CIYA. Ciencias de la Ingeniería y Aplicadas, vol. 7 Nº 2, julio-diciembre de 2023, pp. 124-136

Estudio de la Seguridad de las Redes WLAN de la Zona Urbana de Latacunga

Study of the Security of WLAN Networks in the Urban Area of Latacunga

Diego Geovanny Falconí Punguil[1]

RESUMEN:

Este artículo aborda la seguridad de las redes WLAN en la zona urbana de Latacunga, evaluando la preferencia entre redes de acceso abierto y cerrado, así como las diferencias en seguridad entre los protocolos WEP, WPA y WPA2. La investigación, basada en un enfoque de campo, recopiló datos reales para analizar la aceptación y demanda de redes cerradas, revelando una clara preferencia en la población latacungueña. Los resultados indicaron que el protocolo WPA2 es el más empleado en redes cerradas, destacándose por su mayor seguridad en comparación con WEP y WPA. Estos hallazgos sugieren una creciente conciencia de seguridad inalámbrica y una tendencia hacia protocolos más avanzados. En conclusión, la investigación subraya la importancia de considerar estas preferencias en el diseño de políticas de seguridad para redes urbanas, tomando como referencia la ciudad de Latacunga, promoviendo prácticas más seguras y fomentando la adopción de medidas de encriptación más recientes.

Palabras claves: WEP, WPA, WPA2, Redes WLAN.

Recibido 30 de noviembre de 2023; revisión aceptada 8 de diciembre de 2023

ABSTRACT:

This article addresses the security of WLAN networks in the urban area of Latacunga, evaluating the preference between open and closed access networks, as well as the security differences among WEP, WPA, and WPA2 protocols. The research, based on a field approach, collected real data to analyze the acceptance and demand for closed networks, revealing a clear preference among the population of Latacunga. The results indicated that the WPA2 protocol is the most utilized in closed networks, standing out for its greater security compared to WEP and WPA. These findings suggest a growing awareness of wireless security and a trend towards more advanced protocols. In conclusion, the research emphasizes the importance of considering these preferences in the design of security policies for urban networks, using

[1] Universidad Técnica de Cotopaxi, Latacunga, Cotopaxi, Ecuador, diego.falconi4@utc.edu.ec

Latacunga as a reference, promoting safer practices, and encouraging the adoption of more recent encryption measures.

***Keywords**: WEP, WPA, WPA2, WLAN Networks.*

Recibido 30 de noviembre de 2023; revisión aceptada 8 de diciembre de 2023

1. INTRODUCCIÓN

Las redes inalámbricas constituyen un conjunto de dispositivos informáticos interconectados mediante ondas de radio o infrarrojo [1]. En particular, las redes de acceso local buscan proporcionar parámetros que fomenten la flexibilidad en la conectividad y el uso, la movilidad, minimizando el impacto estético en las instalaciones y optimizando la eficiencia de la infraestructura [2]. En 1996, el IEEE aprobó el estándar 802.11b o Wi-Fi para este tipo de redes [3]

Una Red de Área Local Inalámbrica (WLAN) abarca un área específica, como una red local empresarial, con un alcance aproximado de cien metros. Facilita la conexión entre terminales ubicadas dentro de su área de cobertura [1]. El rendimiento de esta red se define por el tráfico y el tamaño de los bytes de carga útil transmitidos durante el tiempo de espera [4]. Este análisis de rendimiento se utiliza para dimensionar y planificar la red, determinando el número máximo de dispositivos conectados y garantizando la velocidad de transferencia de información requerida para el servicio [6]. En la figura 1 se puede apreciar el esquema básico de las Redes WLAN en un hogar.

Figura 1. Esquema de redes WLAN en un hogar. [7]

En los últimos años, las redes WLAN han experimentado un aumento significativo en popularidad a medida que mejoran sus prestaciones y se descubren nuevas aplicaciones. Esta red, al ser móvil y eliminar la necesidad de cables, añade flexibilidad a la infraestructura, incrementando la productividad y eficiencia en las empresas donde está implementada. Los

usuarios en una red WLAN tienen la capacidad de transmitir y recibir voz, datos y video tanto dentro de edificios como entre edificios, campus universitarios e incluso áreas metropolitanas.

Las Redes de Área Local Inalámbrica, también conocidas como Wireless Local Area Network (WLAN), ofrecen notables ventajas que mejoran significativamente la vida cotidiana de la sociedad. No obstante, es crucial destacar sus desventajas, siendo la principal de ellas la vulnerabilidad a ataques de usuarios no autorizados, lo que plantea preocupaciones de seguridad [7]. Es relevante mencionar que las ondas electromagnéticas no se confinan fácilmente a una geografía limitada, lo que permite a un hacker escuchar la red si los datos transmitidos no están cifrados. Por ende, se deben implementar todas las medidas necesarias para asegurar la privacidad de los datos transmitidos a través de estas redes inalámbricas

En este tipo de redes, es común que los usuarios finales, entusiasmados por el auge alcanzado por las WLAN, adquieran e instalen equipos sin una planificación y diseño adecuados. Esto puede resultar en un rendimiento deficiente y, en casos extremos, en el robo de información [8]. Es fundamental recordar que el medio de comunicación de dispositivos inalámbricos es el espacio, y cualquier individuo con los dispositivos apropiados puede rastrear las señales y aprovechar los recursos de la red con fines malintencionados.

Históricamente, han existido tres métodos de encriptación para asegurar las redes WLAN. Desde finales de la década de 1990, los algoritmos de seguridad Wi-Fi han experimentado múltiples actualizaciones, con una depreciación gradual de los algoritmos más antiguos y una revisión sustancial de los algoritmos más recientes. En términos cronológicos, estos son:

A. WEP (Wired Equivalent Privacy)
B. WPA (Wi-Fi Protected Access)
C. WPA2 (Wi-Fi Protected Access, version 2)

Seguridad WEP, WPA y WPA2:

Los acrónimos WEP, WPA y WPA2 se refieren a protocolos de cifrado inalámbrico diseñados para salvaguardar la información transmitida y recibida a través de redes inalámbricas. Estos protocolos fueron desarrollados por WiFi Alliance, una asociación que comprende más de 300 empresas en la industria de redes inalámbricas. El primer protocolo introducido por WiFi Alliance fue WEP (Wired Equivalent Privacy) a fines de la década de 1990 [9]. Aunque WEP presentaba deficiencias de seguridad significativas, su uso persiste ampliamente, creando una percepción falsa de seguridad para quienes aún confían en él como protocolo de cifrado para sus redes inalámbricas [10].

Al igual que WPA reemplazó a WEP, WPA2 ha sucedido a WPA como el protocolo de seguridad más reciente. WPA2 implementa los últimos estándares de seguridad, incluyendo el cifrado de datos de "nivel gubernamental" [11]. Desde 2006, todos los productos con certificación WiFi deben cumplir con los estándares de seguridad de WPA2. A continuación, se detallan los protocolos de seguridad inalámbrica WEP, WPA y WPA2:

Protocolo WEP

WEP se basa en un sistema de encriptación propuesto por el comité IEEE 802.11 [12]. Se implementa en la capa MAC (Control de Acceso de Medios), ubicada en la capa de enlace del modelo OSI. WEP comprime y cifra los datos transmitidos a través de ondas de radio. La tarjeta de red encripta el cuerpo de los paquetes de información y el CRC (Comprobación de Redundancia Cíclica) de cada trama 802.11 antes de la transmisión, utilizando el algoritmo de encriptación RC4 proporcionado por The Security Division of EMC Corporation (RSA Security). La estación receptora, ya sea un punto de acceso o una estación cliente, se encarga de desencriptar la trama. WEP especifica una clave secreta compartida de 40 o 64 bits para cifrar y descifrar información, utilizando en su proceso la encriptación simétrica [12]. La vulnerabilidad de WEP radica en la longitud insuficiente del vector de inicialización y la estática persistencia de las claves de cifrado [13].

Protocolo WPA

WPA, cuyo acrónimo significa Wireless Protected Access (Acceso Inalámbrico Protegido), es un protocolo de seguridad propuesto en 2003 y desarrollado por la Wi-Fi Alliance para abordar las debilidades encontradas en WEP, basado en el borrador del estándar IEEE 802.11i [14]. WPA incorpora el protocolo TKIP (Integridad Temporal de Clave Protocolo), con un vector de inicialización de 48 bits y una criptografía de 128 bits. Con la utilización del TKIP, la clave se modifica en cada paquete y se sincroniza entre el cliente y el punto de acceso; también emplea autenticación de usuario a través de un servidor central. [15]

Protocolo WPA2

WPA2, la implementación respaldada por la Wi-Fi Alliance del estándar IEEE 802.11i, representa un hito crucial en la seguridad de las redes WLAN. El grupo WPA2 de la Wi-Fi Alliance desempeña un papel fundamental en la certificación del estándar IEEE 802.11i. Aprobado oficialmente en junio de 2004, WPA2 se erige como la solución definitiva a las vulnerabilidades encontradas en WEP. Este protocolo ofrece un nivel de seguridad superior al de WPA, ya que utiliza el cifrado AES, capaz de admitir claves de 128, 192 y 256 bits, en lugar

de RC4/TKIP. Además, reemplaza el algoritmo Michael por el protocolo CCMP, reconocido como criptográficamente seguro [16].

Las redes WLAN basadas en WPA2 son ampliamente consideradas como las más seguras. Sin embargo, es crucial que todos los nodos de la red estén familiarizados con ellas. Aunque un atacante podría descubrir la clave mediante el intercambio entre el punto de acceso inalámbrico (AP) y el cliente, se recomienda el uso de WPA2 Empresarial para garantizar la confidencialidad mediante el cifrado a nivel de enlace. En el caso de optar por una solución más simple como WPA2 Personal, se deben tomar precauciones al elegir la clave. WPA2, al basar su cifrado en el algoritmo AES (Estándar de Cifrado Avanzado), no experimenta los problemas asociados con RC4. Sin embargo, es importante destacar que esta elección de cifrado conlleva requisitos de procesamiento, lo que puede requerir la actualización del hardware existente en la red WLAN si no es compatible [17].

En el modo Enterprise, el sistema opera de manera gestionada asignando a cada usuario una clave de identificación única, proporcionando un nivel de seguridad elevado. Para la autenticación, el sistema utiliza el protocolo 802.1x previamente mencionado y, para la encriptación, un algoritmo de cifrado superior al TKIP, es decir, el AES. En el caso de operación en la versión personal, se emplea una clave compartida (PSK) introducida manualmente por el usuario tanto en el punto de acceso como en las máquinas cliente. Las diferencias con WEP en este sentido se centran en el algoritmo de cifrado de los datos. [18]

2. METODOLOGÍA

La investigación de campo realizada en la ciudad de Latacunga se basó en un enfoque integral y exhaustivo para analizar detalladamente el panorama de las redes inalámbricas en la zona urbana. Esta estrategia metodológica se diseñó considerando diversos elementos, desde el diseño y enfoque hasta la selección de métodos, profundidad, tipo, técnica e instrumento. A continuación, se detallan los aspectos clave de esta estrategia:

2.1. Diseño de la Investigación

El diseño de la investigación se conceptualizó como exploratorio y descriptivo. La naturaleza exploratoria permitió una inmersión profunda en el entorno de las redes inalámbricas, mientras que el enfoque descriptivo facilitó la obtención de información detallada y precisa sobre la situación actual. Este diseño se reveló como la elección idónea para entender la complejidad y diversidad de las redes inalámbricas en la zona urbana de Latacunga.

Enfoque de Campo

La selección de un enfoque de campo fue crucial para obtener datos directos y contextualizados. La presencia física en la zona urbana posibilitó una observación detallada de las condiciones reales de las redes inalámbricas, capturando matices que podrían pasar desapercibidos en enfoques más distantes. Este acercamiento cualitativo aportó una perspectiva rica y auténtica.

Método de Recolección de Datos

Se optó por la aplicación de las técnicas de Wardriving y Warchalking como métodos de recolección de datos. Wardriving involucró el uso de dispositivos móviles con capacidades inalámbricas para explorar activamente la ciudad, identificando Access Points (AP) y registrando información relevante. La técnica de Warchalking, por su parte, complementó esta fase al permitir la marcación gráfica de la ubicación y características de los AP encontrados, ofreciendo una representación visual y ordenada.

Profundidad de la Investigación

La investigación se caracterizó por su enfoque profundo, que implicó una inmersión detallada en las características y distribución de las redes inalámbricas en Latacunga. La profundidad de la investigación fue esencial para capturar la complejidad de las interconexiones y la diversidad de las redes presentes en la ciudad.

Tipo de Investigación

La naturaleza de la investigación se alineó con un tipo principalmente cualitativo. Esto permitió una comprensión holística de las percepciones, comportamientos y condiciones que rodean a las redes inalámbricas, enriqueciendo el análisis con insights contextuales y cualitativos.

Técnica de Análisis de Datos

Para analizar los datos recopilados, se implementó la técnica de CROSSTAB o tablas cruzadas. Esta técnica estadística se enfocó en examinar la posible relación entre diversas variables, presentando los resultados de manera clara y estructurada mediante la distribución de porcentajes. La elección de esta técnica se justificó por su eficacia en explorar las conexiones y patrones dentro de los datos recolectados.

Instrumento Utilizado

El instrumento principal para la recolección de datos fue la combinación de dispositivos móviles con capacidades inalámbricas, utilizados en el proceso de Wardriving y Warchalking. Estos

dispositivos, respaldados por aplicaciones especializadas, permitieron una identificación precisa de Access Points y la documentación detallada de su ubicación y características.

Consideraciones Éticas

En todas las etapas de la investigación, se mantuvo un enfoque ético, respetando la privacidad y confidencialidad de la información recopilada. Se obtuvo el consentimiento apropiado para la recolección de datos y se adoptaron medidas para garantizar la seguridad y protección de la información sensible.

3. ANÁLISIS DE RESULTADOS

Se realizó el análisis estableciendo una muestra de población en la ciudad de Latacunga de 1000 registros, en la figura 2 se observan parte de los datos en formato CSV:

PARROQUIA	PROVEEDOR	TIPO_SEGURIDAD	SEGURIDAD WPS
IGNACION FLORES	PUNTO NET	WPA	VERDADERO
JUAN MONTALVO	CNT	WEP	FALSO
JUAN MONTALVO	MEGA SPEED	WPA2	FALSO
SAN BUENAVENTURA	SISCOM	WEP	VERDADERO
IGNACION FLORES	NETLIFE	WEP	VERDADERO
IGNACION FLORES	ATVCABLE	WPA	VERDADERO
IGNACION FLORES	SISCOM	WPA	FALSO
LA MATRIZ	ATVCABLE	WPA2	VERDADERO
LA MATRIZ	SISCOM	WPA2	FALSO
IGNACION FLORES	CNT	WPA	FALSO
LA MATRIZ	NETLIFE	WPA2	FALSO
SAN BUENAVENTURA	AJNET	WPA	VERDADERO
LA MATRIZ	PUNTO NET	WPA	VERDADERO
ELOY ALFARO	AJNET	WPA2	FALSO
JUAN MONTALVO	AJNET	WPA	FALSO
SAN BUENAVENTURA	SISCOM	WPA	FALSO
JUAN MONTALVO	NETLIFE	WPA2	FALSO
IGNACION FLORES	CNT	WPA2	VERDADERO
SAN BUENAVENTURA	CNT	WPA	VERDADERO
SAN BUENAVENTURA	ATVCABLE	WPA2	VERDADERO
IGNACION FLORES	ATVCABLE	WEP	VERDADERO
SAN BUENAVENTURA	NETLIFE	WEP	FALSO
LA MATRIZ	NETLIFE	WPA	VERDADERO
LA MATRIZ	CNT	WEP	FALSO
ELOY ALFARO	NETLIFE	WEP	FALSO
LA MATRIZ	NETLIFE	WEP	VERDADERO

Figura 2. Datos recolectados

Una vez recolectados los datos realizamos un algoritmo en Python como se muestra en la figura 3, para representar los datos recolectados por parroquia como se lo puede apreciar en la figura 4. En la figura 4 se puede interpretar en la muestra obtenida, las parroquias Ignacio Flores y la Matriz, fueron en las que más datos se recolectaron, superando los 200 registros

```python
import pandas as pd
import matplotlib.pyplot as plt
import seaborn as sns

df = pd.read_excel('data.xlsx')

# Gráfico de barras para la frecuencia de redes por parroquia
parroquia_counts = df['PARROQUIA'].value_counts()
sns.barplot(x=parroquia_counts.index, y=parroquia_counts.values, palette='viridis')
plt.title('Cantidad de Redes por Parroquia')
plt.xlabel('Parroquia')
plt.ylabel('Cantidad de Redes')
plt.xticks(rotation=45, ha='right')
plt.show()
```

Figura 3. Algoritmo de gráfico de frecuencia de redes por parroquia

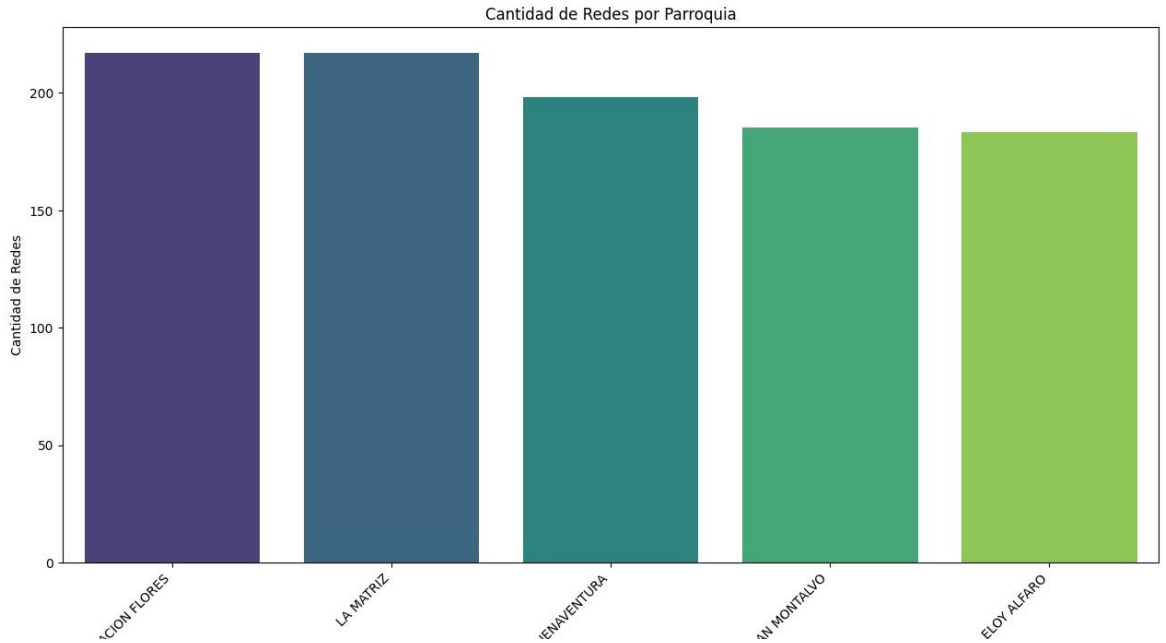

Figura 4. Gráfico de frecuencia de redes por parroquia

Posteriormente con el algoritmo de la figura 5 logramos representar un gráfico de barras de las frecuencias de las seguridades de las redes dentro de la base de datos como se lo representa en la figura 6, en el mismo podemos concluir que el tipo de seguridad WPA2 es el más utilizado a comparación de los otros tipos de seguridad:

```python
# Gráfico de barras para la frecuencia de cada tipo de seguridad
seguridad_counts = df['TIPO_SEGURIDAD'].value_counts()
plt.figure(figsize=(8, 6))
sns.barplot(x=seguridad_counts.index, y=seguridad_counts.values, palette="viridis")
plt.title('Frecuencia de Tipos de Seguridad')
plt.xlabel('Tipo de Seguridad')
plt.ylabel('Frecuencia')
plt.show()
```

Figura 5. Algoritmo de gráfico de frecuencia por tipo de seguridad.

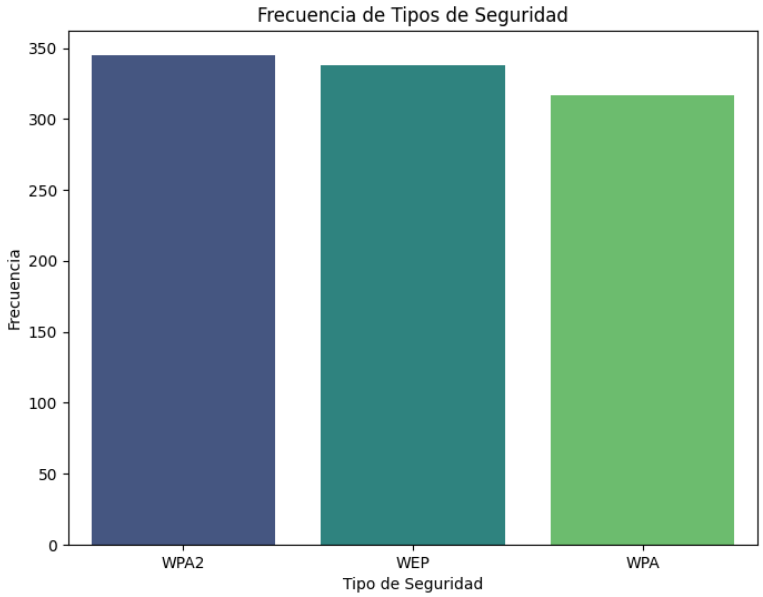

Figura 6. Gráfico de frecuencia por tipo de seguridad.

En la misma podemos concluir que la seguridad tipo WPA2 es la más utilizada dentro de todo el conjunto de muestra, seguida por la WEP y por último la WPA. Para lograr entender cuales son los proveedores que han sido más usados en el estudio, se emplea un algoritmo que se muestra en la figura 7 para generar un gráfico estadístico de valores porcentuales que se muestra en la figura 8.

```
# Gráfica de pastel para motrar el porcentage de los proveedores analizados
proveedor_counts = df['PROVEEDOR'].value_counts()
plt.figure(figsize=(8, 8))
plt.pie(proveedor_counts, labels=proveedor_counts.index, autopct='%1.1f%%', startangle=90, colors=sn
plt.title('Distribución de Proveedores')
plt.show()
```

Figura 7. Algoritmo de gráfico de porcentaje de proveedores analizados.

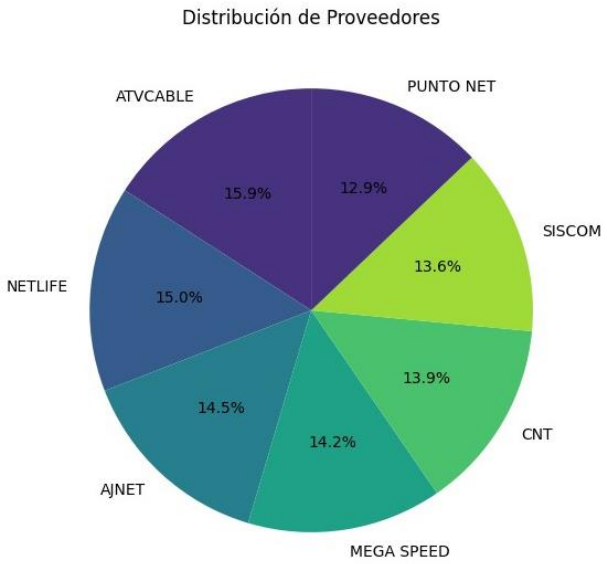

Figura 8. Gráfico de porcentaje de proveedores analizados.

En ella podemos ver que los proveedores más usados son ATV Cable y Netlife los mismos que tiene el 15% de aprobación cada uno. Esto se debe talvez a que ambos ofrecen fibra óptica y buenos planes en cuanto a velocidad. A continuación, empleamos la técnica de CROSSTAB, para normalizar datos y realizar un estudio de las variables de proveedores relacionados con otros indicadores, por ejemplo, en la figura 9 se puede apreciar el algoritmo que genera un estudio de datos entre la variable Proveedor y la variable Seguridad_WPS, el mismo que se representa de manera visual en la figura 10:

```
# Analisis de seguridad WPS por proveedor
crosstab_result = pd.crosstab(df['PROVEEDOR'], df['SEGURIDAD_WPS'])
sns.heatmap(crosstab_result, annot=True, cmap='viridis', linewidths=.5)
plt.title('Relación entre Proveedor y Seguridad WPS')
plt.xlabel('Seguridad WPS')
plt.ylabel('Proveedor')
plt.show()
```

Figura 9. Algoritmo de análisis de seguridad WPS por proveedor.

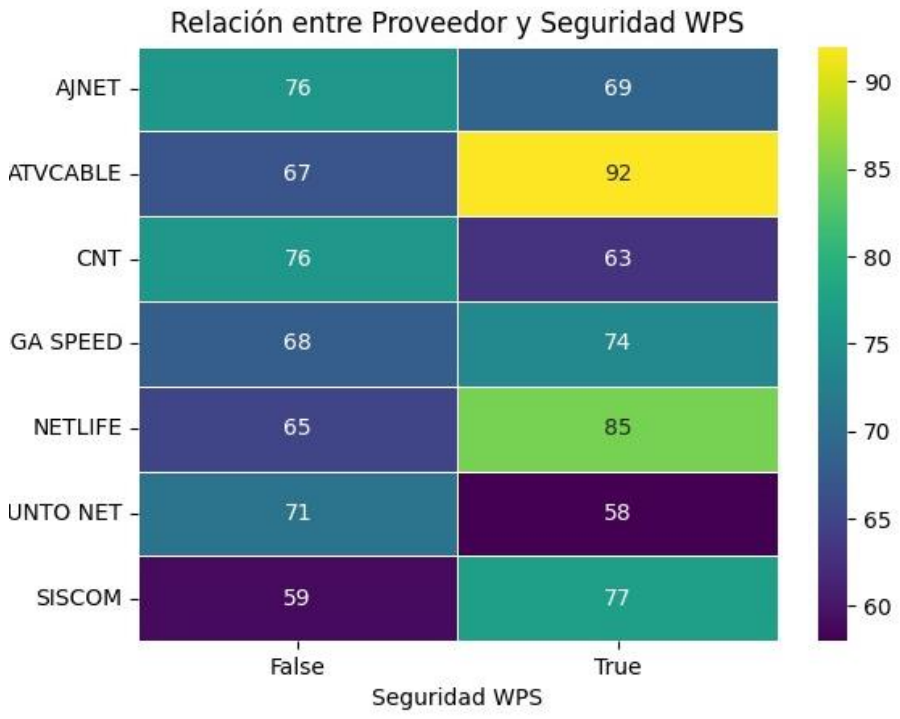

Figura 10. Análisis de seguridad WPS por proveedor.

En la figura 10 se puede apreciar que las empresas ATV Cable y Netlife, ofrecen mayor seguridad WPS en sus redes.

Luego de revisar la seguridad WPS, se procede a realizar una comparativa entre los proveedores y los tipos de seguridad WPA2, WEP y WPA, los mismo que gracias al algoritmo de la figura 11, en la cual también se emplea el método CROSSTAB, arroja como resultado la grafica de la

figura 12, la misma que nos ayuda a verificar que en su totalidad, los proveedores ofrecen los tres tipos de seguridades, sin embargo según los datos recolectados, la empresa Mega Speed seguida por ATV cable y Punto Net, son los que más redes han implementado con el tipo de seguridad WPA2 que hoy en día se lo conoce como el nivel de seguridad más optimo dentro del campo de redes WLAN:

```
# Graficar un gráfico de barras apiladas
crosstab_result = pd.crosstab(df['PROVEEDOR'], df['TIPO_SEGURIDAD'], normalize='index')
plt.figure(figsize=(10, 6))
ax = crosstab_result.plot(kind='bar', stacked=True, colormap='viridis', ax=plt.gca())
plt.title('Proporción de Tipos de Seguridad por Proveedor')
plt.xlabel('Proveedor')
plt.ylabel('Proporción')
plt.legend(title='Tipo de Seguridad', bbox_to_anchor=(1.05, 1), loc='upper left')
ax.legend(loc='center left', bbox_to_anchor=(1, 0.5), title='Tipo de Seguridad')
plt.tight_layout()
plt.show()
```

Figura 11. Algoritmo de análisis de tipo de seguridad por proveedor.

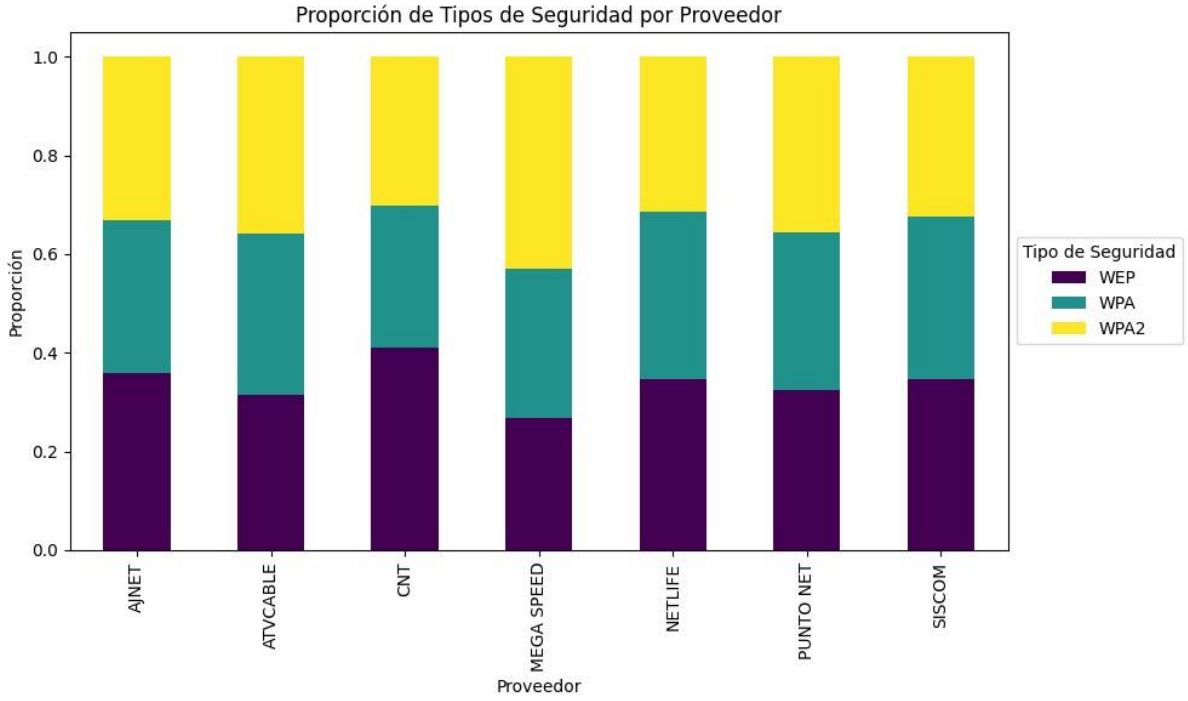

Figura 12. Análisis de tipo de seguridad por proveedor.

4. CONCLUSIONES

- Una vez realizadas las pruebas se puede evidenciar que la totalidad de los proveedores de internet están empleando un tipo de seguridad WPA2, lo que es algo favorable ya que se estima que, en los próximos años, la totalidad de las redes de internet WLAN tenga este tipo de protección.

- Independientemente de que proveedor es el favorito por el mercado y cuáles son las causas, se evidencia una distribución paralela en cuanto a preferencia de los clientes, ya que, si bien es cierto, ATV Cable y Netlife son los favoritos, la mayoría de proveedores supera el 14% de aprobación, por lo que es probable que con el pasar del tiempo, los niveles y tipos de seguridad mejores a la par para poder ofrecer mejor servicio y garantizar la experiencia del cliente.

5. BIBLIOGRAFÍA

[1] Y. V. Vargas Méndez, «ANALISIS DE LAS VULNERABILIDADES DE LAS REDES INALAMBRICAS DE LA UNIVERSIDAD PRIVADA LEONARDO DA VINCI, UNIVERSIDAD PRIVADA "LEONARDO DA VINCI", Perú, 2016.

[2] J. A. Monsalve Pulido, F. A. Aponte Novoa y F. Chaparro Becerra, «Análisis de seguridad de una muestra de redes WLAN en la ciudad de Tunja, Boyacá, Colombia,» DYNA, vol. 82, nº 189, pp. 226-232, 2014.

[3] J. R. C. Raya, Redes Locales, Colombia: Alafa Omega, 2003.

[4] E. Astaiza, H. Bermúz y D. Méndez, «Selección y validación experimental del modelo teórico bellalta para caracterización del tráfico heterogéneo en redes 802.11 una alternativa para el dimensionamiento de capacidad.,» Revista Gerencia Tecnológica Informática, vol. 12, pp. 45-56, 2013.

[5] R. Piyare y S. Lee, «Performance Analysis of XBee ZB Module Bases Wireless Sensor Networks,» International Journal of Scientifc & Engineering Research, vol. 4, pp. 1615-1621, 2013.

[6] S. Gowrishankar, Issues in Wireless Sensor Networks, London, U.K.: Procces of the Word Congress on Engineering, 2008.

[7] J. Salazar, REDES INALÁMBRICAS, Uruguay: Erasmus+, 2016.

[8] H. J. López, «DISEÑO DE UNA ZONA WI-FI COMO HERRAMIENTA DE APOYO AL MODELO EDUCATIVO DE LA UNIVERSIDAD AUTÓNOMA INDÍGENA DE MÉXICO,» Ra Ximhai, vol. 1, nº 2, pp. 389-412, 2005.

[9] Só Física, Como funcionam as redes Wi-Fi?, Virtuous Tecnologia da Informação, 20082018. Consultado em 12/07/2018 às 10:57. Disponível na Internet em http://www.sofisica.com.br/conteudos/curiosida des/wi_fi.php, [Accessed: 10- Jul-2018].

[10] J. Geier, "Designing and Deploying 802.11 Wireless Networks: A Practical Guide to Implementing 802.11n and 802.11ac Wireless Networks For Enterprise-Based Applications, 2nd Edition", Ciscopress.com, 2015. [Online]. Available:

http://www.ciscopress.com/store/designingand-deploying-802.11-wireless-networks-a-9781587144301. [Accessed: 10- Jul- 2018].

[11] M. Pinola, "Is Your Network an Easy Target for Hackers? Understand WEP/WPA/WPA2", Lifewire, 2017. [Online]. Available: https://www.lifewire.com/what-are-wep-wpaand-wpa2-which-is-best-2377353. [Accessed: 10- Jul- 2018].

[12] A. Lashkari, M. Danesh y B. Samadi, «A survey on wireless security protocols (WEP, WPA and WPA2/802.11i),» Computer Science and Information Technology, pp. 48-52, 2009.

[13] S. Reddy, R. Sai, R. K. S. Ali y C. Reddy, « Wireless hacking – a WiFi hack by cracking WEP,» Education Technology and Computer, pp. 189-193, 2010.

[14] A. G. Paz, D. B. Casanova y E. R. Fuentes Gari, «PROPUESTA DE PROTOCOLOS DE SEGURIDAD PARA LA RED INALÁMBRICA LOCAL DE LA UNIVERSIDAD DE CIENFUEGOS,» Revista Universidad y Sociedad, vol. 8, nº 4, pp. 130-137, 2016.

[15] R. C. Guevara Calume, Riesgos con las redes Wi-Fi públicas del centro de Medellín, Colombia, Colombia: Fondo Editorial Corporación Universitaria Remington, 2017.

[16] A. S. Rumale y D. N. Chaudhari , «IEEE 802.11x, and WEP, EAP,WPA / WPA2,» Comp. Tech, vol. 2, nº 6, pp. 1945-1950 , 2011.

[17] J. RUZ MALUENDA, B. RIVEROS VASQUEZ y A. VARAS ESCOBAR, «Redes WPA/WPA2 SU VULNERABILIDAD,» Universidad Federico Santa María, Chile, 2013.

[18] L. C. da Silva, «Teleco Intelligence em Telecomunicações,» 8 Marzo 2010. [En línea]. Available: http://www.teleco.com.br/tutoriais/tutorialwifirou bo/pagina_4.asp. [Último acceso: 15 Julio 2018].