancho de banda", o "el ancho de banda no es suficiente". En este punto cuando el ancho de banda se aumenta, el número de ondas

electromagnéticas debe aumentar en determinado intervalo de tiempo, es decir, el número de ondas portadoras enviadas en un intervalo determinado debe ser mayor en el mismo intervalo para poder confirmar que este aumentó. El problema surge cuando se presentan accesos no autorizados a la red, ya que muy pocos módems son los que están configurados para dividir el ancho de banda equitativamente, pues, generalmente, el router-módem, reparte el ancho de banda en el número de dispositivos conectados a él, por lo que al ancho de banda disminuye considerablemente, de manera que un solo equipo puede absorber la mayor parte del servicio de internet, dejando en espera al resto de la red. Durante la etapa de pruebas se pudo confirmar esta situación.

- Seguridad comprometida: si el rendimiento de la red ha bajado con los factores mencionados anteriormente, este punto es de vital importancia para los propietarios de los negocios, pues en ella recae la integridad de sus datos e información. Posiblemente datos de ventas y proveedores mantengan cierta seguridad con programas y claves de acceso, pero no por ello dejan de estar en riesgo; es muy común encontrar equipos de cómputo que comparten dispositivos e impresoras, carpetas y documentos escaneados, archivos que pueden ser copiados o eliminados por terceros con el simple hecho de estar compartiendo la red. Si bien este no es el objetivo principal de los usuarios que acceden sin permiso, se corre el riesgo de perder tan vital información.

Andrés Velázquez, presidente y fundador de MaTTica, primer laboratorio de Cómputo Forense en América Latina, comentó: "Asegurar nuestra red WiFi es mucho más importante de lo que la gente piensa. El riesgo no es solamente que algún vecino se cuelgue de nuestra red y esta se vuelva mucho más lenta, sino que un delincuente pueda meterse a nuestra red y –además de amenazar nuestra información y dispositivos conectados a ella– desde allí cometer toda clase de delitos. Cuando los investigadores rastreen a ese maleante, a donde llegarán será a la puerta de nuestra casa, y tendremos que enfrentar muchos problemas simplemente por no haber cerrado nuestra red".

Resultados

La etapa de resultados comienza con las respuestas obtenidas de una entrevista realizada a los encargados de las tiendas departamentales (muestra), a fin de conocer algunos aspectos generales, como el giro de la empresa, el interés por la seguridad en su red inalámbrica y una posible inversión para mejorar su red. La tabla 4 muestra algunas de estas respuestas.

Tabla 4. Número de respuestas obtenidas por los encargados de los negocios.

PREGUNTAS	RESPUESTAS	
1. **¿Conoce cuáles son las características generales de su dispositivo de red-módem como marca o modelo?**	3 Sí	18 No
2. **¿Conoce cuál es la inversión de contar con este equipo y servicio de red?**	2 Sí	19 No
3. **¿Ha tenido algún problema referente con la seguridad y vulnerabilidad de la información que maneja?**	7 Sí	14 No
4. **¿Considera que en horas o días de mayor aglutinamiento, el rendimiento de su red disminuye?**	16 Sí	5 No
5. **¿Conoce cuáles son los efectos y consecuencias de las intrusiones?**	2 Sí	19 No
6. **¿Ha sido notificado de accesos no autorizados en su red?**	5 Sí	16 No
7. **¿Estaría dispuesto a realizar una mayor inversión con el fin de mejorar su seguridad?**	21 Sí	--

Como se puede observar, la mayoría de los encargados desconoce aspectos técnicos de sus dispositivos. Esto se puede entender debido a factores o circunstancias que tienen mayor prioridad en su oficio, sin embargo, el que desconozcan implica que son blanco fácil para usuarios externos o maliciosos. En la entrevista también se comprobó que son pocos los establecimientos que saben que hay accesos no autorizados a su red, cuando en la prueba de acceso se comprobó que no es así, ya que la mayoría de ellos se pudo vulnerar (tabla 6) con equipos conectados e independientes al negocio.

En relación a los resultados técnicos de los tipos de cifrado, se obtuvo la siguiente tabla comparativa (tabla 5):

Tabla 5. Resultados y características obtenidas de los tipos de cifrados

		WEP	WPA	WPA2	WPA2-PSK	WPAWPA2 -PSK
Autenticación	Autenticación	WEP	802 1X + EAP	802 1 + EAP PSK	PSK	PSK2
	Pre-autenticación	No	No	Opcional	Opcional	Sí
Cifrado	Negociación de Cifrado	No	Sí	Sí	Sí	Sí
	Cifrado	RC4 40 bit o 104 bit	TKIP	AES	AES	AES y TKIP
	Vector de inicialización	24 bits	48 bits	128 bits	128 bits	256 bits
	Integridad de la cabecera	No	MIC	CCMP	CCMP	CCMP
	Integridad de los Datos	CRC-32	MIC	CCMP	CCMP	CCMP
	Protección de Respuesta	No	Basada en EAP	EAP/PSK	EAP/PSK	PSK2
	Gestión de Claves	Manual	Dinámica	Dinámica	Dinámica	Dinámica
	Distribución de Claves	Red	Paquete sesión y usuario	Paquete sesión y usuario	Paquete sesión y usuario	Paquete sesión y usuario
	Clave asignada a:	No	No	Sí	Sí	Sí
Otros	Seguridad ad-hoc IBSS	WEP	802 1X + EAP	802 1 + EAP PSK	PSK	PSK PSK2

Según el estudio realizado, el tipo de cifrado más seguro es el WPA/WPA2-PSK, pues actualmente es el que representa un mayor número de ataques sin éxito, además de que no todos los dispositivos son compatibles debido a la modulación con la que cuentan, factor por el cual los usuarios muestran interés por otras redes. La tabla 5 muestra en color rojo los cifrados con mayor grado de vulnerabilidad y en verde los más eficaces, con mayores características de seguridad.

Tabla 6. Resultados obtenidos en la prueba de acceso y vulnerabilidad.

Total de muestra	Acceso a red e internet	Acceso denegado	Acceso libre	Método utilizado	Negocios con WEP	Negocios con WPA	Negocios con WPA2	Accesos No autorizados
21	16 **Acceso a recursos** 10 de 16	4	1	JumpStart WPS-PIN	7	9	4	En 15 de 16 negocios

Finalmente, se realizó la prueba de "acceso y vulnerabilidad" con la muestra seleccionada y se determinó que, del total de la muestra, 76 % fue fácilmente vulnerado. Asimismo se obtuvo acceso al servicio de internet, y de estos, 10 negocios ponen en riesgo carpetas y documentos que están compartidos en red, por lo que comprometen información relacionada con ventas y registro de clientes, también se comprobó el registro de direcciones MAC ajenas a los equipos del negocio en 15 de 16 negocios a los que se obtuvo acceso (tabla 6).

Después de haber proporcionado la información acerca de los riesgos y consecuencias de los accesos no autorizados a los encargados y haber modificado las características de los dispositivos con los negocios que aceptaron la propuesta de mejora, se realizaron nuevamente las pruebas de acceso, obteniendo resultados satisfactorios, dado que el total de la muestra obtuvo una mejora en el ancho de banda y los accesos no autorizados fueron eliminados en 81 % (tabla 7).

Tabla 7. Resultados obtenidos en la prueba de acceso y vulnerabilidad posteriores a la propuesta de mejora

Total de muestra	Acceso a red e internet	Acceso denegado	Acceso libre	Método utilizado	Negocios con WEP	Negocios con WPA	Negocios con WPA2	Accesos No autorizados
21	3 **Acceso a recursos** --	17	1	JumpStart WPS-PIN	-	-	20	En 3 de 3 negocios

Las propuestas de mejoras son las siguientes:

Aplicar mayor seguridad a la red inalámbrica

- Cambiar la contraseña que viene por defecto en el módem, preferentemente utilizar más de 8 caracteres con mayúsculas, minúsculas y números. Puede ser un poco fastidioso, pero este tipo de claves son las de mayor grado de seguridad.
- Cambiar el tipo de cifrado, utilizar mínimo el WPA2 y preferentemente el WPA/WPA2.
- Instalar en el equipo alguna aplicación básica de monitoreo de red, que pueda demostrar en tiempo real cuáles son los dispositivos conectados a la red (abrir la consola cmd del equipo con el comando arp -a).

- No compartir la contraseña y buscar cambiarla con los mismos parámetros cada determinado tiempo.
- Utilizar el filtrado MAC, esta es probablemente la mejor medida para evitar los accesos no autorizados, puede ser vulnerada pero requiere de más tiempo y herramientas para hacerlo, por lo que los usuarios abandonarán esta red en busca de alguna con menor seguridad. El objetivo del filtrado MAC es restringir el acceso a la red a ciertos dispositivos o, viéndolo de otra manera, permitir el acceso solo a los dispositivos que le indiquemos con la dirección MAC con la que cuentan todos los dispositivos con una tarjeta de red inalámbrica. Para hacerlo, se requiere acceder a la configuración del módem y habilitar esta opción, posteriormente se escribe la lista de las direcciones MAC que se va a permitir o denegar según sea el caso.
- Modificar el tráfico de ancho de banda a los dispositivos que lo requieren con mayor prioridad, esta opción no está activa en el módem, pero puede habilitarse para indicar a cuáles equipos se les dará mayor prioridad en el tráfico de red o bien limitar el ancho de banda para algunos otros dispositivos.
- No publicar la identificación del SSID, todas las redes se identifican por un nombre que les asigna el administrador de red, conocido como SSID. El dispositivo de red puede anunciar este nombre y cuando lo hace, cualquier usuario en su área de cobertura que explore las redes disponibles intentará acceder a ella, si no se anuncia el SSID no aparecerá en la lista de redes disponibles y, por lo tanto, no invitará a su conexión.
- Activar firewall de módem; tener el firewall activado previene los ataques a la red para que los intrusos no puedan acceder, es indispensable que los administradores de red tomen en cuenta la importancia de implementar herramientas que ayuden a mantener una red segura.

Optimizar el ancho de banda:

- Cerrar completamente los programas que dejemos de utilizar, no basta con dar clic en botón de cerrar, hay que identificar en el botón de íconos ocultos los programas que aún siguen activos y cerrarlos para eliminar el servicio de la aplicación.
- De contar con un servicio de banda ancha de menor caudal, evitar utilizar varios programas con acceso a internet o en red.

- Si se cuenta o se requiere el uso de programas P2P (Peer to peer), limitar la transferencia de descarga, en aplicaciones tales como Ares, UTorrent, BitTorrrent, comúnmente es fácil de configurar.
- Abrir páginas de streaming de audio o video (YouTube) suele ser muy pesado para reducir el ancho de banda, es preferible descargar estos videos o música en horas muertas y tenerlas almacenadas en el disco duro del equipo para reproducirlas de forma local.
- Al abrir cualquier navegador de internet, cerrar pestañas que no son utilizadas, actualmente es muy común encontrar páginas web que requieren actualizarse constantemente para mostrar nueva información o propaganda.
- Contar con un monitor de red puede ayudar a determinar si el consumo de ancho de banda debe ser más alto o bien evitar gastos innecesarios.

Reducir interferencias:

- Acceder a la configuración del dispositivo y cambiar los canales de la red inalámbrica; utilizar canales entre 2,4 y 5 GHz reducen significativamente las interferencias.
- Evitar o reducir el número de dispositivos con señal de Bluetooth activo conectado al equipo receptor o bien cercano a él.
- Colocar el dispositivo emisor en el centro del área a utilizar, preferentemente sujetado al techo o techo falso del establecimiento.

Conclusión

Los accesos no autorizados en redes inalámbricas son muy comunes no solo en este tipo de negocios, también es común en nuestros hogares o trabajos conforme la protección y seguridad va mejorando, también lo están haciendo los programas y aplicaciones dedicados a la infiltración y obtención de claves WiFi. Como pudimos observar a lo largo de la investigación, los encargados de las MiPyME no se percatan de la poca o nula seguridad con la que cuentan, pero sí ven reflejados algunos inconvenientes con la pérdida de señal o ancho de banda en sus equipos creyendo que se debe al servicio del proveedor; se comprobó la existencia de un registro o historial de equipos que estuvieron conectados a su red en algún momento, siendo objetivos fáciles de vulnerar.

De acuerdo con la investigación se encontró que el cifrado WPA/WPA2-PSK es el cifrado más seguro y de mayor protección, aunque cabe mencionar que se requiere de equipos con mayores prestaciones para trabajar con este protocolo de seguridad. Finalmente, la información obtenida no solo beneficia a las MiPyME sino también a cualquier hogar o empresa que cuente con el servicio inalámbrico, ya que les permite conocer las vulnerabilidades de sus redes inalámbricas y con ello saber qué medidas de seguridad deben tomar. Entre las medidas más seguras no solo está el usar este cifrado, también se podría utilizar el filtrado MAC y ocultar el SSID con el fin de que no sea detectada la red. Los beneficios de conocer las vulnerabilidades son que se disminuyen los accesos no autorizados, el ancho de banda no se reduce al no haber intrusos en la red, se evita el robo de información, acceso y control de los dispositivos conectados a esta, además de que se mejora la productividad del negocio ya que el rendimiento de la red aumenta.

Bibliografía

Aransay, A. L. (10 de julio de 2009). *Universidad de Vigo: redes personales y locales.* Obtenido de http://www.albertolsa.com/wp-content/uploads/2009/07/alberto-los-santos-seguridad-en-wi-fi.pdf

Caballar, J. A. (2007). *Wi-Fi Instalación, Seguridad y Aplicaciones.* México: Alfaomega grupo editor S.A. de C.V.

Cisco, R. (s.f.). *Redes Cisco.* Obtenido de Redes Cisco.

Laffont Ediciones Electrónicas S.A. (2007). *Diccionario de Informática e Internet.* República Argertina: Laffont Ediciones Electrónicas S.A.

Lehembre, G. (enero de 2006). *Seguridad Wi-Fi – WEP, WPA y WPA2 Revista hakin9.* Obtenido de http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_ES.pdf

Li, C., Hwang, M., & Chu, Y. (2008). *A secure and efficient communication scheme with authenticated*. Obtenido de http://isrc.ccs.asia.edu.tw/www/myjournal/P227.pdf

Mastermagazine. (s.f.). *Definición de Full Duplex.* Obtenido de http://www.mastermagazine.info/termino/5092.php

Mastermagazine. (s.f.). *Definición de Módem.* Obtenido de http://www.mastermagazine.info/termino/5931.php

Mitchell, J., & He, C. (2005). *Security Analysis and Improvements for IEEE.*

Montoya, N. P. (2005). *Universidad de La Salle*. Obtenido de http://revistas.lasalle.edu.co/index.php/sv/article/view/1666

N. Borisov, I. G. (julio de 2001). *Intercepting mobile.* Obtenido de http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf

Pellejero, I., Andreu, F., y Lesta, A. (2006). Fundamentos y aplicaciones de seguridad en redes WLAN. En I. Pellejero, F. Andreu, y A. Lesta, *Fundamentos y aplicaciones de seguridad en redes WLAN: de la teoría a la práctica*. Marcombo, p. 160.