Universidad Nacional de Loja

Facultad de la Energía, las Industrias y los Recursos Naturales No Renovables

Maestría en Telecomunicaciones

Fortalecimiento Cibernético: Análisis Integral de la Seguridad en Redes Wi-Fi Públicas en Loja y Estrategias Innovadoras de Mejora.

Trabajo de titulación, previo a la obtención del título de Magister en Telecomunicaciones.

AUTOR:

Ing. Andy René Peña Cueva

DIRECTOR:

Ing. Juan Carlos Solano Jiménez, Mg. Sc.

Loja – Ecuador

2024

Certificación

Universidad Nacional de Loja

1859

Sistema de Información Académico Administrativo y Financiero - SIAAF

CERTIFICADO DE CULMINACIÓN Y APROBACIÓN DEL TRABAJO DE TITULACIÓN

Yo, **SOLANO JIMENEZ JUAN CARLOS**, director del Trabajo de Titulación denominado **FORTALECIMIENTO CIBERNÉTICO: ANÁLISIS INTEGRAL DE LA SEGURIDAD EN REDES WI-FI PÚBLICAS EN LOJA Y ESTRATEGIAS INNOVADORAS DE MEJORA**, perteneciente al estudiante **ANDY RENÉ PEÑA CUEVA**, con cédula de identidad N° **1104112683.**

Certifico:

Que luego de haber dirigido el **Trabajo de Titulación**, habiendo realizado una revisión exhaustiva para prevenir y eliminar cualquier forma de plagio, garantizando la debida honestidad académica, se encuentra concluido, aprobado y está en condiciones para ser presentado ante las instancias correspondientes.

Es lo que puedo certificar en honor a la verdad, a fin de que, de así considerarlo pertinente, el/la señor/a docente de la asignatura de **Titulación**, proceda al registro del mismo en el Sistema de Gestión Académico como parte de los requisitos de acreditación de la Unidad de Titulación del mencionado estudiante.

Loja, 23 de Agosto de 2024

JUAN CARLOS SOLANO JIMENEZ

F) ----------

DIRECTOR DE TRABAJO DE TITULACIÓN

Certificado TIC/TT.: UNL-2024-002639

1/1

Educamos para **Transformar**

Autoría

Yo, **Andy René Peña Cueva**, declaro ser autor del presente trabajo de titulación y eximo expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos de posibles reclamos y acciones legales, por el contenido del mismo. Adicionalmente acepto y autorizo a la Universidad Nacional de Loja la publicación de mí del trabajo de integración curricular o de titulación en el Repositorio Digital Institucional – Biblioteca Virtual.

Firma: 

Cédula de Identidad: 1104112683

Fecha: 17 de octubre de 2024

Correo electrónico: andy.pena@unl.edu.ec

Teléfono: 0994286603

Carta de autorización por parte del autor para la consulta de producción parcial o total, y publicación electrónica de texto completo del trabajo de titulación.

Yo **Andy René Peña Cueva** declaro ser autor del trabajo de titulación denominado: **Fortalecimiento Cibernético: Análisis Integral de la Seguridad en Redes Wi-Fi Públicas en Loja y Estrategias Innovadoras de Mejora.**, como requisito para optar el título de **Magister en Telecomunicaciones,** autorizo al sistema Bibliotecario de la Universidad Nacional de Loja para que con fines académicos muestre la producción intelectual de la Universidad, a través de la visibilidad de su contenido de la siguiente manera en el Repositorio Institucional.

La Universidad Nacional de Loja, no se responsabiliza por el plagio o copia del trabajo de titulación que realice un tercero.

Para constancia de esta autorización, suscribo, en la ciudad de Loja, a los diecisiete días del mes de octubre del dos mil veinticuatro.

Firma: Firmado electrónicamente por: ANDY RENE PENA CUEVA

Autor: Andy René Peña Cueva

Cédula: 1104112683

Dirección: Loja, Av. Benjamín Carrión y José de San Martín

Correo electrónico: andy.pena@unl.edu.ec

Celular: 0994286603

DATOS COPLEMENTARIOS:

Director del trabajo de titulación: Ing. Ingeniería, Juan Carlos Solano Jiménez, Mg. Sc.

Dedicatoria

Primeramente, agradezco a Dios, por ser mi guía y fuente de fortaleza en cada paso de mi vida. A mis padres, Hugo y Azucena, por su amor incondicional, por ser mis pilares de apoyo y por enseñarme el valor del esfuerzo y la perseverancia. A mis hermanos, Víctor, Bryan y David, por acompañarme en este viaje y ser una fuente constante de ánimo y apoyo. A mi novia Thalía, por su amor, paciencia y comprensión, siendo mi refugio en los momentos más difíciles, este logro también es tuyo.

Este trabajo también va dedicado mi tía Mercy y mi abuelita Bertha, que desde el cielo han sido mis ángeles guardianes. Su amor y ejemplo siguen presentes en mi corazón y me inspiran cada día.

Andy René Peña Cueva

Agradecimiento

A mi familia, mi novia y mis amigos, quienes han sido pilares fundamentales en mi desarrollo personal y profesional. Su amor incondicional, apoyo constante y motivación en cada etapa de mi vida han sido cruciales para alcanzar este logro. No puedo agradecerles lo suficiente por estar siempre a mi lado, brindándome su compañía y aliento.

A mis compañeros y amigos de la Maestría en Telecomunicaciones, gracias por el respaldo y la camaradería que han hecho este trayecto más llevadero y enriquecedor.

Al Ingeniero Juan Carlos Solano, le extiendo mi más sincero agradecimiento por su valiosa contribución, por compartir su vasta experiencia y conocimientos, y por guiarme con acierto durante este proceso. Su orientación fue decisiva para la culminación exitosa de este trabajo.

A todos ustedes, les expreso mi más sincero agradecimiento por su fe en mí y por acompañarme a lo largo de este gratificante recorrido.

Andy René Peña Cueva

Índice de Contenidos

Índice de Figuras

Índice de Tablas

Índice de Anexos

1. Titulo

Fortalecimiento Cibernético: Análisis Integral de la Seguridad en Redes Wi-Fi Públicas en Loja y Estrategias Innovadoras de Mejora.

2. Resumen

En la actual era digital donde la conectividad inalámbrica se ha transformado en un punto esencial para la comunicación y la productividad, el acceso a redes Wi-Fi públicas se ha convertido en una práctica común, sin embargo, esta práctica expone a los usuarios a diversas amenazas cibernéticas, como el robo de datos, ataques de intermediarios y vulnerabilidades de seguridad. Las redes WLAN abiertas y el uso de protocolos de seguridad obsoletos como WEP aumentan estos riesgos. Este trabajo de investigación aborda el estudio de la vulnerabilidad de las redes Wi-Fi públicas en Loja mediante un análisis exhaustivo de su seguridad, identificando las principales amenazas y deficiencias. Además, se examina la posición de Ecuador en el Índice Global de Ciberseguridad de la UIT (Unión Internacional de Telecomunicaciones), destacando la necesidad urgente de mejorar la protección cibernética en el país. El análisis de las redes Wi-Fi públicas de Loja se lleva a cabo mediante el uso de herramientas como Kali Linux y Nessus. Se aplican técnicas de hacking ético, incluyendo pruebas de fuerza bruta, para encontrar las vulnerabilidades en las redes. También, se evalúan los protocolos de cifrado, como WEP y WPA, y se plantea la adopción de tecnologías nuevas como WPA2 y WPA3. La metodología incluye también la recolección y análisis de datos sobre los ciberataques en estas redes. El estudio reveló que las redes Wi-Fi públicas en Loja presentaban serias vulnerabilidades debido al uso de protocolo de seguridad obsoletos y falta de medidas de protección apropiadas. Se detectaron múltiples deficiencias que permiten el ataque de hackers. Se concluye que es importante mejorar la seguridad de las redes Wi-Fi públicas en Loja para reducir los riesgos de ciberataques. La implementación nuevos protocolos, como WPA3, junto con la educación sobre ciberseguridad, es importante para proteger a los usuarios. Las instituciones deben actualizar sus infraestructuras y adoptar medidas preventivas, para garantizar una conectividad segura en lugares públicos y minimizar vulnerabilidades.

Palabras clave: *Wifi, WLAN, ciberataque, ciberseguridad, ingeniería social, WEP, WPA, WPA2, WPA3, Kali Linux, Nessus.*

Abstract

In today's digital age, wireless connectivity has become essential for communication and productivity, leading to the widespread use of public Wi-Fi networks. However, this practice exposes users to various cyber threats, such as data theft, man-in-the-middle attacks, and security vulnerabilities. Open WLANs and outdated security protocols like WEP increase these risks. This research focuses on studying the vulnerability of public Wi-Fi networks in Loja through a comprehensive security analysis, identifying the main threats and deficiencies. Additionally, it examines Ecuador's position in the ITU (International Telecommunication Union) Global Cybersecurity Index, highlighting the urgent need to improve cyber protection in the country. The analysis of Loja's public Wi-Fi networks is conducted using tools such as Kali Linux and Nessus. Ethical hacking techniques, including brute force testing, are applied to find networks' vulnerabilities. Encryption protocols such as WEP and WPA are also evaluated, with the adoption of new technologies like WPA2 and WPA3. The methodology also includes the data collection and analysis of cyber-attacks on these networks. The study revealed that public Wi-Fi networks in Loja presented serious vulnerabilities due to obsolete security protocols' usage and a lack of appropriate protection measures. Multiple deficiencies that allow hackers to attack were detected. Improving the security of public Wi-Fi networks in Loja is essential to reduce the risks of cyber-attacks. Implementing new protocols, such as WPA3 with cybersecurity education, is important to protect users. Institutions must update their infrastructures and adopt preventive measures to ensure secure connectivity in public places and minimize vulnerabilities.

Keywords: *Wi-Fi, WLAN, cyberattack, cybersecurity, social engineering, WEP, WPA, WPA2, WPA3, Kali Linux, Nessus.*

3. Introducción

Hoy en día la dependencia de la sociedad hacia la conectividad inalámbrica en entornos públicos ha crecido considerablemente, por lo que el mundo se ha transformado cada vez más en un sitio digital, para facilitar la comunicación, productividad y el acceso a información de gran validez. Sin embargo, con el acceso a este tipo de redes públicas los usuarios se han expuesto a innumerables tipos de amenazas cibernéticas, como el robo de datos, los ataques de intermediarios y las fallas de seguridad.

Los ciberdelincuentes avanzaron rápidamente durante estos tiempos de avance en las redes informáticas, desarrollando técnicas y métodos para comprometer sistemas de seguridad que aún no estaban plenamente desarrollados, aprovechando la falta de preparación de las autoridades para hacer frente a este problema emergente (Pons, 2017).

El acceso a las redes WLAN abiertas para un atacante experimentado puede ser fácil y así llevar a cabo actividades maliciosas sin restricciones, dado que son altamente vulnerables a la suplantación, dando consecuencias como el robo de datos confidenciales, la vigilancia del tráfico de la red, inclusive la inyección de malware.

El protocolo de seguridad WEB indica deficiencias graves, ya que la encriptación WEP de 40 a 128 bits no establece la suficiente protección para una red de ataques actuales. Un atacante especializado puede lograr descifrar una clave WEP en un tiempo corto (Monsalve et al., 2015).

Con el progresivo desarrollo de la tecnología y el aumento de las ciberamenazas, se ha hecho indispensable identificar y minimizar las vulnerabilidades que puedan surgir, con el fin de prevenir ataques sorpresivos, y así proteger la información personal y sensible de las personas conectadas a una red Wi-Fi pública, protegiendo la confidencialidad, integridad y disponibilidad de sus datos.

Por tanto, las empresas que quieran expandirse en el mercado deben aplicar de inmediato procesos de seguridad de la información más sólidos y actualizados para impedir la entrada y el robo de datos sensibles. Los intrusos pueden beneficiarse de las vulnerabilidades para introducirse en la red de una organización y manipular, robar o atentar contra la integridad de los datos con el fin de suplantar identidades, ralentizar procesos o incluso paralizar servicios (Pilco, 2015).

Es comprensible que los ciberdelincuentes utilicen con mayor frecuencia vulnerabilidades antiguas con el fin de poner en peligro la seguridad de usuarios y empresas en Latinoamérica. No obstante, según los datos de telemetría de ESET, también se han identificado detecciones para las vulnerabilidades más recientes. Esto demuestra que el sector del

cibercrimen está formado por un ecosistema diverso de ciberdelincuentes dispuestos a aprovechar las diversas vulnerabilidades existentes en busca de tecnologías obsoletas. Incluso si esto implica ataques más complejos o requiere la creación de nuevos *exploits* (ESET, 2024).

A pesar que la inteligencia artificial se está utilizando para mejorar la detección de ataques potenciales y acelerar la respuesta a amenazas, los ciberdelincuentes también pueden utilizar la famosa herramienta ChatGPT para crear código malicioso y malware que resulte difícil de identificar. Aunque la herramienta cuenta actualmente con más restricciones y políticas para impedir su uso, el acceso a su API permite explotarlas. Sin embargo, existe una variedad de *hacks* o *jailbreaks* que pueden engañar al *chatbot* para que proporcione contenido insuficiente. La capacidad de procesamiento de datos de ChatGPT permite que los ciberdelincuentes descifren contraseñas o preguntas de seguridad (ESET, 2024).

De manera similar, cuando la tecnología de comunicación móvil 5G llegue a una masa crítica, tendrá un impacto en casi todas las organizaciones, lo que representa un nuevo desafío en la gestión de grandes volúmenes de datos en tiempo real para la protección contra ciberataques en diversas industrias, ya sea en el ámbito de la salud, las finanzas y en las telecomunicaciones. Por tanto, las organizaciones deberán reforzar sus estrategias de ciberseguridad, adaptándose a las complejidades y particularidades que plantea 5G (José et al., 2022).

En Ecuador según el Índice Global de Ciberseguridad de la Unión Internacional de Telecomunicaciones, se encuentra ubicada en el puesto 119 de 182 países en lo que respecta a las vulnerabilidades frente a ataques cibernéticos, tales como phishing, troyanos, malware e ingeniería social. Debido a esto, es fundamental tomar en cuenta las medidas de precaución cuando se trata de información sensible y enviada a través de la red, comúnmente cuando se trata de datos bancarios, siendo estos susceptibles a ataques de phishing, ya que buscan engañar a los usuarios con el simple objetivo de adquirir claves y números de cuentas.

El Estado debe actuar proactivamente en la defensa y seguridad del ciberespacio, ya que es un lugar donde el terrorismo puede actuar. Para lograr esto, es relevante determinar el nivel de madurez cibernética del Estado. Esto se puede lograr a través del análisis de la estrategia de ciberseguridad y la guía de ciberdefensa, así como de la operacionalización efectiva de estas estrategias (Paredes & Semanate, 2024).

La falta de protección de la red, particularmente para los equipos de red, es un problema creciente, ya que los atacantes están aumentando. Muchos propietarios de redes WIFI no saben lo importante que es usar técnicas de hacking éticas para encontrar vulnerabilidades en sus

sistemas y redes. Como resultado, no se basan en medidas preventivas para proteger su red, lo que deja su información sensible a ataques malintencionados.

El hacking ético es el uso legítimo y ético de métodos y herramientas de hacking para detectar vulnerabilidades en sistemas y redes informáticos. En lo que respecta a las redes wifi, esta práctica consiste en evaluar la seguridad de la red inalámbrica y sus dispositivos, buscando posibles fallos que puedan ser aprovechados por atacantes con intenciones maliciosas (Vivar, 2023).

Para contrarrestar este tipo de ataques en importante que la población sepa a que se expone al navegar en redes wifi con carencia de ciberseguridad, y de los métodos que ciertas instituciones aplican para exponer los datos confidenciales de sus usuarios ya que destaca que las entidades financieras nunca solicitan información confidencial a través de correo electrónico o mensajes de texto, y aconsejan no responder a correos que parezcan sospechosos (Garzón et al., 2024).

Esta investigación busca la necesidad urgente de evaluar las redes Wi-Fi públicas en Loja, reconociendo la importancia de un acceso confiable, protegido en entornos urbanos y espacios públicos, ya que este proyecto no solo se enfoca en el análisis actual, sino que también busca proponer estrategias innovadoras para mejorar la seguridad en redes Wi-Fi públicas, adaptándose a los dinámicos cambios de la ciberseguridad.

La aplicación de medidas proactivas y específicas, resultantes de una evaluación exhaustiva de los protocolos de seguridad existentes, debería dar lugar a un entorno de conectividad más seguro y resistente para los residentes y visitantes, promoviendo la confianza en el uso de estas redes en entornos urbanos.

4. Marco Teórico

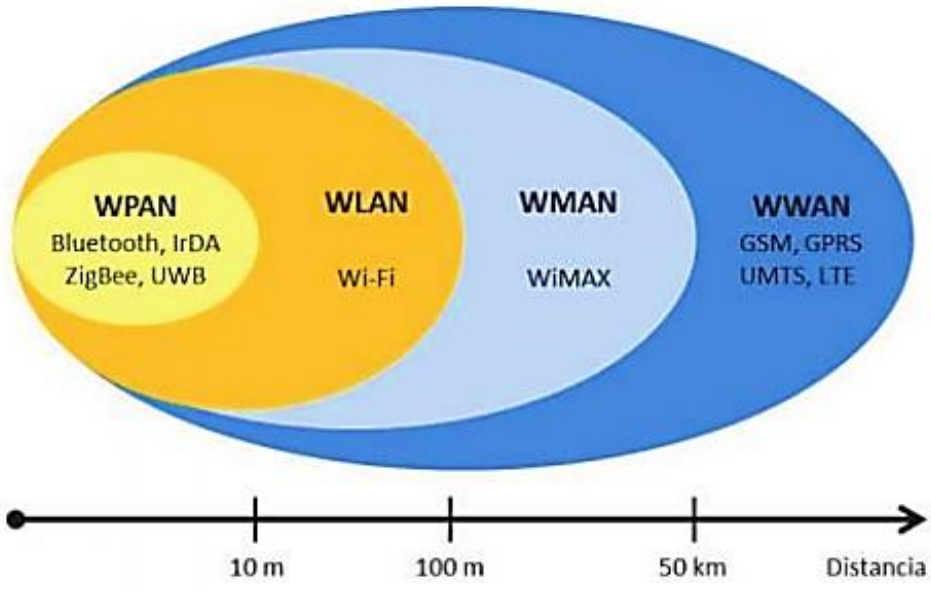
4.1. Tecnologías Inalámbricas

Las tecnologías inalámbricas han evolucionado con el tiempo hasta convertirse en un elemento central de la tecnología, ya que muchos dispositivos dependen ahora de las redes inalámbricas para su comunicación, debido a ventajas como la flexibilidad, la expansión de la red y los bajos costos de despliegue, entre otras.

El propósito principal de las tecnologías inalámbricas es mantener conectados a todos los dispositivos que no pueden utilizar medios cableados, facilitando así la comunicación entre ellos. A continuación, en la Figura 1 se observa los distintos tipos de tecnologías inalámbricas (Pilco, 2015).

Figura 1

Clasificación de las redes inalámbricas

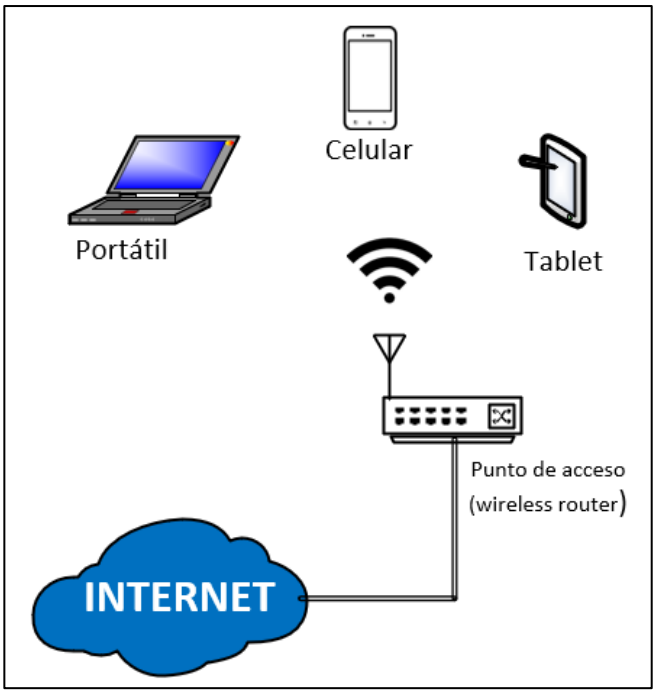


Nota. Adaptado de (Pilco, 2015).

Concentrándonos en las WLAN, estos son sistemas diseñados para proporcionar conectividad inalámbrica en espacios con un alcance habitual de hasta 100 metros y utilizadas principalmente en entornos domésticos, educativos, oficinas o salas de ordenadores, estas redes permiten a los usuarios desplazarse dentro de un área de cobertura local sin desconectarse de la red (véase la Figura 2). Estas redes se basan en la norma IEEE 802.11 y se las conoce comercialmente como Wi-Fi. (J. Salazar, 2012).

Figura 2

Esquema de una red WLAN en domicilio.



4.1.1. Tipos de Redes Inalámbricas

Básicamente en las redes inalámbricas se tiene dos formas de trabajar, según la topología Ad-hoc y según la topología de infraestructura, a continuación, se las describe.

4.1.1.1. Modo de Infraestructura. Se entiende por topología de infraestructura a aquella que amplía una LAN cableada ya existente para la incorporación de dispositivos inalámbricos a través de una estación base, denominada punto de acceso, este punto de acceso conecta la LAN inalámbrica y la LAN cableada para que sirva como controlador central de la LAN inalámbrica. El punto de acceso coordina la transmisión y recepción de varios dispositivos inalámbricos dentro de un rango específico, como se muestra en la Figura 3; el rango y el número de dispositivos dependerá del estándar de conexión inalámbrica empleado y del modelo de producto.

En la modalidad de infraestructura, puede haber varios puntos de acceso para dar cobertura a una zona grande o un único punto de acceso para una zona pequeña, ya sea un hogar o un edificio pequeño (M. Mora, 2004).

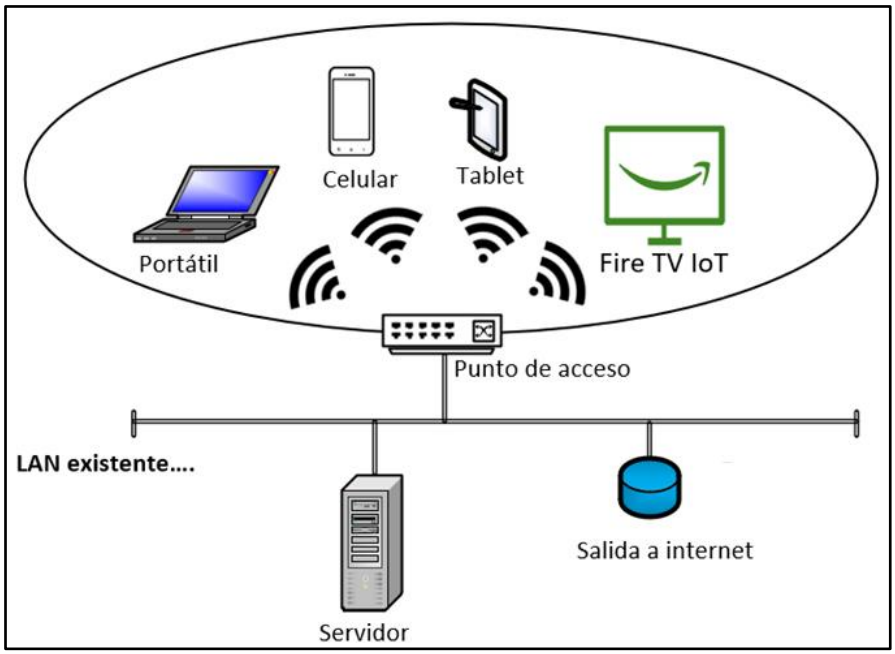
A continuación, se muestra las características de una topología de Infraestructura:

- Son las más comunes.

- Cada celda opera su propio canal.
- Utilizan dispositivos llamados Access Point (AP).
- La BSS se define por la distancia al AP.

Figura 3

Red de la modalidad infraestructura.



4.1.1.2. Topología Ad – Hoc. Dentro de una topología ad hoc, los mismos dispositivos inalámbricos constituyen la LAN, por lo tanto, no existe un controlador central ni puntos de acceso. Cada dispositivo se comunica directamente con los demás dispositivos de la red en lugar de pasar por un controlador central.

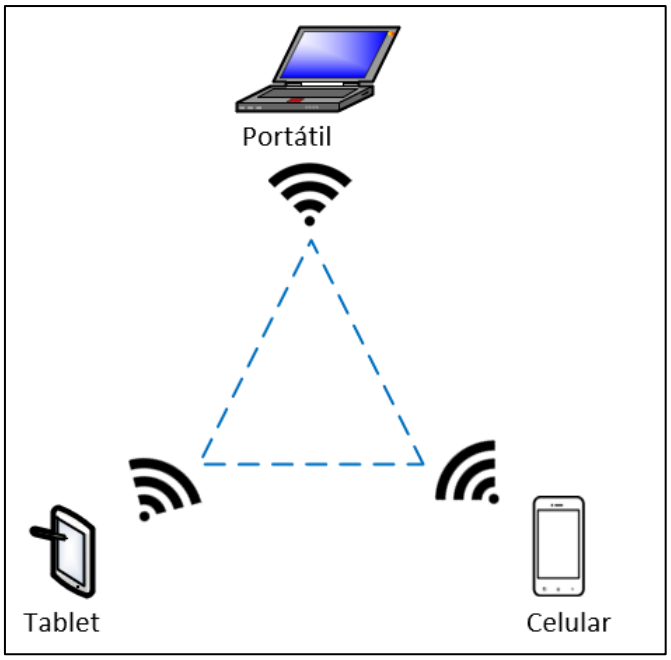
Esta topología resulta útil en entornos donde se reúnen pequeños grupos de equipos que no necesitan acceder a otra red. Algunos ejemplos de entornos en los que se podrían utilizar redes ad hoc inalámbricas serían un hogar sin red cableada o una sala de conferencias donde los equipos se reúnen regularmente para intercambiar ideas, como se muestra en la Figura 4.

Algunas características de una topología de Ad Hoc(Santiago, 2006) se presentan a continuación:

- Solo punto a punto.
- Son fácil de configurar.
- Las redes independientes no utilizan Access Point (AP).

Figura 4

Red de modalidad Ad-Hoc.



4.2. Redes abiertas

4.2.1. Redes Wi-Fi

Antes de describir las características de una red abierta, es importante introducir los conceptos relacionados con las redes Wi-Fi. Wi-Fi se trata de una tecnología de redes inalámbricas que permite a dispositivos como ordenadores (portátiles y de sobremesa), dispositivos móviles (smartphones y accesorios) y otros equipos (impresoras y videocámaras) conectarse a Internet.

Esta tecnología facilita que estos dispositivos intercambien información entre sí y formen una red. Para proteger estos dispositivos y la información que transmiten, también existen diferentes protocolos de encriptación, como *Wired Equivalent Privacy* (WEP), Wi-Fi *Protected Access* (WPA) y *Wi-Fi Protected Access* 2 (WPA2), que se describen en el apartado 4.3 «Protocolos de seguridad en redes Wi-Fi».

La conexión a Internet se consigue a través de un router inalámbrico que, al acceder a Wi-Fi, permite establecer una conexión con dicho router, lo que hace posible que los dispositivos compatibles con Wi-Fi interactúen con Internet.

Desde un punto de vista técnico, la norma IEEE 802.11 define los protocolos que facilitan la comunicación con los dispositivos inalámbricos Wi-Fi actuales, como los routers y

los puntos de acceso inalámbricos. Los puntos de acceso inalámbricos son compatibles con varias normas IEEE.

Cada estándar es una modificación que se aprueba tras un cierto periodo de tiempo, dichos estándares operan en frecuencias diferentes que disponen de distintos anchos de banda y soportan distintos números de canales. (Verde, 2022).

4.2.2. Introducción a las Redes abiertas.

Las redes abiertas o públicas son aquellas que no están protegidas por ninguno de los protocolos mencionados anteriormente. Al no utilizar cifrado, la información transmitida por los dispositivos conectados a la red queda vulnerable, además, estas redes no requieren una contraseña para la conexión, permitiendo que cualquier usuario se conecte fácilmente, exponiéndose a posibles ataques sin darse cuenta.

Algunas de estas redes, después de establecer la conexión, solicitan un inicio de sesión en una página genérica para acceder a los servicios de red; sin embargo, esto no mejora la seguridad de la red. Estas características favorecen dos factores, por una parte, que mucha gente con necesidad de conexión a Internet entre en la red y, por otra parte, que sea más sencillo realizar ataques en este tipo de redes. La combinación de estos dos factores crea un entorno ideal para que un atacante se aproveche de usuarios desprevenidos y pueda llevar a cabo diversos ataques de manera imperceptible.

Las razones por las cuales el atacante ve estas redes libres como escenario perfecto para atacar y que no debería hacer el usuario es utilizar apps de navegación y GPS, el consumo de datos móviles, conectarse a las redes sociales, conectarse al trabajo, acceder a servicios de streaming o consultar cuentas bancarias, entre otras.

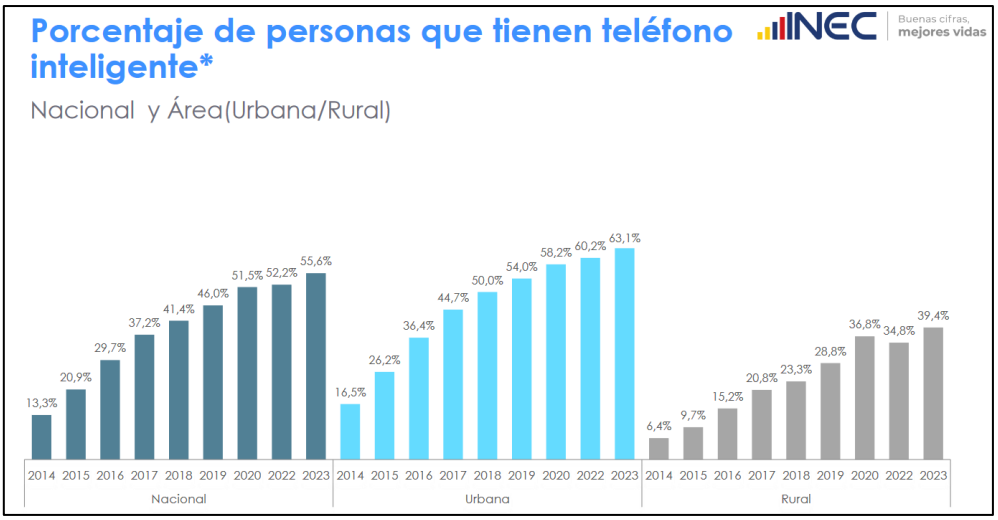
En definitiva, se expone información personal que puede ser de gran provecho para un atacante (Verde, 2022).

En Ecuador en 2023 hubo un crecimiento del 8.2% que equivale a 1.1 millones de nuevos usuarios con acceso a internet. Según estadísticas del INEC (2023), en Ecuador el uso de dispositivos inteligentes o smartphones está en aumento, como se muestra en la Figura 5.

De igual manera, el uso de la tecnología inalámbrica Wi-Fi para acceder a Internet ha crecido, tal como se observa en la Figura 6 (INEC, 2023).

Figura 5

Porcentaje de personas que tienen teléfonos inteligentes en el Ecuador.

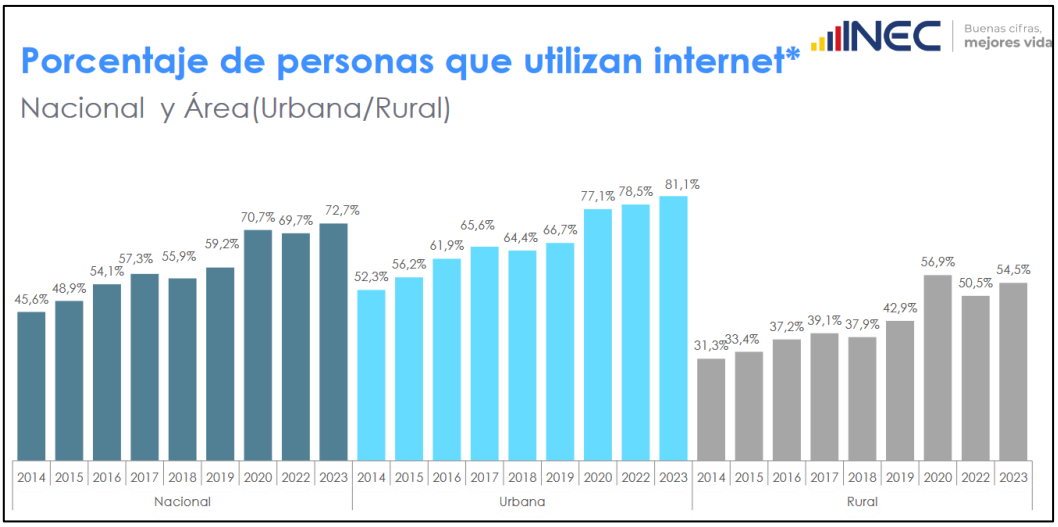


Nota. Adaptado de INEC, 2023.

En la Figura 5 se puede observar un análisis estadístico de cómo ha ido creciendo el porcentaje de usuarios con teléfonos inteligentes a nivel nacional, urbana y rural, en 2014 con respecto a nivel nacional, el número de usuarios con teléfonos inteligentes abarcaba el 13.3%, en el área rural un 16.5% y a nivel rural un 6.4%, para 2023 el número de usuarios creció exponencialmente, a nivel nacional se elevó a un 55.6%, en el área urbana un 63.1% y a nivel rural un 39.4%.

Figura 6

Porcentaje de personas con acceso a internet en el Ecuador.



Nota. Adaptado de (INEC, 2023)

La Figura 6 refleja el porcentaje de personas que utilizan internet a nivel nacional, urbana y rural, y su crecimiento a partir del 2014 a 2023. En 2014 con respecto a nivel nacional el porcentaje de personas usando internet estimó un porcentaje del 45.6%, en el área urbana un 52.3% y el área rural un 31.3%, para el año 2023 el crecimiento de usuarios creció, a nivel nacional con el 72.7%, en el área urbana con el 81.1% y en el área rural con el 54.5%.

En cuanto al acceso a redes Wi-Fi, la mayoría de los usuarios tienden a utilizar estas conexiones desde sus hogares o en lugares con acceso controlado. Sin embargo, la disponibilidad de redes Wi-Fi públicas también está en aumento, especialmente en áreas urbanas y espacios públicos como cafeterías, parques y centros comerciales.

4.2.3. Redes abiertas en la ciudad de Loja.

Actualmente existe un convenio entre el Municipio de Loja y siete empresas proveedoras de internet, mismo que permitió ofrecer servicio de internet gratuito en 100 puntos estratégicos del cantón. Este acuerdo, fue firmado el miércoles 1 de noviembre de 2023. Las empresas participantes son las siguientes:

- Fored
- Nettplus
- Nodo
- Vilcanet
- Xtrim
- Indynet
- Loja System-Velocity

Estas empresas tienen el compromiso de instalar y mantener puntos de acceso a internet en una variedad de espacios públicos. Entre estos lugares se incluyen canchas deportivas, plazas, mercados, paradas de autobús y escuelas municipales, ampliando significativamente el acceso a internet para la comunidad.

Mayra Guaycha, directora de Tecnología del municipio, destacó que estas compañías han decidido donar su infraestructura durante un periodo de cuatro años para promover la inclusión digital en sectores urbanos y rurales (Jaramillo, 2023).

Aunque el convenio entre el Municipio de Loja y las empresas proveedoras de internet tiene el potencial de beneficiar significativamente a la comunidad, también existen desventajas inherentes al uso de redes Wi-Fi públicas, ya que las redes Wi-Fi públicas, al ser abiertas y accesibles para cualquier usuario, son particularmente vulnerables a ataques cibernéticos. Los

atacantes pueden interceptar fácilmente la información transmitida a través de estas redes, incluyendo datos personales, contraseñas y detalles financieros.

Se debe resaltar la importancia de que los usuarios sean conscientes de los riesgos asociados al uso de redes Wi-Fi públicas y tomen medidas para protegerse, como el uso de redes privadas virtuales (VPN), evitando realizar transacciones sensibles y desconectándose de la red cuando no sea necesaria, la iniciativa de proporcionar Wi-Fi gratuito en Loja puede ser muy beneficiosa si se implementan y comunican adecuadamente las mejores prácticas de seguridad para los usuarios.

4.2.4. Estándar 802.11

Es un estándar de autenticación que controla el acceso a los servicios de red a través de sus puertos, funciona en la capa dos del modelo OSI, garantiza el intercambio de credenciales de usuario o dispositivo e impide cualquier ingreso no autorizado a la red. Una infraestructura de red 802.1x necesita de tres elementos para funcionar: solicitante, equipo autenticador y servidor de autenticación.

La tecnología 802.11 se utiliza para realizar conexiones en redes inalámbricas y debido al rápido desarrollo de la tecnología han aparecido diferentes variantes, denominadas estándares por el IEEE de esta tecnología.

El primer estándar que se adoptó de forma generalizada fue el IEEE 802.11b, que permitía velocidades de hasta 11 Mbps en la banda de 2,4 GHz sin la necesidad de una licencia. Posteriormente, se introdujo la norma IEEE 802.11g como una evolución de 802.11b, que ofrecía un mayor ancho de banda. Los dispositivos compatibles con IEEE 802.11g pueden funcionar tanto con clientes 802.11b como 802.11g. Del mismo modo, los dispositivos con tarjetas IEEE 802.11g pueden conectarse tanto a los puntos de acceso 802.11b existentes como a los nuevos puntos de acceso 802.11g, esto se debe a que ambos estándares comparten la misma banda de frecuencia de 2,4 GHz.

Aunque la velocidad de transferencia máxima teórica para IEEE 802.11g es de 54 Mbps, esta puede reducirse automáticamente en condiciones de señal débil o interferencias (J. Salazar, 2012). A continuación, se explican con más detalle cada uno de los estándares más significativos:

- **802.11a**

Define un rango operativo de 5 GHz, con la atribución de 8 canales dentro de ese espectro. Aunque se menciona una velocidad teórica de unos 54 Mbps, en la realidad esta cifra puede variar debido a que se centra en el ancho de banda compartido. Este planteamiento

implica que el rendimiento se divide entre los usuarios que utilizan el espacio simultáneamente y, a medida que se incrementa la distancia, disminuye la eficiencia. Este estándar tiene ventajas notables, como la reducción de interferencias al utilizar la banda de 5 GHz y una velocidad máxima de 54 Mbps, que supera a la de sus competidores (802.11 b/g). Sin embargo, presenta notables desventajas, entre las que destacan está que su precio sigue siendo elevado, esto se debe al aumento de la producción de los estándares b y g por parte de los fabricantes de dispositivos inalámbricos.

Además, la limitada cobertura es un aspecto a tener en cuenta en comparación con otros estándares. Si un usuario decide migrar a esta tecnología, sería necesario instalar más puntos de acceso para garantizar un rendimiento eficiente, lo que conllevaría un aumento de los costes.

- **802.11b**

Este protocolo es ampliamente adoptado debido a su operación en la frecuencia de 2,5 GHz, lo que elimina la necesidad de pagar por el uso del espectro. Este estándar designa tres canales en su funcionamiento, y su velocidad máxima alcanza los 11 Mbps, ya que opera con un ancho de banda compartido, similar al estándar mencionado anteriormente. A medida que la distancia aumenta, la tasa de transferencia de datos disminuye. Su principal ventaja radica en su amplia compatibilidad, siendo el estándar actual para redes WLAN, y sus costos son significativamente más bajos en comparación con otros protocolos. No obstante, su desventaja más destacada es su velocidad limitada de 11 Mbps, lo que lo hace menos adecuado para la transmisión de archivos grandes. Al utilizar la frecuencia de 2,4 GHz, está más expuesto a interferencias en comparación con el estándar anterior. Dada su mayor alcance, también es más susceptible a accesos no autorizados, lo que compromete la seguridad de este estándar.

- **802.11g**

Este protocolo fue concebido como una extensión de los estándares 802.11a y 802.11b, combinando la velocidad de 54 Mbps del primero con la compatibilidad del segundo. En otras palabras, posibilita la creación de redes en la banda de 2,4 GHz, manteniendo la compatibilidad con 802.11b, pero operando con el ancho de banda de 802.11a.

Ofrece una compatibilidad completa en comparación con otros estándares, y proporciona una velocidad de 54 Mbps, similar a 802.11a, pero utilizando la misma frecuencia de 2,5 GHz, lo que permite el uso de las mismas antenas que 802.11b. Sin embargo, al emplear la frecuencia de 2,5 GHz, enfrenta los mismos desafíos que el estándar mencionado previamente.

- **802.11n**

Se trata de un estándar de cuarta generación que es compatible con los estándares 802.a, 802.b, y 802.g, el cual opera en las frecuencias: 2,4 GHz (802.11b y 802.11g) y 5 GHz

(802.11a), tiene un funcionamiento en las frecuencias de 2.4 y 5 GHz. La velocidad real de transmisión podría llegar a los 300 Mbps, por lo cual su velocidad debería ser al menos 10 veces más rápida que una red que trabaja en los estándares 802.11a y 802.11g, y 40 veces más rápida que una red en el estándar 802.11b. Alcanza además una operación mayor gracias al servicio de la tecnología MIMO *Múltiple Input – Múltiple Output*, ya que ofrece el uso de varios canales al mismo tiempo para enviar y recibir información. (Acuña & Aponte, 2013).

- **802.11ac**

Este estándar es una actualización del 802.11n, brinda un similar alcance, pero aumenta la velocidad de transmisión. Opera en la banda de 5 GHz e incorpora la tecnología de formación de haz, banda ancha y múltiples antenas para ofrecer 28 velocidades de datos teóricas de hasta 1,3 Gbps, más del doble que las tasas de pico de 600 Mbps alcanzadas con el estándar 802.11n (J. Salazar, 2012).

- **802.11ax**

Debido a la constante evolución de las redes inalámbricas y la necesidad de conectar un amplio mundo de dispositivos electrónicos para el acceso a internet, surge el estándar 802.11ax, este estándar tiene como objetivo mejorar la capacidad y la confiabilidad inalámbrica para ofrecer una mejor experiencia al usuario. Esta fue diseñada para optimizar las redes inalámbricas, el 802.11ax introduce nuevas características en comparación con sus predecesores, como, por ejemplo, enlace descendente y ascendente OFDMA, enlace descendente y ascendente MIMO multiusuario, reutilización espacial, consumo de energía reducido, etc (A. Mora et al., 2021). En la Tabla 1, se describe la comparativa entre los estándares mencionados.

Tabla 1. Comparativa de tecnologías Wi-Fi.

Estándar Wi-Fi	Año de Introducción	Frecuencia	Velocidad Máxima
802.11b	1999	2.4 GHz	11 Mbps
802.11a	1999	5 GHz	54 Mbps
802.11g	2003	2.4 GHz	54 Mbps
802.11n (Wi-Fi 4)	2009	2.4 GHz y 5 GHz	600 Mbps
802.11ac (Wi-Fi 5)	2013	5 GHz	3.5 Gbps
802.11ax (Wi-Fi 6)	2019	2.4 GHz y 5 GHz	9.6 Gbps
802.11ax (Wi-Fi 6E)	2020	6 GHz	Similar a Wi-Fi 6

4.3. Protocolos de Seguridad en Redes Wi-Fi

4.3.1. Definición y Características

Las tecnologías inalámbricas simplifican la conexión a Internet desde cualquier ubicación y posibilitan la movilidad de los usuarios al eliminar las conexiones físicas a las redes. No obstante, las características inherentes a la transmisión en redes inalámbricas han suscitado inquietudes en cuanto a la seguridad, ya que la información se intercambia en el espacio, facilitando la interceptación y el uso malicioso por parte de cualquiera que disponga del equipo apropiado. Por lo tanto, es necesario desarrollar servicios de seguridad proporcionados por protocolos.

La confidencialidad, impidiendo el acceso no autorizado a los contenidos de un mensaje, se logra mediante la protección del contenido de los datos con el cifrado. El cifrado es opcional en las WLAN, pero sin él, cualquier dispositivo compatible con el estándar dentro del alcance de la red puede leer todo su tráfico. Múltiples protocolos de seguridad han sido desarrollados para proteger las redes Wi-Fi contra amenazas y accesos no autorizados, a continuación, se describen algunos (J. Salazar, 2012).

4.3.1.1. Wired Equivalent Privacy (WEP). Este protocolo tiene como objetivo proporcionar un nivel de privacidad comparable al de una red cableada. Se trata de un protocolo de seguridad que se basa en el método de cifrado RC4, ofreciendo opciones de claves de 64 bits o 128 bits. Ambas opciones utilizan un vector de inicialización de 24 bits, pero difieren en la longitud de la clave secreta, siendo de 40 bits o 104 bits. Aunque todos los productos Wi-Fi son compatibles con la criptografía de 64 bits, no todos admiten la de 128 bits. Además del cifrado, incorpora un proceso de verificación de redundancia cíclica mediante el patrón CRC-32, que se emplea para garantizar la integridad del paquete de datos. Es importante señalar que el WEP no asegura la totalidad de la conexión, sino únicamente el paquete de datos. Este protocolo no es completamente seguro, ya que existen programas capaces de descifrar las claves de cifrado si la red es monitoreada durante un período considerable de tiempo.

4.3.1.2. Wi-Fi Proyected Access (WPA). Diseñado con el propósito de salvaguardar tanto las versiones presentes como futuras de los dispositivos IEEE 802.11, el WPA representa un subconjunto de la especificación IEEE 802.11i y sustituye al WEP mediante la implementación de una nueva tecnología de cifrado denominada Protocolo de Integridad de Clave Temporal (TKIP) con Verificación de Integridad del Mensaje (MIC).

Asimismo, introduce un esquema de autenticación mutua que hace uso del protocolo IEEE 802.1X/*Extensible Authentication* (EAP) o la tecnología de clave precompartida (PSK) (INCIBE, 2011). Concebido para abordar las deficiencias de seguridad del WEP, el WPA incorpora un protocolo conocido como TKIP (Protocolo de Integridad de Clave Temporal), con un vector de inicialización de 48 bits y una criptografía de 128 bits. Al emplear TKIP, la clave se modifica en cada paquete y se sincroniza entre el cliente y el punto de acceso; además, se beneficia de la autenticación del usuario mediante un servidor central (INCIBE, 2011).

4.3.1.3. WPA 2. Representando una mejora con respecto al WPA, el WPA2 incorpora el algoritmo de cifrado conocido como AES (*Advanced Encryption Standard*). Este protocolo proporciona una protección avanzada contra ataques a redes inalámbricas. Al hacer uso del cifrado AES, que se equipara al nivel de cifrado gubernamental, y del estándar IEEE 802.1X/EAP, el WPA2 ofrece una autenticación mutua sólida basada en estándares, así como un cifrado avanzado para resguardar la red Wi-Fi de diversas amenazas y ataques. Ante la identificación de una vulnerabilidad en la seguridad del protocolo utilizado en la versión 1 del WPA, la Wi-Fi Alliance desarrolló una segunda versión para abordar dicho problema. Esta nueva versión impone la implementación del protocolo de encriptación AES, que se utiliza de manera predeterminada en la norma WPA versión 2 (Guevara, 2017). En la Tabla 2 se describe de manera resumida las características principales de WEP, WPA y WPA2.

Tabla 2. Descripción WEP, WPA y WPA2

Estándar Wi-Fi	Año de Introducción	Encriptación	Seguridad	Vulnerabilidades conocidas	Compatibilidad de dispositivos	Observaciones
WEP	1997	RC4	Baja	Numerosas	Alta	Primera implementación de seguridad Wi-Fi, muy vulnerable a ataques.
WPA	2003	TKIP (Temporal Key Integrity Protocol)	Moderada	Algunas	Alta	Mejora sobre WEP, pero aún con vulnerabilidades, usado como medida temporal.
WPA 2	2004	AES (Advanced Encryption Standard)	Alta	Pocas	Alta	Estándar más seguro, recomendado para todas las redes modernas.

4.4. Ciberseguridad

4.4.1. Introducción

La ciberseguridad es un tema que ha abarcado mucho en esta era digital, debido a una sociedad que se encuentra conectada todo el tiempo a la red, y propensos a los ciberataques perpetrados por diversos actores, como delincuentes, el crimen organizado o terroristas, dando origen a que, las naciones y organizaciones respondan gradualmente a esta situación para hacer frente a esta amenaza global. En consecuencia, se han desarrollado estrategias y sistemas de respuesta para proteger la seguridad de ciudadanos y empresas, lo que ha implicado ajustes y adaptaciones en la legislación nacional e internacional.

En el ámbito jurídico global, de acuerdo al *ius ad bellum* de la Carta de las Naciones Unidas, los ataques cibernéticos entre naciones pueden ser considerados como un uso de poder, ocasionando enfrentamientos a nivel internacional y la nación amenazada poseería el derecho de defensa por medio de una respuesta armada. En términos generales, el Consejo de Seguridad tiende a calificar estos actos como agresiones y amenazas a la paz, teniendo que involucrarse para restablecer la tranquilidad y la seguridad internacional (Pons, 2017).

En consecuencia, la relevancia de la ciberseguridad ha crecido considerablemente; se han generado adelantos para salvaguardar sistemas, dispositivos y redes. La relación entre ciberseguridad e innovación es bidireccional, por un lado, la ciberseguridad permite la entrada de innovaciones en todos los sectores de la economía digital al generar confianza en los usuarios de las tecnologías de la información; por otro, las distintas innovaciones tecnológicas permiten a las empresas especializadas en ciberseguridad diseñar dispositivos y sistemas para mejorar la capacidad de protección de las organizaciones, las redes y los datos (José et al., 2022).

4.4.2. Contexto e importancia de la Ciberseguridad

Se entiende por ciberseguridad como el conjunto de instrumentos, políticas, principios de seguridad, salvaguardias, procesos de gestión de riesgos, acciones, formación, buenas prácticas, seguros y tecnologías utilizados para proteger los activos de una organización y a sus usuarios en el entorno cibernético. Tiene la finalidad de preservar la confidencialidad, integridad y disponibilidad de la información en el ciberespacio, definido como el complejo entorno resultante de la interacción entre personas, software y servicios en Internet, a través de dispositivos tecnológicos y redes conectadas, que no tienen existencia física.

Se basa en la seguridad de las infraestructuras informáticas y de la información que transita a través de las redes, así como en el diseño de normas, procedimientos, métodos y técnicas que garanticen la seguridad y fiabilidad de los sistemas de comunicación. Esto es de

gran importancia, ya que los ataques en el ciberespacio no sólo afectan al ámbito digital, sino que también pueden tener repercusiones en el mundo físico, como dañar los sistemas estructurales de una organización, una nación o una región (C. Castillo, 2021).

En conclusiones generales, podemos entender que la ciberseguridad es aquella que tiene la capacidad de salvaguardar el ciberespacio contra ataques informáticos, con el único propósito de prevenir el acceso, manipulación, o destrucción no autorizada de datos almacenados digitalmente. A diferencia de la seguridad informática convencional, la atención principal en la ciberseguridad ha recaído en el desarrollo de tecnologías y métodos innovadores, así como en la capacitación del personal para hacer frente a los riesgos digitales emergentes (U. Castillo & Polanco, 2023).

La seguridad cibernética va más allá de lo técnico; implica la implementación de nuevas estrategias organizativas, políticas públicas y normas de conducta en línea. Estos elementos, que constituyen conocimientos flexibles y activos intangibles, son esenciales para garantizar un entorno de seguridad cibernética eficiente y económicamente viable (José et al., 2022).

4.4.3. Políticas de seguridad.

Las políticas de seguridad son un conjunto de normas y prácticas que establecen y regulan los servicios de seguridad dentro de una organización o sistema, con el objetivo de proteger sus recursos críticos y sensibles. En otras palabras, es una declaración que define lo que está permitido y lo que no está permitido hacer.

Las políticas de seguridad constituyen el fundamento esencial para la protección y gestión de la seguridad de un sistema, en estas políticas se describen de manera detallada los servicios de seguridad que el sistema debe proporcionar. Además, se especifica quién está autorizado para acceder a los recursos del sistema y qué acciones están permitidas o prohibidas para dichos recursos, este aspecto es crucial ya que define los límites y las responsabilidades de los usuarios y administradores del sistema.

Dentro de las políticas de seguridad, también se delinean las estrategias y procedimientos que deben seguirse para implementar los servicios de seguridad, esto incluye la definición de medidas específicas para proteger los datos, las aplicaciones y la infraestructura tecnológica contra posibles amenazas y vulnerabilidades. Las políticas pueden abarcar desde el uso de contraseñas fuertes y la encriptación de datos, hasta la configuración segura de dispositivos y la respuesta a incidentes de seguridad.

La implementación concreta de una política de seguridad se lleva a cabo mediante diversos mecanismos de seguridad, estos pueden incluir software de protección, como antivirus

y firewalls, así como prácticas y procedimientos operativos, como auditorías de seguridad, copias de seguridad regulares y monitoreo continuo de la red.

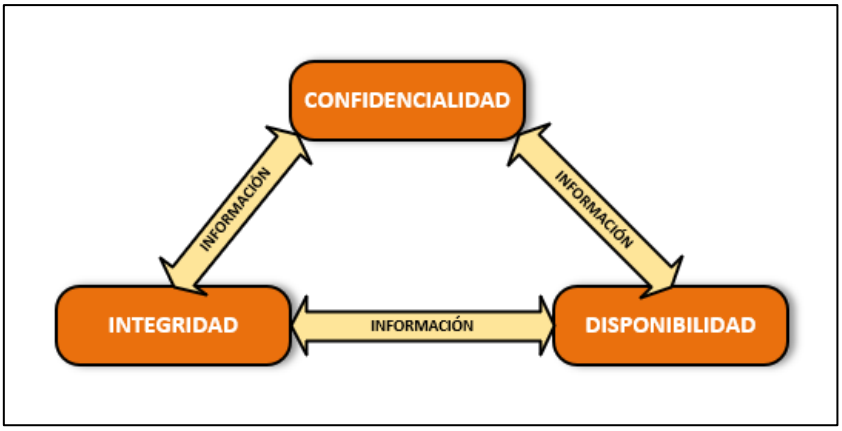
Es importante destacar que las políticas de seguridad no siempre tienen que ser una declaración formal escrita en un lenguaje técnico y estructurado, en muchos casos, puede consistir en un conjunto de directrices y recomendaciones simples sobre la seguridad del sistema, expresadas en un lenguaje claro y accesible, estas directrices pueden ser igual de efectivas para guiar el comportamiento seguro de los usuarios y administradores del sistema (Navarro, 2011).

4.4.4. Principios de confidencialidad, integridad y disponibilidad.

Tres de los elementos fundamentales de la seguridad de la información son la confidencialidad, la integridad y la disponibilidad, conocidos comúnmente como la tríada de la seguridad de la información, véase la Figura 7.

Figura 7

Tríada de seguridad de la información.



Esta tríada, que se utiliza desde hace más de 20 años, proporciona un esquema que permite conceptualizar y debatir las problemáticas de seguridad, con especial atención a la protección de datos. Estos tres principios son interdependientes y juntos constituyen la base de una estrategia de seguridad completa.

La implementación eficaz de la confidencialidad, la integridad y la disponibilidad permite a las organizaciones proteger sus contenidos de información, mitigar los riesgos y preservar la confianza de sus clientes y socios. (Vega, 2021). Cada uno de los principios mencionados se los describe a continuación:

- **Confidencialidad.**

La confidencialidad es un concepto relacionado, pero distinto de la privacidad, mientras que la privacidad es más amplia, la confidencialidad se enfoca específicamente en proteger nuestros datos de accesos no autorizados, los datos deben estar disponibles únicamente para las personas, procesos o dispositivos que están autorizados a verlos o usarlos, los métodos comunes para asegurar la confidencialidad incluyen la encriptación, las contraseñas y los controles de acceso, este concepto es crucial para la privacidad y puede aplicarse en varios niveles dentro de un proceso.

Un ejemplo común es el de una persona que retira dinero de un cajero automático, en este caso, la persona probablemente intentará proteger su número de identificación personal (PIN) para poder extraer dinero con su tarjeta de forma segura, además, el operador del cajero automático protegerá la confidencialidad del número de cuenta, saldo y cualquier otra información necesaria para comunicarse con el banco correspondiente. Por su parte, el banco mantendrá la confidencialidad de la transacción y la actualización del saldo en la cuenta después de que se hayan retirado los fondos.

La confidencialidad puede comprometerse de varias maneras, como la posible pérdida de un ordenador portátil que contenga alguna información sensible, que alguien nos esté observando mientras tecleamos una contraseña, que se envíen archivos adjuntos de correo electrónico al destinatario equivocado o que un atacante acceda a nuestros sistemas a través de aplicaciones *man in the middle* (MITM).

- **Integridad.**

La integridad se refiere a la capacidad de proteger los datos contra alteraciones no autorizadas o no deseadas. Para mantener la integridad, no sólo es un requisito impedir las modificaciones no autorizadas, sino también tener la capacidad de corregir los cambios autorizados. Un buen ejemplo de mecanismos para controlar la integridad se encuentra en los sistemas de archivos de muchos sistemas operativos modernos, como Windows y Linux.

Estos sistemas comúnmente incorporan permisos que restringen las acciones que un usuario sin autorización puede realizar en un archivo específico, evitando así cambios no autorizados. Además, algunos de estos sistemas y muchas aplicaciones, como las bases de datos, ofrecen la posibilidad de deshacer o revertir cambios no deseados, la integridad es crucial cuando se trata de datos que sirven de base para tomar otras decisiones.

- **Disponibilidad.**

La disponibilidad se relaciona con la capacidad de acceder a los datos cuando los necesitamos, esto implica que los sistemas deben estar operativos y los datos deben ser

accesibles cuando los necesitamos, la falta de disponibilidad puede englobar una amplia gama de interrupciones en cualquier punto de la cadena de comunicación que permita el acceso a nuestros datos.

Estos problemas pueden estar causados por cortes de electricidad, fallos del sistema operativo o de las aplicaciones, ataques a la red de datos, sistemas comprometidos u otros inconvenientes que no permitan a los usuarios su libre acceso a la información. Estos problemas suelen estar causados por ataques de denegación de servicio (DoS) avanzados y conocidos.

4.4.5. El protocolo RADIUS en la ciberseguridad.

RADIUS es un sistema de autenticación y contabilidad utilizado por la mayor parte de los proveedores de servicios de Internet (ISP), aunque no es una norma oficial. Cuando un usuario se conecta a su ISP, debe ingresar su nombre de usuario y contraseña, esta información es enviada a un servidor RADIUS, que verifica su validez y autoriza el acceso al sistema del proveedor si los datos son correctos. Este protocolo es crucial en el campo de la ciberseguridad, especialmente en la gestión de acceso a la red, proporciona una estructura robusta para la autenticación, autorización y contabilidad (AAA) de los usuarios que acceden a la red, lo que garantiza que sólo los usuarios autorizados pueden conectarse y que todas las actividades se monitorizan adecuadamente, básicamente es un software de dominio público que se encarga de identificar a los usuarios que acceden remotamente a un servidor, permitiéndoles asignarles direcciones de red de manera dinámica.

Una de las principales características del protocolo RADIUS es su capacidad para gestionar sesiones, registrando el inicio y el final de una conexión. Esto permite determinar el consumo del usuario y facturarlo en consecuencia. Además, los datos recogidos pueden utilizarse con fines estadísticos, como se muestra en la Figura 8.

Las tres funciones principales implementadas por RADIUS (AAA) en ciberseguridad son fundamentales para la gestión y seguridad de redes informáticas. Estas funciones son Autenticación (*Authentication*), Autorización (*Authorization*) y Contabilidad (*Accounting*) (Dafonte & Pallardó, 2015). A continuación, se describe cada uno de ellos.

- **Autenticación**

Provee un método para identificar a los usuarios mediante diferentes mecanismos, como usuario y contraseña, o reto y respuesta, y selecciona el método de encriptación adecuado según el protocolo de seguridad elegido. En otras palabras, la autenticación es el servicio que verifica la identidad de un usuario antes de determinar a qué servicios de red o aplicaciones puede

acceder. Entre los métodos se puede incluir contraseñas, certificados digitales, biometría, tokens, etc.

- **Autorización**

El servicio de autorización se refiere a conceder acceso a determinadas aplicaciones o servicios de red a un usuario, basado en su autenticación previa. La autorización también puede estar sujeta a restricciones, tales como limitaciones de tiempo, ubicación física, o el número de accesos permitidos para un mismo usuario.

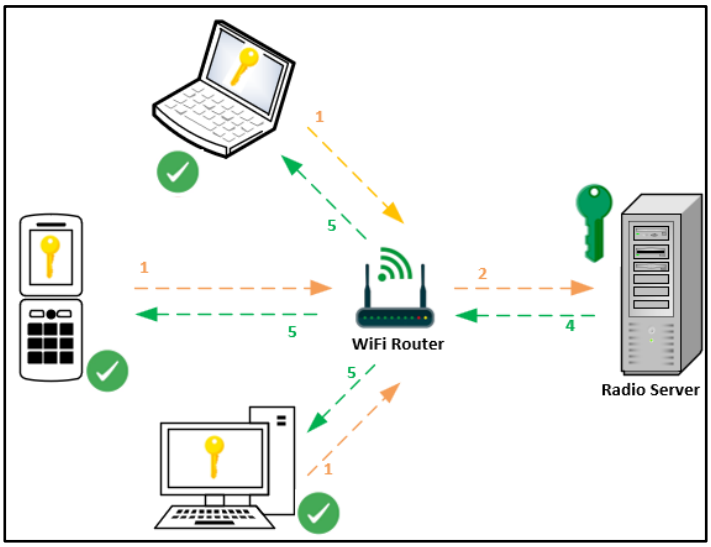
Este servicio opera mediante la combinación de varios atributos que definen lo que el usuario puede o no hacer. Para determinar los atributos de cada usuario, se realiza una consulta a una base de datos específica, cuyo resultado se envía al servicio AAA, esta base de datos puede estar localizada en el dispositivo de acceso a la red (como un servidor de acceso o enrutador) o en un servidor remoto. Entre los métodos se puede incluir controles de acceso, políticas de uso, roles y permisos.

- **Contabilidad (Accounting)**

Este componente involucra el seguimiento y registro de las actividades del usuario, como la duración de la sesión, los recursos utilizados y cualquier acción realizada durante el acceso a la red. Los registros contables son útiles para realizar auditorías, identificar patrones de uso y resolver problemas de seguridad (Weyman, 2024).

Figura 8

Proceso del protocolo RADIUS.



El servidor Radius se ocupa de comprobar que los datos del usuario que está tratando de ingresar a la red sean los correctos. Si la solicitud es correcta, el servidor finaliza la autenticación y envía al cliente la información de autorización solicitada, en cambio, si no es válido la solicitud, el servidor envía la información de error de autorización al cliente (WISP, 2020).

4.4.6. Amenazas comunes en las redes Wi-Fi Públicas

Las redes Wi-Fi públicas, aunque resultan ser cómodas, conllevan numerosos riesgos de seguridad que comprometen tanto a los usuarios como a las organizaciones. Cuando no son seguras, transmiten datos libremente, lo que permite a quien disponga de la tecnología adecuada interceptar esa información y acceder a ella.

Además, las mejoras en las tecnologías de redes inalámbricas han ampliado considerablemente el alcance y la cobertura, lo que aumenta la probabilidad de que el tráfico sea captado en un radio más amplio alrededor del equipo de origen de la red, y entre los tipos más comunes de ciberataques se incluyen los siguientes:

- **Delito cibernético**

Se habla de todas las actividades ilegales asociadas al crimen convencional, pero trasladadas al ámbito digital, usualmente, estas acciones buscan obtener beneficios económicos y sus blancos suelen ser diversos, apuntando a individuos vulnerables con recursos financieros para cumplir con sus exigencias (José et al., 2022).

- **Ciberterrorismo**

Se examina la definición proporcionada por el Consejo de Seguridad Europeo, que describe el ciberterrorismo como la utilización de las tecnologías de la información y la comunicación por parte de grupos terroristas, con el propósito de amedrentar, extorsionar y presionar a la sociedad, todo ello impulsado por motivaciones políticas o religiosas (Paredes & Semanate, 2024).

- **Ciber espionaje**

Ciberataques llevados a cabo para obtener secretos de Estado, información comercial confidencial o datos personales (José et al., 2022).

4.4.7. Amenazas cibernéticas

Las ciberamenazas se refieren a posibles ataques malintencionados o intentos de conseguir acceso no autorizado a los servicios de información, con el objetivo de robar, modificar, destruir o perturbar los datos. Estos ataques son llevados a cabo por

ciberdelincuentes, que pueden ser individuos o grupos, y que tienen motivos que van desde la delincuencia financiera y el espionaje hasta la interrupción del servicio y la guerra cibernética (Guamán et al., 2023).

A continuación, se describen algunos métodos y herramientas utilizados como amenazas cibernéticas.

- **Malware**

Software malicioso que daña o toma el control de sistemas informáticos sin autorización. Incluye virus, gusanos y ransomware.

- **Phishing**

Técnica de engaño en la que los ciberdelincuentes se hacen pasar por entidades legítimas para robar información confidencial.

- **Ataques de denegación de servicio (DoS)**

Sobrecarga intencional de un sistema con tráfico malicioso para dejarlo inaccesible a usuarios legítimos.

- **Ataques de denegación de servicio distribuido (DDoS)**

Variante del ataque DoS, que utiliza múltiples dispositivos para coordinar un ataque masivo y dificultar la mitigación.

- **Espionaje cibernético**

Infiltración en sistemas informáticos o redes para obtener información confidencial o secretos empresariales.

- **Ataques de día cero**

Aprovechamiento de vulnerabilidades previamente desconocidas en software o sistemas operativos.

- **Ataques de fuerza bruta**

Método que prueba todas las combinaciones posibles para descifrar contraseñas o claves encriptadas.

4.4.8. Vulnerabilidades cibernéticas

Las vulnerabilidades cibernéticas se refieren a las debilidades o fallos presentes en sistemas informáticos, redes o software que pueden ser explotados para llevar a cabo actividades malintencionadas. Estas vulnerabilidades pueden ser aprovechadas por actores maliciosos, como hackers o ciberdelincuentes, quienes pueden utilizar estas fallas para infiltrarse en un sistema, alterar su funcionamiento, robar datos o causar daños de diversas

maneras, estas acciones maliciosas pueden incluir desde la modificación de datos sensibles, la interrupción de servicios críticos, hasta el acceso no autorizado a información confidencial.

Las vulnerabilidades cibernéticas pueden originarse de múltiples fuentes, entre las más comunes se encuentran los errores de programación, que pueden introducir fallos en el software, permitiendo que los atacantes ejecuten código malicioso, las configuraciones incorrectas de sistemas y aplicaciones que también pueden dejar puertas abiertas para el acceso no autorizado, además, los fallos de hardware pueden proporcionar puntos de entrada para los atacantes.

Las prácticas de seguridad deficientes, como el uso de contraseñas débiles o la falta de actualizaciones de seguridad, también aumentan el riesgo de explotación, finalmente, los errores humanos, como la falta de capacitación adecuada o el descuido en la implementación de medidas de seguridad, pueden crear vulnerabilidades significativas.

La manipulación de estas vulnerabilidades puede tener implicaciones graves y de gran alcance. En primer lugar, puede comprometer la seguridad y la privacidad de la información, exponiendo datos sensibles a individuos no autorizados, incluida información personal, datos financieros, secretos comerciales y propiedad intelectual. En segundo lugar, puede afectar a la sostenibilidad de las operaciones, causando interrupciones en servicios críticos y afectando a la capacidad de una organización para funcionar de forma eficaz. En tercer lugar, puede dañar la imagen de una organización, afectando a la confianza de clientes, socios y otras partes interesadas.

En un contexto nacional, las vulnerabilidades cibernéticas son aquellas debilidades o fallos en los sistemas de información que ponen en riesgo la seguridad de un país. Estas vulnerabilidades pueden hacer que un atacante ponga en peligro la integridad, disponibilidad o confidencialidad de información crítica para el funcionamiento de un gobierno (Guamán et al., 2023).

4.5. Ingeniería Social

La ingeniería social implica el uso de engaños para obtener información confidencial de las personas, lo que puede poner en riesgo la seguridad. Su uso ha aumentado debido al crecimiento significativo de los usuarios conectados a las redes sociales, correos electrónicos y otras formas de comunicación en línea, estas técnicas de manipulación psicológica se utilizan para engañar a las personas y obtener información confidencial de ellas. Se basa en explotar la confianza, la curiosidad y la falta de atención, y puede incluir pretextos, phishing, malware y otras tácticas engañosas para lograr sus objetivos.

La ingeniería social representa un riesgo importante para la seguridad de la información y la privacidad, por lo que es crucial que individuos y organizaciones estén conscientes de los riesgos y tomen medidas para protegerse.

4.5.1. Tipos de ciberdelitos más comunes en Ecuador

Los ciberdelincuentes a menudo crean perfiles falsos, enlaces con virus, comercios electrónicos falsos y sitios web fraudulentos que, en muchas ocasiones, la identificación de estos ciberdelincuentes resulta complicada.

A continuación, se presenta la definición de los delitos informáticos más frecuentes (Juca & Medina, 2023).

- **Robo de información personal**

Los ciberdelincuentes obtienen datos confidenciales de sus víctimas, como son las contraseñas y números de tarjetas de crédito, utilizando métodos como el phishing y el malware.

- **Fraude en línea**

Los delincuentes pueden engañar a las personas para lograr obtener su dinero utilizando sitios web falsos, correos electrónicos y mensajes de texto, disfrazándose de instituciones bancarias o gubernamentales para solicitar datos personales o hacer pagos**.**

- **Ataques informáticos a empresas y entidades públicas**

En Ecuador se han registrado un índice alto de ataques informáticos dirigidos a empresas y organizaciones públicas en los últimos años. Más de 16,000 cuentas de correo electrónico fueron severamente perjudicadas por un ataque cibernético a la Contraloría General del Estado en 2019.

- **Sextorsión**

La sextorsión en Ecuador es una forma de delito cibernético que ha ido creciendo en los últimos años. El chantaje implica recopilar imágenes o videos privados de la víctima y usarlos para extorsionarla.

- **Ciberacoso**

En Ecuador, los niños y adolescentes son víctimas principales de este tipo de delito informático, ya que los acosadores intimidan, hostigan o amenazan a sus víctimas por medio de las redes sociales y otras plataformas en línea.

Es importante saber que el COIP es el órgano encargado de sancionar estos delitos en Ecuador, y que cada una de estas formas de ciberdelitos están clasificadas a continuación en la Tabla 3.

Tabla 3. Delitos más comunes y su sanción en el artículo respectivo

Descripción	Articulo	Sanción (años de prisión)
Pornografía infantil	103	13 a 16
Violación al derecho a la intimidad	178	1 a 3
Revelación ilegal de información de bases de datos	229	1 a 3
Interceptación de comunicaciones	476	3 a 5
Ataque a la integridad de sistemas informáticos	232	3 a 5
Delitos contra la información pública reservada legalmente	233	3 a 5
Acceso no consentido a un sistema informático, telemático o de telecomunicaciones	234	3 a 5

Nota. Adaptado de (Juca & Medina, 2023)

4.6. Seguridad de la información y ciberseguridad en Ecuador.

Ecuador se ha enfrentado a varios ciberataques importantes que han marcado un precedente en la historia de la ciberseguridad del país, entre los que destacan el ataque de ransomware al municipio de Quito en el año 2022, que comprometió el 20% de su base de datos, y la vulneración de la plataforma CIES, que afectó a los subsistemas de Inteligencia de la Policía y las Fuerzas Armadas.

Estos incidentes no solo han impactado al sector gubernamental, sino también al privado, como lo demuestra el ciberataque al Banco Pichincha en octubre de 2021, que provocó la paralización de sus operaciones y que estos hechos han motivado una respuesta nacional que involucra al Gobierno, al sector privado, a la academia y a la sociedad civil, que desembocó en la creación de un Comité de Ciberseguridad desde 2017.

La Policía Nacional de Ecuador identificó en 2023 varios tipos de estafas cibernéticas en el país, como *phishing, spear phishing* y *smishing*, cuyo objetivo es el de engañar a los usuarios para conseguir su información de carácter confidencial; además, se denunciaron otros delitos graves, como la violación de la privacidad, la interceptación ilegal de datos y los ataques a centros informáticos, que contemplan penas de hasta siete años de prisión.

El incremento de denuncias de estas estafas durante la pandemia puso de manifiesto la urgente necesidad de tomar las medidas preventivas y seguir las recomendaciones de seguridad para así proteger la información personal de los ciudadanos ecuatorianos. Estos resultados ponen de manifiesto una brecha significativa en la capacidad de Ecuador para responder y prevenir las ciberamenazas.

El aumento de ciberdelitos en Ecuador ha mostrado un incremento preocupante, pasando de 682 casos en 2020 a 1.852 en 2021, y sumando 393 en 2022, este incremento se debe a la falta de cultura digital en el país, donde, aunque un 75.6% de la población utiliza internet, solo un 10% posee conocimientos digitales adecuados. Delitos comunes como la apropiación fraudulenta y la suplantación de identidad, sancionados por el Código Orgánico Integral Penal (COIP) de Ecuador, reflejan la necesidad urgente de aumentar la concienciación y la educación en seguridad digital.

Los clientes bancarios son a menudo el punto más vulnerable en cuanto a ciberseguridad, lo que pone de relieve la necesidad de una educación digital adecuada para evitar ser víctima de la ciberdelincuencia.

En 2022, los pagos a los ciberdelincuentes en Ecuador superaron los 7,8 millones de USD debido a diversos ataques, con esto la Unidad de Cibercrimen de la Policía Nacional registró 1340 casos de ciberataques, concentrados principalmente en provincias como Guayas, Pichincha, Manabí, Imbabura, Carchi y Azuay. Estos ataques pueden emplear diversos métodos, pero su objetivo común es obtener información personal para cometer fraudes.

Ejemplos de estos incluyen engaños a través de correos electrónicos personales y corporativos, ofertas de mensajería puerta a puerta, supuestos viajes ganados y promociones, donde la clave de su efectividad radica en la personalización del engaño para hacerlo creíble y convincente.

4.7. Organismos nacionales de ciberseguridad en Ecuador

La Unidad Nacional Especializada en Investigación de Ciberdelito de la Fiscalía y la Unidad de Ciberdelito de la Policía Nacional son los organismos con la misión de garantizar la ciberseguridad del país a través de métodos de seguridad informática. Ambos organismos se encargan de cuidar la seguridad informática del país, con personal capacitado.

La Unidad Nacional Especializada de Investigación de Ciberdelitos de la fiscalía esta encargada de orientar investigaciones relacionada a los ciberdelitos, además de la correcta interpretación de los delitos informáticos entregando la evidencia necesaria, este organismo trabaja juntamente con la Unidad de ciberdelitos de la Policía Nacional, compartiendo toda información que tenga que ver con la investigación.

Estos dos organismos trabajan arduamente para cuidar la seguridad informática del país y la reducción del índice de ciberdelitos en el país, mediante técnicas de monitoreo y procesos forenses que entreguen información de este tipo de delitos, además de alertar de ciberdelitos

que perjudiquen a la ciudadanía, instituciones en las que sus datos se vean amenazados por delincuentes informáticos. (Fiscalia General del Estado, 2024).

4.8. Estándares ISO de Ciberseguridad Internacional

Los estándares de seguridad son técnicas reconocidas en publicaciones para proteger el entorno cibernético de usuarios u organizaciones, que incluyen redes, dispositivos, software, procesos, información, aplicaciones, servicios y sistemas conectados a las redes.

Su principal objetivo es reducir riesgos, como la prevención y mitigación de ciberataques. Esto incluye herramientas, políticas, conceptos, salvaguardas, guías, enfoques de gestión de riesgos, acciones, capacitación, mejores prácticas, aseguramiento y tecnologías (F. Salazar, 2021).

Algunos de los estándares ISO internacionales asociados a la ciberseguridad se describen a continuación:

- **ISO 15504**

Denominado como *Software Process Improvement Capability Determination*, tiene como objetivo ofrecer un modelo para evaluar la capacidad en los procesos de desarrollo de productos de software.

- **ISO 22301**

Este estándar ayuda a gestionar la continuidad de un negocio o con las actividades de una organización, estableciendo una base de conocimientos para proteger y defender los intereses de sus empleados y partes interesadas, manteniendo la reputación ante cualquier amenaza.

- **ISO 27001**

La norma ISO 27001 considera el diseño e implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI) que tiene como objetivo la preservación de la confidencialidad, la integridad y disponibilidad de la información, dando confianza a clientes y proveedores.

- **ISO 27002**

El propósito principal de la norma ISO 27002 es establecer pautas y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización, incluyendo la selección, implementación y administración de controles, teniendo en cuenta los entornos de riesgo encontrados en la empresa. Esta norma puede apoyar la implantación del SGSI.

- **ISO 27005**

La norma ISO 27005 asocia la gestión de riesgos de seguridad de la información, que proporciona pautas para administrar los diferentes tipos riesgos en una empresa y se puede decir que es apropiado para cualquier organización que tenga que controlar los riesgos relacionados con la seguridad de sus datos.

No establece una metodología específica porque depende de una variedad de factores, como el alcance del SGSI y la industria comercial.

- **ISO 27014**

La norma 27014 busca que una organización no solo cumpla con los requisitos contractuales y reglamentarios, sino que también pueda brindar un valor a sus partes interesadas, mejora la supervisión de la seguridad de la información a nivel directivo, gestiona sus operaciones de manera eficiente e invierte en seguridad de la información de manera estratégica y efectiva.

4.9. Análisis específico de la situación actual de la ciberseguridad en Ecuador y Loja.

Los datos estadísticos aportados por la Dirección de Estadísticas y Sistemas de Información de la fiscalía general del Estado son esenciales para comprender la situación actual de los ciberataques en Ecuador. Este análisis tiene como objetivo evaluar la magnitud del problema, determinar patrones y tendencias, y establecer una sólida base para el desarrollo de estrategias de mitigación y respuesta.

En Ecuador, los ciberataques representan una amenaza creciente para la seguridad nacional y la integridad de las infraestructuras críticas, es crucial contar con un diagnóstico preciso que permita la formulación de políticas efectivas y la implementación de medidas preventivas adecuadas.

Este capítulo se centra en un enfoque cuantitativo para examinar la frecuencia, los tipos de ciberataques, los sectores más afectados y la evolución temporal de estos incidentes en el país.

A continuación, se presenta un desglose detallado de los datos más relevantes que ofrecen una interpretación de los resultados obtenidos a partir de las estadísticas oficiales, el período analizado abarca desde enero de 2023 hasta marzo de 2024.

En la Tabla 4 se muestra el número total de denuncias por delitos penales, también conocidas como noticias del delito (NDD), registradas a nivel nacional durante el período analizado, esta tabla proporciona una visión detallada de la incidencia de estos delitos en todo el país.

Tabla 4. Delitos penales a nivel nacional

Tipo penal	Total 2023	Total, 01ene - 30jun2024	Total NDDs	Porcentaje
Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.	488	446	934	40.33%
Ataque a la integridad de sistemas informáticos.	174	138	312	13.47%
Comercialización de pornografía con utilización de niñas, niños o adolescentes.	38	13	51	2.20%
Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos.	173	81	254	10.97%
Delitos contra la información pública reservada legalmente.	5	1	6	0.26%
Falsificación informática.	67	58	125	5.40%
Interceptación ilegal de datos.	61	46	107	4.62%
Pornografía con utilización de niñas, niños o adolescentes.	141	72	213	9.20%
Revelación ilegal de base de datos.	29	24	53	2.29%
Transferencia electrónica de activo patrimonial.	165	96	261	11.27%
Total, NDDs	1341	975	2316	100.00%

Nota. Basado en los datos de la fiscalía general del Estado

Como se puede observar en la Tabla 4, a nivel nacional existe una enorme cantidad de noticias de delito de diferentes tipos, en el año 2023 se produjo 1341 delitos y para mediados del 2024 se produjo 975 delitos, dando un total de 2316 delitos producidos, el delito más comúnmente producido en el año 2023, es el acceso no consentido a un sistema informático, telemático o de telecomunicaciones, incluso hasta mediados del año 2024 sigue siendo el delito más producido, dando un total de 934 delitos de esta clase que comprende el 40.33% en comparación con otros delitos hasta el momento. En cambio, el delito menos frecuente es de delitos contra la información pública reservada legalmente, que solo se han detectado 5 delitos de este tipo en el año 2023 y 1 hasta en junio del 2024, que comprende el 0.26% del total de este tipo de delito.

En la Tabla 5 se muestra el número total de denuncias por delitos penales, registradas por provincia durante el período analizado.

Tabla 5. Cantidad de delitos a nivel provincial

Provincia de incidente	Total 2023	Total, 01ene - 30jun2024	Total NDDs	Porcentaje
Azuay	55	30	85	3.67%
Bolívar	14	13	27	1.17%
Cañar	12	4	16	0.69%
Carchi	11	16	27	1.17%
Chimborazo	61	30	91	3.93%
Cotopaxi	9	11	20	0.86%
El oro	19	24	43	1.86%
Esmeraldas	25	8	33	1.42%
Galápagos	3	0	3	0.13%
Guayas	264	188	452	19.52%
Imbabura	22	26	48	2.07%
Loja	19	43	62	2.68%
Los Ríos	28	16	44	1.90%
Manabí	68	55	123	5.31%
Morona Santiago	14	3	17	0.73%
Napo	15	5	20	0.86%
Orellana	13	5	18	0.78%
Pastaza	2	2	4	0.17%
Pichincha	595	431	1026	44.30%
Santa Elena	16	8	24	1.04%
Santo Domingo de los Tsáchilas	19	17	36	1.55%
Sucumbíos	21	24	45	1.94%
Tungurahua	30	8	38	1.64%
Zamora Chinchipe	6	8	14	0.60%
Total, NDDs	1.341	975	2316	100.00%

Nota. Basado en los datos de la fiscalía general del Estado

Como se puede observar en la Tabla 5, la provincia que más ha sufrido delitos cibernéticos durante el año 2023 es Pichincha con un total de 595 delitos, y sigue siendo el de mayor ataque durante el 2024 con 431 delitos, que en total lleva 1026 delitos hasta junio del 2024, con un porcentaje del 44.30%. En cambio, la provincia con menos frecuencia en sufrir ataques cibernéticos es Pastaza con un total de 4 delitos entre el año 2023 hasta junio de 2024.

La provincia de Loja entre el año 2023 y mediados del 2024 ha sufrido 62 denuncias de delito, que comprende el 2.68%.

En la Tabla 6 se muestra el número total de denuncias por delitos penales, registradas por cantones en la provincia de Loja, durante el periodo 2023-junio 2024.

Tabla 6. Cantidad de delitos a nivel cantonal en la provincia de Loja

Provincia, cantón de incidente y tipo penal	Total 2023	Total, 01ene - 30jun2024	Total NDDs	Porcentaje
CALVAS	**1**	**1**	**2**	**3.23%**
Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.	1	1	2	3.23%
CHAGUARPAMBA	**1**		**1**	**1.61%**
Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos.	1		1	1.61%
ESPINDOLA		**2**	**2**	**3.23%**
Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos.		1	1	1.61%
Interceptación ilegal de datos.		1	1	1.61%
LOJA	**15**	**37**	**52**	**83.87%**
Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.	1	9	10	16.13%
Ataque a la integridad de sistemas informáticos.		1	1	1.61%
Comercialización de pornografía con utilización de niñas, niños o adolescentes.	1		1	1.61%
Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos.	4	1	5	8.06%
Falsificación informática.	1		1	1.61%
Interceptación ilegal de datos.		17	17	27.42%
Comercialización de pornografía con utilización de niñas, niños o adolescentes.	3	3	6	9.68%
Transferencia electrónica de activo patrimonial.	5	6	11	17.74%
PUYANGO		**1**	**1**	**1.61%**
Interceptación ilegal de datos.		1	1	1.61%
SOZORANGA		**1**	**1**	**1.61%**
Revelación ilegal de base de datos.		1	1	1.61%
ZAPOTILLO	**2**	**1**	**3**	**4.84%**
Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.	2		2	3.23%
Falsificación informática.		1	1	1.61%
Total, NDDs en la Provincia de Loja	19	43	62	100.00%

Nota. Basado en los datos de la fiscalía general del Estado

La Tabla 6 nos presenta los diferentes delitos producidos a nivel cantonal en la provincia de Loja, en el año 2023 la misma capital Loja ha sufrido una variedad de denuncias por delito con un números de 15 delitos, siendo las comunes el contacto con finalidad sexual con menores de dieciocho años por medios electrónicos y de transferencia electrónica de activo patrimonial, en lo que va del año 2024 se ha duplicado la cifra produciéndose un total de 37 delitos, siendo

la intercepción ilegal de datos la más frecuente, la capital de Loja tiene el 83.87% de delitos producidos a nivel de la provincia.

4.10. Análisis de Redes Wifi-Públicas

En el panorama digital actual, las redes Wi-Fi públicas se han convertido en una herramienta omnipresente y esencial para la conectividad inalámbrica en entornos urbanos, comerciales y sociales. Sin embargo, la creciente dependencia de estas redes conlleva importantes desafíos en términos de seguridad, rendimiento y fiabilidad, por ende, el análisis de redes se perfila como una herramienta fundamental para escanear y evaluar la infraestructura de las redes Wi-Fi públicas, abordando aspectos cruciales como la configuración, los protocolos de seguridad, las contraseñas y las políticas de acceso.

De los aspectos más críticos en el análisis de redes es la seguridad, ya que las redes Wi-Fi públicas son generalmente vulnerables a diversas amenazas cibernéticas, desde ataques de intrusos hasta la interceptación de datos confidenciales. Analizando a fondo la configuración de la red es posible detectar puntos débiles y posibles fallos de seguridad, como las contraseñas y protocolos de cifrado obsoletos, estableciendo una evaluación preventiva que va a permitir a los administradores de red fortalecer las defensas y poder mitigar los riesgos de vulnerabilidad, garantizando así la integridad y confidencialidad de los datos transmitidos por la red.

Además, el análisis de redes facilita la evaluación y optimización de los protocolos de seguridad utilizados en las redes Wi-Fi públicas. Desde el despliegue de estándares de cifrado robustos hasta la implementación de mecanismos de autenticación multifactorial, estas herramientas proporcionan información detallada sobre la efectividad y la adecuación de los protocolos de seguridad existentes, al identificar protocolos débiles u obsoletos, los administradores pueden actualizar y mejorar la seguridad de la red, garantizando así una protección más sólida contra ataques maliciosos y amenazas emergentes.

Las redes Wi-Fi públicas son comúnmente los objetivos de ataques cibernéticos, ya que son accesibles para la mayoría de usuarios. Analizar la infraestructura de estas redes permite identificar posibles vulnerabilidades en la configuración, como puntos de acceso mal configurados o protocolos de seguridad débiles, haciendo que los administradores puedan tomar medidas proactivas para fortalecer la seguridad y proteger los datos confidenciales de los usuarios.

4.10.1. Herramientas para el análisis de Redes.

El uso de herramientas de análisis de redes para escanear y evaluar la infraestructura de las redes Wi-Fi públicas es esencial para garantizar la seguridad, el rendimiento, la disponibilidad y la eficiencia de estas redes, lo que a su vez contribuye a una experiencia de usuario satisfactoria y a la protección de la información sensible. A continuación, se detallan algunas de las herramientas más usadas.

- **Aircrack-ng**

Es un completo conjunto de herramientas que auditan redes inalámbricas Wi-Fi, esta herramienta se centra en diferentes áreas de la seguridad en redes inalámbricas como monitorización de paquetes, ataques, pruebas y cracking. Permite realizar ataques de fuerza bruta para descifrar contraseñas de redes Wi-Fi protegidas con WEP o WPA/WPA2, así como también capturar paquetes y realizar análisis detallados de los protocolos de seguridad utilizados (Aircrack-ng, 2024).

- **Linset**

Aplicación para auditar redes inalámbricas que no utiliza diccionarios de descifrado para obtener el código de acceso a la red. Con esta herramienta, la cooperación del usuario, que desconoce el ataque, es de vital importancia, lo que implica que el usuario tiene poco o ningún conocimiento de seguridad informática. Linset crea un punto de acceso falso con el mismo ESSID que el que estamos atacando y sin ningún tipo de cifrado; además, autentica los puntos de acceso de los clientes legítimos, impidiendo que se autentiquen y haciendo que accedan al punto de acceso creado por esta herramienta e introduzcan la contraseña de la red (Acosta et al., 2018).

- **Kismet**

Es una herramienta de detección de redes inalámbricas que permite escanear y monitorear redes Wi-Fi en tiempo real. Kismet puede identificar redes ocultas, detectar dispositivos cercanos y analizar los protocolos de seguridad utilizados en las redes Wi-Fi públicas, esto lo hace mediante la utilización de tarjetas wireless en los estándares 802.11a, 802.11b y 802.11g, además muestra información sobre los clientes conectados a la red y el tipo de protección (WEP, WPA…)(Seguridad Wireless, 2024).

- **Nessus**

Nessus es un sistema informático que permite observar las vulnerabilidades, además de los puertos abiertos que se encuentran en los equipos de red (Tenable, 2024). Este interfaz web permite hacer un análisis de los puertos de acuerdo con la criticidad del resultado del escaneo,

la herramienta Nessus indica 5 niveles de criticidad del resultado de vulnerabilidades, en la Tabla 7 se indica por niveles de criticidad según su color, que informa la interfaz en los resultados.

Tabla 7. Niveles de vulnerabilidad según su color

Clasificación	Descripción	Ejemplo
Critico	Información que explica que el escaneo puede haber afectado la disponibilidad o integridad de la aplicación web.	**El servicio dejó de responder:** El escáner canceló el análisis después de encontrar demasiados tiempos de espera de solicitud consecutivos.
Alto	Información que explica que el análisis se detuvo inesperadamente antes de que el escáner terminara de analizar los objetivos de la aplicación web	**El escaneo se bloqueó:** El análisis falló por un motivo inesperado. Como resultado, los resultados del análisis no aparecen o están incompletos.
Medio	Información que explica por qué los resultados del análisis faltan o están incompletos	**URL fuera de alcance:** El escáner no escaneó la URL de destino porque coincide con uno de los criterios de exclusión de alcance especificados en la configuración de la plantilla de escaneo.
Bajo	Información que explica las variaciones en la duración del análisis. Los hallazgos no afectan la aplicación web ni los resultados del análisis.	**La respuesta de destino se ha truncado:** Los errores en la recopilación y evaluación de datos pueden resultar de una información truncada.
Información	Información que no afecta los resultados del escaneo, pero que puede ayudarle a configurar sus ajustes de escaneo de manera más eficiente.	**Autenticación detectada:** El escáner detectó un formulario de autenticación o inicio de sesión de servidor HTTP.

Nota. Adaptado de (Tenable, 2024)

- **Nmap (Network Mapper)**

Puede utilizarse para identificar dispositivos Wi-Fi, escanear puertos abiertos en puntos de acceso y evaluar la configuración de seguridad de los dispositivos de red, ya que es una herramienta de código abierto para escanear redes y hacer auditorías de seguridad.

Está ideada para escanear con rapidez grandes redes, aunque también funciona muy bien con ordenadores individuales. Utiliza paquetes IP «en bruto» para saber qué ordenadores están accesibles en una red, qué servicios ofrecen, con qué sistemas operativos y sus versiones funcionan, qué tipo de filtros de paquetes se están utilizando, así como otras muchas funciones.

- **NetStumbler**

Esta herramienta se utiliza para detectar redes inalámbricas en un área determinada y proporciona información detallada sobre la intensidad de la señal, el canal utilizado y el tipo de seguridad implementado. Es útil para identificar redes Wi-Fi públicas cercanas y evaluar su configuración de seguridad, permite visualizar los AP que estén disponibles, también entrega información acerca de la MAC del AP el SSID y que tipo de seguridad tiene el dispositivo (Ramos, 2006).

5. Metodología

5.1. Introducción y consideraciones previas

Para el presente análisis, se llevará a cabo una investigación analítica descriptiva centrada en la seguridad en redes Wi-Fi públicas en la ciudad de Loja, examinando las principales formas de ciberataques y las barreras de seguridad implementadas que existen para mitigarlos. La creciente dependencia de la sociedad hacia la conectividad inalámbrica en entornos públicos, en un mundo cada vez más digital, ha hecho que el acceso a redes Wi-Fi públicas se convierta en una práctica común, facilitando la comunicación, la productividad y el acceso a información crucial, sin embargo, estas prácticas también han expuesto a los usuarios a diversas amenazas cibernéticas, como el robo de datos, ataques de intermediarios y vulnerabilidades de seguridad.

Se abordará la necesidad apremiante de evaluar y mejorar la seguridad en las redes Wi-Fi públicas en Loja, reconociendo la importancia de un acceso confiable y protegido en entornos urbanos y espacios públicos, ya que este proyecto no solo se enfoca en el análisis actual, sino que también busca proponer estrategias innovadoras para mejorar la seguridad en redes Wi-Fi públicas, adaptándose a los dinámicos cambios de la ciberseguridad**.**

Para el desarrollo de esta práctica de hacking ético para el análisis de redes, se utilizará una máquina virtual donde se instalará la herramienta de Kali Linux, el cual nos permitirá hacer las pruebas de penetración y auditorias de seguridad informática; adicionalmente se usará otra herramienta muy práctica para el análisis de vulnerabilidades en una red llamado Nessus, que funciona dentro de Kali Linux.

La siguiente metodología es llevar a cabo una fase de desarrollo donde se ejecuta una encuesta a la ciudadanía lojana a nivel urbanístico para determinar la efectividad de las técnicas aplicadas de ingeniería social y el nivel de conocimiento de los usuarios en lo que respecta al uso de redes públicas y la inseguridad que estas pueden presentar; con el análisis de la información de los resultados obtenidos de las encuestas realizadas se procedió a establecer recomendaciones preventivas, con el fin de fomentar el conocimiento y generar defensas contra ciertas amenazas.

Además, se elaboró una entrevista con una serie de preguntas dirigidas a proveedores de internet de la ciudad de Loja, con el propósito de comprender y dar a conocer las prácticas de seguridad en las redes Wi-Fi públicas que estas ofrecen y las posibles mejoras que puedan optar según el análisis de sus resultados.

5.2. Formato de encuesta dirigida a las personas de Loja

A continuación, se presenta el formato de encuesta, diseñado con preguntas claves dirigidas a la ciudadanía lojana.

Edad:

- *Menos de 18 años*
- *18-25 años*
- *26-35 años*
- *36-45 años*
- *Más de 45 años*

Género:

- *Masculino*
- *Femenino*

Ocupación:

- *Estudiantes*
- *Empleado (a)*
- *Independiente*
- *Desempleado (a)*
- *Otro*

¿Cuál es su nivel de conocimiento sobre tecnología?

- *Básico*
- *Intermedio*
- *Avanzado*

¿Utiliza frecuentemente redes Wi-Fi públicas?

- Si
- No

Si respondió "No" en la pregunta anterior, ¿Cuál es la razón principal? (Si respondió "Si", pase a la siguiente pregunta).

- *Preocupaciones*
- *Bajo rendimiento de la red*
- *Prefiero utilizar mi propio plan de datos*
- *Otro*

¿Qué tipo de actividades realiza normalmente cuando se conecta a una red Wi-Fi pública? (Puede seleccionar más de una opción).

- *Navegar por internet*
- *Revisar correo electrónico*

- *Uso de redes sociales*
- *Operaciones bancarias*
- *Transacciones en línea*
- *Otro*

¿Ha recibido alguna vez un aviso o advertencia sobre posibles riesgos al usar una red Wi-Fi pública?

- *Si*
- *No*

¿Qué tan seguro se siente al utilizar redes Wi-Fi pública?

- *Muy seguro*
- *Algo seguro*
- *Neutral*
- *Algo inseguro*
- *Muy inseguro*

¿Está familiarizado con alguna de las siguientes medidas de seguridad para redes Wi-Fi públicas? (Puede seleccionar más de una opción).

- *Uso de VPN*
- *Uso de conexiones cifradas (https)*
- *Desactivación de la conexión automática a redes Wi-Fi*
- *No compartir archivos o carpetas en la red*
- *No estoy familiarizado con ninguna*
- *Otro*

¿Cuál es su principal preocupación al usar redes Wi-Fi públicas?

- *Robo de datos personales*
- *Fraude o estafas en línea*
- *Acceso no autorizado a mis dispositivos*
- *Ninguna preocupación en particular*
- *Otro*

¿Qué tan probable es que evite realizar transacciones bancarias o compras en línea mientras está conectado a una red Wi-Fi pública?

- *Muy probable*
- *Probable*
- *Poco probable*
- *No lo evitaría*

¿Cree que las redes Wi-Fi públicas en Loja son lo suficientemente seguras?

- *Si*

- *No*
- *No estoy seguro*

¿Ha experimentado alguna vez una situación de inseguridad mientras usaba una red Wi-Fi públicas en Loja?

- *Si*
- *No*

¿Qué medidas adicionales considera que debería implementarse para mejorar la seguridad de las redes Wi-Fi públicas? (Puede seleccionar más de una opción).

- *Implementación de autenticación segura*
- *Educación y concienciación sobre riesgos de seguridad*
- *Soporte técnico disponible*
- *Cifrado de todas las conexiones*
- *Otro*

¿Cuál es su nivel de satisfacción general con las redes Wi-Fi públicas disponibles en Loja?

- *Muy satisfecho*
- *Satisfecho*
- *Neutral*
- *Insatisfecho*
- *Muy insatisfecho*

5.3. Formato de entrevista a ISP de la ciudad de Loja

A continuación, se presenta el formato de entrevista dirigida a los proveedores de internet de la ciudad de Loja con respecto a la seguridad de las redes Wi-Fi públicas.

Preguntas:

1. *¿Podría proporcionarnos una visión general de los servicios de redes Wi-Fi públicas que su empresa ofrece en Loja? ¿Por lo general en que lugares se ofrece este servicio?*
2. *¿Cuál es el perfil típico de los usuarios que se conectan a sus redes Wi-Fi públicas?*
3. *¿Qué tan seguros se sienten con las medidas de seguridad que tienen en sus redes Wi-Fi públicas? ¿Qué hacen para proteger a los usuarios?*
4. *¿Su empresa realiza monitoreo en tiempo real del tráfico en las redes Wi-Fi públicas?*
5. *¿Qué tipo de autenticación utilizan los usuarios para acceder a las redes Wi-Fi públicas?*
6. *¿Han implementado alguna estrategia específica para proteger a los usuarios contra ataques como el phishing o el robo de datos en sus redes Wi-Fi públicas?*

7. *¿Alguna vez ha tenido que lidiar con problemas de seguridad en estas redes? ¿Cómo lo manejaron?*
8. *¿Cuáles son los principales desafíos que enfrentan al mantener la seguridad en las redes Wi-Fi públicas?*
9. *¿Cree que hay algo que se pueda mejorar en la seguridad de las redes Wi-Fi públicas? ¿Tiene planes para hacer cambios?*
10. *¿Qué piensa sobre el equilibrio entre mantener la red segura y al mismo tiempo que sea fácil de usar para todos?*
11. *¿Hacen algo para informar a los usuarios sobre cómo mantenerse seguros al usar sus redes Wi-Fi públicas?*
12. *¿Están probando o considerando nuevas tecnologías para mejorar la seguridad en sus redes Wi-Fi?*

5.4. Selección de herramientas y software de programación

5.4.1. Características técnicas del computador

A continuación, en la Tabla 8 se describen las características técnicas del computador utilizado para el análisis de redes Wi-Fi.

Tabla 8. Características técnicas del computador

Especificaciones técnicas del computador	
Especificaciones	**Características**
Dispositivo (marca)	DESKTOP-MIKR8J4 (DELL)
Memoria RAM	8.00 GB (5.89 GB usable)
Tipo de sistema	Sistema operativo de 64 bits, procesador basado en x64
Procesador	AMD Ryzen 5 3450U *with Radeon Vega Mobile* Gfx 2.10 GHz
Sistema operativo	Windows 11 *Home Single Language*

5.4.2. Adaptador de Red Wi-Fi

Para el desarrollo de pruebas de seguridad se utilizó un adaptador de red, que es un dispositivo que se conecta a nuestro ordenador, ya sea de sobremesa o portátil, mediante un puerto USB y que permite a su vez conectarnos a redes Wi-Fi, ver Figura 9.

Figura 9

Adaptador de red Wi-Fi

Nota. Adaptador de red ALFA, modelo AWUS036NHA

Para escoger el adaptador adecuado se tuvo en cuenta algunos aspectos básicos, primeramente, estar seguro si el adaptador se pueda activar en modo monitor, caso contrario no servirá para el escaneo de redes, después es muy importante conocer el modelo de su Chipset ya que, dependiendo de este podrá trabajar para un tipo de red a la cual se pueda conectar.

Existen varios modelos de Chipset pero se toma en cuenta dos modelos principales: el Atheros AR9271 que funciona solo a la frecuencia de 2.4 GHz y el REALTECK TRL8812AU que funciona para las frecuencias de 2.4 GHz y 5GHz, para este trabajo de investigación se escogió el Chipset de Atheros AR9271 ya que este Chipset funciona directamente con Kali Linux, es decir, conectar y funcionar, lo que es suficiente para el análisis de redes que operan en dicha frecuencia, en cambio el modelo REALTECK TRL8812AU a pesar que trabaja para dos redes, necesita realizar configuraciones, activaciones de drives dependiendo del Chipset y el sistema operativo de la máquina. A continuación, en la Tabla 9 se presenta las especificaciones del modelo de adaptador de red escogido, siendo de la marca ALFA, modelo AWUS036NHA.

Tabla 9. Especificaciones de adaptador de red

Especificaciones Adaptador USB Wireless	
Interface	Puerto mini USB
Antena	Una antena dipolo externa de 5dBi
Frecuencia	2.4 GHz
Standard	Wi-Fi IEEE 802.11b/g/n
Velocidad Inalámbrica	Hasta 150 Mbps
Chipset	Atheros AR971
Seguridad	WEB, WPA, WPA2, WPA-PSK, WPA2-PSK
Soporte	Windows XP, Vista, Win 7, Linux

Nota. Especificaciones de Adaptador USB Wireless Alfa Network, modelo AWUS036NHA.

5.4.3. Análisis de hacking en Kali Linux

Kali Linux es una plataforma basada en GNU/Linux que se utiliza para realizar auditorías de seguridad y pruebas de penetración, ya que este permite el uso de varias herramientas de hacking, capturas de información, identificación de vulnerabilidades. Kali Linux incluye la suite de software de seguridad de Aircrack-ng que se ejecuta a través del terminal de comandos (Paspuel, 2018).

En este proyecto de investigación para las pruebas de hacking ético se optó por el uso del sistema operativo Kali Linux versión: 2023.3, en este caso para la virtualización se usó una máquina virtual en VirtualBox.

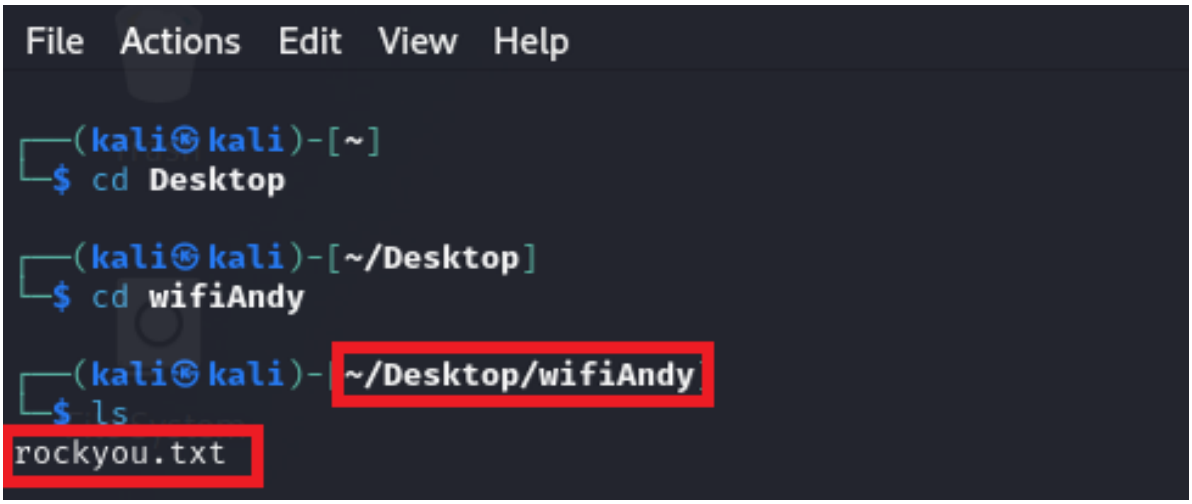
A continuación, se describe los pasos a realizar para la práctica de hacking ético en una red wifi pública.

Primeramente, se va a crear un directorio de usuario para guardar en esa carpeta los archivos que se vaya obteniendo del proceso de hacking, y además mover los archivos descargados hacia esta carpeta, véase en la siguiente Figura 10.

En la misma Figura 10 se puede observar un archivo llamado “rockyou.txt”, este archivo es descargable de la web y se trata de un diccionario que contiene millones de contraseñas posibles, existen más diccionarios en páginas web para hacking ético, pero rockyou es el más popular para realizar ataque por diccionario, una vez descargado se lo puede mover hacia la carpeta de trabajo creada, se escribe el comando “ls” para verificar que el archivo este en la carpeta nueva.

Figura 10

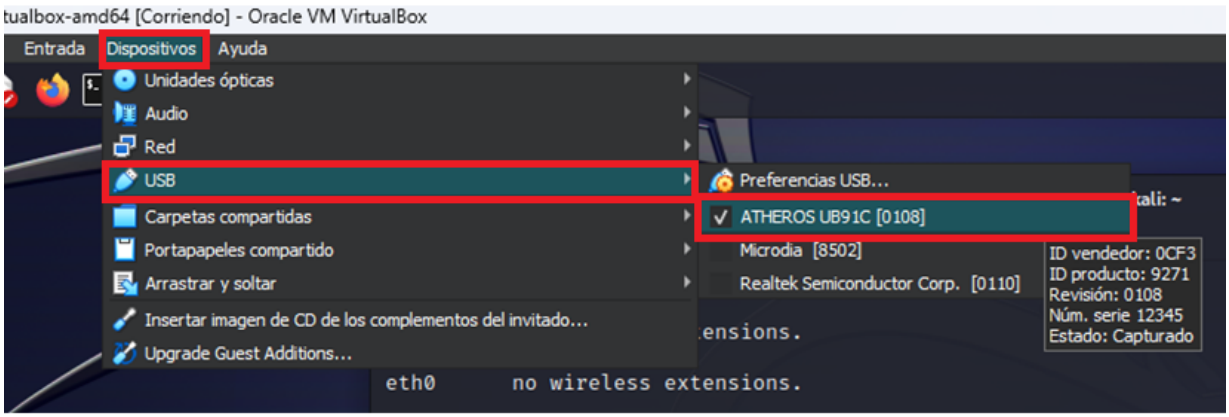
Captura de pantalla de un directorio en Kali Linux



Para iniciar el proceso de hacking, una vez ya instalada el Kali Linux se inserta la antena wifi o adaptador de red en el puerto USB, se comprueba su conexión seleccionando "dispositivos", luego USB y se abre una pestaña donde se observa el nombre del Chipset del adaptador, véase en la Figura 11.

Figura 11

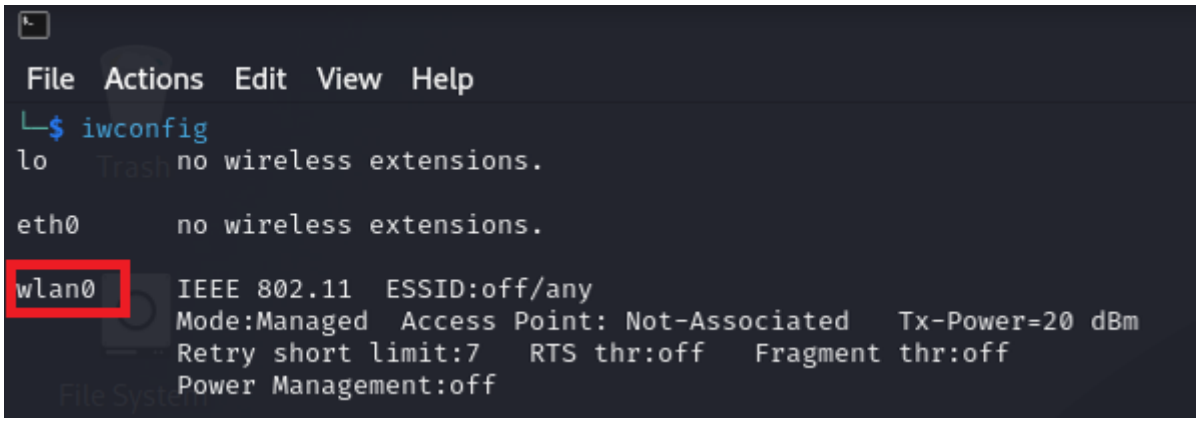
Conexión del adaptador de red en Kali Linux



A continuación, se abre una terminal y se verifica si la antena es reconocida ejecutando el comando "*iwconfig*", se observa que aparece el término "*wlan0*" que es el nombre de interfaz del adaptador de red en Kali Linux. Véase en la Figura 12.

Figura 12

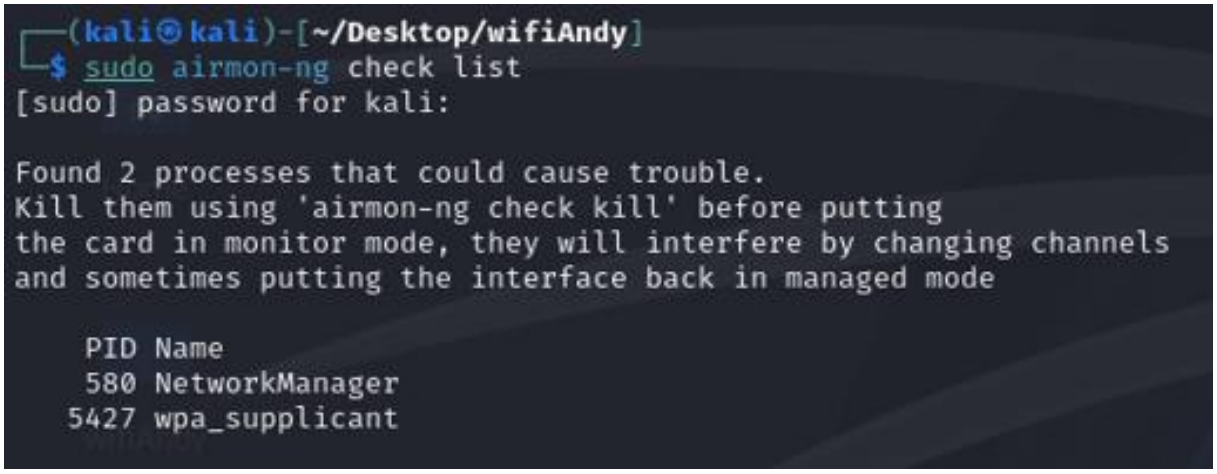
Verificación de conexión de la antena



Antes de continuar, se debe deshabilitar cualquier proceso que pueda interferir con la captura de paquetes, por ende, se puede escribir el comando "*airmon-ng check list*" ver Figura 13.

Figura 13

Captura de pantalla del comando check list



Una vez que se puede reconocer el nombre del interfaz de red se procede a activarlo en modo monitor, para esto se ejecuta con el comando "*sudo airmon-ng start wlan0*". Véase en la Figura 14.

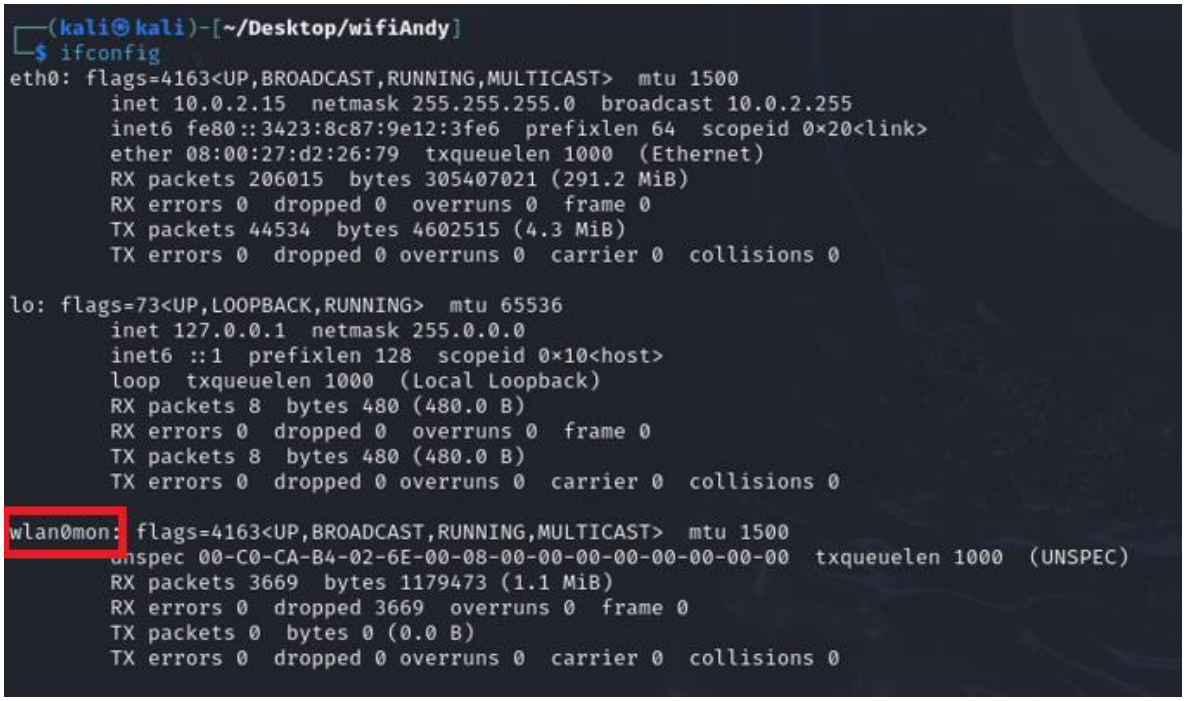
Para comprobar que la antena este activa en modo monitor se ejecuta el comando "*ifconfig*", donde se observa que el nombre de la interfaz ha optado por el nombre de "wlan0mon" lo que indica que ya está en modo monitor. Véase en la Figura 15.

Figura 14

Activación de la antena en modo monitor

Figura 15

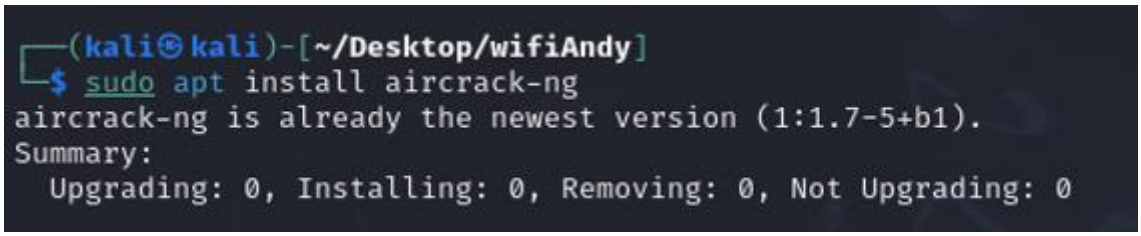
Verificación de la antena en modo monitor



A continuación, se procede a instalar la herramienta de aircrack-ng, esto fácilmente se lo puede hacer usando el comando "*sudo apt install aircrack-ng*", como se muestra en la Figura 16.

Figura 16

Comando para instalación de AirCrack-ng en Kali Linux



Completado el proceso anterior, se puede iniciar con el escaneo de todas las redes wifi disponibles y para su realización se procede a usar el comando "*sudo airodump-ng wlan0mon*", como se puede observar en la Figura 17, el tipo de seguridad que existen en estas redes siendo la más común WPA2, además de la información que está viajando a través de dichas redes, de las cuales se debe buscar la red objetivo para su análisis, una vez identificado se toma en cuenta el canal "CH" y el "BSSID" que es la dirección MAC de dicha red. Luego se precede con un nuevo comando donde se escribe el número del canal, el BSSID de la red, y "-w" que es el archivo de captura donde se guardarán los paquetes, a este archivo le podemos dar un nombre, en este caso llamado "estudio" que posteriormente se usará para hacer el ataque por diccionario, y por último no olvidar el nombre de la interfaz de red, con esto podemos observar las estaciones "*station*" conectadas en la red, véase la Figura 18.

Figura 17

Escaneo de redes disponibles

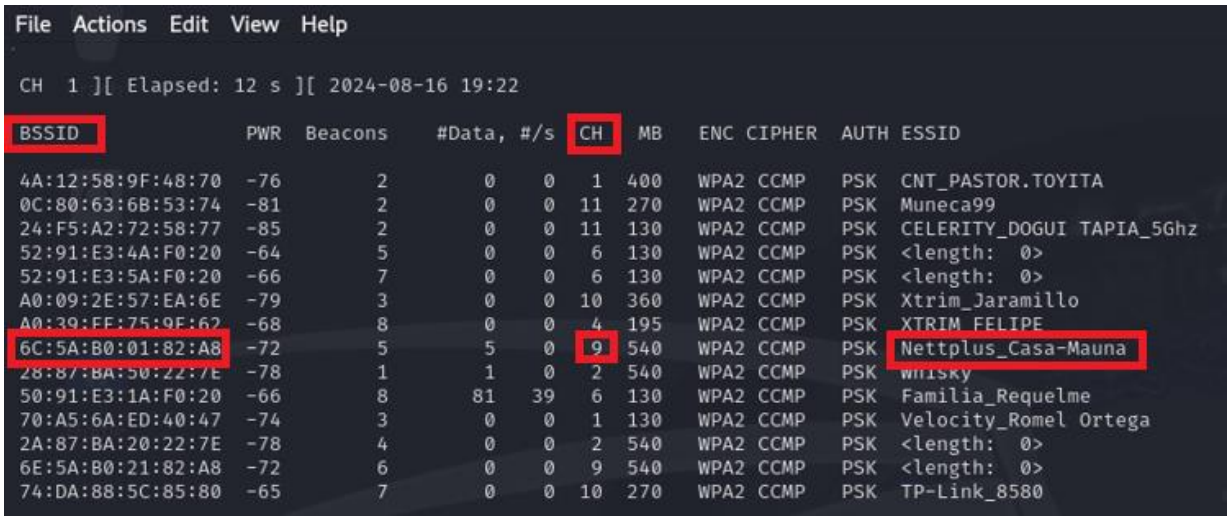
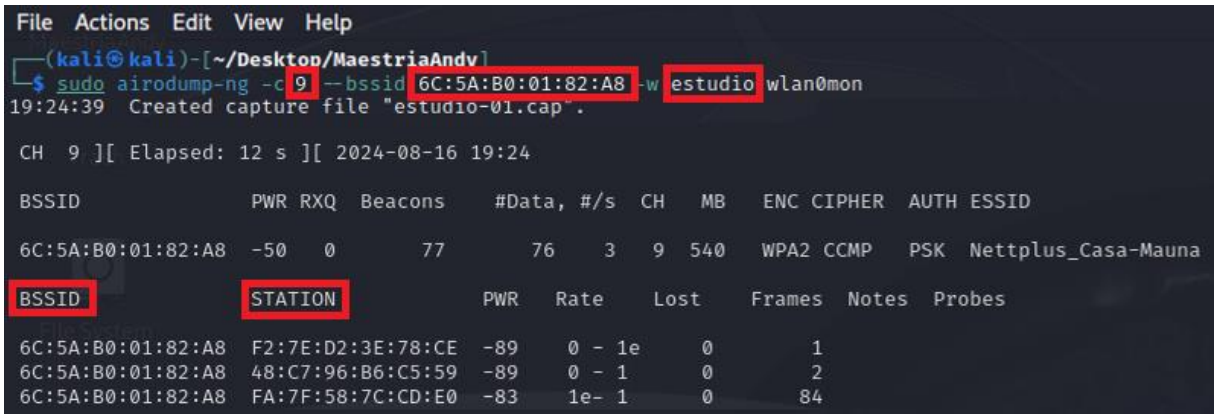


Figura 18

Ejecución del comando airodump-ng



5.4.3.1. Lanzamiento de un ataque deauth. Para este proceso se abre una nueva terminal, se inicia el ataque *deauth* para desconectar todos los usuarios que se encuentran conectados a la red, usando el comando "*sudo aireplay-ng*", seguido del "-0" que se utiliza para el ataque *dauth*, el "9" es el número de paquetes *dauth* para ser enviados, el "-a" es usado para ubicar el BSSID de la red y un "-c" para ubicar una estación escogida, como indica la Figura 19, dando como resultado la obtención del *handshake* en la primera terminal principal, Ver Figura 20. El término *handshake* significa que se establece un procedimiento de autenticación y una de sus principales habilidades es el intercambio de claves, es decir, que se produce un acuerdo entre cliente (Usuario) y servidor (Access Point) para poder iniciar una comunicación, con la posibilidad de extraer la clave de un AP.

Figura 19

Lanzamiento de un ataque deauth

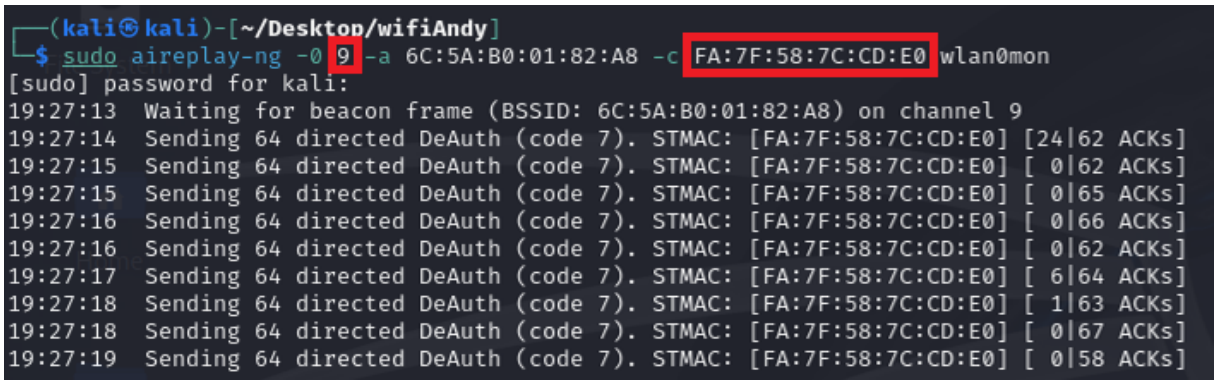
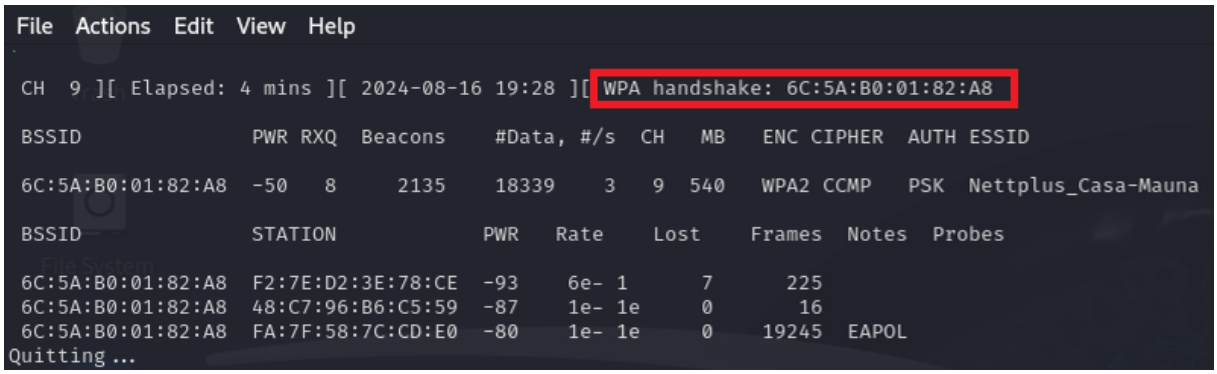


Figura 20

Captura del handshake

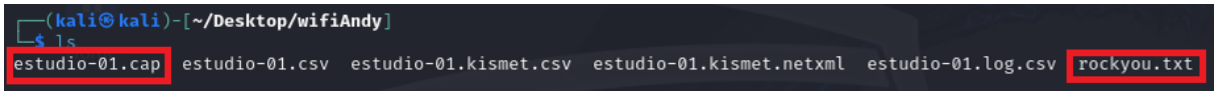


Después del ataque *dauth* y haber logrado conseguir el *handshake* wpa, se puede escribir el comando Ctrl+C para limpiar el terminal, esto no afecta el procedimiento, también se puede cerrar el segundo terminal.

A continuación, se escribe un "ls" para observar los archivos de captura generados por airodump-ng, y aparte del archivo "rockyou.txt", se puede leer también varios archivos de los cuales el archivo exacto de registro "estudio-01.cap" es el que interesa para ser usada en el ataque final por fuerza bruta. Ver Figura 21.

Figura 21

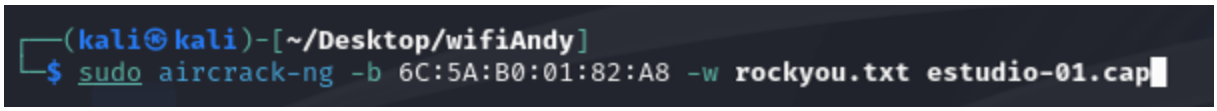
Archivos de captura generados por airodump-ng



5.4.3.2. Descifrando contraseña Wi-Fi por fuerza bruta. El siguiente paso es descifrar la clave con Aircrack-ng, para ello se escribe el comando "*sudo aircrack-ng*", seguido del comando "-b" escribimos el *handshake* obtenido, con el comando "-w" se escribe "rockyou.txt" para el ataque por diccionario y por último el archivo "estudio-01.cap", se ejecuta y con esto Aircrack-ng comienza a trabajar para intentar descifrar la clave, que dependiendo de la complejidad de la misma puede descifrarlo en un instante o tardar varios minutos, ver Figura 22. En el apartado de resultados se observará como el Aircrack-ng arroja el resultado de obtención de una contraseña.

Figura 22

Descifrando contraseña Wi-Fi usando AirCrack-ng



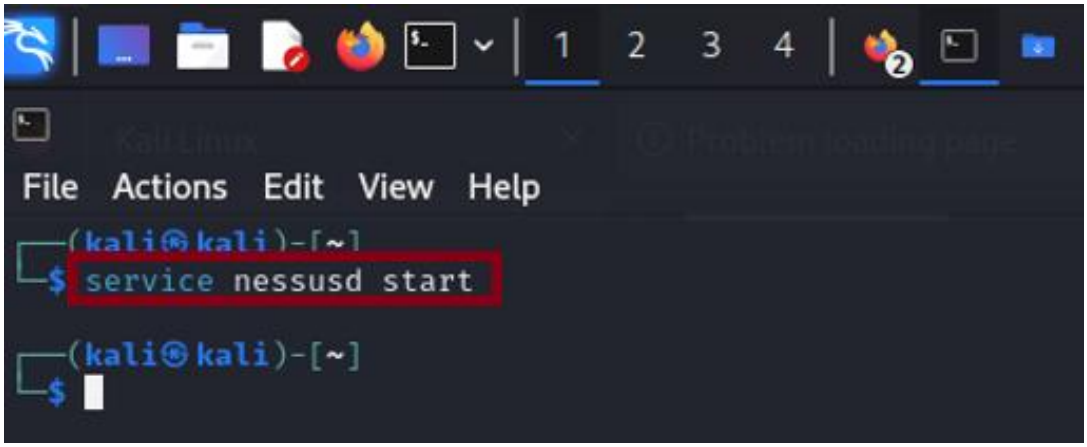
5.5. Análisis de Vulnerabilidades con la herramienta Nessus

Para el escaneo de vulnerabilidades en una red pública se ha escogido la herramienta Nessus Essentials, ya que esta versión de la herramienta es gratuita, y que es muy ampliamente usada por profesionales de seguridad de la información para identificar y evaluar las vulnerabilidades en sistemas de redes, debido a las ventajas que presenta al momento de presentar resultados específicos, además, Nessus tiene la capacidad de exportar un documento en formatos como html, pdf y xml, con el reporte detallado donde se incluye la información de las vulnerabilidades encontradas, así como recomendaciones para corregir o mitigar las anomalías (Aplicación de hacking ético).

Para iniciar el llamado del programa Nessus, se abre una nueva terminal en Kali Linux y ejecutamos el siguiente comando "*service nessusd star*" como se indica en la siguiente Figura 23.

Figura 23

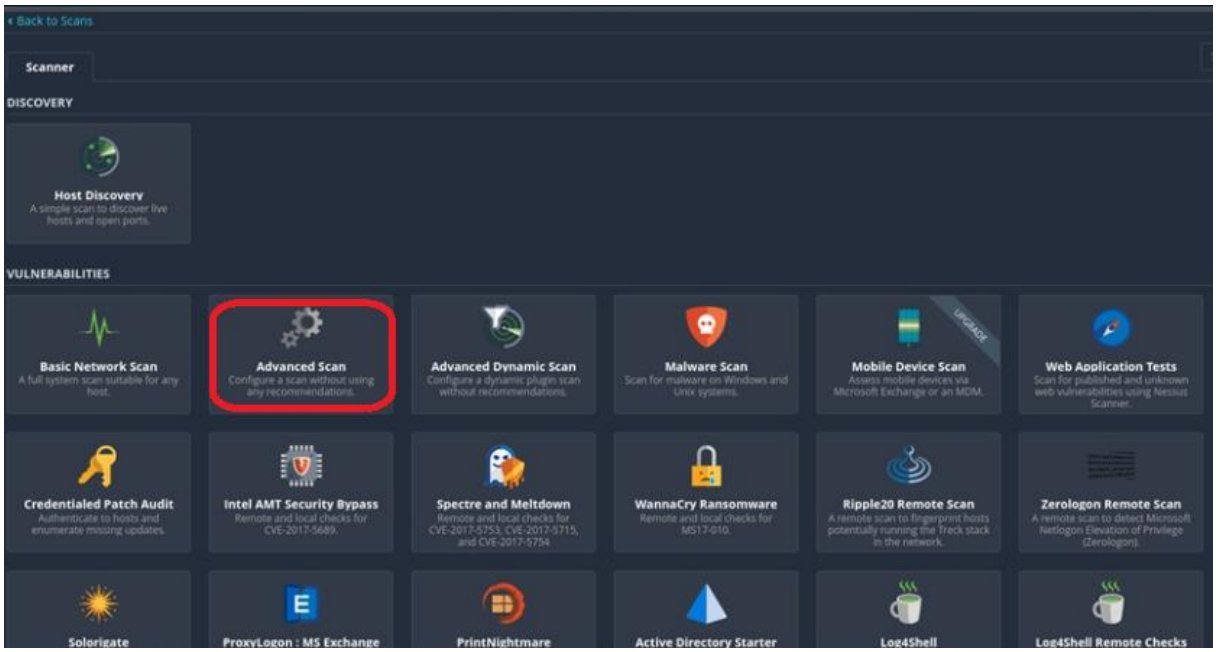
Activación del servicio de Nessus en Kali Linux



Una vez dentro de Nessus, la plataforma presenta varios tipos de escaneo para el análisis de una red, en este caso se tomó la opción de escaneo avanzado. Véase la Figura 24.

Figura 24

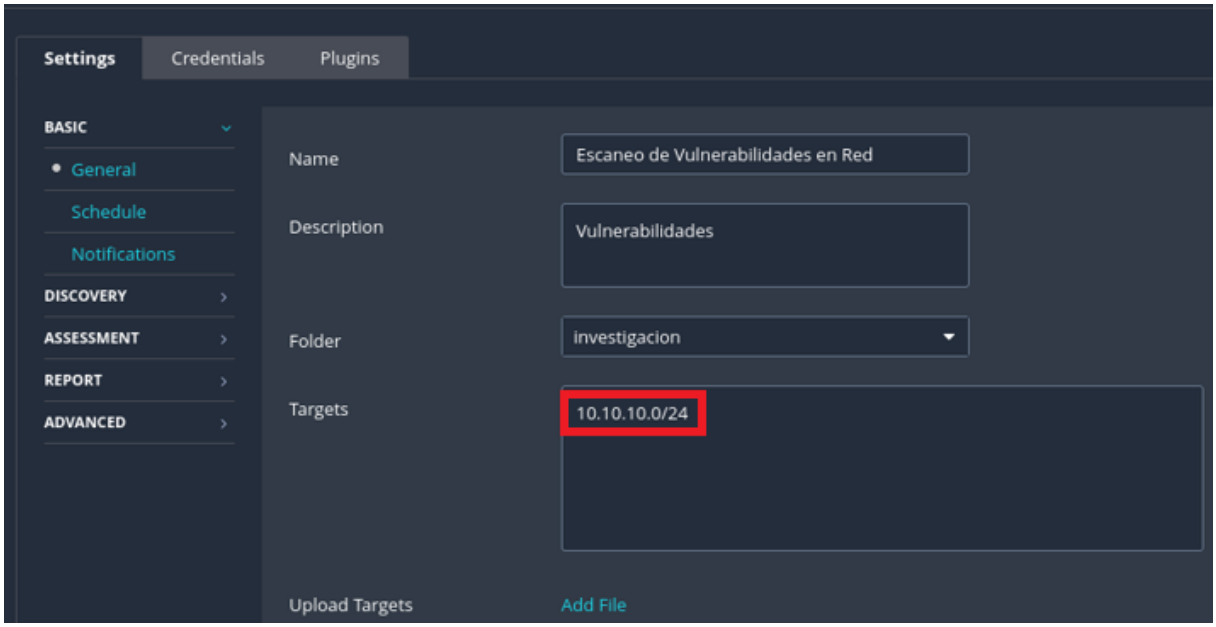
Opción de escaneo avanzado en Nessus



El siguiente paso es agregar un nombre al escaneo para ser identificado, además de una descripción simple, en la zona de targets se coloca una o más direcciones IP, o en caso de desear escanear toda la red se escribe el rango de red /24. Véase la Figura 25.

Figura 25

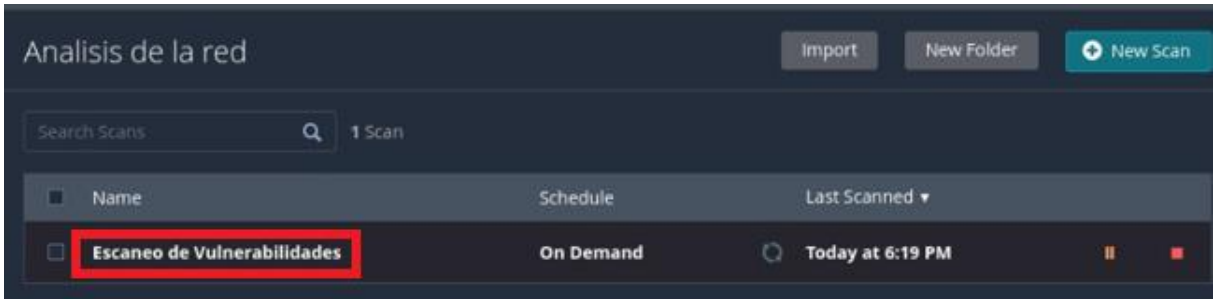
Ingreso de datos en Nessus



La Figura 26 presenta el inicio del escaneo de la red informática para la detección de vulnerabilidades.

Figura 26

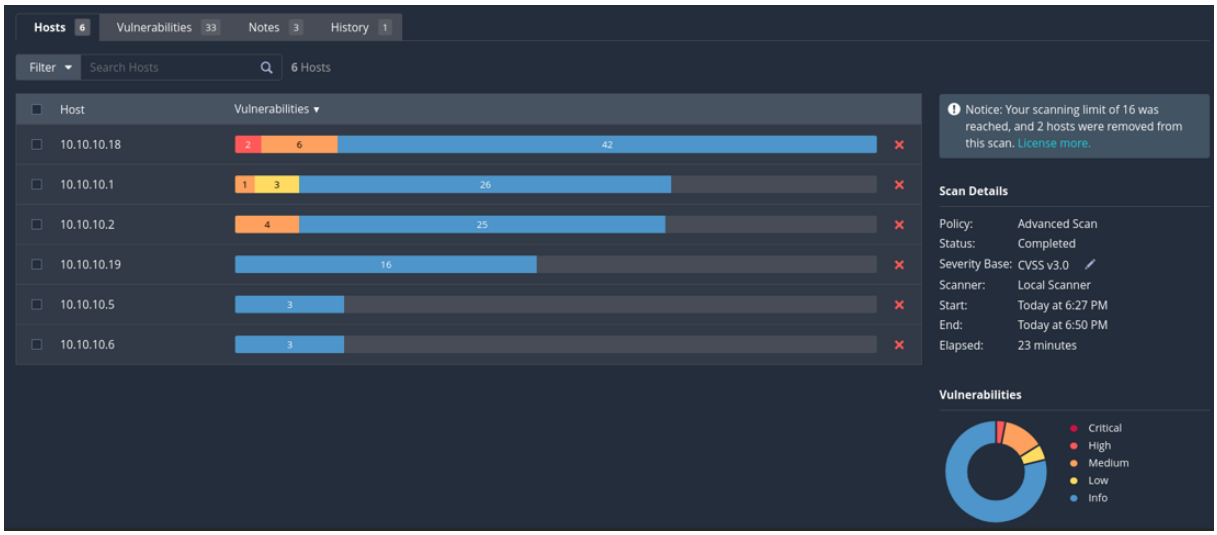
Inicio de análisis de vulnerabilidades de red



A continuación, la Figura 27 indica algunas de las vulnerabilidades detectadas en dicha red, que se encuentran organizadas según su nivel de riesgo, sea crítico, alto, medio y bajo, además presenta cierta información adicional de la red, toda esta lista de debilidades detectadas tiene asignado un color para una mejor comprensión.

Figura 27

Finalización de escaneo en Nessus



6. Resultados

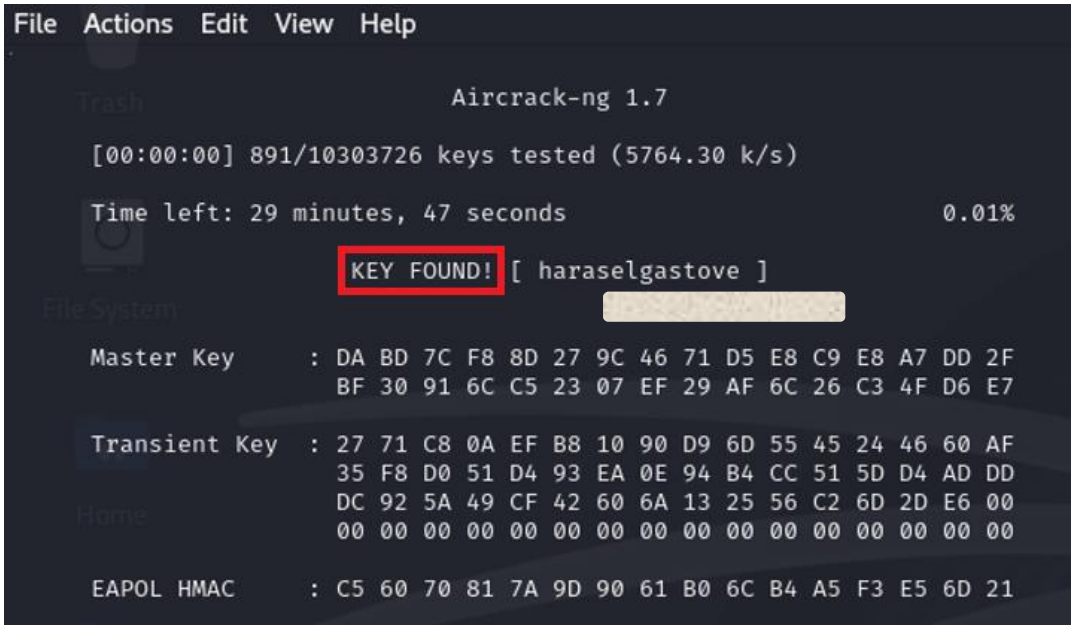
En esta sección de resultados se presenta un resumen de respuestas obtenidas con el uso de Aircrack-ng de Kali Linux para el descifrado de una contraseña aplicado en un bar-restaurante y el programa Nessus para detección de vulnerabilidades, orientado a dos escenarios de red pública en la ciudad de Loja.

6.1. Resultado de la herramienta AirCrack-ng de Kali Linux

Después de hacer pruebas en varios escenarios con el ataque AirCrack-ng de Kali Linux y usar herramientas de fuerza bruta, se logró acceder a una red wifi, dando como resultado la obtención de la contraseña de un sitio público, en este caso un bar restaurant, que son lugares visitados muy frecuente. La Figura 28 muestra el resultado de una clave encontrada, ¡Key Found!

Figura 28

Respuesta Key Found de AirCrack-ng



Nota. La contraseña es oculta con fines de seguridad

6.2. Resultados de vulnerabilidades, escenario 1 (Parada de bus)

A continuación, la Tabla 10 presenta el resumen del análisis de vulnerabilidades con la ayuda de la herramienta Nessus para el escaneo de una red pública en un primer escenario, usando una dirección de servidor para toda la red.

Tabla 10. Resultado de escaneo en Nessus (escenario 1)

Resultados de análisis con Nessus	
Vulnerabilidades encontradas	16
Información adicional	115
Total	131
Tipo de análisis	Análisis avanzado
Tiempo de inicio	6:27 PM
Tiempo final	6:50 PM
Duración total	23 minutos
Vulnerabilidades criticas	0
Vulnerabilidades altas	2
Vulnerabilidades medias	11
Vulnerabilidades bajas	3

En la Tabla 11 se detallan los tipos de vulnerabilidades detectados, incluyendo su nivel de gravedad y su descripción.

Tabla 11. Lista de vulnerabilidades de una red pública, escenario 1

N°	Vulnerabilidad	Gravedad	CVSS V 3.0	Descripción
1	MS17-010: *Security Update for Microsoft Windows SMB Server* (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) *(WannaCry) (EternalRocks) (Petya) (uncredentialed check)*	Alto	8.1	El host Windows remoto está afectado por múltiples vulnerabilidades.
2	SSL *Medium Strength Cipher Suites Supported* (SWEET32)	Alto	7.5	El servicio remoto soporta el uso de cifrados SSL de fuerza media
3	*Unencrypted Telnet Server*	Medio	6.5	El servidor Telnet remoto transmite el tráfico en texto claro
4	SSL *Certificate Cannot Be Trusted*	Medio	6.5	El certificado SSL para este servicio no es de confianza.
5	SSL *Self-Signed Certificate*	Medio	6.5	La cadena de certificados SSL para este servicio termina en un certificado auto firmado no reconocido
6	TLS Versión 1.0 *Protocol Detection*	Medio	6.5	El servicio remoto cifra el tráfico utilizando una versión antigua de TLS.
7	TLS Version 1.1 Deprecated Protocol	Medio	6.5	El servicio remoto cifra el tráfico utilizando una versión antigua de TLS.

N°	Vulnerabilidad	Gravedad	CVSS V 3.0	Descripción
8	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medio	5.9	El host remoto soporta el uso de RC4 en una o más suites de cifrado
9	SSL Certificate Expiry	Medio	5.3	El certificado SSL del servidor remoto ya ha caducado.
10	SMB Signing not required	Medio	5.3	No es necesario firmar en el servidor SMB remoto.
11	SSH Server CBC Mode Ciphers Enabled	Bajo	3.7	El servidor SSH está configurado para soportar encriptación Cipher Block Chaining (CBC).
12	SSH Weak Key Exchange Algorithms Enabled	Bajo	3.7	El servidor SSH remoto está configurado para permitir algoritmos de intercambio de claves débiles.
13	SSH Weak MAC Algorithms Enabled	Bajo	2.6	El servidor SSH remoto está configurado para permitir los algoritmos MD5 y MAC de 96 bits.

Como se puede observar en la Tabla 11, el escaneo en Nessus para toda esta red no entregó ninguna vulnerabilidad critica, pero si presenta dos tipos de vulnerabilidades altas con un nivel de puntación de 8.1 y 7.5 de gravedad. Además de ocho tipos de vulnerabilidades de nivel medio con una puntuación de impacto de 6.5, 5.9 y 5.3 de gravedad, y por último el escaneo indica tres tipos de vulnerabilidades de nivel bajo con una puntuación de vulnerabilidad de 3.7 y 2.6.

Severidad alta

Durante el proceso de escaneo de vulnerabilidades al servidor 10.10.10.0/24 se obtuvo dos resultados de severidad alta, las cuales se presentan en la siguiente lista:

- MS17-010: *Security Update for Microsoft Windows* SMB *Server* (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (*EternalRock*s) (*Petya*) (*uncredentialed check*)
- SSL *Medium Strength Cipher Suites Supported* (SWEET32)

Solución recomendada

Para los sistemas operativos Windows que no reciben soporte, por ejemplo, Windows XP, Microsoft recomienda que los usuarios dejen de usar SMBv1 porque carece de funciones de seguridad que se incluyeron en versiones posteriores de SMB. Esta recomendación es en cuanto a la primera vulnerabilidad alta encontrada en el escaneo.

En la segunda vulnerabilidad de gravedad alta se recomienda reconfigurar la aplicación afectada si es posible para evitar el uso de cifrados de fuerza media.

Severidad media

En el reporte entregado obtenido por la aplicación Nessus se presentan las siguientes vulnerabilidades medias, presentadas en la siguiente lista:

- *Unencrypted Telnet Server*
- SSL *Certificate Cannot Be Trusted*
- SSL *Self-Signed Certificate*
- TLS *Version* 1.0 *Protocol Detection*
- TLS *Version* 1.1 *Deprecated Protocol*
- SSL RC4 *Cipher Suites Supported* (Bar Mitzvah)
- SSL *Certificate Expiry*
- SMB *Signing not required*

Solución recomendada

Se recomienda para la primera vulnerabilidad media desactivar el servicio Telnet y utilice SSH en su lugar. Para la segunda, tercera y séptima vulnerabilidad media se sugiere adquirir un certificado SSL adecuado para este servicio. Para la cuarta y quinta vulnerabilidad media se sugiere habilitar el soporte para TLS 1.2 y/o 1.3, y deshabilite el soporte para TLS 1.0 y TLS 1.1. En la sexta vulnerabilidad se recomienda reconfigurar la aplicación afectada, si es posible, para evitar el uso de cifrados RC4. Considere el uso de TLS 1.2 con suites AES-GCM sujetas a la compatibilidad del navegador y el servidor web. Para la última vulnerabilidad de grado medio se recomienda aplicar la firma de mensajes en la configuración del host. En Windows, se encuentra en la configuración de directiva *Microsoft network server: Digitally sign communications* (*always*).

Severidad baja

En cuanto a las vulnerabilidades bajas encontradas con la aplicación web Nessus, fueron las siguientes:

- SSH *Server* CBC *Mode Ciphers Enabled*
- SSH *Weak Key Exchange Algorithms Enabled*
- SSH *Weak* MAC *Algorithms Enabled*

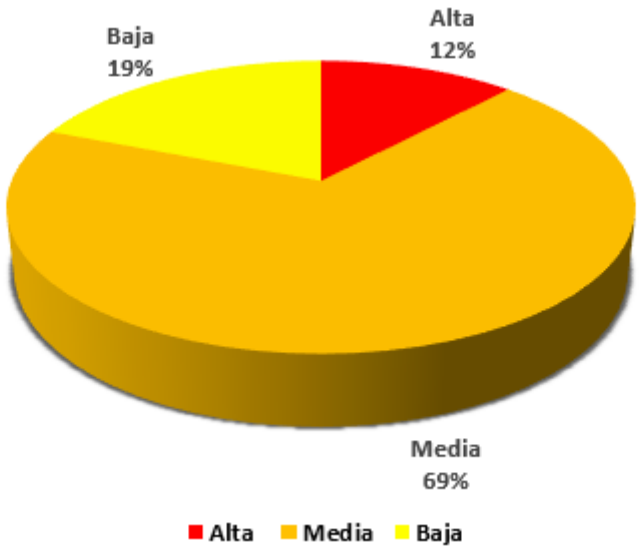
Solución recomendada

Para la primera vulnerabilidad baja se recomienda desactivar el cifrado en modo CBC y activar el cifrado en modo CTR o GCM.

En la segunda y tercera vulnerabilidad se recomienda desactivar los algoritmos MD5 y MAC de 96 bits. En este escenario las vulnerabilidades de información marcadas con color azul fueron un total de 88 vulnerabilidades. La siguiente Figura 29 indica el porcentaje de cada vulnerabilidad según su nivel de gravedad.

Figura 29

Gravedad porcentual de vulnerabilidades, escenario 1



6.3. Resultados de vulnerabilidades, escenario 2 (Patio de comidas)

A continuación, la Tabla 12 presenta el resumen del análisis de escaneo en Nessus para una red pública en un segundo escenario, usando la dirección de servidor en un solo host.

Tabla 12. Resultado de escaneo en Nessus (escenario 2)

Resultados de análisis con Nessus	
Vulnerabilidades encontradas	10
Información adicional	55
Total	65
Tipo de análisis	Análisis avanzado
Tiempo de inicio	17:36 PM
Tiempo final	17:48 PM
Duración total	12 minutos
Vulnerabilidades criticas	1
Vulnerabilidades altas	2
Vulnerabilidades medias	6
Vulnerabilidades bajas	1

En la Tabla 13 se detallan los tipos de vulnerabilidades detectados, incluyendo su nivel de gravedad y su descripción.

Tabla 13. Lista de vulnerabilidades de una red pública, escenario 2

N°	Vulnerabilidad	Gravedad	CVSS V 3.0	Resumen
1	*Microsoft* SQL *Server Unsupported Version Detection (remote check)*	Crítico	10	Se está ejecutando una versión no compatible de un servidor de base de datos en el host remoto
2	SSL *Certificate Signed Using Weak Hashing Algorithm*	Alto	7.5	Un certificado SSL de la cadena de certificados se ha firmado utilizando un algoritmo hash débil.
3	SSL *Medium Strength Cipher Suites Supported (SWEET32)*	Alto	7.5	El servicio remoto soporta el uso de cifrados SSL de fuerza media.
4	SSL *Certificate Cannot Be Trusted*	Medio	6.5	El certificado SSL para este servicio no es de confianza.
5	SSL *Self-Signed Certificate*	Medio	6.5	La cadena de certificados SSL para este servicio termina en un certificado auto firmado no reconocido.
6	TLS Versión 1.0 *Protocol Detection*	Medio	6.5	El servicio remoto cifra el tráfico utilizando una versión antigua de TLS.
7	TLS Versión 1.1 *Deprecated Protocol*	Medio	6.5	El servicio remoto cifra el tráfico utilizando una versión antigua de TLS.
8	SMB *Signing not required*	Medio	5.3	No es necesario firmar en el servidor SMB remoto.
9	mDNS *Detection* (Remote Network)	Medio	5.0	Es posible obtener información sobre el host remoto.
10	SSL *Certificate Chain Contains* RSA *Keys Less Than* 2048 bits	Bajo	N/A	La cadena de certificados X.509 utilizada por este servicio contiene certificados con claves RSA inferiores a 2048 bits.

Como se puede observar en la Tabla 13, el escaneo en Nessus para la dirección IP de un host, entregó una vulnerabilidad critica con una puntuación de nivel 10 de gravedad, seguido de dos tipos de vulnerabilidades altas con un nivel de puntación de 7.5 de gravedad, además de seis tipos de vulnerabilidades de nivel medio con una puntuación de impacto de 6.5, 5.3 y 5.0 de gravedad, y por último el escaneo indica solo un tipo de vulnerabilidad de nivel bajo.

Severidad crítica

Durante el proceso de escaneo de vulnerabilidades al servidor 40.40.11.37 se obtuvo un resultado crítico:

- Microsoft SQL *Server Unsupported Version Detection (remote check)*

Solución recomendada

Actualizar a una versión de *Microsoft* SQL *Server* compatible en la actualidad.

Severidad alta

Al momento del escaneo se obtuvieron en los resultados dos vulnerabilidades clasificadas con severidad alta:

- SSL *Certificate Signed Using Weak Hashing Algorithm*
- SSL *Medium Strength Cipher Suites Supported* (SWEET32)

Solución recomendada

En la primera vulnerabilidad alta se recomienda ponerse en contacto con la autoridad de certificación para que vuelva a emitir el certificado SSL.

En la segunda vulnerabilidad se recomienda reconfigure la aplicación afectada si es posible para evitar el uso de cifrados de fuerza media.

Severidad Media

Durante el análisis se encontraron vulnerabilidades medias representadas de color naranja, las cuales son 6 tipos de vulnerabilidades encontradas:

- SSL *Certificate Cannot Be Trusted*
- SSL *Self-Signed Certificate*
- TLS *Version 1.0 Protocol Detection*
- TLS *Version 1.1 Deprecated Protocol*
- SMB *Signing not required*
- mDNS *Detection (Remote Network)*

Solución recomendada

Se recomienda en la primera y segunda vulnerabilidad media adquirir o generar un certificado SSL adecuado para este servicio

En la tercera y cuarta vulnerabilidad se recomienda habilitar el soporte para TLS 1.2 y 1.3, y deshabilite el soporte para TLS 1.0.

Para la quinta vulnerabilidad se debe aplicar la firma de mensajes en la configuración del host. En Windows, se encuentra en la configuración de directiva *'Microsoft network server: Digitally sign communications (always)'*.

En la última vulnerabilidad media se recomienda filtrar el tráfico entrante al puerto UDP 5353.

Severidad baja

La vulnerabilidad de gravedad baja que se encontró en el escaneo es la siguiente:

- SSL *Certificate Chain Contains* RSA *Keys Less Than* 2048 bits

Solución recomendada

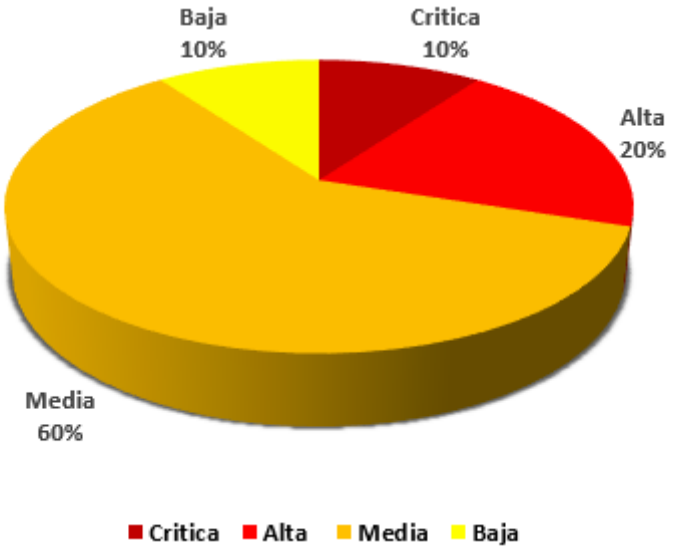
Sustituya el certificado de la cadena con la clave RSA de menos de 2048 bits de longitud por una clave más larga y vuelva a emitir todos los certificados firmados por el certificado antiguo.

En este escenario las vulnerabilidades de información encontradas con aplicación web las representa de color azul. Las cuales en este escaneo fueron un total de 36 vulnerabilidades de grado informativo.

La Figura 30 indica el porcentaje de cada vulnerabilidad del escenario 2 según su nivel de gravedad.

Figura 30

Gravedad porcentual de vulnerabilidades, escenario 2



6.4. Resultados de las encuestas dirigidas a los usuarios de la ciudad de Loja

A continuación, la Tabla 14 muestran los resultados obtenidos de la encuesta realizada en la ciudad de Loja. Las encuestas que se aplicaron fueron en línea, con un total de 385 muestras, obteniendo los siguientes porcentajes:

Tabla 14. Resultados de la encuesta a usuarios de la ciudad de Loja

1. Edad	
Menos de 18 años	3.9 %
18-25 años	32.7%
26-35 años	42.1%
36-45 años	14.3%
Más de 45 años	7%
2. Género	
Masculino	50.9%
Femenino	49.1%
3. Ocupación	
Estudiante	26%
Empleado (a)	44.4%
Independiente	23.5%
Desempleado (a)	5.2%
Otro	0.9%
4. ¿Cuál es su nivel de conocimiento sobre tecnología?	
Básico	41.5%
Intermedio	44.2%
Avanzado	14.3%
95. ¿Utiliza frecuentemente redes Wi-Fi públicas?	
Si	47%
No	53%
6. Si respondió "No" en la pregunta anterior, ¿Cuál es la razón principal? (Si respondió "Si", pase a la siguiente pregunta)	
Preocupaciones de seguridad	18.6%
Bajo rendimiento de la red	31.9%
Prefiero utilizar mi propio plan de datos	46.6%
Otro	2.9%
7. ¿Qué tipo de actividades realiza normalmente cuando se conecta a una red Wi-Fi pública? (Puede seleccionar más de una opción)	
Navegar por internet	48.8%
Revisar correo electrónico	40.5%
Uso de redes sociales	74.8%
Operaciones bancarias	16.4%
Transacciones en línea	14%
Otro	4.7%
8. ¿Ha recibido alguna vez un aviso o advertencia sobre posibles riesgos al usar una red Wi-Fi pública?	
Si	44.4%
No	55.6%
9. ¿Qué tan seguro se siente al utilizar redes Wi-Fi públicas?	
Muy seguro	2.9%
Algo seguro	13%
Neutral	44.1%
Algo inseguro	30.6%
Muy inseguro	9.4%
10. ¿Está familiarizado con alguna de las siguientes medidas de seguridad para redes Wi-Fi públicas? (Puede seleccionar más de una opción)	
Uso de VPN	40%
Uso de conexiones cifradas (https)	26.2%

Desactivación de la conexión automática a redes Wi-Fi	30.4%
No compartir archivos o carpetas en la red	36.4%
No estoy familiarizado con ninguna	27.8%
Otro	0%
11. ¿Cuál es su principal preocupación al usar redes Wi-Fi públicas?	
Robo de datos personales	40.5%
Fraude o estafas en línea	17.1%
Acceso no autorizado a mis dispositivos	30.6%
Ninguna preocupación en particular	10.6%
Otro	1.2%
12. ¿Qué tan probable es que evite realizar transacciones bancarias o compras en línea mientras está conectado a una red Wi-Fi pública?	
Muy probable	30.9%
Probable	33.8%
Poco probable	29.1%
No lo evitaría	6.2%
13. ¿Cree que las redes Wi-Fi públicas en Loja son lo suficientemente seguras?	
Si	6.8%
No	40.2%
No estoy seguro	53%
14. ¿Ha experimentando alguna vez una situación de inseguridad mientras usaba una red Wi-Fi pública en Loja?	
Si	19.7%
No	80.3%
15. ¿Qué medidas adicionales considera que deberían implementarse para mejorar la seguridad de las redes Wi-Fi públicas en Loja? (Puede seleccionar más de una opción)	
Implementación de autenticación segura	46.2%
Educación y concientización sobre riesgos de seguridad	56.4%
Soporte técnico disponible	33.5%
Cifrado de todas las conexiones	44.7%
Otro	0.3%
16. ¿Cuál es su nivel de satisfacción general con las redes Wi-Fi públicas disponibles en Loja?	
Muy satisfecho	2.1%
Satisfecho	13.5%
Neutral	56.1%
Insatisfecho	24.7%
Muy insatisfecho	3.6%

Analizando la Tabla 14, de manera más detallada para cada pregunta se puede describir que del total de personas encuestadas (385 personas), en la categoría de edad se distribuye de la siguiente manera:

- 15 personas (3.9%) son menores de 18 años.
- 126 personas (32.7%) son de 18 a 25 años.
- 162 personas (42.1%) son de 26 a 35 años.
- 55 personas (14.3%) son de 36 a45 años.
- 27 personas (7%) son de más de 45 años.

En cuanto a la categoría género, 189 personas (49.1%) son de sexo femenino y 196 personas (50.9%) son de sexo masculino.

Según la categoría de ocupación se presentan los siguientes resultados:

- 100 personas (26%) corresponde a estudiantes.
- 171 personas (44.4%) personas corresponde a empleados.
- 91 personas (23.6%) personas corresponde a independientes.
- 20 personas (5.2%) personas corresponde a desempleados.
- 3 personas (0.9%) personas indican otro tipo de ocupación.

Los resultados indican que 160 personas (41.6%) tienen un conocimiento básico sobre tecnología, mientras que 170 personas (44.2%) tienen un conocimiento intermedio sobre tecnología, y 55 personas (14.3%) tienen un conocimiento avanzado sobre tecnología.

En lo que respecta al uso frecuente de las redes Wi-Fi públicas existen 181 personas (47%) que, si usan estas redes, y 204 personas (53%) indicaron que no suelen usar este tipo de redes públicas. De las personas que respondieron "No", entre las razones principales por las que no acostumbran a usar este tipo de redes públicas son: las preocupaciones de seguridad siendo el 18.6% (38 personas), por bajo rendimiento de la red 31.9% (65 personas), el 46.6% (95 personas) prefieren utilizar su propio plan de datos, y el 2.9% (6 personas) indican otras razones.

En relación a las actividades que realizan normalmente los usuarios cuando se conectan a una red Wi-Fi pública, tomando en cuenta que una persona puede realizar una o varias actividades, las 385 personas seleccionaron las siguientes:

- 188 personas (48.8%) navegan por internet.
- 156 personas (40.5%) revisan su correo electrónico.
- 288 personas (74.8%) revisan sus redes sociales.
- 63 personas (16.4%) realizan operaciones bancarias.
- 54 personas (14%) realizan transacciones en línea.
- 16 personas (4.7%) realizan otras actividades.

Según los datos de la encuesta 171 personas (44.4%) han recibido un aviso o advertencia sobre posibles riesgos al usar una red Wi-Fi pública, en cambio 214 personas (55.6%) no han recibido o no han tenido la oportunidad de leer alguna advertencia sobre los riesgos de usar redes públicas.

En cuanto a la seguridad que sienten las personas al usar redes Wi-Fi publicas indican que el 2.9% (11 personas) se siente muy seguro al usar estas redes, el 13% (50 personas) se

siente algo seguro, el 44.2% (170 personas) se siente neutral, el 30.6% (118 personas) se siente algo inseguro y el 9.4% (36 personas) se siente muy inseguro.

De acuerdo con los resultados, las 385 personas indican que están familiarizados con una o varias medidas de seguridad, descritas a continuación:

- El uso de VPN lo conoce el 40% (154 personas).
- El uso de conexiones cifradas https lo conoce el 26.2% (101 personas).
- Desactivación de la conexión automática a redes Wi-Fi lo conoce el 30.4% (117 personas).
- No compartir archivos o carpetas en la red lo conoce el 36.4% (140 personas).
- No está familiarizado con ninguna de las opciones anteriores corresponde al 27.8% (107 personas).

De acuerdo a las preocupaciones que sienten las personas al usar redes Wi-Fi públicas, ciertas personas creen que les pueda suceder las siguientes:

- Robo de datos personales el 40.5% (156 personas).
- Fraude o estafas en líneas el 17.1% (66 personas).
- Acceso no autorizado a mis dispositivos el 30.6% (118 personas).
- Ninguna preocupación en particular el 10.6% (41 personas).
- Otras preocupaciones el 1.2% (4 personas).

En cuanto a la probabilidad de las personas para evitar realizar transacciones bancarias o compras en línea en una red Wi-Fi pública, el 30.9% (119 personas) indica que es muy probable no realizar estas transacciones, el 33.8% (130 personas) indica que es probable, el 29.1% (112 personas) indica que es poco probable, y el 6.2% (24 personas) indica que no evitaría realizar este tipo de transacciones.

De las 385 personas encuestadas, el 6.8% (26 personas) manifiesta que las redes Wi-Fi públicas son seguras, el 40.2% (155 personas) piensa que no son los suficientemente seguras, y el 53% (204 personas) indica que desconocen que las redes Wi-Fi públicas sean seguras en Loja.

El 19.7% (76 personas) indica que si ha experimentado al menos una situación de inseguridad mientras usaba una red Wi-Fi pública en Loja, en cambio el 80.3% (309 personas) comenta no haber experimentado alguna situación de inseguridad.

De acuerdo a las medidas adicionales planteadas para mejorar las redes Wi-Fi públicas en Loja, de las 385 personas el 46.2% (178 personas) considera que debería implementarse la autenticación segura, el 56.4% (217 personas) considera que debería fomentarse la educación

y concienciación sobre riesgos de seguridad, el 33.5 % (129 personas) considera que debería existir un soporte técnico disponible, el 44.7% (172 personas) considera el cifrado de todas las conexiones y el 0.3% (1 personas) propone otras opciones.

En cuanto al nivel de satisfacción en general con respecto a las redes Wi-Fi públicas en Loja, las personas indicaron los siguientes grados de satisfacción:

- Muy satisfecho el 2.1% (8 personas)
- Satisfecho el 13.5 % (52 personas)
- Neutral el 56.1% (216 personas)
- Insatisfecho el 24.7% (95 personas)
- Muy insatisfecho el 3.6% (14 personas)

6.5. Resultados de la entrevista por parte de un ISP de Loja

En el apartado de Anexo 5 se presenta las respuestas de la entrevista dirigida a un proveedor de internet de la ciudad de Loja con relación a la seguridad de las redes Wi-Fi públicas. En este caso el entrevistado fue el Ing. Tito Muñoz, gerente de operaciones de "*Velocity*", su fotografía se lo puede apreciar en Anexo 6.

6.6. Mejoras a futuro

Dado los resultados obtenidos con hacking ético para el análisis de ciberseguridad en las redes públicas de Loja, a continuación, se presentan algunas mejoras e implementaciones que se podrían tomar en cuenta para una mejor seguridad en las redes wifi.

- La implementación de un autentificador multifactor para el acceso a la red, combinando contraseñas haciendo uso de métodos como tokens físicos, aplicaciones móviles o datos biométricos.
- Hacer uso de un cifrado de datos avanzados como WPA3, ya que permite lograr una mejor protección en la comunicación entre dispositivos y la red, este tipo de estándar es un protocolo más nuevo que WPA2 ofreciendo una mejor autenticación y cifrado, para una mejor seguridad contra amenazas.
- La implementación de un sistema de detección y prevención de intrusiones (IDPS) para la supervisión de la red en tiempo real, la detección de intrusos con actividades sospechosas y enviar alertas para la toma de acciones automáticas y bloqueo de amenazas.
- La utilización de redes definidas por Software (SDN) ayudará a la adaptación creciente de los requisitos de red de forma ágil y flexible, al separar los planos de control y de reenvío de

la red, permitiendo una mejor configuración de seguridad y una respuesta máxima ante amenazas.

- Ya que la seguridad de las redes es primordial para proteger la privacidad de los usuarios y los datos, el uso de la inteligencia artificial en el tráfico de red puede ayudar a identificar patrones inusuales y prevenir amenazas potenciales a la seguridad de la red. Esto ha mejorado la precisión de detección de amenazas en un 95%, según Cisco.
- Fomentar el manejo de las VPNs (Redes Privadas Virtuales) para los usuarios, ya que esta herramienta garantiza una capa adicional de cifrado y seguridad en la transmisión de datos.
- Establecer las medidas necesarias para los dispositivos IoT conectados a la red, tomando en cuenta el firmware actualizado.
- La educación y concientización sobre las redes informáticas es muy importante en la sociedad, por ende, se debe establecer programas de educación donde los usuarios conozcan y tengan prácticas de ciberseguridad, como evitar sitios web no seguro y no inviar información delicada a través de wifi público.

7. Discusión

Los resultados obtenidos en esta investigación evidencian que existe un número de vulnerabilidades significativas en las redes Wi-Fi públicas analizadas en la ciudad de Loja. Los riesgos encontrados parten desde certificados de seguridad inapropiados o caducados además de la falta de mecanismos de seguridad que evitan el ataque de fuerza bruta. Esto demuestra que, aunque existe un avance en los dispositivos tecnológicos, no existe un alto grado de conciencia sobre la ciberseguridad de la redes Wi-Fi públicas, la información que se entrega en los resultados indica que muchos de los riegos presentes en estas redes, se deben al no cumplir con estándares básicos de protección de información, provocando que los usuarios estén expuestos a posibles ataques cibernéticos, como el robo de datos personales, ataques intermediarios o la instalación de un malware en sus dispositivos.

Las herramientas de ciberseguridad entregaron datos cuantitativos que indican el porcentaje de las vulnerabilidades de las redes públicas en Loja clasificadas de acuerdo con su gravedad, como crítica, alta, media y baja. Esta información demuestra que no existen protocolos actualizados, además carecen de una encriptación segura, a pesar de existir un avance en los mecanismos de encriptación. Los resultados presentados en la investigación coinciden con las demás investigaciones que analizan las vulnerabilidades presentes en las redes e indican la falta de mecanismos de seguridad en las redes Wi-Fi públicas. Por lo tanto, son puntos claves que indican donde están los problemas de ciberseguridad de las redes públicas.

Al comparar estos resultados con estudios previos sobre la seguridad en redes Wi-Fi públicas, se observa una tendencia similar en términos de la presencia de vulnerabilidades críticas y la falta de implementación de prácticas de seguridad actualizadas. Un estudio realizado en Coruña, España sobre el análisis de riesgos de conexión a redes públicas (Verde, 2022), revela patrones comunes de vulnerabilidades como sistemas obsoletos, el uso de cifrados débiles y falta de concientización de los usuarios, provocando que las redes públicas sigan siendo potencialmente peligrosas, a pesar de los numerosos mecanismos de seguridad que existen para proteger a los usuarios en la actualidad.

Los resultados del análisis tienen importantes implicaciones tanto para los usuarios como para los proveedores de redes Wi-Fi públicas en Loja. Primeramente, la presencia de vulnerabilidades críticas y de alta severidad pone en riesgo no solo la privacidad de los usuarios, sino también la integridad de los sistemas conectados. Esto es especialmente preocupante en entornos de alto tráfico como paradas de autobuses y patios de comidas, donde las personas confían en la disponibilidad de Wi-Fi para acceder a servicios sensibles como transacciones en línea o revisión de su correo electrónico.

Los resultados de las encuestas presentan hallazgos importantes en torno a la seguridad y el uso de las redes públicas por parte de los usuarios. Estos resultados indican que, si bien un porcentaje considerable de la población utiliza estas redes (47%), existe una gran preocupación por su seguridad. Esto se refleja en el hecho de que el 40,2% de los encuestados afirmó que la red no era lo suficientemente segura, y un 53% no está seguro al respecto. Esta percepción está relacionada con la baja adopción de medidas de seguridad avanzadas por parte de los usuarios.

A pesar de que un 40% de los encuestados conoce y utiliza herramientas de protección como las VPN, una cuarta parte (27.8%) no está familiarizada con ninguna medida de seguridad. Este dato es significativo ya que indica que existe una falta de conciencia y educación sobre los riesgos inherentes al uso de redes públicas. Tal como se menciona en el documento de estrategias de seguridad cibernética del Ecuador (Maino, 2022), la educación y el conocimiento sobre ciberseguridad puede contribuir a la creación de una sociedad digital más competente y consciente, y de tal manera se puede reducir la exposición a riesgos en redes públicas.

Otro punto que destacar es la realización de actividades sensibles usando estas redes. A pesar de que la mayoría de los encuestados utilizó las redes Wi-Fi públicas para navegar y acceder a las redes sociales, un número considerable de encuestados realizó actividades de mayor riesgo, como operaciones bancarias, con un 16.4% y las transacciones en línea con un 14%. Esto representa un potencial peligro debido a la vulnerabilidad de estas redes frente a ataques como la suplantación de identidad y acceder al dispositivo de un usuario sin permiso, una amenaza contra la que el 30.6% de los encuestados no estaba protegido.

Asimismo, el 55.6% de los encuestados nunca ha recibido una advertencia sobre los peligros de usar estas redes. Por lo tanto, las campañas de concienciación son necesarias, y deben ser iniciadas tanto por las autoridades locales como los proveedores de servicios de internet.

En cuanto a las estrategias de mejora propuestas, la autenticación segura (46.2%) y la educación sobre los riesgos de seguridad (56.4%) son las más conocidas por los usuarios. Esto refuerza la hipótesis de que un enfoque integral que combine tanto medidas tecnológicas como educativas sería la mejor solución para incrementar la seguridad de las redes Wi-Fi públicas en la ciudad de Loja. Según los usuarios, implementar cifrado en todas las conexiones y ofrecer soporte técnico también son estrategias que podrían aumentar su confianza y reducir el riesgo de los ataques cibernéticos.

Los resultados de la investigación, aunque proporcionan información valiosa, tienen algunas limitaciones importantes. En primer lugar, el escaneo de vulnerabilidades realizado con

Nessus revela los aspectos estáticos de las debilidades de seguridad, que son relevantes solo en un punto en el tiempo. Esto se debe a que las vulnerabilidades podrían haber cambiado desde entonces: pueden parchearse las vulnerabilidades, o las configuraciones de red pueden haberse ajustado.

Como parte de las estrategias innovadoras para el plan de mejora, se propone la implementación de un sistema de detección y prevención de intrusiones (IDPS), esto puede ayudar a identificar pautas inusuales y prevenir amenazas potenciales a las redes públicas, haciendo un monitoreo de vulnerabilidades presentes de manera periódica. Estas estrategias son posibles y pueden ser implementadas en las mayorías de las redes públicas de la ciudad. Lo más importante es la aceptación de estas propuestas por parte de los proveedores del servicio de internet.

Por último, esta investigación destaca la importancia de contar con la colaboración de los gobiernos y de los proveedores del servicio de internet para mejorar la seguridad de los usuarios de las redes públicas de Loja. De igual importancia, es necesario la creación de leyes que regulen y exijan a los proveedores cumplir con normas básicas de seguridad cibernética para los usuarios.

8. Conclusiones

El uso de la herramienta AirCrack-ng de Kali Linux fue esencial, siendo una suite de seguridad inalámbrica que permite establecer este tipo de ataques y comprobar el nivel de seguridad de una contraseña Wi-Fi.

A pesar que varios sitios públicos de Loja tienen una buena seguridad en su contraseña, aun así, se pudo obtener el acceso eficaz a la red wifi de un establecimiento, por lo que indica que el nivel de seguridad en la contraseña es bajo, ya que una de las razones es el uso de palabras muy comunes, y estas contraseñas comunes pueden estar escritas en varios diccionarios que son utilizadas para hackear una red de forma ilícita.

Existe otro tipo de herramienta llamada Wireshark, que cumple con un similar funcionamiento para la realización de este tipo de ataques, por ende, también es muy usada.

De acuerdo con los resultados presentados se evidencia la existencia de vulnerabilidades en las redes públicas de Loja. La gravedad de las vulnerabilidades va desde crítico, alto, medio y bajo, demostrando que los usuarios son vulnerables a ataques cibernéticos, por lo tanto, comprometiendo su privacidad. Si bien las redes públicas proporcionan conexión a internet, también pueden ser un punto de riesgo debido a su falta de ciberseguridad.

Identificar y fortalecer los puntos de acceso que se encuentran vulnerables, haciendo una prueba de hacking ético se puede determinar los factores de amenaza, riesgo y vulnerabilidad dentro de una red Wi-Fi. Al implementarse estas prácticas de seguridad darían como resultado una mejora en la privacidad y confidencialidad de los datos enviados a través de ella, garantizando la integridad en el ámbito digital.

La prevención es primordial en la seguridad de la información, al permitir estrategias frente a actividades inusuales e imprevistas, garantizando la estabilidad de un negocio, haciendo una gestión de riesgos que permita evaluar estos riesgos para el beneficio de la empresa y facilitar la toma de decisiones en lo que respecta a la inversión y desarrollo de proyectos nuevos.

Al hablar de seguridad no es solo implementar sistemas de seguridad, sino que también incluye muchos factores más, es decir, para asegurar la integridad, disponibilidad y confidencialidad, se debe analizar la red interna, las instalaciones, los procedimientos y el personal.

Es necesario mencionar que para la elaboración de este trabajo de hacking ético se lo realizó con fines académicos, y con los permisos requeridos, ya que el ataque a una red sin consentimiento se considera una actividad ilegal.

De acuerdo a los resultados de la encuesta establecida y dirigida a las personas de la ciudad de Loja, se concluye que de la muestra de las 385 personas encuestadas existe el 41.6%

que tiene un conocimiento básico de tecnología, el 47% acceden a las redes públicas, de las personas que dijeron que si usan redes públicas el 74.8% ingresa a sus redes sociales, el 40.5% revisan su correo electrónico, el 16.4% realizan operaciones bancarias y el 14% realizan transacciones en línea, se puede notar que existen porcentajes alarmantes por parte de la ciudanía Lojana, que usan este tipo de redes para realizar ciertas actividades delicadas sin conocer que pueden estar en riesgo su información.

Con respecto a la ciberseguridad los resultados indican que el 27.8% no está familiarizado o nunca ha escuchado sobre las medidas de seguridad que pueden optar para proteger su información, razón de que el 56.8% nunca ha recibido alguna advertencia o aviso sobre el uso de estas redes públicas, a pesar que existe un 40.5 % de usuarios que si tienen una preocupación de que les pueda suceder el robo de datos personales y un 30.6% en referencia al acceso no autorizado a sus dispositivos.

Existe un 6.8% de los encuestados indicando que las redes Wi-Fi públicas en Loja no son seguras, estas personas son aquellas que tienen un avanzado conocimientos en tecnología, también se indica un 40.5% que cree que no son suficientemente seguras que probablemente estas personas hayan recibido alguna información preventiva sobre el uso de estas redes, pero el 53% establece que desconoce si las redes públicas sean seguras o no, dando la probabilidad de que ciertas personas se puedan conectar en algún momento y puedan realizar actividades que comprometan su datos, ya que los resultados informa que un 19.7% de los encuestados si ha recibido o experimentado situaciones de inseguridad mientras usaban las redes Wi-Fi públicas.

Por lo tanto, el 56.4% requiere que se fomente la educación y concienciación sobre riesgos de seguridad y el 47.2% considera que se aplique la autenticación segura.

Analizando la entrevista realizada a un proveedor de internet de la ciudad de Loja, la empresa ofrece acceso a sus redes Wi-Fi públicas mediante autenticación WPA2 y WPA3, pero no ha implementado estrategias específicas para proteger a los usuarios contra ataques cibernéticos como el phishing o el robo de datos. Además, no educan a los usuarios sobre cómo mantenerse seguros al usar estas redes. Esto sugiere que, si bien cumplen con estándares mínimos de seguridad, existen áreas de mejora para garantizar una protección más robusta para los usuarios.

Aunque la empresa reconoce la importancia de mantener un equilibrio entre la seguridad y la facilidad de uso, aún enfrentan dificultades para implementar medidas más avanzadas sin afectar la experiencia del usuario. Por ejemplo, el uso de WPA3 brinda mayor seguridad, pero no se ha implementado completamente debido a la incompatibilidad con algunos dispositivos, lo que refleja la necesidad de adaptar la tecnología sin perder funcionalidad.

Si bien la empresa realiza monitoreo del tráfico y el consumo de ancho de banda en tiempo real, han enfrentado problemas de seguridad y su principal enfoque ha sido bloquear puertos y establecer políticas de firewall, sin considerar herramientas avanzadas de protección proactiva. Esto indica que la infraestructura de seguridad podría mejorarse con la implementación de tecnologías más avanzadas y orientadas a la prevención de amenazas.

9. Recomendaciones

Establecer una buena contraseña con caracteres alfanuméricos puede ayudar a garantizar una mejor seguridad, ya que un diccionario, aunque tenga millones de contraseñas posibles, no podría descifrar la contraseña y así evitar que el acceso sea imposible de realizar.

Dada la implementación de los diferentes protocolos de seguridad en una red local, una medida de seguridad agregada sería el bloqueo de acceso a una IP desconocida de acuerdo a la cantidad de intentos permitidos para ingresar a la red.

Se determina que la mayoría de redes wifi públicas en Loja no son redes seguras, por lo tanto, si nos conectamos a una de estas redes libres se aconseja no enviar información delicada como datos personales, cuentas bancarias, no ingresar a correos electrónicos ya que estos se pueden usar para acceder a cuentas financieras y a cuentas sociales, todos estos datos pueden estar en riesgo ya que toda información viaja desde nuestro dispositivo hacia ese sitio web.

Una excelente recomendación para ambientes empresariales es la de establecer una red de usuarios con acceso a internet libre y otra para usuarios pertenecientes a la empresa con un filtro de autenticación a través de un portal de acceso, ya que esta separación de red no solo mejora la seguridad y el control, sino también mejora el rendimiento de la red y la confianza del usuario corporativo.

Para un mejor control de seguridad, es necesario llevar a cabo registros sobre incidentes de seguridad, para aumentar la confiabilidad y mejorar los resultados en la evaluación de riesgos.

Es recomendable llevar un análisis de seguridad cada cierto tiempo, aun si no ha existido inconvenientes, con el fin de asegurar y garantizar que la red Wi-Fi se encuentre protegida contra ataques posibles. Esto puede conllevar a pruebas de penetración, auditorias de seguridad y evaluaciones de vulnerabilidades, utilizando medidas necesarias en la red wifi, como la actualización frecuente del firmware del router, el uso de un software de seguridad actualizado y un firewall correctamente configurado.

10. Bibliografía

Acosta, A., Melo, E., & Linares, P. (2018). Evaluation of the WPA2-PSK wireless network security protocol using the Linset and Aircrack-ng tools. In *Revista Facultad de Ingeniería* (Vol. 27, Issue 47). https://doi.org/10.19053/01211129.v27.n47.2018.7748

Acuña, J., & Aponte, D. (2013). Análisis Del Rendimiento En Redes Wlan Caso Estudio: Wlan – Universidad Católica De Colombia Sede El Claustro (SCUCC). *Journal of Chemical Information and Modeling*, *53*(9), 1689–1699. http://repository.ucatolica.edu.co/bitstream/10983/1300/1/Documento.pdf

Aircrack-ng. (2024). *Introduction*. http://www.aircrack-ng.org/doku.php

Castillo, C. (2021). Ciberseguridad: Por dónde Empezar…. *Revista de Tecnología*, *18*(1), 1–12.

Castillo, U., & Polanco, M. (2023). ¿Qué es la ciberseguridad? *Scitum*, 1–16. https://www.ibm.com/mx-es/topics/cybersecurity2/13

Dafonte, P., & Pallardó, C. (2015). RADIUS: Seguridad en Sistemas de Información. *RADIUS: Seguridad En Sistemas de Información*, 1–28. http://sabia.tic.udc.es/docencia/ssi/old/2006-2007/docs/trabajos/11 - Radius.pdf

ESET. (2024). *Segurity Report Latinoamérica 2024*. 1–23.

Fiscalia General del Estado. (2024). *Unidad Nacional Especializada en Investigación de Ciberdelito*. https://www.fiscalia.gob.ec/accesibilidad/unidad-nacional-especializada-en-investigacion-de-ciberdelito/

Garzón, C., Illicachi, A., Navas, C., Espinoza, R., & Estrella, G. (2024). Análisis de los ataques de ingeniería Social en Ecuador. *Ciencia Latina Revista Científica Multidisciplinar*, *8*(1), 4354–4367. https://doi.org/https://doi.org/10.37811/cl_rcm.v8i1.9777

Guamán, M., Zenteno, J. A. C., Urgilés, C. F., Urgilés, C. F., & Egas, M. R. (2023). Análisis de riesgos y amenazas de ciberseguridad en el estado ecuatoriano, utilizando la metodología Magerit. *Pro Sciences*, *7*(49), 139–165. https://doi.org/https://doi.org/10.29018/issn.2588- 1000vol7iss49.2023pp139-165

Guevara, R. (2017). Riesgos con las redes Wi-Fi públicas del centro de Medellín, Colombia. In Fondo Editorial Remington (Ed.), *Riesgos con las redes Wi-Fi públicas del centro de Medellín, Colombia*. https://doi.org/10.22209/9789585613201

INCIBE. (2011). Seguridad en Redes Wi-Fi: una guía de aproximación para el empresario. *Seguridad En Redes Telematicas*, 1–29.

INEC. (2023). Tecnologías de la Información y comunicación. In *Ecuador en Cifras*. https://www.ecuadorencifras.gob.ec/documentos/web-inec/Estadisticas_Sociales/TIC/2023/202307_Tecnologia_de_la_Informacion_y_Comunicacion-TICs.pdf

Jaramillo, D. (2023). *Se contará con internet gratuito en los espacios públicos de la ciudad y parroquias*. https://www.loja.gob.ec/noticia/2023-11/se-contara-con-internet-gratuito-en-los-espacios-publicos-de-la-ciudad-y-parroquias

José, S., Castañón, R., Guillén, Á., Hernández, T., & Solís, N. (2022). Vigilancia tecnológica en CIBERSEGURIDAD. *ABC de La Ciberseguridad*, *1*, 1–36.

Juca, F., & Medina, R. (2023). Ciberdelitos en Ecuador y su impacto social; panorama actual y futuras perspectivas. *Portal de La Ciencia*, *4*(3), 325–337. https://doi.org/https://doi.org/10.51247/pdlc.v4i3.394

Maino, V. (2022). Estrategia Nacional de Ciberseguridad del Ecuador. *Ministerio de Telecomunicaciones y de La Sociedad de La Información*, 30–45. https://asobanca.org.ec/wp-content/uploads/2022/08/ESTRATEGIA-NACIONAL-DE-CIBERSEGURIDAD-DEL-ECUADOR-2022481.pdf

Monsalve, J., Aponte, F., & Chaparro, F. (2015). Security analysis of a WLAN network sample in Tunja, Boyacá, Colombia. *Dyna*, *82*(189), 226–232. https://doi.org/10.15446/dyna.v82n189.43259

Mora, A., Macías, R., Rodríguez, J., & Sacón, H. (2021). Estudio de la tecnología de comunicación inalámbrica en el estándar IEEE 802.11ax orientada al despliegue en Ecuador para el desarrollo del internet de las cosas. *Revista Cientifica Dominio de Las Ciencias*, *7*(4), 729–762. https://doi.org/http://dx.doi.org/10.23857/dc.v7i4.2447

Mora, M. (2004). Tecnologías para redes LAN inalámbricas. *Télématique*, *3*(1), 79–93.

Navarro, G. (2011). Introducción a las vulnerabilidades. *UOC*, 1–24.

Paredes, M., & Semanate, A. (2024). El ciberterrorismo y la seguridad nacional. *Academia de Guerra Del Ejército Ecuatoriano*, *17*(1), 144–158.

Paspuel, M. (2018). Hack de Redes Wireless con Aircrack-ng. *Nexos Científicos*, *2*(2), 16–20. https://nexoscientificos.vidanueva.edu.ec/index.php/ojs/article/view/20/155%0Ahttps://nexoscientificos.vidanueva.edu.ec/index.php/ojs/article/view/20

Pilco, M. (2015). *Análisis de vulnerabilidades en redes wifi Ad-Hoc mediante software libre para mejorar la seguridad en ambientes outdoor*. Escuela Superior Politécnica de Chimborazo.

Pons, V. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. *URVIO*, *20*, 80–93. https://doi.org/http://dx.doi.org/10.17141/urvio.20.2017.2563 Internet,

Ramos, S. (2006). Aspectos de seguridad en aplicaciones basadas en WIFI. *Redes*, *5*, 801–802.

Salazar, F. (2021). *Estándares ISO de Ciberseguridad*. https://es.linkedin.com/pulse/estándares-iso-de-ciberseguridad-fernanda-salazar

Salazar, J. (2012). Redes Inalámbricas. In *European Virtual Learning Platform for Electrical and Information Engineering* (Versión de, Vol. 2, Issue 1). https://upcommons.upc.edu/bitstream/handle/2117/100918/LM01_R_ES.pdf

Santiago, E. J. (2006). Redes Móviles Ad-Hoc. *Prospectiva*, *4*(2), 7–11. http://www.redalyc.org/articulo.oa?id=496251108002%0ACómo

Seguridad Wireless. (2024). *KISMET*. https://www.seguridadwireless.net/kismet/

Tenable. (2024). *Scan Notes in Severity Details*. https://docs.tenable.com/web-app-scanning/Content/WAS/Scans/ScanNotesSeverity.htm

Vega, E. (2021). *Seguridad de la Información*. https://doi.org/https://doi.org/10.17993/tics.2021.4

Verde, I. (2022). *Análisis de riesgos de conexión a redes públicas* [Universidad de Jaén]. https://ruc.udc.es/dspace/handle/2183/31652

Vivar, I. (2023). *Aplicacion de hacking etico para identificar amenazas, riesgos y vulnerabilidades en la red wifi*. *5*, 1–14. https://www.ncbi.nlm.nih.gov/books/NBK558907/

Weyman, H. (2024). *Seguridad informática*. 1–6.

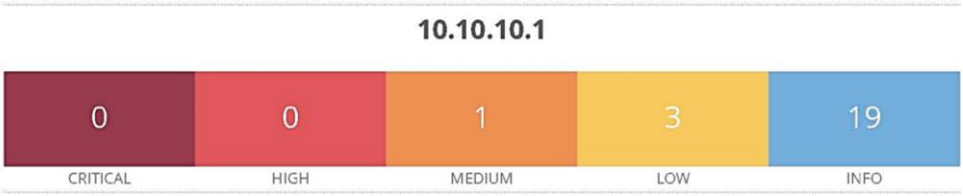
WISP. (2020). *¿Qué es Radius?* https://wispcontrol.com/que-es-radius/

11. Anexos

Documentos exportados del informe de Análisis de vulnerabilidades de la Red 10.10.10.0/24 con Nessus.

Anexo 1

Captura de imagen del informe exportado en Nessus para una Red Wi-Fi



Vulnerabilities Total: 23

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	6.5	-	42263	Unencrypted Telnet Server
LOW	3.7	-	70658	SSH Server CBC Mode Ciphers Enabled
LOW	3.7	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	2.6*	-	71049	SSH Weak MAC Algorithms Enabled
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	19689	Embedded Web Server Detection
INFO	N/A	-	10092	FTP Server Detection
INFO	N/A	-	30212	MikroTik RouterOS Detection
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	70657	SSH Algorithms and Languages Supported
INFO	N/A	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	10881	SSH Protocol Versions Supported
INFO	N/A	-	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	10267	SSH Server Type and Version Information
INFO	N/A	-	22964	Service Detection

INFO	N/A	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	10281	Telnet Server Detection
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	11154	Unknown Service Detection: Banner Retrieval

* indicates the v3.0 score was not available; the v2.0 score is shown

10.10.10.2

Vulnerabilities Total: 24

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	42263	Unencrypted Telnet Server
MEDIUM	5.3	-	15901	SSL Certificate Expiry
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	10884	Network Time Protocol (NTP) Server Detection
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	10863	SSL Certificate Information
INFO	N/A	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	136318	TLS Version 1.2 Protocol Detection

INFO	N/A	-	10281	Telnet Server Detection
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	11154	Unknown Service Detection: Banner Retrieval
INFO	N/A	-	10386	Web Server No 404 Error Code Check
INFO	N/A	-	10302	Web Server robots.txt Information Disclosure

* indicates the v3.0 score was not available; the v2.0 score is shown

10.10.10.5

Vulnerabilities Total: 3

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	135860	WMI Not Available

* indicates the v3.0 score was not available; the v2.0 score is shown

10.10.10.6

Vulnerabilities Total: 3

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	135860	WMI Not Available

* indicates the v3.0 score was not available; the v2.0 score is shown

10.10.10.18

0	2	6	0	30
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 38

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
HIGH	8.1	-	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
HIGH	7.5	-	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	157288	TLS Version 1.1 Deprecated Protocol
MEDIUM	5.9	-	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	-	57608	SMB Signing not required
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	10736	DCE Services Enumeration
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
INFO	N/A	-	11011	Microsoft Windows SMB Service Detection

INFO	N/A	-	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	-	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	10940	Remote Desktop Protocol Service Detection
INFO	N/A	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	10863	SSL Certificate Information
INFO	N/A	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	51891	SSL Session Resume Supported
INFO	N/A	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	-	121010	TLS Version 1.1 Protocol Detection
INFO	N/A	-	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	64814	Terminal Services Use SSL/TLS
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	135860	WMI Not Available
INFO	N/A	-	10150	Windows NetBIOS / SMB Remote Host Information Disclosure

* indicates the v3.0 score was not available; the v2.0 score is shown

10.10.10.19

0	0	0	0	16
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 16

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	39520	Backported Security Patch Detection (SSH)
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	181418	OpenSSH Detection
INFO	N/A	-	70657	SSH Algorithms and Languages Supported
INFO	N/A	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	10881	SSH Protocol Versions Supported
INFO	N/A	-	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	10267	SSH Server Type and Version Information
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	10287	Traceroute Information

* indicates the v3.0 score was not available; the v2.0 score is shown

Documento exportado del informe de Análisis de vulnerabilidades de la IP 40.40.11.37 con Nessus.

Anexo 2

Captura de imagen del informe exportado en Nessus para una IP

Vulnerabilities Total: 46

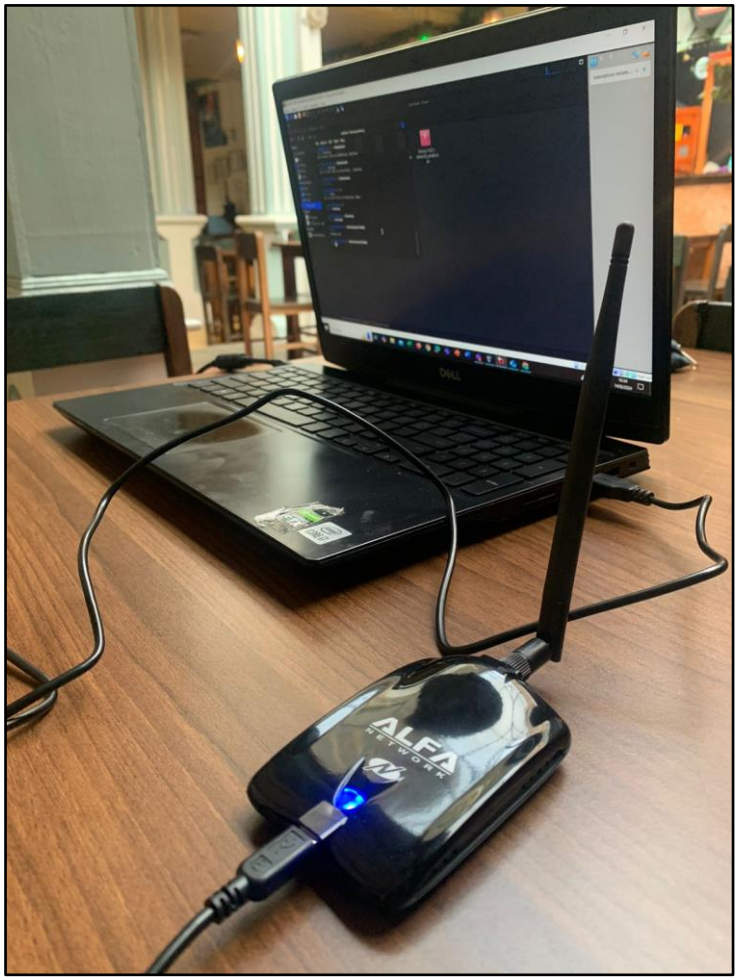
SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	10.0	-	-	73756	Microsoft SQL Server Unsupported Version Detection (remote check)
HIGH	7.5	4.9	0.0111	35291	SSL Certificate Signed Using Weak Hashing Algorithm
HIGH	7.5	5.1	0.0053	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	6.5	-	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	-	157288	TLS Version 1.1 Deprecated Protocol
MEDIUM	5.3	-	-	57608	SMB Signing not required
MEDIUM	5.0*	-	-	12218	mDNS Detection (Remote Network)
LOW	N/A	-	-	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	10736	DCE Services Enumeration
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	62351	Erlang Port Mapper Daemon Detection
INFO	N/A	-	-	43111	HTTP Methods Allowed (per directory)
INFO	N/A	-	-	10107	HTTP Server Type and Version
INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	108761	MSSQL Host Information in NTLM SSP

INFO	N/A	-	-	69482	Microsoft SQL Server STARTTLS Support
INFO	N/A	-	-	10144	Microsoft SQL Server TCP/IP Listener Detection
INFO	N/A	-	-	10674	Microsoft SQL Server UDP Query Remote Version Disclosure
INFO	N/A	-	-	42410	Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure
INFO	N/A	-	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	-	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
INFO	N/A	-	-	11011	Microsoft Windows SMB Service Detection
INFO	N/A	-	-	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	-	-	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remo check)
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	24786	Nessus Windows Scan Not Performed with Admin Privileges
INFO	N/A	-	-	11936	OS Identification
INFO	N/A	-	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	-	45410	SSL Certificate 'commonName' Mismatch
INFO	N/A	-	-	10863	SSL Certificate Information
INFO	N/A	-	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	-	22964	Service Detection
INFO	N/A	-	-	121010	TLS Version 1.1 Protocol Detection
INFO	N/A	-	-	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	-	-	10287	Traceroute Information
INFO	N/A	-	-	135860	WMI Not Available
INFO	N/A	-	-	11239	Web Server Crafted Request Vendor/Version Information Disclosure
INFO	N/A	-	-	72427	Web Site Client Access Policy File Detection
INFO	N/A	-	-	10150	Windows NetBIOS / SMB Remote Host Information Disclosure

* indicates the v3.0 score was not available; the v2.0 score is shown

Anexo 3

Pruebas de hacking ético en un bar-restaurante



Anexo 4

Modelo de encuesta para usuarios de la ciudad de Loja

ENCUESTA: USO Y SEGURIDAD EN REDES Wi-Fi PÚBLICAS EN LOJA

Objetivo: Recopilar información sobre el uso y la percepción de seguridad de las redes Wi-Fi públicas por parte de los habitantes de Loja, para identificar posibles áreas de mejora.

Instrucciones: Sus respuestas son anónimas y serán utilizadas únicamente con fines académicos. Por favor, responda con la mayor sinceridad posible.

Acceder a Google para guardar el progreso. Más información

* Indica que la pregunta es obligatoria

Correo electrónico *

Tu dirección de correo electrónico

Fecha *

Fecha

dd/mm/aaaa

1) Edad: *

- ◯ Menos de 18 años
- ◯ 18-25 años
- ◯ 26-35 años
- ◯ 36-45 años
- ◯ Más de 45 años

2) Género *

- ◯ Masculino
- ◯ Femenino

3) Ocupación *

- ◯ Estudiante
- ◯ Empleado (a)
- ◯ Independiente
- ◯ Desempleado (a)
- ◯ Otros: _____

4) ¿Cuál es su nivel de conocimiento sobre tecnología? *

- ◯ Básico
- ◯ Intermedio
- ◯ Avanzado

5) ¿Utiliza frecuentemente redes Wi-Fi públicas? *

- ◯ Si
- ◯ No

6) Si respondió "No" en la pregunta anterior, ¿Cuál es la razón principal? (Si respondió "Sí", pase a la siguiente pregunta)

- ◯ Preocupaciones de seguridad
- ◯ Bajo rendimiento de la red
- ◯ Prefiero utilizar mi propio plan de datos
- ◯ Otros: _____

7) ¿Qué tipo de actividades realiza normalmente cuando se conecta a una red Wi-Fi pública? (Puede seleccionar más de una opción) *

- [ ] Navegar por internet
- [ ] Revisar correo electrónico
- [ ] Uso de redes sociales
- [ ] Operaciones bancarias
- [ ] Transacciones en línea
- [ ] Otros: _____

8) ¿Ha recibido alguna vez un aviso o advertencia sobre posibles riesgos al usar una red Wi-Fi pública? *

- ◯ Si
- ◯ No

9) ¿Qué tan seguro se siente al utilizar redes Wi-Fi públicas? *

- ◯ Muy seguro
- ◯ Algo seguro
- ◯ Neutral
- ◯ Algo inseguro
- ◯ Muy inseguro

10) ¿Está familiarizado con alguna de las siguientes medidas de seguridad para redes Wi-Fi públicas? (Puede seleccionar más de una opción) *

- [ ] Uso de VPN
- [ ] Uso de conexiones cifradas (https)
- [ ] Desactivación de la conexión automática a redes Wi-Fi
- [ ] No compartir archivos o carpetas en la red
- [ ] No estoy familiarizado con ninguna
- [ ] Otros: _____

11) ¿Cuál es su principal preocupación al usar redes Wi-Fi públicas? *

- ◯ Robo de datos personales
- ◯ Fraude o estafas en línea
- ◯ Acceso no autorizado a mis dispositivos
- ◯ Ninguna preocupación en particular
- ◯ Otros: _____

12) ¿Qué tan probable es que evite realizar transacciones bancarias o compras en línea mientras está conectado a una red Wi-Fi pública? *

- ◯ Muy probable
- ◯ Probable
- ◯ Poco probable
- ◯ No lo evitaría

13) ¿Cree que las redes Wi-Fi públicas en Loja son lo suficientemente seguras? *

- ◯ Sí
- ◯ No
- ◯ No estoy seguro

14) ¿Ha experimentado alguna vez una situación de inseguridad mientras usaba una red Wi-Fi pública en Loja? *

- ◯ Sí
- ◯ No

15) ¿Qué medidas adicionales considera que deberían implementarse para mejorar la seguridad de las redes Wi-Fi públicas en Loja? (Puede seleccionar más de una opción) *

- [ ] Implementación de autenticación segura
- [ ] Educación y concienciación sobre riesgos de seguridad
- [ ] Soporte técnico disponible
- [ ] Cifrado de todas las conexiones
- [ ] Otros: _____

16) ¿Cuál es su nivel de satisfacción general con las redes Wi-Fi públicas disponibles en Loja? *

- ○ Muy satisfecho
- ○ Satisfecho
- ○ Neutral
- ○ Insatisfecho
- ○ Muy insatisfecho

Anexo 5

Respuesta a la entrevista a un proveedor de Internet

Universidad Nacional de Loja | POSGRADO

Maestría en Telecomunicaciones

Entrevista para Proveedores de Internet sobre Seguridad en Redes Wi-Fi Públicas en Loja

Objetivo: Comprender las prácticas actuales de seguridad en las redes Wi-Fi públicas ofrecidas por los ISP en Loja y explorar estrategias para su mejora.

Fecha:

PREGUNTAS.

1. **¿Podría proporcionarnos una visión general de los servicios de redes Wi-Fi públicas que su empresa ofrece en Loja? ¿Por lo general en que lugares se ofrece este servicio?**

   Las redes Wi-Fi proporcionan conexiones inalámbricas a Internet a diferentes velocidades mediante la transmisión de ondas de radio en diferentes frecuencias. Suelen dividirse en bandas de frecuencia de 2.4 GHz, 5 GHz y 6 GHz. Sin embargo, dependiendo de tus necesidades, las frecuencias más altas no siempre son la mejor opción. Las frecuencias más bajas, como 2.4 GHz, transmiten durante más tiempo y proporcionan un mayor alcance a velocidades inferiores a 6 GHz, lo que proporciona mayor velocidad y rendimiento, pero menos rango de movimiento. Las redes wifi públicas son puntos de conexión gratuita a internet que podemos encontrar en multitud de espacios públicos tales como canchas, plazas, mercados, paradas del bus y escuelas municipales etc.

2. **¿Cuál es el perfil típico de los usuarios que se conectan a sus redes Wi-Fi públicas?**

   El perfil típico de los usuarios que se conectan a redes Wi-Fi públicas suele ser, estudiantes, turistas, profesionales, usuarios ocasionales, personas en general.

3. **¿Qué tan seguros se sienten con las medidas de seguridad que tienen en sus redes Wi-Fi públicas? ¿Qué hacen para proteger a los usuarios?**

   Las redes Wi-Fi públicas que tiene actualmente Velocity se encuentran abiertas mediante el uso de un portal cautivo, en donde el usuario que intenta conectarse tiene que aceptar ciertas condiciones para poder hacer uso del servicio de internet.

4. **¿Su empresa realiza monitoreo en tiempo real del tráfico en las redes Wi-Fi públicas?**

   Se puede verificar el nivel de consumo de ancho de banda, por cada determinado tiempo y por cada Access Point, número de dispositivos conectados por marca y el tiempo de conexión de cada dispositivo.

5. **¿Qué tipo de autenticación utilizan los usuarios para acceder a las redes Wi-Fi públicas?**

   Se utiliza autenticación como WPA2 y WPA3, a través de una contraseña predeterminada donde todos los dispositivos puedan conectarse.

6. **¿Han implementado alguna estrategia específica para proteger a los usuarios contra ataques como el phishing o el robo de datos en sus redes Wi-Fi públicas?**

   Actualmente no.

7. **¿Alguna vez ha tenido que lidiar con problemas de seguridad en estas redes? ¿Cómo lo manejaron?**

   Implementando políticas de seguridad en firewall de la empresa, deshabilitando puertos conocidos, como telnet, ftp, servidores de correo.

8. **¿Cuáles son los principales desafíos que enfrentan al mantener la seguridad en las redes Wi-Fi públicas?**

   Establecer políticas de seguridad, como el acceso a páginas de contenido para adultos, establecer configuraciones lógicas adecuadas en el Access Point, evitar las herramientas de monitoreo más robustas.

9. **¿Cree que hay algo que se pueda mejorar en la seguridad de las redes Wi-Fi públicas? ¿Tiene planes para hacer cambios?**

   Si, establecer conexiones seguras como https a través de un portal cautivo.

10. **¿Qué piensa sobre el equilibrio entre mantener la red segura y al mismo tiempo que sea fácil de usar para todos?**

    La combinación entre mantener la red segura y que sea fácil de usar, permite conllevar una infraestructura tecnológica al más alto nivel, tanto como el recurso humano, tecnológico y de seguridad lógica.
    Actualmente se puede lograr ese equilibrio, gracias al avance tecnológico ya que nos permite la facilidad de conexión a redes inalámbricas y al mismo tiempo implementar medidas de seguridad, para evitar ataques, suplantación de identidad. Un claro ejemplo de ellos es el Wi-Fi que ya se encuentra disponible en las instituciones bancarias, que hace 3 o 4 años no se podía hacer el uso de las mismas.

11. **¿Hacen algo para informar a los usuarios sobre cómo mantenerse seguros al usar sus redes Wi-Fi públicas?**

    No.

12. **¿Están probando o considerando nuevas tecnologías para mejorar la seguridad en sus redes Wi-Fi?**

    Actualmente con Wi-Fi 6 se está incorporando la autenticación con WPA3 que brinda mayor seguridad, sin embargo, por compatibilidad de dispositivos de usuarios finales se utiliza aun WPA2.

Anexo 6

Fotografía del Gerente de Operaciones de Internet "Velocity"

Anexo 7

Certificado de traducción del resumen

UNIDAD EDUCATIVA FISCOMISIONAL SANTA JUANA DE ARCO "LA SALLE"

Cariamanga, 04 de octubre del 2024

Lic. Andrea Gaona

DOCENTE DE INGLES DE LA UNIDAD EDUCATIVA FISCOMISIONAL SANTA JUANA DE ARCO "LA SALLE"

A petición verbal de la parte interesada:

CERTIFICA

Que, la traducción del documento adjunto solicitado por el Ing. **Andy René Peña Cueva** con cédula de identidad Nº **1104112683,** cuyo tema de investigación se titula **FORTALECIMIENTO CIBERNÉTICO: ANÁLISIS INTEGRAL DE LA SEGURIDAD EN REDES WI-FI PÚBLICAS EN LOJA Y ESTRATEGIAS INNOVADORAS DE MEJORA**, ha sido realizado por mi persona, Andrea Silvana Gaona Abad, docente de Inglés. Esta es una traducción textual del documento adjunto. Lo certifico en honor a la verdad, facultando al portador del presente documento hacer uso legal pertinente.

Atentamente,

Lic. Andrea Gaona

EFL Teacher

Registro SENESCYT: 1031-2020-2226204