Tipo de artículo: Artículo original

Análisis de seguridad de las redes inalámbricas en la carrera de Tecnologías de Información

Security analysis of wireless networks in the Information Technology career

Edwin Antonio Mero Lino [1*], https://orcid.org/0000-0003-4456-1734
María Mercedes Ortiz Hernández [2], https://orcid.org/0000-0002-2757-9345
Jamileth Monserrate Yanangómez Zambrano [3], https://orcid.org/0000-0003-4881-5922
Alberto Rodríguez Rodríguez [4], https://orcid.org/0000-0002-1238-0106

[1] Universidad Estatal del Sur de Manabí, Facultad de Ciencias Técnicas, UNESUM. edwin.mero@unesm.edu.ec
[2] Universidad Estatal del Sur de Manabí, Facultad de Ciencias Técnicas, UNESUM. maria.ortiz@unesm.edu.ec
[3] Universidad Estatal del Sur de Manabí, Facultad de Ciencias Técnicas, UNESUM. ymyz1997@hotmail.com
[4] Universidad Estatal del Sur de Manabí, Facultad de Ciencias Técnicas, UNESUM. alberto.rodriguez@unesum.edu.ec

*** Autor para correspondencia:** edwin.mero@unesm.edu.ec

Resumen

La investigación de este proyecto fue realizada y puesta en marcha tomando en cuenta la importancia de las redes inalámbricas y la seguridad en cuanto al tráfico de información en general, con el objetivo de encontrar protocolos, normas y métodos de seguridad por medio de un "Análisis de seguridad de las redes inalámbricas" la misma que fue realizado por medio de diferentes métodos de investigación histórico-lógico, inductivo-deductivo y bibliográfico, y programas de auditorías de redes, contribuyendo de manera significativa en el transcurso de la investigación. Como resultado se logró determinar cierta variedad de protocolos de seguridad y de diferentes métodos que permitirán mejorar la integridad de los datos y la seguridad de la información, por medio del Hacking ético se concluye que utilizando nuevos protocolos y métodos de seguridad se logrará obtener resultados factibles y valiosos en la protección de información de la red inalámbrica.

Palabras clave: auditorias; hacking; integridad; protocolos.

Abstract

The research of this project was carried out and launched taking into account the importance of wireless networks and security in terms of information traffic in general, with the aim of finding protocols, standards and security methods by means of an "Analysis security of wireless networks ", which was carried out by means of different methods of inquiry and historical-logical, inductive-deductive and bibliographic research, and network audit programs, contributing significantly in the course of the investigation. As a result, it was possible to determine a certain variety of security protocols and different methods that will allow to improve the integrity of the data and the security of the information, through ethical Hacking it is concluded that using new protocols and security methods it will be possible to obtain feasible results and valuable in protecting wireless network information.

Keywords: *audits; hacking; integrity; protocols.*

Recibido: 10/04/2021
Aceptado: 20/07/2021

Introducción

Las redes inalámbricas son de gran utilidad, las cuales son muy utilizadas en la actualidad por ser un gran medio de comunicación flexible en las diferentes organizaciones. Estas redes tienen gran acogida en la mayoría de instituciones estudiantiles por las ventajas que ofrecen a los usuarios, pero también presenta ciertos inconvenientes o problemas por ser transmitida por medio de ondas de radio, creando dificultad en mantener la información completamente segura de algún tipo de ataque en la red.

Según (Cedeño, 2019) expresa en su investigación sobre las amenazas y vulnerabilidades en la red, que la seguridad informática es unas de las partes más importante dentro de las empresas, porque esta permite dar protección a la integridad, privacidad y confidencialidad de los datos e información que se dan dentro de ella.

Un ataque informático consiste en que un individuo, mediante un sistema informático, intenta tomar el control, desestabilizar o dañar otro sistema informático, ya sea el caso de un host, una red privada o un servidor, lo cual tendrá como consecuencia perdida de información y/o pérdidas económicas en alguna organización (Medina Rojas et al., 2019).

En la actualidad los estudiantes no cuentan con la seguridad que necesitan la red de su carrera, permitiendo así crear gran vulnerabilidad en el tráfico de información y en la confidencialidad y privacidad de su información, para ello, existen protocolos de seguridad los cuales pueden lograr optimizar la seguridad de los datos y de esta manera mantener un control en dicha red.

La carrea de Tecnología de Información puede evitar este problema, basta con investir un poco y conectar sus equipos con medios cableados; otro factor que impide el buen rendimiento en la red es el tipo de cifrado que se utiliza para conecta a estudiantes, pues actualmente existen diversos protocolos de para las redes inalámbricas como el WEP, WPA y WPA2. 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 la los estudiantes que necesitan conectarse a Internet, 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.

Materiales y métodos

La información del presente artículo de investigación, se obtuvo de las publicaciones de los medios especializados en la temática como: libros, artículos, tesis, que permitió evidenciar y realizar el análisis de seguridad de las redes inalámbricas. Para el desarrollo de este proyecto se consideró la población participante de 910 estudiantes de la carrera de Tecnologías de la Información de la Universidad Estatal del Sur de Manabí, el cual se obtuvo una muestra por medio de formula dando el siguientes resultado de 368 estudiantes, misma que permitió realizar una encuesta sobre la situación actual de seguridad de las redes inalámbricas de la carrera de Tecnologías de la Información.

Fundamento teórico

(Según J et al., 2015), desarrollaron un estudio como resultado de la investigación del proyecto "Diagnóstico de seguridad informática aplicado a una muestra de organizaciones de la ciudad de Tunja", financiado por la Universidad Santo Tomás Seccional Tunja, en la que recopilaron información que fue analizada y a través de ella se tomó la decisión de utilizar las técnicas "Warchalking y Wardriving" en una representación significativa de redes inalámbricas de empresas públicas, privadas, entidades educativas y hogares; ubicados geográficamente en diferentes sectores de la ciudad; en la que tuvieron como resultado diferentes niveles de riesgo con respecto a configuraciones de tecnología de algunos dispositivos de las entidades públicas, privadas y sectores residenciales que mejorarán el nivel de seguridad por medio de buenas prácticas a nivel de configuración y uso de estas redes.

Según, (Sánchez E et al., 2018) llevaron una investigación sobre la aplicación de una metodología de seguridad avanzada en redes inalámbricas creada en base a las necesidades que presenta la Universidad Católica del Ecuador con Sede en la ciudad de Ibarra, demostraron que las redes WLAN (802.11) se utilizan actualmente para brindar acceso a Internet a hogares e instituciones, esto con el propósito de disminuir un conjunto de cableado que suele ser incómodo para espacios pequeños en donde se realiza su instalación, pero así mismo se han creado diferentes tipos de usuarios con fines maliciosos los cuales aprovechan el tráfico de datos por aire para realizar el robo de datos e información confiable que ingresa el usuario mediante la Red Inalámbrica que utiliza.

(Rosario V et al., 2019) realizaron la evaluación de una red inalámbrica de banda ancha para VoIP, en la provincia de Huaytará para la conectividad y acceso a Internet, el propósito de los investigadores era verificar y evaluar los parámetros de rendimiento que tenía la Red Inalámbrica en la que muchos usuarios accedían diariamente a realizar

diferentes trámites. En cuanto a la evaluación de los parámetros de QoS se determinó que son favorables para las aplicaciones multimedia que desee utilizar el usuario a través de su navegación, a su vez, determinaron que los usuarios que acceden a esta red tienen disponibilidad de 2.4G y de 65 Mbps en la banda de 5.8G contando con un nivel de seguridad mínimo sobre los que deberían de constar.

Los investigadores analizaron el funcionamiento de los algoritmos de cifrado sobre los cuales funcionan los protocolos WEP, WPA y WPA2 con el fin de proporcionar una visión de cómo y por qué protocolos inalámbricos de protección y cifrado deben lograr una base más científica para detectar y prevenir ataques, además de lograr como resultado suplir las falencias asociadas a los algoritmos de encriptación que se presentan en la actualidad. (Méndez M et al., 2015).

(Bermúdez Castro 2016) realizó un proyecto con el objetivo de sugerir una herramienta para realizar auditorías de seguridad inalámbrica, existen aspectos que no se toman en cuenta en una auditoria, y el esquema que se detalla en este documento deja claro que una red inalámbrica con encriptación WPA y WPA2, es vulnerable a una variedad de ataques.

La metodología utilizada por la investigadora propone un ataque “tipo pichinga” en donde se consigue engañar a los usuarios autorizados para que revelen información que compromete la integridad del sistema, además sugiere el uso de la herramienta Linset en este proyecto de titulación, y así mismo también busca recomendar a los usuarios sobre las medidas de seguridad que se deben tener en cuenta al configurar una Red Inalámbrica y el establecimiento de contraseñas seguras.

Resultados y discusión

Ballesteros, Chaparro (2016) en su investigación propusieron la realización de una auditoria en redes bajo funcionamiento de protocolo IEEE 802.11xx, las cuales son redes utilizadas para la comunicación entre dispositivos de casa y oficina, dicha investigación fue realizada para ejecutar la verificación de la seguridad que garantizan las mismas y demostrar que son factibles para el uso que se les designe. Además utilizaron un software libre que funciona bajo Sistema Operativo LINUX, específicamente con la suite de Aircrack; y como resultado de este procedimiento los autores presentan la auditoria de las redes que funcionan con encriptación WEP y WPA, populares y utilizadas en redes inalámbricas de este tipo; concluyendo así de esta manera con los diferentes tipos de ataques disponibles por mencionar, conocidos como sniffers, ataques de denegación de servicio y autenticaciones falsas con clonación de direcciones MAC, particularmente.

(Toshiro B et al., 2019) presentan su investigación los delitos informáticos actualmente que generan un riesgo exponencial en las organizaciones, mismos que son realizados por personal interno, siendo la medida de seguridad más usual la implementación de sistemas de detección de intrusos para detectar incidentes de seguridad, así como la restricción de acceso a cierto tipo de información o dominios web.

(Gonzáles et al., 2016) elaboraron una propuesta de protocolos de seguridad para la Red Inalámbrica local de la Universidad de Cienfuegos de Cuba, a través de ella examinaron los diferentes protocolos para la seguridad de las redes WLAN tales como: WEP, 802.11i, WPA y WPA2, y a su vez examinaron el tipo de cableado con la que contaba la institución actualmente. Para cumplir el objetivo de la investigación, realizaron previamente un análisis comparativo entre todos los protocolos de seguridad a utilizar en la red local WLAN (Wireless Local Área Network) basándose en el método de autenticación y la técnica de cifrado de cada uno de ellos, se debía de estudiar cada uno de ellos minuciosamente para poder así eliminar la red de extensos cableados, por transmisiones de ondas de aire en las que el usuario puede transmitir sus datos a través de ondas de radio de forma inalámbrica y puntos de acceso (AP).

Con respecto al análisis estadístico de las encuesta a los estudiantes de la Carrera de Tecnologías de la Información, sobre el análisis de seguridad de las redes inalámbricas. Se tiene los siguientes resultados.

1. ¿Usted considera necesario analizar las redes inalámbricas cada determinado tiempo para mantener un mejor control de seguridad?

Tabla 1. Resultado de la pregunta N° 1 de la encuesta.

Alternativas	Cantidad	Porcentajes
Si	100%	100%
No	0	0%
Total	368	100%

Mediante la obtención de información de la pregunta N°1 realizada en las encuestas, se logró determinar que el total de los estudiantes encuestados el 100% consideran necesario analizar las redes inalámbricas cada determinado tiempo para mantener un control optimo en las mismas.

El análisis de seguridad contribuirá significativamente al personal administrativo y estudiantes, ayudando a optimizar la seguridad en la gestión académica y cumpliendo con los pilares de la seguridad informática.

2. ¿Usted considera importante la inclusión de normas y protocolos de seguridad para resguardar con mayor eficacia la Información de la red de su carrera?

Tabla 2. Resultado de la pregunta N° 2 de la encuesta.

Alternativas	Cantidad	Porcentajes
Si	184	50%
No	184	50%
Total	368	100%

Como se logra observar en la pregunta N°2 por medio de los datos obtenidos en la interrogante antes expuesta, se determinó que el 50% de los estudiantes encuestados consideran de gran relevancia la inclusión de normas o protocolos de seguridad, mientras que un 50% consideran que no existe gran impacto en la implementación de protocolos o modelos de seguridad.

La incorporación de protocolos normas y métodos de seguridad podría crear un cambio significativo, creando un nivel de seguridad alto, ayudando a eliminar gran parte de los distintos problemas o dificultades en la red.

3. ¿Usted qué tipo de autentificación considera que presentan las redes Inalámbricas de su carrera?

Tabla 3. Resultado de la pregunta N° 3 de la encuesta.

Alternativas	Cantidad	Porcentajes
WPA	239	65%
WPA2	129	35%
No conozco ninguno	0	0%
Total	368	100%

Mediante la obtención de información recolectada a través de la pregunta 8 realizada en la pregunta antes expuesta se logró determinar que, un 65% de estudiantes consideran importante usar el tipo de autentificación WPA, mientras que el 35% restante considera más óptima la autentificación WPA2. Conocer el tipo de autentificación es de gran relevancia en el manejo de red puesto que la seguridad parte de ello. Es recomendable usar el tipo de autentificación WPA2 por tener menos errores y ser más actualizada que otros tipos de autentificación.

4. ¿Usted considera importante realizar hacking ético para exponer el nivel de seguridad de una red inalámbrica?

Tabla 4. Resultado de la pregunta N° 4 de la encuesta.

Alternativas	Cantidad	Porcentajes
Si	276	75%
No	92	25%
Total	368	100%

A través de los datos obtenidos en la interrogante N°4 expuesta anteriormente, se logró determinar por el total de estudiantes encuestados que un 75% cree que realizar hacking ético si brindara exponer información de la red, mientras que un 25% considera poco fiable la utilización de este método.

El hacking ético es considerado como un método de seguridad permitiendo conocer cuál es la seguridad actual de la red, su aplicación es recomendada mientras sea usada de la manera correcta y cumpliendo con las normas de seguridad apropiadas, con el único fin de mejorar falencias en la red.

Conclusiones

Como resultado se logró determinar cierta variedad de protocolos de seguridad y de diferentes métodos que permitirán mejorar la integridad de los datos y la seguridad de la información, por medio del Hacking ético se concluye que utilizando nuevos protocolos y métodos de seguridad se logrará obtener resultados factibles y valiosos en la protección de información de la red inalámbrica de la carrera de Tecnologías de Información de la Universidad Estatal del Sur de Manabí.

Conflictos de intereses

Los autores de la presente investigación declaran que no poseen conflictos de intereses.

Contribución de los autores

1. Conceptualización: Edwin Antonio Mero Lino, María Mercedes Ortiz Hernández, Jamileth Monserrate Yanangómez Zambrano, Alberto Rodríguez Rodríguez.
2. Curación de datos: Edwin Antonio Mero Lino, Alberto Rodríguez Rodríguez.
3. Análisis formal: Edwin Antonio Mero Lino.
4. Investigación: María Mercedes Ortiz Hernández, Alberto Rodríguez Rodríguez.

5. Metodología: Edwin Antonio Mero Lino, Jamileth Monserrate Yanangómez Zambrano.
6. Administración del proyecto: María Mercedes Ortiz Hernández, Alberto Rodríguez Rodríguez.
7. Recursos: María Mercedes Ortiz Hernández.
8. Supervisión: María Mercedes Ortiz Hernández, Alberto Rodríguez Rodríguez.
9. Validación: Edwin Antonio Mero Lino, Jamileth Monserrate Yanangómez Zambrano.
10. Visualización: Edwin Antonio Mero Lino, Alberto Rodríguez Rodríguez.
11. Redacción – borrador original: Edwin Antonio Mero Lino, María Mercedes Ortiz Hernández, Jamileth Monserrate Yanangómez Zambrano, Alberto Rodríguez Rodríguez.
12. Redacción – revisión y edición: Edwin Antonio Mero Lino, María Mercedes Ortiz Hernández, Jamileth Monserrate Yanangómez Zambrano, Alberto Rodríguez Rodríguez.

Financiamiento

La investigación no requirió fuente de financiamiento.

Referencias

Ballesteros, J., & Chaparro, F. (2016). Seguridad en Redes Inalámbricas de Acceso Local Bajo. TECNIA Vol. 26 No1, 57-64.

Bermúdez Castro, E. (2016). Análisis de uso y ventajas de Linset para auditorías de redes inalámbricas con encriptación WPA Y WPA2. Tesis de grado. Universidad de Guayaquil, Guayaquil.

Cedeño, B. L. (2019). Análisis de amenazas y vulnerabilidades en la red. Obtenido de dspase: http://dspace.utb.edu.ec/bitstream/handle/49000/7943/CAIZA%20CEDE%C3%91O.pdf?sequence=1&isAllowed=y

Gonzáles Paz, A., Casanova Beltrán, D., & Fuentes Gari, E. R. (2016). PROPUESTA DE PROTOCOLOS DE SEGURIDAD PARA LA RED INALÁMBRICA LOCAL DE LA UNIVERSIDAD DE CIENFUEGOS. ISSN 2218-3620.

Medina Rojas, J. D., & Rivas Montalvo, Y. Y. (2019). Evaluación del Rendimiento de un Sistema de Detección de Intrusos para Redes Inalámbricas 802.11 Contra Ataques Informáticos. Tesis de Pregrado. UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO, LAMBAYEQUE.

Méndez Moreno, W. A., Mosquera Palacios, D. J., & Trujillo Rivas, E. (2015). Vulnerabilidad de protocolos de encriptación WEP, WPA y WPA2 en Redes. Tecnura • p-ISSN: 0123-921X • e-ISSN: 2248-7638 , 79-87.

Monsalve Posada, J. F., Londoño Arias, A., & Mejía Arango, J. G. (2015). Desempeño de redes inalámbricas y redes industriales inalámbricas en procesos de control en tiempo real bajo ambientes industriales. Tecno Lógicas, 87-99.

Sánchez Espinosa, F., Garcia Vivero, J., & Llanos Baroja, D. (2018). Aplicación de una metodología de seguridad avanzada en redes inalámbricas. RISTI.

Rosario Villareal, M. A., Marño Arroyo, J. B., Márquez Camarena, J., & Núñez Lira, L. A. (2019). Evaluación de una red inalámbrica de banda ancha para VoIP. On-line ISSN 1390-6542versión impresa ISSN 1390-9363.

Toshiro Nagata, B., Rivas Almonte, F., & Toro Flores, Y. (2019). Análisis de seguridad en tráfico de redes empleando minería de datos. RISTI, Nº E21, 314–326.