Tipo de artículo: Artículo original

Seguridad informática en redes inalámbricas

Computer security in wireless networks

Oscar Stalin Baque Pinargote [1*], **https://orcid.org/0000-0003-1954-211X**
José Efraín Álava Cruzatty [2], **https://orcid.org/0000-0002-2133-7556**
Julio Alberto Cedeño Ferrin [3], **https://orcid.org/0000-0001-5069-378X**
Gabriela Nicole Ponce Robles[4], **https://orcid.org/0000-0003-1746-2212**

[1] Ingeniero en Sistemas y Máster en Telecomunicaciones. Personal académico auxiliar Profesor, Miembro de la Comisión de Titulación de la carrera. Universidad Estatal del Sur de Manabí. Jipijapa, Manabí – Ecuador. Portoviejo, Manabí, Ecuador. Correo electrónico: oscar.baque@unesum.edu.ec
[2] Ingeniero en Telecomunicaciones y Máster en Telecomunicaciones. Personal académico auxiliar Profesor, Miembro de la Comisión de Aseguramiento de la Calidad de la carrera de Tecnologías de la Información. Universidad Estatal del Sur de Manabí. Jipijapa, Manabí – Ecuador. Doctorante de la Universidad Nacional de Piura; Portoviejo, Manabí, Ecuador. Correo electrónico: jose.alava@unesum.edu.ec
[3] Ingeniero. Docente de la carrera de Tecnologías de la Información de la Facultad Ciencias Técnicas de la Universidad Estatal del Sur de Manabí, Jipijapa, Ecuador. Correo electrónico: julio.cedeno@unesum.edu.ec
[4] Ingeniera en Tecnologías de la Información. Docente de la Unidad Educativa "Nuestra Señora de la SABIDURIA" Lomas de Sargentillo, Guayas. Correo electrónico: ponce-gabriela2423@unesum.edu.ec

*** Autor para correspondencia: oscar.baque@unesum.edu.ec**

Resumen

En la actualidad es necesario realizar el análisis que permitan la seguridad informática en redes inalámbricas, estas son utilizadas en varias organizaciones y entidades por su fácil instalación, conexión y su económico costo. El propósito de esta investigación es dar a conocer cómo prevenir las vulnerabilidades de la red inalámbrica, aumentando la inseguridad de la información y la confianza de los usuarios. En estas redes la información viaja por medio de ondas de radio quedando la información vulnerable a los ataques con fines maliciosos, aprovechándose de que los protocolos existentes ya no son seguros, un análisis cada cierto tiempo aporta seguridad en las redes, de esta forma se evita ataques cibernéticos, para detectar las vulnerabilidades, se utilizan herramientas que permitan observar el nivel de seguridad verificando ataques, las indicaciones recomendadas, permiten mejorar la seguridad en la red inalámbrica. Se utilizó una metodología de enfoque cuantitativo, exploratorio, utilizando métodos científicos del nivel teórico y empírico, los que facilitaron el análisis para determinar la seguridad de las redes inalámbricas y su importancia en la actualidad, se realizaron encuestas para conocer el grado de conocimiento acerca del tema tratado. Los resultados dieron las pautas necesarias para enfrentar los desafíos de estar actualizados en lo referente a la seguridad de las redes inalámbricas, aplicando herramientas tecnológicas que permitan detectar falencias. Se concluyó que es necesario tener un plan de acción preventivo y cumplir con las políticas de seguridad.

Palabras clave: ciberseguridad; herramientas tecnológicas; vulnerabilidad.

Abstract

At present it is necessary to carry out the analysis that allows computer security in wireless networks, these are used in various organizations and entities for their easy installation, connection and their economic cost. The purpose of this research is to make known how to prevent vulnerabilities in the wireless network, increasing the insecurity of information and the trust of users. In these networks, the information travels by means of radio waves, leaving the information vulnerable to attacks for malicious purposes, taking advantage of the fact that the existing protocols are no longer secure, an analysis from time to time provides

security in the networks, thus avoiding cyber-attacks, to detect vulnerabilities, tools are used to observe the level of security by verifying attacks, the recommended indications allow improving security in the wireless network. A quantitative, exploratory approach methodology was used, using scientific methods of the theoretical and empirical level, which facilitated the analysis to determine the security of wireless networks and their importance today, surveys were conducted to find out the degree of knowledge about the treated topic. The results gave the necessary guidelines to face the challenges of being up-to-date regarding the security of wireless networks, applying technological tools that allow detecting shortcomings. It was concluded that it is necessary to have a preventive action plan and comply with security policies.

Keywords: *cybersecurity; Technological tools; vulnerability.*

Recibido: 08/01/2023
Aceptado: 26/03/2023
En línea: 01/04/2023

Introducción

El uso de las tecnologías de la información y redes WiFi es cada vez más extenso en el mundo, por tal razón, la seguridad informática hoy en día es un tema de preocupación e importancia para cualquier empresa u organización, lo que significa que las entidades deben reconsiderar por completo la forma de proteger sus redes y dispositivos, las vulnerabilidades aumentan cada momento que pasa, las redes inalámbricas están propensas a ataques, que conllevan la exposición de activos críticos y la revelación de información confidencial.

Las redes WiFi facilitan la conectividad de las personas en todo momento y en cualquier lugar. Sin embargo, pese a todas sus ventajas, también presentan ciertos riesgos de los que se debe ser consciente a la hora de usar una red de este tipo, especialmente si se trata de una red pública (Pacheco & Rodríguez, 2013; Rodríguez, 2016; Rodríguez et al., 2021).

Las Redes Inalámbricas de Área Local (WLAN) en la actualidad son utilizadas por organizaciones, universidades, debido a su fácil instalación y conexión como también a sus bajos costos. En este tipo de redes la información viaja por medio de ondas de radio quedando la información vulnerable a ataques por personas con fines maliciosos y más aún cuando los protocolos existentes ya no son considerados seguros (Mendoza et al., 2017).

Se han realizado estudios en diferentes países en cuanto a la seguridad de las redes inalámbricas, dando resultados alarmantes de la situación de las mismas. Según estudios internacionales realizados en Bolivia, México, Uruguay, Argentina, Canadá, España y entre otros se dice que, de 905 redes, 374 el 41.33% disponen de algún sistema de cifrado, mientras que de 531 redes el 2 58.37% carecen de cifrado (González, 2019), (Álava et al., 2022).

Ecuador también se ve afectado por estos problemas de seguridad en las redes inalámbricas, debido a los diferentes ataques que se han efectuado en las páginas web del gobierno. A raíz de este acontecimiento se ha puesto más interés

a las seguridades que deben poseer las organizaciones para prevenir ataques. En el área de la seguridad en redes según un estudio realizado en la ciudad de Quito empleando programas informáticos para estos fines, se dice que un 93% de las redes inalámbricas son vulnerables a ataques maliciosos (Sánchez, 2021), (de la Parra Aguirre & Morales-Sandoval, 2019).

Se puede decir que dentro del uso de redes existen sus ventajas y flexibilidad, pues, dentro de la zona de cobertura de la red inalámbrica los nodos se podrán comunicar y no estarán atados a un cable para poder estar comunicados.

En ocasiones la falta de planificación afecta, por ejemplo, lo relacionado a las redes cableadas. Antes de cablear un edificio o unas oficinas se debe pensar mucho sobre la distribución física de las máquinas, mientras que con una red inalámbrica sólo nos tenemos que preocupar de que el edificio o las oficinas queden dentro del ámbito de cobertura de la red.

Es importante el diseño, los receptores son bastante pequeños y pueden integrarse dentro de un dispositivo y llevarlo en un lugar estratégico, ante eventos inesperados que pueden ir desde un usuario que se tropieza con un cable o lo desenchufa, hasta un pequeño terremoto o algo similar. Una red cableada podría llegar a quedar completamente inutilizada, mientras que una red inalámbrica puede aguantar bastante mejor este tipo de percances inesperados (Jurado-Calero et al., 2022).

Se llama comunicación inalámbrica a la que se lleva a cabo sin la intervención de cables. La telefonía móvil es el ejemplo más conocido de comunicación inalámbrica y ha tenido un desarrollo tan impresionante en estos últimos años que se ha convertido en más universal que la propia telefonía fija. El espectacular desarrollo de Internet y la introducción de dispositivos informáticos cada vez más personales (ordenadores portátiles, Tablet PC y PDA, especialmente) hace que los usuarios demanden con mayor asiduidad unas comunicaciones de datos más móviles, flexibles y cómodas (A. Rodríguez et al., 2022; A. R. Rodríguez, W. L. S. Álava, et al., 2022; A. R. Rodríguez, M. I. R. Castro, et al., 2022).

Las redes inalámbricas ofrecen algunos inconveniente que ha tenido siempre este tipo de comunicaciones ha sido la falta de un estándar que hiciese compatibles los equipos de distintos fabricantes, lo cual quedó superado en 1999 con la aparición de Wi-Fi. La tecnología Wi-Fi permite crear redes de área local inalámbrica de una forma fácil y manejable y, sobre todo, económica (Li et al., 2020).

Las redes inalámbricas de área local (WLAN) tienen un papel cada vez más importante en las comunicaciones del mundo de hoy (Fikriyadi et al., 2020). Debido a su facilidad de instalación y conexión, se han convertido en una

excelente alternativa para ofrecer conectividad en lugares donde resulta inconveniente o imposible brindar servicio con una red alambrada. La popularidad de estas redes ha crecido a tal punto que los fabricantes de computadores y motherboards están integrando dispositivos para acceso a WLAN en sus equipos; tal es el caso de Intel,1 que fabrica el chipset Centrino para computadores portátiles (Wang et al., 2019), (Zheng et al., 2021), (Fikriyadi et al., 2020).

Principales riesgos de seguridad informática en redes Wifi

Redes fraudulentas. En estos casos, un hacker o pirata informático configura redes que parecen ser legítimas y confiables. Usan un nombre atractivo y carecen de contraseña de conexión para hacerla aún más atractiva.

Sitios web de destino que otorgan acceso a la red. Sospecha de aquellas conexiones en las que necesitas entrar a una página web para poder usar la red. Muchos de estos sitios buscan tener acceso a los datos almacenados en tu computador o dispositivo móvil.

Gusanos. Son similares a todos los virus que pueden infectar tus dispositivos, solo hay una pequeña diferencia. Un virus convencional necesita un programa al cual adherirse, mientras que el gusano puede propagarse libremente. Si tus configuraciones de seguridad no están al día, puedes recibir un gusano de otro usuario conectado a la misma red.

Medidas débiles de seguridad. Un gran problema a la hora de usar conexiones inalámbricas es que algunos propietarios redes no se preocupan por darles suficiente seguridad. Si las contraseñas son débiles cualquier usuario puede compartir conexión y acceder a tu información.

Robo de datos. La interacción por medio de redes WiFi que no son seguras, deja abierta la puerta para que ojos que no quieres cerca puedan ver tus archivos multimedia, servicios de mensajería instantánea e incluso datos financieros, corporativos y que violan la propiedad intelectual.

Pérdida de velocidad de ancho de banda. Una red que no está bien configurada es fácil de intervenir. Por eso es importante que haya mecanismos de protección que eviten tener cientos de usuarios conectados dividiendo y reduciendo el ancho de banda.

Uso de la red para propósitos ilegales. Los intrusos también pueden llegar a usar tus datos y tu conexión para cometer cualquier tipo de delito. Las repercusiones legales pueden caer sobre el dueño oficial de la red.

Es recomendable evitar exponerse a todos estos riesgos y conéctate solamente a las redes de confianza y a las que siguen protocolos adecuados de seguridad, así se evita la posibilidad de perder tu privacidad y poner en riesgo los datos que no quieres que caigan en manos de los ciberdelincuentes.

Es necesario garantizar la seguridad de una red inalámbrica:

Se considera una red inalámbrica segura, cuando cumple con los siguientes requisitos:

- Las ondas de radio deben confinarse tanto como sea posible. Esto es difícil de lograr totalmente, pero se puede hacer un buen trabajo empleando antenas direccionales y configurando adecuadamente la potencia de transmisión de los puntos de acceso.
- Debe existir algún mecanismo de autenticación en doble vía, que permita al cliente verificar que se está conectando a la red correcta, y a la red constatar que el cliente está autorizado para acceder a ella.
- Los datos deben viajar cifrados por el aire, para evitar que equipos aje nos a la red puedan capturar datos mediante escucha pasiva (Wang et al., 2019).

Materiales y métodos

El presente estudio se realizó por docentes de la carrera de Tecnologías de la Información de la Facultad Ciencias Técnicas, aplicando en la investigación un enfoque cuantitativo, de carácter exploratorio, utilizando métodos científicos del nivel teórico y empírico:

Teórico: análisis – síntesis: se utilizó para determinar la seguridad de las redes inalámbricas y su importancia en la actualidad. El método histórico – lógico: se usó en la construcción de la investigación determinando ventajas específicas y características del tema tratado.

Del nivel empírico se utilizó el método revisión bibliográfica: el que permitió la búsqueda y recopilación de la información para la elaboración de la investigación, mediante documentos web, sitios web, artículos científicos, libros, entre otros.

Encuestas: realizadas a 200 personas perteneciente a la carrera Tecnologías de la Información.

Estadístico – Matemático: para conocer los resultados reales de las encuestas realizadas.

Resultados y discusión

Se realizó una encuesta con las preguntas pertinentes, las que permitieron conocer la importancia de expandir este conocimiento acerca de las redes inalámbricas y su seguridad, así como realizar un respectivo análisis cada cierto tiempo en las redes con el uso de herramientas tecnológicas, algunas de las preguntas más relevantes fueron:

1 ¿Consideras usted segura las redes inalámbricas que se utilizan en su institución?

Tabla 1: Resultado sobre si consideras usted segura las redes inalámbricas que se utilizan en su institución.

Opción	Respuestas	Porcentaje
SI	60	35%
NO	140	65%
TOTAL	200	100%

Se puede apreciar como resultado que el 35% si consideras segura la red inalámbrica, mientras que un 65% piensa que la seguridad no es segura y que podría mejorarse.

2 ¿Conoce usted los diferentes tipos de redes inalámbricas?

Tabla 2: Resultado sobre si conoce usted los diferentes tipos de redes inalámbricas.

Opción	Respuestas	Porcentaje
SI	50	25%
NO	150	75%
TOTAL	200	100%

Se obtuvo un resultado: el 25 % favorable que conocen los diferentes tipos de redes inalámbricas, mientras que un 75% no tiene conocimiento sobre el tema mencionado.

3 ¿Usted ha sufrido robo o pérdida de información por la inseguridad de las redes inalámbricas?

Tabla 3: Resultado sobre ha sufrido robo o pérdida de información por la inseguridad de las redes inalámbricas.

Opción	Respuestas	Porcentaje
SI	100	50%
NO	100	50%
TOTAL	200	100%

Se dio a conocer que el 50% han sufrido robo o pérdida de información por la inseguridad que existe en las redes inalámbricas, mientras que un 50% no ha sufrido está perdida.

4 ¿Considera usted importante conocer cómo mejorar la seguridad de las redes inalámbricas?

Tabla 4: Resultado sobre si considera usted importante conocer cómo mejorar la seguridad de las redes inalámbricas.

Opción	Respuestas	Porcentaje
SI	150	75%
NO	50	25%
TOTAL	200	100%

Esta pregunta dio como resultado, el 75 % cree importante conocer cómo mejorar la seguridad de las redes inalámbricas, mientras que un 25% no conoce la importancia de mejorar la seguridad de las redes.

Los resultados de las encuestas dan las pautas necesarias para saber que la sociedad se enfrenta a los desafíos de estar actualizados con lo referente a la seguridad de las redes inalámbricas, aplicando herramientas tecnológicas que permitan detectar estas falencias.

Las 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. También, son definidas como 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 (Fikriyadi et al., 2020; Mendoza et al., 2017; Wang et al., 2019).

Conclusiones

Es necesario tener un plan de acción preventivo y la posibilidad de contratar un seguro para la red, para prevenir los ataques maliciosos y el uso indebido de los empleados que comprometan la privacidad de los datos de una organización.

Hacer cumplir las políticas de seguridad para uso inalámbrico, uso de contraseñas tanto dentro como fuera de sus instalaciones. Ya sea que una compañía haya autorizado o no el uso de tecnologías inalámbricas debe también realizar auditorías de software a sus empleados.

Las instituciones deben capacitar a los usuarios en materia de seguridad informática, así podrán detener ataques potenciales, y adoptar medidas para proteger a su organización a través de toda su red.

Conflictos de intereses

Los autores no poseen conflictos de intereses.

Contribución de los autores

1. Conceptualización: Oscar Stalin Baque Pinargote, José Efraín Álava Cruzatty, Julio Alberto Cedeño Ferrin, Gabriela Nicole Ponce Robles.
2. Curación de datos: Oscar Stalin Baque Pinargote, José Efraín Álava Cruzatty.
3. Análisis formal: Julio Alberto Cedeño Ferrin, Gabriela Nicole Ponce Robles.
4. Investigación: Oscar Stalin Baque Pinargote, José Efraín Álava Cruzatty.
5. Metodología: Oscar Stalin Baque Pinargote, José Efraín Álava Cruzatty.
6. Administración del proyecto: Oscar Stalin Baque Pinargote.
7. Software: Julio Alberto Cedeño Ferrin, Gabriela Nicole Ponce Robles.
8. Supervisión: Oscar Stalin Baque Pinargote.
9. Validación: Julio Alberto Cedeño Ferrin, Gabriela Nicole Ponce Robles.
10. Visualización: Julio Alberto Cedeño Ferrin, Gabriela Nicole Ponce Robles.
11. Redacción – borrador original: Oscar Stalin Baque Pinargote, José Efraín Álava Cruzatty, Julio Alberto Cedeño Ferrin, Gabriela Nicole Ponce Robles.
12. Redacción – revisión y edición: Oscar Stalin Baque Pinargote, José Efraín Álava Cruzatty, Julio Alberto Cedeño Ferrin, Gabriela Nicole Ponce Robles.

Financiamiento

La investigación no requirió fuente de financiamiento.

Referencias

Álava, W. L. S., Rodríguez, A. R., Ávila, X. L. A., & Cornelio, O. M. (2022). Redes inalámbricas, su incidencia en la privacidad de la información. *Journal TechInnovation*, *1*(2), 104-109. https://revistas.unesum.edu.ec/JTI/index.php/JTI/article/download/25/42

de la Parra Aguirre, R., & Morales-Sandoval, M. (2019). Esquemas de seguridad ligeros en aplicaciones de redes inalámbricas de área corporal. *Avances en Ciencias en Ingenierıa y Tecnologıas Computacionales-TopTamaulipas*, 25-27. https://www.tamps.cinvestav.mx/~mmorales/divulg/SWBAN.pdf

Fikriyadi, F., Ritzkal, R., & Prakosa, B. A. (2020). Security Analysis of Wireless Local Area Network (WLAN) Network with the Penetration Testing Method. *Jurnal Mantik*, *4*(3), 1658-1662. http://iocscience.org/ejournal/index.php/mantik/article/download/974/674

González, C. (2019). Desafíos de seguridad en redes 5G. *Technology Inside by CPIC*, *3*, 36-45. https://cpic-sistemas.or.cr/revista/index.php/technology-inside/article/download/47/47

Jurado-Calero, R., Castillo-Montes, C., Mera, M. V. V., & Ortiz, P. S. (2022). Red MESH como modelo alternativo de conectividad en instituciones de educación superior, caso de estudio Universidad Técnica Luis Vargas Torres de Esmeraldas. *Sapienza: International Journal of Interdisciplinary Studies*, *3*(2), 125-135. https://journals.sapienzaeditorial.com/index.php/SIJIS/article/download/314/189

Li, X., Huang, M., Liu, Y., Menon, V. G., Paul, A., & Ding, Z. (2020). I/Q imbalance aware nonlinear wireless-powered relaying of B5G networks: Security and reliability analysis. *IEEE Transactions on Network Science and Engineering*, *8*(4), 2995-3008. https://arxiv.org/pdf/2006.03902

Mendoza, C. M. H., Vidal, L. M. R., & Almanza, M. A. (2017). Análisis de seguridad en redes inalámbricas de las MiPyME y propuesta de mejora. *Revista Iberoamericana de Producción Académica y Gestión Educativa*, *4*(7). http://www.pag.org.mx/index.php/PAG/article/download/647/793

Pacheco, H., & Rodríguez, A. (2013). Gestión, tipos, gestión investigativa, enfoques. *Recuperado de: http://doctxs6. blogspot. com. co/2013/01/gestion-tipos-gestion-investigativa_27. html*.

Rodríguez, A. (2016). *La orientación profesional pedagógica hacia la Licenciatura en Educación Matemática-Física en el Preuniversitario* Doctoral Thesis). Universidad de La Habana].

Rodríguez, A., Escobedo, Y. V., García, L. J. P., & Lucas, H. B. D. (2021). Evaluación del aprendizaje mediante un enfoque constructivista a partir del método ponderación lineal. *Serie Científica de la Universidad de las Ciencias Informáticas*, *14*(7), 156-165. https://dialnet.unirioja.es/servlet/articulo?codigo=8590664

Rodríguez, A., Lucas, H. B. D., Mero, C. J. Á., Pisco, R. J. L., & Castro, F. I. G. (2022). Método computacional de recomendación sobre la evaluación del aprendizaje bajo el paradigma constructivista. *Serie Científica de la Universidad de las Ciencias Informáticas*, *15*(1), 178-187. https://dialnet.unirioja.es/servlet/articulo?codigo=8590599

Rodríguez, A. R., Álava, W. L. S., Jara, L. D. S., & Castro, F. I. G. (2022). Las Categorías Enseñanza, Aprendizaje; Desarrollo, Innovación Educativa y formación. Relaciones entre ellas. *Revista Científica Arbitrada Multidisciplinaria PENTACIENCIAS-ISSN 2806-5794.*, *4*(3), 178-183. http://www.editorialalema.org/index.php/pentaciencias/article/view/160

Rodríguez, A. R., Castro, M. I. R., Pilay, M. A. T., & Quimiz, L. R. M. (2022). Sistema inteligente para la evaluación de competencias docentes mediante un enfoque constructivista. *Revista Científica Arbitrada Multidisciplinaria PENTACIENCIAS-ISSN 2806-5794.*, *4*(2), 316-325. http://editorialalema.org/index.php/pentaciencias/article/view/63

Sánchez, P. C. A. (2021). Modelo de seguridad de la información en redes inalámbricas de tecnologías de la información para minimizar ataques de denegación de servicios. *INF-FCPN-PGI Revista PGI*, 149-152. https://ojs.umsa.bo/ojs/index.php/inf_fcpn_pgi/article/view/73/60

Wang, N., Wang, P., Alipour-Fanid, A., Jiao, L., & Zeng, K. (2019). Physical-layer security of 5G wireless networks for IoT: Challenges and opportunities. *IEEE Internet of Things Journal*, *6*(5), 8169-8181. https://people-ece.vse.gmu.edu/~kzeng2/publications/2019/Physical%20Layer%20Security%20of%205G%20Wireless%20Networks%20for%20IoT%20Challenges%20and%20Opportunities.pdf

Zheng, G., Gong, B., & Zhang, Y. (2021). Dynamic network security mechanism based on trust management in wireless sensor networks. *Wireless Communications and Mobile Computing*, *2021*, 1-10. https://www.hindawi.com/journals/wcmc/2021/6667100/