PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

SEDE ESMERALDAS.

ESCUELA DE SISTEMAS Y COMPUTACIÓN.

INFORME DE ESTUDIO DE CASO

TÍTULO:

ESTUDIO DE VULNERABILIDADES EN PROTOCOLOS DE ENCRIPTACIÓN PARA REDES INALÁMBRICAS EN LA FRECUENCIA 2.4 GHZ CASO PRÁCTICO: PROVEEDORES DE SERVICIO DE INTERNET DE ESMERALDAS

PREVIO A LA OBTENCIÓN DE TÍTULO DE INGENIERO EN SISTEMAS Y COMPUTACIÓN

AUTOR:

CAICEDO FRANCO LUCAS STALIN

ASESOR:

MGT. JUAN CASIERRA CAVADA

FECHA:

ESMERALDAS, AGOSTO 2017.

Estudio de caso aprobado luego de haber dado cumplimiento a los requisitos exigidos, previo a la obtención del título de INGENIERO EN SISTEMAS Y COMPUTACIÓN.

TRIBUNAL DE GRADUACIÓN

Título: "ESTUDIO DE VULNERABILIDADES EN PROTOCOLOS DE ENCRIPTACIÓN PARA REDES INALÁMBRICAS EN LA FRECUENCIA 2.4 GHZ CASO PRÁCTICO: PROVEEDORES DE SERVICIO DE INTERNET DE ESMERALDAS"

Autor: LUCAS STALIN CAIEDO FRANCO

Mgt. Juan Casierra Cavada **f.-…….**
Asesor/a

Mgt. Cesar Godoy Rosero **f.-…….**
Lector #1

Lector #2
Mgt. Fabián Martínez Estupiñan **f.-……**

Director de Escuela
Mgt. Xavier Quiñonez Ku **f.-……**

Ing. Maritza Demera Mejía **f.-……....**

Secretaria general PUCESE

Esmeraldas, Ecuador, agosto 2017

DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

Yo, **LUCAS STALIN CAICEDO FRANCO** portador de la cédula de identidad No. **0804258895** declaro que los resultados obtenidos en la investigación que presento como informe final, previo a la obtención del título de **"Ingeniero en Sistemas y Computación**" son absolutamente originales, auténticos y personales.

En tal virtud, declaro que el contenido, las conclusiones y los efectos legales y académicos que se desprenden del trabajo propuesto de investigación y luego de la redacción de este documento son y serán de mi sola, exclusiva responsabilidad legal y académica.

LUCAS STALIN CAICEDO FRANCO

CI 0804258895

CERTIFICACIÓN

Mgt. Juan Casierra Cavada Docente investigador de la PUCESE, certifica que:
El estudio de caso realizado por LUCAS STALIN CAICEDO FRANCO bajo el título "ESTUDIO DE VULNERABILIDADES EN PROTOCOLOS DE ENCRIPTACIÓN PARA REDES INALÁMBRICAS EN LA FRECUENCIA 2.4 GHZ CASO PRÁCTICO: PROVEEDORES DE SERVICIO DE INTERNET DE ESMERALDAS" reúne los requisitos de calidad, originalidad y presentación exigibles a una investigación científica y que han sido incorporadas al documento final, las sugerencias realizadas, en consecuencia, está en condiciones de ser sometida a la valoración del Tribunal encargada de juzgarla.

Y para que conste a los efectos oportunos, firma la presente en Esmeraldas, agosto del 2017.

Fdo. Mgt. Juan Casierra Cavada
Asesor

DEDICATORIA

El presente trabajo de investigación está dedicado primeramente a Dios, a mis padres que fueron de vital importancia en el transcurso de mi carrera universitaria. A mis hermanos que en cada momento me dieron su apoyo para seguir adelante, especialmente a mi ángel que me guía desde allá arriba, gracias.

AGRADECIMIENTO

Agradezco infinitamente a Dios por darme la oportunidad de vivir esta linda experiencia, por haberme llenado de sabiduría y paciencia para llegar a la meta.

Me gustaría enfatizar el apoyo de mi familia a lo largo de mi camino por esta prestigiosa institución.

Mis más sinceros agradecimientos a mi asesor y lectores que me guiaron de manera correcta en el desarrollo de la investigación, a mis profesores que con el conocimiento adquirido de parte de ellos puedo salir a defenderme en el campo laboral.

Agradecimiento mis abuelas, tías y tíos; también a mi tía que la vida me dio Dolores Perlaza. Por el constante apoyo y animo que me dieron.

RESUMEN

La presente investigación se realizó con el objetivo de analizar las vulnerabilidades de los protocolos de encriptación usados en las redes inalámbricas en la frecuencia 2.4 Ghz, en la zona comercial del centro de la ciudad de Esmeraldas. La investigación se orientó a los protocolos usados por el proveedor con mayor presencia en la zona, analizando cuáles son sus vulnerabilidades. La investigación tuvo un enfoque descriptivo, utilizando métodos de recolección de datos mediante la encuesta a los usuarios y una entrevista al proveedor con mayor cantidad de cliente. Estas técnicas de recolección de datos fueron de tipo cuantitativa y cualitativa respectivamente. En el transcurso del estudio, se pudo evidenciar ataques informáticos a los dispositivos tecnológicos de la población, la cual no posee los conocimientos básicos para detectar los ataques a los cuales fueron sometidos; así mismo se evidenció que los proveedores no están al tanto de la problemática de los usuarios. Los resultados obtenidos, permitieron realizar el diseño de una configuración óptima para los equipos de comunicación inalámbrica con lo cual se puede lograr la disminución de afectaciones por seguridad en la conectividad.

Palabras clave: Protocolos de encriptación, Red inalámbrica, ataques informáticos, Proveedor de internet, Esmeraldas.

ABSTRACT

The present investigation was carried out with the objective of analyzing the vulnerabilities of the encryption protocols used in 2.4 Ghz wireless networks in the downtown commercial area of Esmeraldas. The investigation was oriented to the protocols used by the provider with the presence of the mayor in the area, analyzing their children their vulnerabilities. The research had a descriptive approach, using methods of data collection through the survey of users and an interview with the supplier with more customers. These techniques of data collection were of quantitative and qualitative type, respectively. In the course of the study, it is possible to demonstrate the computer attacks to the technological devices of the population, which does not possess the basic knowledge to detect the attacks to the individuals; also it was evidenced that the suppliers are not so much of the problematic of the users. The obtained results allowed to realize the design of an optimal configuration for the equipment of wireless communication with which it can achieve the decrease of the affections by the safety in the connectivity.

Keywords: encryption protocols, wireless network, computer attacks, internet provider, Esmeraldas.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE ANEXOS

1. INTRODUCCIÓN

La presente investigación desarrollada con título “Estudio de vulnerabilidades en protocolos de encriptación para redes inalámbricas en la frecuencia 2.4 Ghz caso práctico: Proveedores de servicio de internet de Esmeraldas”, plantea una solución factible para los usuarios de internet e intranet que están situados en la zona comercial del centro de la ciudad de Esmeraldas.

El uso de redes inalámbricas está sujeto a recibir ataques informáticos por personas mal intencionado, en el presente estudio se muestra la manera de contrarrestar este tipo de malas acciones. Con la ayuda de nuevas tecnologías se puede poner un muro de seguridad para así disminuir las vulnerabilidades a los que día a día los usuarios están expuestos.

Los actores implicados en la investigación son los usuarios que laboran en la zona comercial del centro de la ciudad de Esmeraldas, comprendidos desde las calles Salinas y Bolívar hasta las calles Juan Montalvo y Bolívar, también contando con la colaboración del proveedor con más usuarios.

Estos fueron de vital importancia al momento del desarrollo del estudio, con los datos obtenidos se pudieron evidenciar diferentes aspectos que se desconocían de los usuarios de internet y así poder tomar las mejores decisiones para poder llevar de mejor manera este caso.

La investigación permite evidenciar las amenazas a las que están expuestos los usuarios cuando una red inalámbrica es insegura, con eso se pretende mejorar este aspecto y tener una red más eficiente, así como socializar la información obtenida.

2. OBJETIVOS

2.1. General.

Establecer el nivel de vulnerabilidades de los protocolos de encriptación de las redes inalámbricas en la frecuencia 2.4 Ghz.

2.2. Específicos.

- Determinar el tipo de configuración de los protocolos de encriptación que aplican los proveedores de internet.

- Especificar el nivel de vulnerabilidad aplicando la metodología OWISAM al estudio de las comunicaciones en los equipos instalados por los proveedores de internet.

- Inducir a los usuarios de internet a la configuración efectiva de sus equipos de conexión WiFi.

3. INFORME DEL CASO

3.1 DEFINICIÓN DEL CASO

Presentación de caso

El campo de la informática es muy amplio compuesto de muchos factores, entre ellos está la telecomunicación y dentro de la misma se encuentra la seguridad de las redes ya sean cableadas o inalámbricas. Estudios realizados por la Pontificia Universidad Católica del Ecuador (Rivas & Arciniegas, 2016) indican sobre las vulnerabilidades en las redes inalámbricas dentro de la ciudad de Esmeraldas, concretamente en sitios muy concurridos como lo son el parque central, el parque infantil, entre otros, por lo que no se ha profundizado en el tema de los protocolos de encriptación, para la seguridad de las mismas se presenta esta investigación.

En el presente estudio se estima mostrar las diferentes vulnerabilidades evidenciadas en el análisis de datos y así realizar comparaciones para poder determinar qué protocolo de encriptación sería el más óptimo para la seguridad de una red inalámbrica.

En la actualidad la tecnología Wi-Fi es el medio para la comunicación inalámbrica, usada en casi la mayoría de los aparatos a nivel mundial por eso siempre está sujeta a ataques informáticos y la mayoría de veces se pasa por alto el tema de la seguridad de la misma. Todo esto conlleva a la utilización de sistemas de encriptación.

Ámbitos de estudio

La investigación se desarrolló en la zona comercial céntrica de la ciudad de Esmeraldas, enfocándose al estudio de la seguridad de las redes inalámbricas con

tecnología Wi-Fi, concretamente a los protocolos de encriptación que funcionan dentro de este tipo de redes.

Actores implicados

En la investigación se contó con la participación de los usuarios que usan la tecnología Wi-Fi dentro de la zona comercial de Esmeraldas (zona 6) comprendidos desde la calles Salinas y Bolívar hasta la calle Juan Montalvo y Bolívar, también con la colaboración del proveedor más requerido por parte de los usuarios.

Identificación del problema

Al momento de usar redes inalámbricas una gran cantidad de usuarios están expuestos a diferentes tipos de ataques, la mayoría de casos los usuarios no están enterados de lo que pasa dentro de la red que utilizan, personas mal intencionadas podrían acceder y realizar actividades ilícitas perjudicando la integridad de la red o la información que se traslada a través de la misma.

La seguridad es una de las principales preocupaciones de las empresas que están interesadas en implementar redes inalámbricas. Afortunadamente, tanto el conocimiento de los usuarios sobre la seguridad como las soluciones ofrecidas por los proveedores de tecnología están mejorando. Las redes inalámbricas actuales incorporan funciones completas de seguridad, y cuando estas redes cuentan con una protección adecuada, las compañías pueden aprovechar con confianza las ventajas que ofrecen. (Cisco Systems, 2013)

Antes de profundizar es de suma importancia saber que es una red inalámbrica y como funciona. Las mismas que se definen como redes de ordenadores que no están conectados por medio de cables de ningún tipo u otro componente como

guía. El uso de una red inalámbrica permite a las empresas evitar el costoso proceso de introducción de cables en edificios o como una conexión entre diferentes ubicaciones de equipos. Las redes inalámbricas utilizan ondas de radio para conectar dispositivos tales como ordenadores portátiles a Internet, la red de negocios y aplicaciones. (Definición de Redes, 2015).

Para esto las redes inalámbricas constan con protocolos de encriptación para darles seguridad, aunque desde la creación de estas han sufrido ataques siendo vulneradas con facilidad, llevando a que estos evolucionen para tratar de suprimir ataques futuros.

Según (Suárez Gutiérrez, 2012) dentro de las redes inalámbricas constan distintos protocolos de encriptación para la seguridad de las mimas, donde los más usados son:

- WEP
- WPA
- WPA2

Tecnología WEP

La tecnología WEP (Wired Equivalent Privacy) fue el primer protocolo implementado por la norma IEEE 802.11, con el objetivo de brindar seguridad y confiabilidad a las redes inalámbricas.

> Está basado en el algoritmo de encriptación RC4, con una clave secreta de 40 o 104 bits, combinada con un Vector de Inicialización (IV) de 24 bits para encriptar el mensaje de texto M y su checksum – el ICV (Integrity Check Value). El mensaje encriptado C se determinaba utilizando la siguiente fórmula: C = [M || ICV (M)] + [RC4 (K || IV)]. Donde || es un operador de concatenación y + es un operador XOR. Claramente, el vector

de inicialización es la clave de la seguridad WEP, así que para mantener un nivel decente de seguridad y minimizar la difusión, el IV debe ser aplicado a cada paquete, para que los paquetes subsiguientes estén encriptados con claves diferentes. (Lehembre, 2006)

Uno de los principales problemas de seguridad que presenta el protocolo es que el IV es enviado como un texto simple, dado que la norma IEEE 802.11 no exige a que el IV incremente.

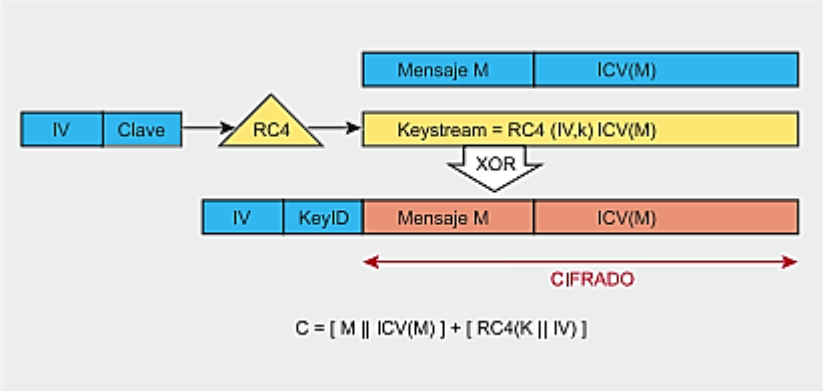


Figura 1.Funcionamiento del protocolo WEP *(Lehembre, 2006)*

Tecnología WPA

Dado que el primer protocolo daba muchas facilidades para ser vulnerado se evolucionó al Wi-Fi Protected Access (WPA), el mismo que tiene función de distribuir claves para un usuario en específico, permitiendo que la información esté íntegra, claro que terceras personas podrán obtener esta clave por diferentes medios, otra desventaja con la que cuenta este protocolo, es que posee una contraseña de mínimo 20 caracteres causando que fácilmente la olviden.

En este nuevo protocolo se solucionaron algunas debilidades que presentaba el WEP, uno de los principales avances fue de duplicar el Vector de Inicialización

(IV) de 24 bist a una longitud de 48 bits, además los fabricantes estaban en la obligación de agregarle reglas de secuencia.

> Los 48 bits permiten generar 2 elevado a 48 combinaciones de claves diferentes, lo cual parece un número suficientemente elevado como para tener duplicados. El algoritmo utilizado por WPA sigue siendo RC4. La secuencia de los IV, conocida por ambos extremos de la comunicación, se puede utilizar para evitar ataques de repetición de tramas. (Barajas, 2007)

Con estas mejoras el protocolo se volvió más dinámico al momento de generar las contraseñas, dando una fuerte ventaja ya que puede ser implementada en todo los equipos, por el motivo que no necesita actualizaciones, siempre y cuando no sea detectada alguna irregularidad en la seguridad.

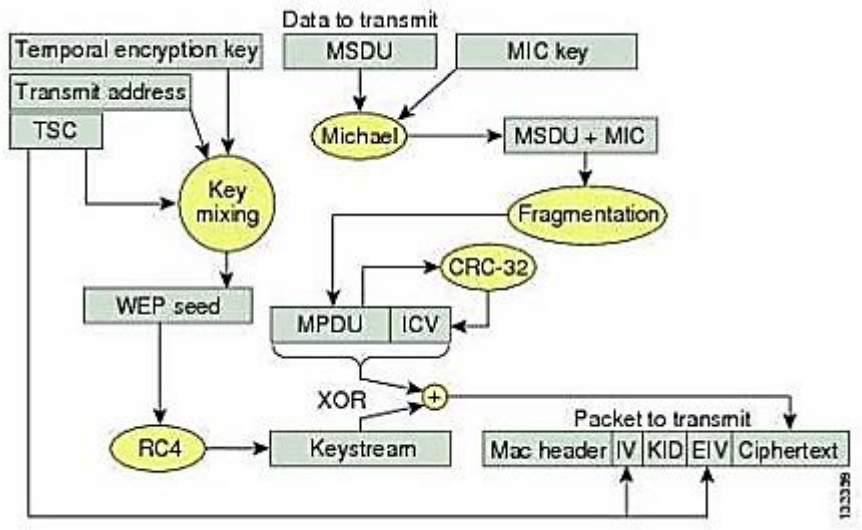


Figura 2.Funcionamiento del protocolo WPA (Luaces, 2013)

Tecnología WPA2

El protocolo WPA tuvo una buena acogida, pero como la tecnología va innovando y evolucionando, al pasar de los días no se tardó mucho en crear un nuevo protocolo llamado WPA2.

> El estándar 802.11i fue adoptado 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. (Zuccardi & Gutiérrez, 2006)

Con esta nueva innovación además de las mejoras antes mencionadas, también se realizaron perfeccionamientos que valen la pena indicar como por ejemplo, Implementando un nuevo algoritmo de cifrado llamado AES (Advanced Encryption Standard) permitiendo realizar un cifrado más efectivo dividiendo la cadena de texto en bloques pequeños y así cifrarlos iterativamente por separado.

También para la autenticidad y la integridad de los mensajes se utilizó el protocolo CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), haciendo uso del AES este cifrado permite manejar llaves con 128 bits y los vectores de inicialización de 48 bits.

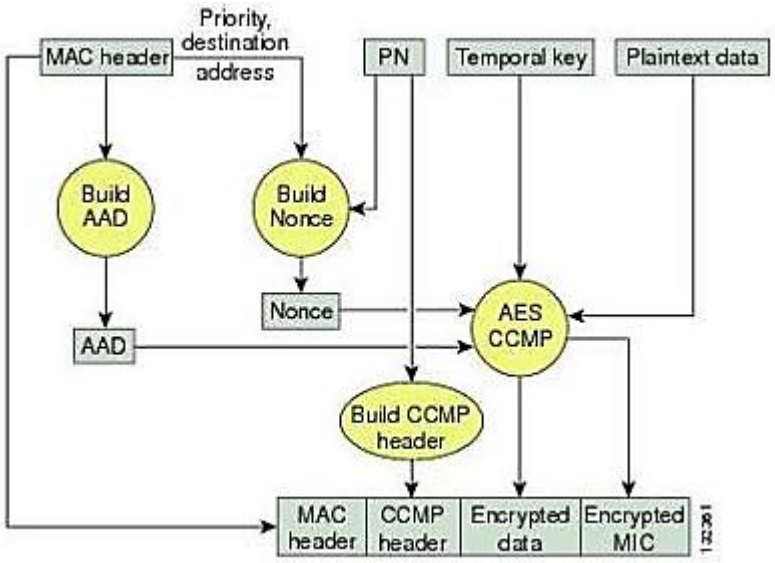


Figura 3 Funcionamiento del protocolo WPA2 *(Luaces, 2013)*

3.2 METODOLOGÍA

Tipo de investigación

El tipo de investigación que se aplicó fue descriptiva, ya que se realizaron diferentes análisis a los protocolos de encriptación en la frecuencia 2.4 Ghz utilizados por los proveedores de internet en la ciudad de Esmeraldas, también se realizó un análisis de la infraestructura tecnológica en los diferentes usuarios.

La investigación desarrollada es cuali-cuantitativa, con respecto a que se realizó una entrevista al encargado de la configuración de los equipos inalámbricos del proveedor con más usuarios en la zona de estudio y por la tabulación de los datos obtenidos de la encuesta realizada a los usuarios.

Para poder medir el nivel de vulnerabilidad de los protocolos de encriptación en las redes inalámbricas se hizo uso de OWISAM-TR-004, que por sus siglas en ingles significa Open Wireless Security Assessment Methodology (Metodologíade evaluación de seguridad Wireless abierta). Esta metodología indica cuáles son los controles de seguridad que se deben verificar sobre redes de comunicaciones inalámbricas para minimizar el impacto de los ataques

informáticos y a garantizar la protección de las infraestructuras Wireless (OWISAM, 2013)

Lista de preguntas

Para el desarrollo de la investigación se platearon las siguientes interrogantes relacionadas al caso que se está tratando:

¿Cómo identificar que proveedor de internet es el más requerido por los usuarios de la zona comercial del centro de Esmeraldas?

¿Será posible evidenciar si existe la necesidad que los usuarios tenga conocimiento de cómo asegurar sus redes inalámbricas?

¿Cómo realizar pruebas a los protocolos de encriptación para poder generar un buen análisis y obtener buenos resultados?

¿Cómo saber si las vulnerabilidades en las redes inalámbricas tienen que ver también con el tipo de hardware que los proveedores usan?

Fuentes de información

Los usuarios que se dedican a las diferentes actividades comerciales en la zona céntrica de Esmeraldas, comprendidos entre las calles Bolívar y Salinas hasta las calles Bolívar y Juan Montalvo son un total de 130, según el departamento de higiene del Gobierno Autónomo Descentralizado de la ciudad de Esmeraldas, a la cual se le ha calculado una muestra dando como resultado 66 usuarios a los cuales se les realizo una encuesta.

Tabla I. Fuentes de información

Fuente	Técnicas Aplicadas	
Usuarios	Encuesta	Cuestionarios de Preguntas
Proveedor de Internet	Entrevista	Cuestionarios de Preguntas

Fuente: Autor

Así mismo, con los datos obtenidos en la encuesta se indica que el proveedor que brinda sus servicios a la mayoría de usuarios es la Corporación Nacional de Telecomunicaciones (CNT).

Con la información obtenida se pudo analizar varios aspectos sobre el tipo de configuración que emplea el proveedor, y la forma de cómo protege la información de los usuarios.

Técnicas para la recolección de información.

Según los objetivos planteados dentro de la investigación, para el levantamiento de información, se aplicaron las técnicas de encuestas y entrevistas, las mismas que devolverán resultados que se tabularan de forma cualitativa y cuantitativa.

Dentro de los actores a intervenir en la investigación se encuentra la Población y Muestra.

Según el departamento de higiene del Gobierno Autónomo Descentralizado Municipal de la ciudad de Esmeraldas, en la zona comercial céntrica de la ciudad se encuentran laborando 130 locales que realizan distintas actividades comerciales

$$n = \frac{k^2 pqN}{(N-1)e^2 + k^2 pq}$$

Datos:

N: Tamaño de la población =130

k: Nivel de confianza = 1.15

e: Error muestral = 0.05

p: Proporción de la población que posee la característica de estudio =0.5

q: Proporción de la población que no posee la característica de estudio=0.5

n: Tamaño de la muestra = ?

$$n = \frac{1.15^2 * 0.5 * 0.5 * 130}{(130-1)0.05^2 + 1.15^2 0.5 * 0.5}$$

$$n = \frac{1.3225 * 0.5 * 0.5 * 130}{129 * 0.0025 + 1.3225 * 0.5 * 0.5}$$

$$n = \frac{42.98125}{0.3225 + 0.330625}$$

$$n = \frac{42.98125}{0.653125}$$

$$n = 65.808612$$

$$n = 66$$

Tabla II. Población objeto de estudio

Población	
Universo	Muestra
130	66

Fuente: GAD Municipal del cantón Esmeraldas

Con el fin de darle fiabilidad a la investigación, se evaluó la confiabilidad de los datos obtenidos, para poder lograrlo se utilizó el coeficiente Alfa de Cronbach mostrado en la Tabla III.

Tabla III. Fiabilidad de la encuesta realizada a los usuarios de internet

Alfa de Cronbach	N de elementos
0,71	66

Fuente: IBM - SPSS Statistics

Según (George & Paul, 2003) para comprobar que los resultados obtenidos tengan fiabilidad, el coeficiente de Alfa de Cronbach debe estar en el rango mostrado a continuación, teniendo en cuenta que:

- Alfa > 0.9 es excelente
- Alfa > 0.8 es bueno
- Alfa > 0.7 es aceptable

Dicho esto se puede evidenciar que la encuesta realizada tiene una fiabilidad aceptable.

Encuesta realizada a los usuarios de internet de la zona comercial céntrica de la ciudad de Esmeraldas.

1. ¿Qué proveedor de internet usa?

Tabla IV. Proveedor de internet más requerido

Opción	Frecuencia	Porcentaje %
CNT	62	94
Punto Net	1	2
Telecomvas	1	2
Solintelsa	2	3
Otros	0	0
Total	66	100

Fuente: Usuarios de internet

El cuestionamiento establecido se lo planteo para determinar cuál de los distintos proveedores de internet es el más utilizado por los usuarios en la zona comercial de Esmeraldas, arrojando un resultado que la empresa pública CNT es la más requerida, con esto se enfocara la investigación a este proveedor que cuenta con casi la totalidad de usuarios.

2. ¿En qué categoría se encuentra su negocio?

Tabla V. Tipo de actividad comercial de los usuarios

Opción	Frecuencia	Porcentaje %
Sucursal Bancaria	0	0
Comerciante	11	17

Pymes	55	83
Fabricante	0	0
Otros	0	0
Total	66	100

Fuente: Usuarios de internet

La pregunta descrita en la Tabla V, se la diseñó con el propósito de tener en cuenta o conocer a que se dedican los usuarios, para así poder determinar si la información que almacenan es de vital importancia para sus negocios, dando como resultado que la mayoría de ellos se dedican a actividades con alto flujo de dinero y de mercadería, donde si no existe la debida seguridad en sus redes, podrían estar en peligro de ser atacados.

3. ¿Ha sido víctima de delitos informáticos?

Tabla VI. Víctimas de delitos informáticos

Opción	Frecuencia	Porcentaje %
Si	4	6
No	62	94
Total	66	100

Fuente: Usuarios de internet

El cuestionamiento que se planteo sirvió para definir si los usuarios en algún momento han sido víctimas de ataques informáticos, obteniendo que un 6% de ellos ha sido vulnerado.

4. ¿Está informado sobre cómo proteger su equipo de ataques informáticos?

Tabla VII. Necesidad sobre protección de equipos a los ataques informáticos

Opción	Frecuencia	Porcentaje %
Mucho	0	0
Poco	8	12
Nada	58	88
Total	66	100

Fuente: Usuarios de internet

La Tabla VII detalla la necesidad de los usuarios de conocer más sobre la seguridad de las redes inalámbricas, con esto se podrá disminuir el índice de ataques y podrán realizar sus actividades con mayor tranquilidad. Claro que de lo que se habla es de una configuración sencilla para sus equipos, ya que ellos no cuentan con altos conocimientos en telecomunicaciones.

5. ¿Cree necesario recibir capacitaciones para un uso seguro de los recursos del internet?

Tabla VIII. Necesidad de capacitaciones por parte de los usuarios

Opción	Frecuencia	Porcentaje %
Si	64	97
No	2	3
Total	66	100

Fuente: Usuarios de internet

La pregunta descrita en la Tabla VIII evidencia la necesidad por parte de los usuarios, de capacitaciones sobre la seguridad de redes inalámbricas con esto ellos podrán empaparse más del tema y así estar más atentos a fluctuaciones que podrían darse en sus redes.

6. ¿Ha recibido información del proveedor orientada a la seguridad de su equipo?

Tabla IX .Comunicación sobre seguridad por parte de los proveedores

Opción	Frecuencia	Porcentaje %
Si	0	0
No	66	100
Total	66	100

Fuente: Usuarios de internet

Generalmente, los proveedores solo se preocupan de instalar sus servicios en los distintos lugares donde pueda llegar su compañía, pero se les pasa por alto brindar información a los usuarios como se evidencia en la Tabla IX, de los peligros que conlleva tener una red sin una buena seguridad, en muchos casos las configuraciones que ellos realizan no son suficientes y esto trae problemas a los usuarios, si los proveedores dieran un poco más de información sobre como protegerse contra los ataques el panorama del servicio fuera muy distinto.

3.3. DIAGNÓSTICO

Habitualmente varios son los delitos informáticos que los cyber-delincuentes pueden realizar, aprovechándose de las vulnerabilidades que las redes inalámbricas poseen.

Muchas personas han perdido información a causa de eso sin darse cuenta, la mayoría de usuarios tienen como conocimiento que con poseer una clave es suficiente para tener una red segura, la información mostrada en la Figura 4 dice todo lo contrario ya

que los delitos van desde el espionaje hasta un fraude, robo de cuentas, acoso, entre otros.

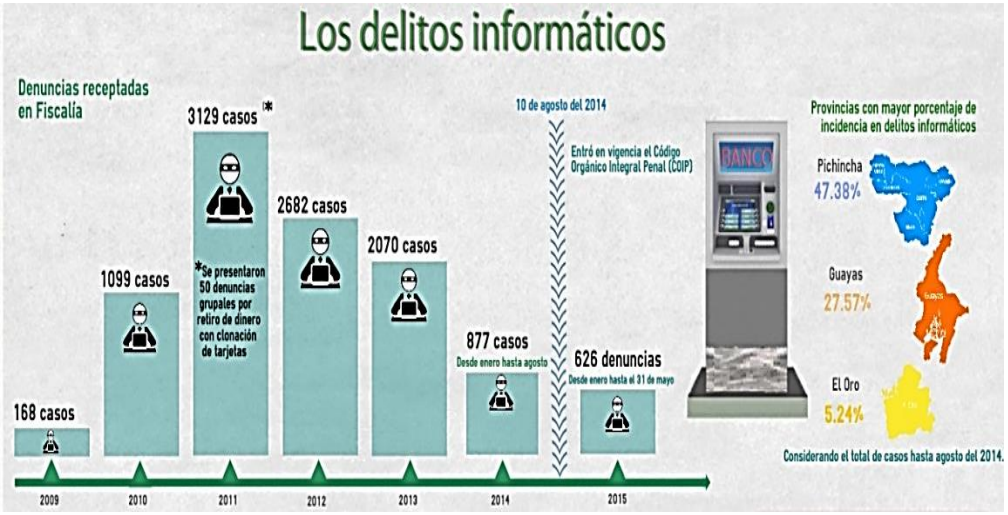


Figura 4.Los delitos informáticos (FGEE, 2015)

La fiscalía del Ecuador facilitó la información detallada en la Figura 4, donde se pudo evidenciar que en el país ha incrementado los ataques a los usuarios de internet, como se demostró en las encuestas, existen usuarios dentro de la ciudad de Esmeraldas que también han sido víctimas de infiltraciones no deseadas en su red.

Lo que evidencia la falta de conocimiento sobre este tema por parte de los usuarios y el abandono de los proveedores de internet para brindarles un camino que seguir para poder evitar este tipo de problemas, con la falta de seguridad en sus redes están expuestos a delitos muy graves.

También en la mayoría de los casos es de conocimiento público la información de cómo están configurados la mayoría de los equipos que usa el proveedor de internet, realizando una pequeña búsqueda desde cualquier navegador es fácil encontrar dicha información como se muestra en la Figura 5.

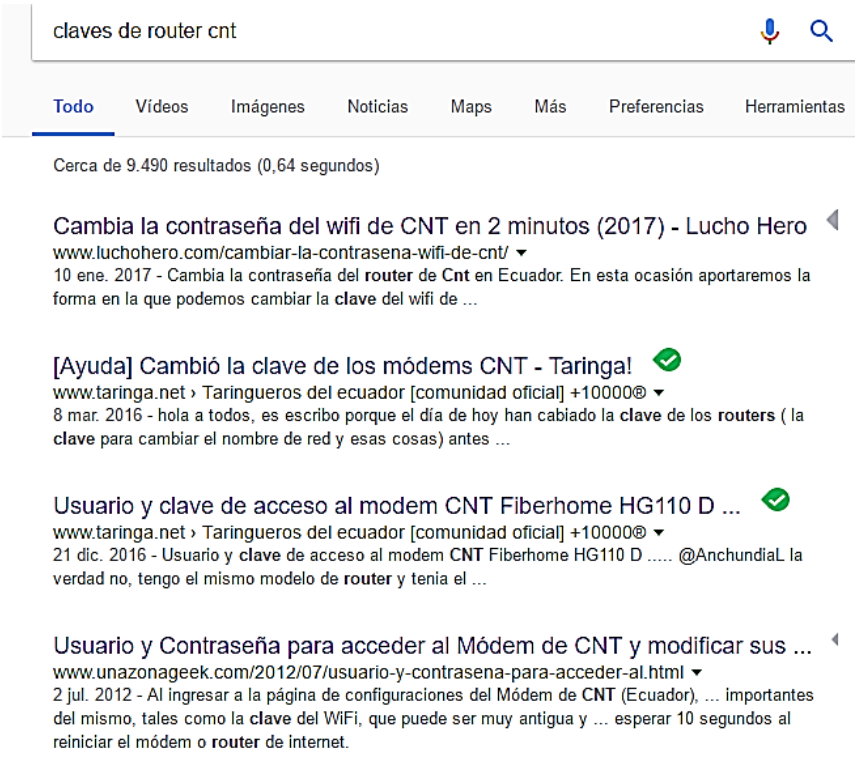


Figura 5.Búsqueda de claves de router CNT (Autor)

Sabiendo que existen varios métodos para realizar ataques a las redes inalámbricas concretamente, estas están a merced de cualquier persona con mucha o poca experiencia en telecomunicaciones e informática, ya que existen varias maneras para obtener estas clases de conocimientos.

Indicando todo esto, se demostró que es posible realizar ataques a una red inalámbrica, con los protocolos de encriptación que fueron objeto de estudio dentro de esta investigación.

Para poder lograrlo se utilizó una computadora portátil con un sistema operativo Kali Linux que es una distribución de Debian, este sistema operativo es de los más usados ya que cuenta con varias herramientas para realizar este tipo de ataques.

Utilizando el método llamado inyección de paquetes para acelerar el crakeo de la red inalámbrica, se usa la herramienta llamada aircrack, los pasos y el manejo son muy sencillos claro que hay que tener cierto conocimiento en comandos de este sistema

operativo, pero como se lo menciono anteriormente existen varias maneras de adquirir este conocimiento, existen, guías, video tutoriales, entre otros.

Para demostrar las vulnerabilidades de los protocolos de seguridad de las redes inalámbricas, se realizó el ataque a una red inalámbrica con el protocolo de encriptación más actual que es el WPA2, mostrada a continuación:

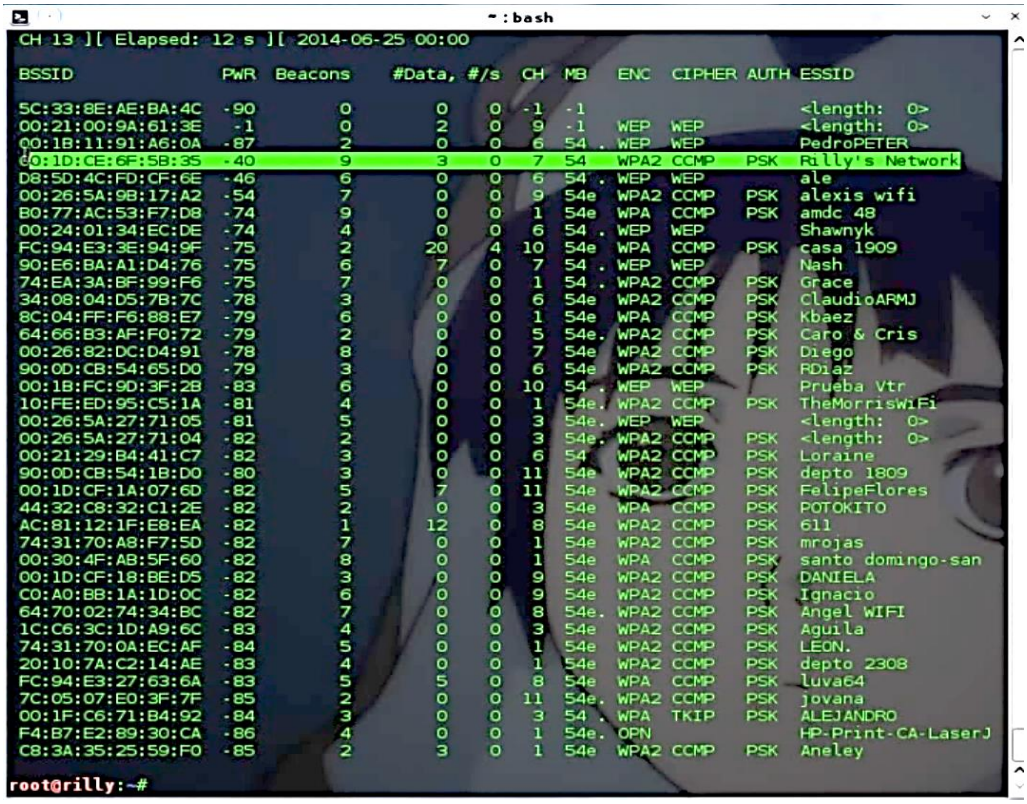


Figura 6. Selección de red inalámbrica para el ataque (Autor)

Como se puede apreciar en la Figura 6, este sistema muestra toda la información de la red inalámbrica, desde la mac de la tarjeta de red hasta el cifrado que usa. Con solo obtener estos datos la persona que está haciendo el ataque puede tener libre acceso a la red de cualquier usuario.

En este caso se utilizó la red con los siguientes aspectos:

Essid: Rilly' s NetWork

Bssid: 00:1D:CE:6F:5B:35

Canal: 7

Con todos estos datos lo único que se necesita es que otro dispositivo esté conectado a la red, para poder capturar el handshake o en español que significa darse la mano, una vez realizada la captura lo que se va a necesitar es un diccionario que contiene distintas combinaciones de contraseñas, la eficiencia de este proceso va a depender del idioma y lo amplio que pueda ser el diccionario, en este caso se utilizó uno que viene con el sistema operativo Kali Linux.

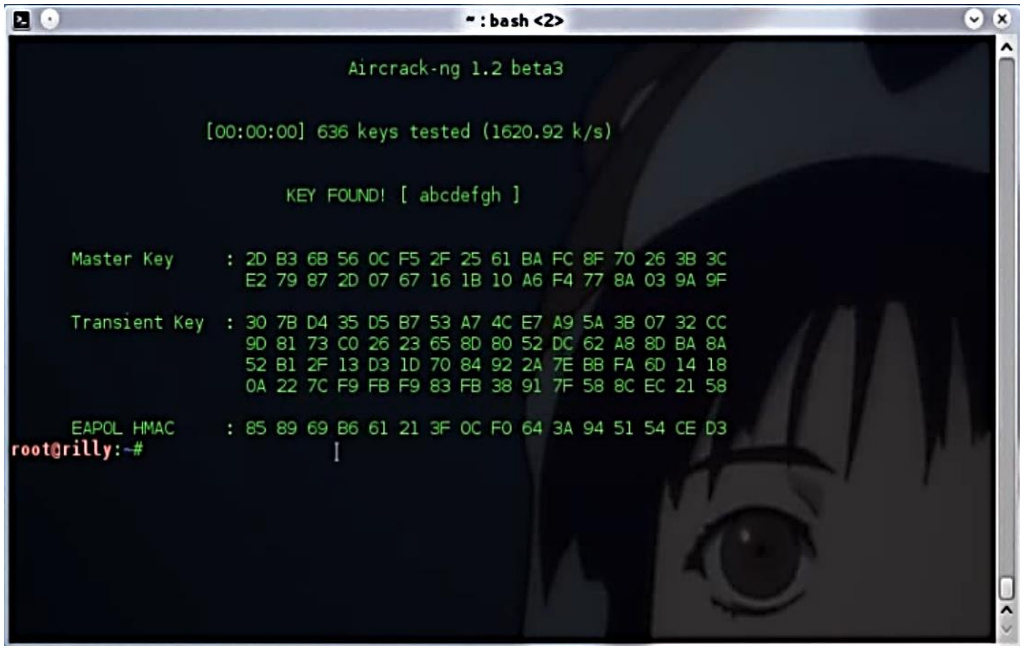


Figura 7. Ataque exitoso a red inalámbrica (Autor)

La Figura 7 demuestra que el ataque a la red inalámbrica fue realizado con éxito, dando a evidenciar que el protocolo más actual también está sujeto a infiltraciones, además el proceso que se realizó también sirve con los otros protocolos mencionados en la presente investigación, demostrando que se necesita más herramientas para darle una mayor seguridad a las redes inalámbricas.

Se debe tomar en cuenta que el dispositivo que se utilizó para la prueba es de uso propio, así se evitan problemas legales ya que esta actividad es ilegal, también se omitieron varias

capturas de los pasos realizados para evitar responsabilidades con el uso de esta información.

No esta demás mencionar los delitos más importantes, que son penados en el país.

Según el Código Orgánico Integral Penal (COIP) las penas por cometer estos delitos son las siguientes:

> **Artículo 190**.- Apropiación fraudulenta por medios electrónicos.- La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años.
>
> La misma sanción se impondrá si la infracción se comete con inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas o encriptadas, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes.

> **Artículo 191**.- Reprogramación o modificación de información de equipos terminales móviles.- La persona que reprograme o modifique la información de identificación de los equipos terminales móviles, será sancionada con pena privativa de libertad de uno a tres años.

> **Artículo 194**.- Comercialización ilícita de terminales móviles.- La persona que comercialice terminales móviles con violación de las disposiciones y procedimientos previstos en la normativa emitida por la autoridad competente de

telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años.

Artículo 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.- La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años. (COIP, 2014)

Como se puede apreciar las leyes son muy estrictas cuando se trata de delitos informáticos, por eso se recomienda abstenerse a cometer este tipo de acciones que afectan de manera negativa al crecimiento de la sociedad, sin embargo siempre van a existir personas que piensan que nunca serán detectadas, pero se debe tomar en cuenta que cuando se realiza este tipo de actividades siempre se deja una puerta abierta para ser descubiertos.

Por eso se crearon estos artículos para tener un mejor control y de cierta manera darle un poco más de seguridad a los usuarios que día a día usan las redes inalámbricas.

3.4. DISCUSIÓN

En la presente investigación se tomaron en cuenta varios aspectos sobre la seguridad de las redes inalámbricas, abordando temas desde las sanciones penales, hasta las consecuencias que se podrían dar si una red inalámbrica no es segura, tomando como objeto de estudio los protocolos de encriptación, con eso se trata de plantear cuál de ellos es el óptimo para un tema tan delicado como es la seguridad y la confiabilidad de los datos que transitan en la red.

De acuerdo al levantamiento de datos realizado, los usuarios de la zona comercial céntrica de la ciudad de Esmeraldas ya han sido víctimas de ataques, teniendo en cuenta que los usuarios no se percatan de lo que pasa a través de su red, por eso se quiere trazar una buen opción de configuración de sus equipos de comunicación inalámbrica para que ellos se sientan seguros y que sus redes no sean atacadas.

Teniendo presente que lo que se busca en la investigación es encontrar una buena manera de configurar sus equipos de comunicación inalámbrica, para aumentar su seguridad e integridad de sus datos, se analizaron varias opciones para ser implementadas y así reducir el nivel de vulnerabilidades de las mismas.

Examinando uno a uno los protocolos de encriptación se ha decidido dejar fuera al protocolo WEP porque ya se encuentra obsoleto y a más de eso tiene una fuerte debilidad según (Barajas, 2007) "WEP no incluye autentificación de usuarios. Lo más que incluye es la autentificación de estaciones descrita (podrán entrar aquellas estaciones que en su configuración tengan almacenada la clave WEP)". (p.3)

Habiendo dicho esto solo quedaría como opciones los dos protocolos más parecidos el WPA y el WPA2 donde su principal diferencia es la de la longitud en las claves que los usuarios usan, por lo que se ha traído como objeto de discusión a (Suarez, sf) donde argumenta que "WPA se distingue por tener distribución dinámica de claves, utilización más robusta del vector de inicialización y nuevas técnicas de integridad y autentificación". (p.18)

Los dos protocolos anteriormente mencionados muestran grandes cualidades, pero hay que tomar en cuenta que en la tecnología la innovación es algo muy importante por eso el protocolo WPA2 tiene una gran ventaja en comparación a los otros, dicho esto se ha tomado el argumento de (Lehembre, 2006) diciendo que "WPA2 introdujo varios cambios fundamentales, como la separación de la autenticación de usuario de la integridad, proporcionando una arquitectura robusta y escalable, que sirve igualmente para las redes locales domésticas como para los grandes entornos de red corporativos". (p.17)

Con lo anteriormente indicado, se ha establecido que el protocolo óptimo para ser usado en la configuración de los equipos de comunicación inalámbrica sea el WPA2, puesto que a comparación con los otros es el más capacitado para la función de

seguridad, siendo contemporáneo y cuenta con un gran número de actualizaciones, así se podrá contrarrestar ataques. Se debe tomar en cuenta que este protocolo también es sujeto a ataques pero a su vez difícil de atacar, no por su estructura sino por su robustez ya que emplearía una mayor cantidad de tiempo al momento de realizar algún tipo de ataque.

Tabla X. Comparación entre los protocolos de encriptación

	Características	Debilidades
WEP	• Utiliza una misma clave simétrica y estática en las estaciones y puntos de acceso. • El estándar no contempla ningún mecanismo de distribución automática de claves, lo que obliga a escribir la clave manualmente en cada uno de los elementos de red. • La clave está almacenada en todas las estaciones, aumentando las posibilidades de que sea comprometida.	• La implementación del vector de inicialización (IV) en el algoritmo WEP tiene varios problemas de seguridad. • La longitud de 24 bits para el IV forma parte del estándar y no puede cambiarse. • El mecanismo de autentificación de secreto compartido tiene el problema de enviar por la red el mismo texto sin cifrar y cifrado con la clave WEP (esta clave coincide con la utilizada para asegurar la confidencialidad).
WPA	• Distribución dinámica de claves. • Utilización más robusta del vector de inicialización (mejora de la	• La vulnerabilidad más práctica es el ataque contra la clave PSK de WPA. • Negacion del servicio durante el 4-way handshake.

	confidencialidad) y nuevas técnicas de integridad y autentificación.	
WPA2	• Incluye el nuevo algoritmo de cifrado AES (Advanced Encryption Standard), desarrollado por el NIS [14]. • Utiliza CCMP (CounterMode / Cipher Block Chaining / Message Authentication Code Protocol) en lugar de los códigos MIC	• La vulnerabilidad más práctica es el ataque contra la clave PSK de WPA2.

Fuente: (Barajas, 2007)

Estando al tanto de las características de los protocolos de encriptación mencionados se realizó un análisis del radio espectro del campo de estudio, donde usando la herramienta Inssider se logró capturar la información relevante de las redes inalámbricas que funcionan en dicha zona, dando como resultado lo mostrado a continuación:

Tabla XI. Redes capturadas con la herramienta Inssider

Canal	Seguridad			Total de redes
	WPE	WPA	WPA2	
1	**x**			2
			x	11
2			**x**	2
3			**x**	3
4			**x**	5
5			**x**	3
6	**x**			1
			x	8
7			**x**	2
8	**x**			1
			x	2
9			**x**	3
10			**x**	1
11	**x**			1
			x	21
Total				**66**

Fuente: Inssider

4. PROPUESTA DE INTERVENCIÓN

4.1. Título

Configuración de dispositivos Mikrotik para establecer estándares de seguridad en redes inalámbricas.

4.2. Descripción

La presente propuesta se enfoca al cumplimiento de los objetivos del estudio, esencialmente permite determinar el tipo de configuración de los protocolos de encriptación que aplican los proveedores de internet.

En base a los hallazgos obtenidos de los usuarios y el proveedor con más influencia en la zona comercial del centro de la ciudad de Esmeraldas, es ineludible exponer una propuesta, para el aumento de la seguridad de las redes inalámbricas y hacer que los usuarios se sientan más seguros.

Partiendo de los datos obtenidos de las auditorías realizadas a los protocolos de encriptación, se pudo evidenciar que el protocolo más actualizado tiene también vulnerabilidades y está sujeto a ataques, esto lleva a idear una buena configuración para disminuir sus falencias, con una buena configuración y un equipo mikrotik como complemento se creará otra barrera entre la información del usuario y los cyber-delincuentes que traten de acceder a la red de forma ilícita.

Con la utilización de mikrotik se podrá mejorar la seguridad creando reglas, para un funcionamiento eficiente, será un complemento idóneo para cumplir con la propuesta planteada.

4.3. Diseño

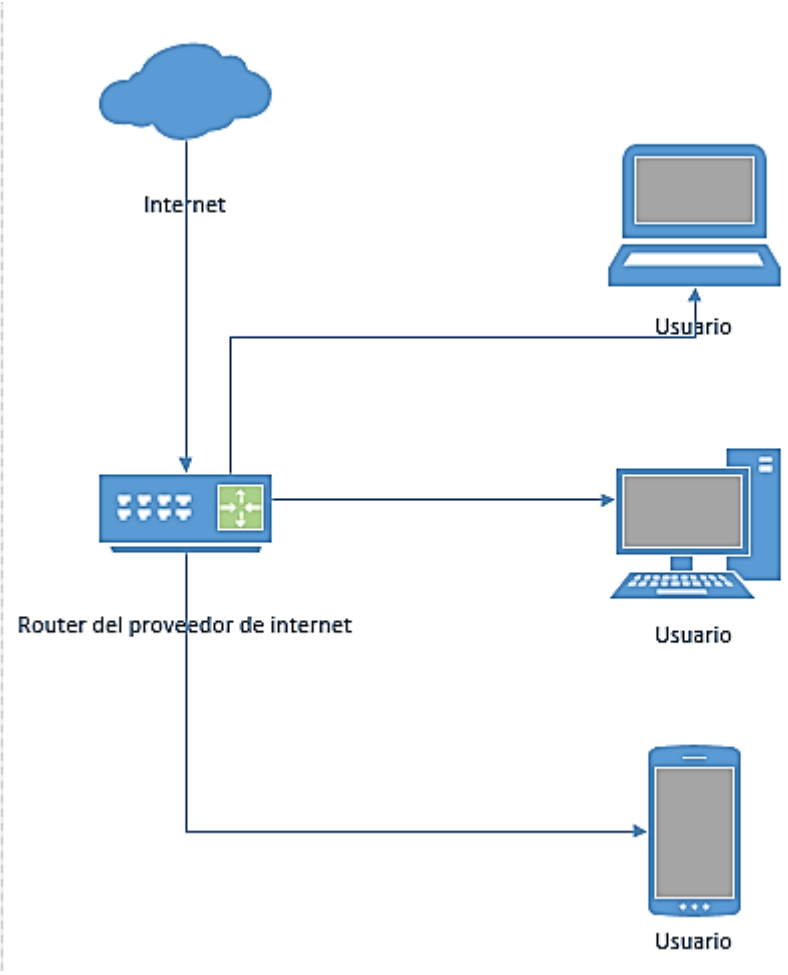


Figura 6. Diseño actual de las redes inalámbricas (Autor)

Como se muestra en la Figura 9 el actual diseño de la configuración de la red que se instala a los usuarios consta de un router que es proporcionado por el proveedor del servicio, este cuenta con una configuración estándar es decir el usuario y la clave son el mismo en la mayoría de equipos, colocando la propagación de la red en la frecuencia 2.4 GHZ y regularmente en el canal 11.

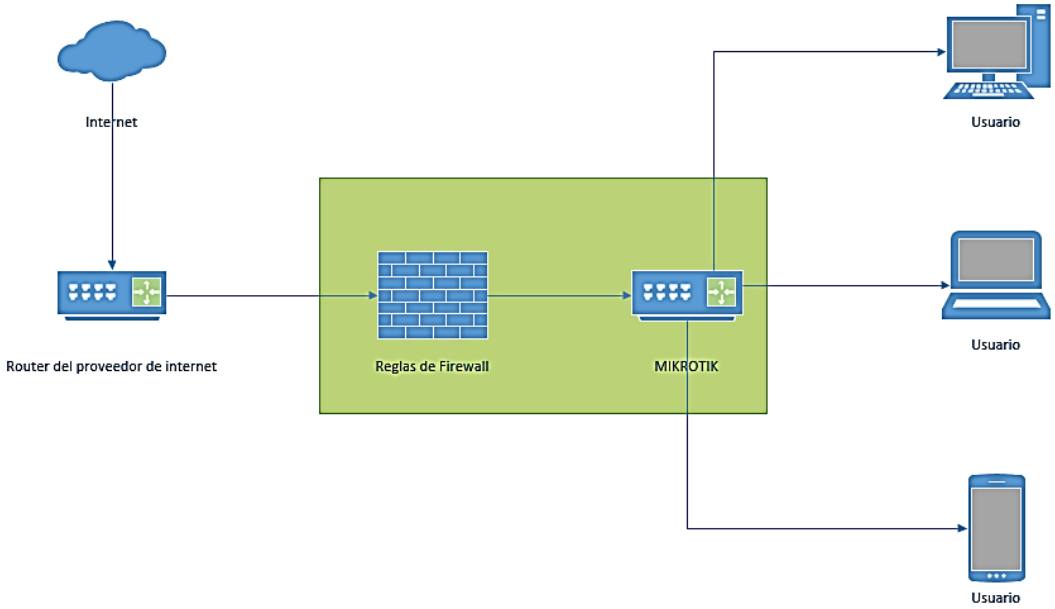


Figura 7. Diseño de la propuesta (Autor)

En la Figura 10 se muestra el diseño de la propuesta de configuración de la red, para aumentar su seguridad. Donde al inicio del ciclo el internet es captado por el router que es proporcionado por el proveedor, a este se le va a desactivar la opción de trabajar con WLAN es decir que trabajará solo de forma cableada, el mismo router le proporcionara internet al Mikrotik, donde se realizará una configuración para que la red sea menos propensa a los ataques, mostrada a continuación:

- Cambiar el usuario y la contraseña que vienen por defecto en el router.
- Usar el protocolo de encriptación WPA2.
- Ocultar la ESSID.
- Asignar las direcciones MAC que se quiere usar en la red, para realizar un filtrado.
- Asignar IP estáticas a los dispositivos y desactivar la asignación por DHCP.

Luego de realizar estas configuraciones para dar un poco más de seguridad se configuró una tabla ARP estática dentro del Mikrotik, con esto se podrá asignar las direcciones MAC e IP, así se podrá filtrar a los infiltrados.

REFERENCIAS

Aguilera, P. (2011). *Redes seguras* . Toledo: Editex.

Aguilera, P. (2011). *Redes seguras (Seguridad informática).* Editex.

Barajas, S. (2007). Protocolos de seguridad en redes inalámbricas.

Cisco Systems. (11 de Junio de 2013). Obtenido de http://www.cisco.com/web/LA/soluciones/comercial/proteccion_wireless.html

COIP. (Mayo de 2014). *Ministerio de Justicia, Derechos humanos y Cultos*. Obtenido de http://www.justicia.gob.ec/wp-content/uploads/2014/05/c%C3%B3digo_org%C3%A1nico_integral_penal_-_coip_ed._sdn-mjdhc.pdf

Definición de Redes. (3 de Septiembre de 2015). Obtenido de http://definicionderedes.blogspot.es/categoria/servidor/

Dordoigne, J. (2015). *Redes informáticas - Nociones fundamentales.* Madrid: Ediciones ENI.

Dordoigne, J. (2015). *Redes informáticas - Nociones fundamentales (5ª edición): (Protocolos, Arquitecturas, Redes inalámbricas, Virtualización, Seguridad, IP v6 ...).* Ediciones ENI.

FGEE. (13 de 06 de 2015). *Fiscalia General del Estado de Ecuador*. Obtenido de http://www.fiscalia.gob.ec/index.php/sala-de-prensa/3630-los-delitos-inform%C3%A1ticos-van-desde-el-fraude-hasta-el-espionaje.html

G. D., & P. M. (2006). *SPSS for Windows step by step: A simple guide and reference.* (11.0 update (4 th ed.) ed.). Boston: Allyn & Bacon.

Jara, H., & Pacheco, F. (2012). *Ethical Hacking.* Buenos Aires: Fox Andina.

Lehembre, G. (2006). Seguridad Wi-Fi – WEP, WPA. *Hakin9*, 26.

Luaces, M. (10 de Enero de 2013). *Openaccess.* Obtenido de http://openaccess.uoc.edu/webapps/o2/bitstream/10609/18804/6/jluacesTFC0113memoria.pdf

OWISAM. (2013). Obtenido de https://www.owisam.org/es/P%C3%A1gina_principal

Rivas, F., & Arciniegas, S. (2016). *Avances y aplicaciones de sistemas inteligentes y nuevas tecnologías.* Ibarra: Mérida, Estado de Mérida, Venezuela : Universidad de Los Andes, Consejo de Publicaciones ; [Ibarra] : Pontificia Universidad Católica de Ecuador, Sede Ibarra (PUCE-SI).

Suárez Gutiérrez , M. (Mayo de 2012). *Universidad Veracruzana.* Recuperado el 10 de Agosto de 2016, de http://www.uv.mx/personal/mansuarez/files/2012/05/Mecanismos-de-Seguridad-en-Redes-InalambricasProtegido.pdf

Suarez, M. (sf). *Mecanismos De Seguridad En Redes Inalámbricas.* Obtenido de http://www.uv.mx/personal/mansuarez/files/2012/05/Mecanismos-de-Seguridad-en-RedesInalambricasProtegido.pdf,

Zuccardi, G., & Gutiérrez, J. (2006). Seguridad Informática en 802.11 .

ANEXOS

Anexo 1. Encuesta realizada a los usuarios de Internet

PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR

SEDE ESMERALDAS

Encuesta para el estudio "ESTUDIO DE VULNERABILIDADES EN PROTOCOLOS DE ENCRIPTACIÓN PARA REDES INALÁMBRICAS EN LA FRECUENCIA 2.4 GHZ CASO PRÁCTICO: PROVEEDORES DE SERVICIO DE INTERNET DE ESMERALDAS"

El objetivo de esta investigación es obtener información confiable sobre su situación con las redes inalámbricas.

Nota: Un delito informático o ciberdelito es toda aquella acción anti jurídica y culpable, que se da por vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet. Por ejemplo, robo de información, infiltración a una red sin permiso del usuario, entre otros.

Preguntas para los usuarios de internet:

¿Qué proveedor de internet usa?

Cnt ( )

Punto Net ( )

Telecomvas ( )

Solintelsa ( )

Otros ( )

¿En qué categoría se encuentra su negocio?

Sucursal Bancaria ( )

Comerciante ( )

Pymes ( )

Fabricante ( )

Otros ( )

¿Ha sido víctima de delitos informáticos?

Si ( )

No ( )

¿Está informado sobre cómo proteger su equipo de ataques informáticos?

Mucho ( )

Poco ( )

Nada ( )

¿Cree necesario recibir capacitaciones para un uso seguro de los recursos del internet?

Si ( )

No ( )

¿Ha recibido información del proveedor orientada a la seguridad de su equipo?

Si ( )

No ( )

Anexo 2. Tabla de valoración para las vulnerabilidades de las redes inalámbricas

Tabla de valoración		
Valor	**Nivel de riesgo**	**impacto**
0 – 2	**Mínimo**	Mínimo riesgo de acceso no autorizado. Un ataque exitoso requeriría de una ventana temporal mayor al definido en el alcance de esta revisión así como un nivel de especialización alto.
3 – 4	**Bajo**	Riesgo muy reducido de que un usuario no asociado a la organización sea capaz de acceder a la infraestructura inalámbrica existente. El impacto que puede tener sobre la infraestructura es limitado.
5 - 6	**Medio**	Existe la posibilidad no despreciable de modificación de información, robo de credenciales o modificación del comportamiento normal del sistema, aunque las consecuencias para el sistema son limitadas. Este ataque es viable dentro de un marco temporal inferior a 1 mes.
7 - 9	**Alto**	La probabilidad de que ocurra un acceso no autorizado a los activos de la Organización es alta, debido principalmente a la existencia de debilidades en las redes inalámbricas existentes. Un atacante podrá impactar significativamente en la operación normal de los sistemas.
10	**Crítico**	La probabilidad de que ocurra un acceso no autorizado en los activos de la organización es muy elevada, debido a la existencia de redes inalámbricas que tienen visibilidad de sistemas internos y que pueden ser accedidas por usuarios externos.

Fuente: (OWISAM, 2013)

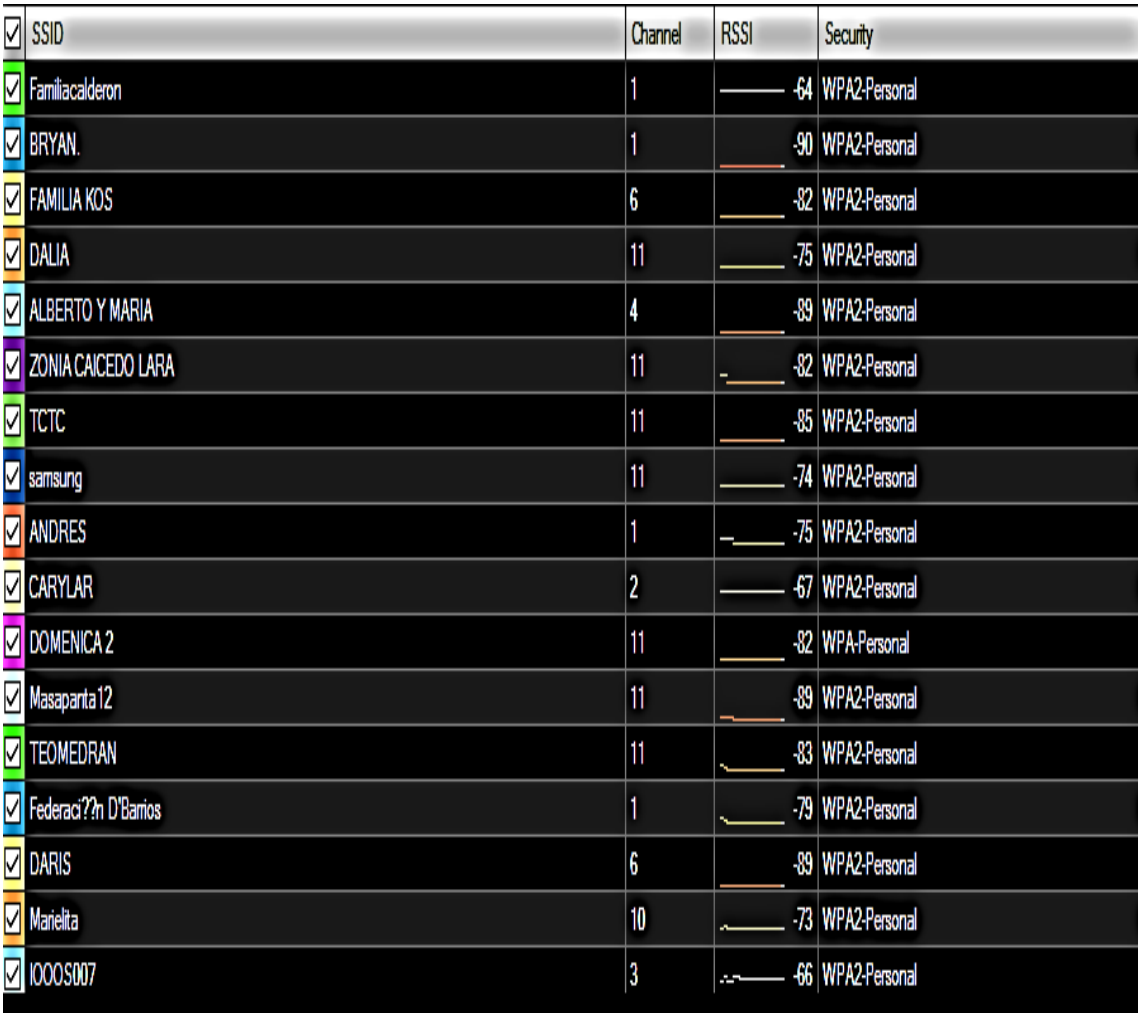
Anexo 3. Redes capturadas por la herramienta Inssider

CANAL	SSID	SEGURIDAD
1	TDA1802	WEP
	ALEXANDER	
	BRYAN	WPA2
	Almaces Paris	
	ZulemaINN4PB	
	TELECOMVAS	
	Vikitiki	
	SALON VERDE	
	dora_giraldo	
	ESTUDIO FOTOGRAFICO	
	Jose Cortes	
	Guidoley	
	Carlos Espana	
2	TDA1739	WPA2
	NAIMA	
3	Cesar	WPA2
	Zhang bo	
	JME	
4	ALBERTOYMARIA	WPA2
	Ofor	
	COPIADORA	
	CASTILLO H.	
	SHOPING2	
5	PUNTONET_MUJICA	WPA2
	JPDA-Esmeraldas	
	HOTELVISTA	
6	TELECOMVAS_2013	WEP
	FAMILIAKOS	WPA2
	LACASADELESTILISTA	
	Bigboy	
	Calzado Gonzalez	
	MARIA	
	TALENTO	
	BIKINIOPENWIFIF	
	Wdh	

7	SCAP040	WPA2
	Oro la tola	
8	LUCIANA	WEP
	CENTRO_AGRICOLA_ESMERALDAS	WPA2
	MIRIA1	
9	Apolo	WPA2
	ADRIAN BERMUDEZ	
	PLANFAILIA	
10	Marielita	WPA2
11	GADPE	WEP
	DALIA	WPA2
	KLEBER VERA	
	Wilson	
	MOVISTAR	
	Juridico Asociados	
	Compaq	
	Nany0328	
	JUPA	
	KARTBAR	
	GObp0	
	Promotores	
	LUIS	
	MARTINEZ	
	RAQUEL PEREZ	
	SANIMORE	
	MODA	
	Abogados	
	INTERNET CNT	
	LAREBAJA	
	Araceli	
	Carlos Espana	

Fuente: Inssider

Anexo 4. Funcionamiento de la herramienta Inssider



SSID	Channel	RSSI	Security
Familiacalderon	1	-64	WPA2-Personal
BRYAN.	1	-90	WPA2-Personal
FAMILIA KOS	6	-82	WPA2-Personal
DALIA	11	-75	WPA2-Personal
ALBERTO Y MARIA	4	-89	WPA2-Personal
ZONIA CAICEDO LARA	11	-82	WPA2-Personal
TCTC	11	-85	WPA2-Personal
samsung	11	-74	WPA2-Personal
ANDRES	1	-75	WPA2-Personal
CARYLAR	2	-67	WPA2-Personal
DOMENICA 2	11	-82	WPA-Personal
Masapanta12	11	-89	WPA2-Personal
TEOMEDRAN	11	-83	WPA2-Personal
Federaci??n D'Barrios	1	-79	WPA2-Personal
DARIS	6	-89	WPA2-Personal
Marielita	10	-73	WPA2-Personal
IOOOS007	3	-66	WPA2-Personal

Fuente: Inssider