REPÚBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA

“SEGURIDADES EN REDES INALÁMBRICAS: UNA PROPUESTA DE MEJORA EN SEGURIDAD PARA UNA INSTITUCIÓN PÚBLICA EN LA PROVINCIA DE IMBABURA”.

Trabajo de Titulación previo a la obtención del título de Magíster en computación mención seguridad informática.

AUTOR: Msc. Xavier Fabricio Abarca Chávez

DIRECTOR: Msc. Iván Patricio Ortiz Garcés

IBARRA - ECUADOR

2025

REPÚBLICA DEL ECUADOR UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN

A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	1709777948		
APELLIDOS Y NOMBRES:	Abarca Chávez Xavier Fabricio		
DIRECCIÓN:	Calles Sucre y Psje. S/N – Chaltura – Antonio Ante.		
E-MAIL:	xfabarcac@utn.edu.ec		
TELÉFONO FIJO:		TELÉFONO MÓVIL:	0992555551
DATOS DE LA OBRA			
TÍTULO:	Seguridades en redes inalámbricas: una propuesta de mejora en seguridad para una institución pública en la provincia de Imbabura.		
AUTOR (ES):	Abarca Chávez Xavier Fabricio		
FECHA: DD/MM/AA	02/06/2025		
SOLO PARA TRABAJOS DE GRADO			
PROGRAMA:	PREGRADO [ ] POSGRADO [**X**]		
TÍTULO POR EL QUE OPTA:	Magister en computación con mención en seguridad informática		
DIRECTOR:	Msc. Iván Patricio Ortíz Garcés		
ASESOR:	PhD. Antonio Quiña Mera		

2. CONSTANCIAS

El autor manifiesta que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es el titular de los derechos patrimoniales, por lo que asume a responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 02 días del mes de junio de 2025.

EL AUTOR:

Msc. Xavier Fabricio Abarca Chávez
C.C: 1709777948

UNIVERSIDAD TÉCNICA DEL NORTE

Acreditada Resolución Nro. 173-SE-33-CACES-2020

FACULTAD DE POSGRADO

Ibarra,24 de marzo de 2025

Dra.
Lucía Yépez
DECANA FACULTAD DE POSGRADO

ASUNTO: Conformidad con el documento final

Señor(a) Decano(a):

Nos permitimos informar a usted que revisado el Trabajo final de Grado "SEGURIDADES EN REDES INALÁMBRICAS: UNA PROPUESTA DE MEJORA EN SEGURIDAD PARA UNA INSTITUCIÓN PÚBLICA EN LA PROVINCIA DE IMBABURA" del maestrante Xavier Fabricio Abarca Chávez, de la Maestría en Computación Mención Seguridad Informática, certificamos que han sido acogidas y satisfechas todas las observaciones realizadas.

Atentamente,

	Apellidos y Nombres	Firma
Director/a	Msc. Iván Patricio Ortiz Garcés	IVAN PATRICIO ORTIZ GARCES
Asesor/a	PhD. Antonio Quiña Mera	JOSE ANTONIO QUIÑA MERA

DEDICATORIA

Este trabajo de titulación, le dedico a Dios por permitirme mantenerme con vida, salud y junto a mis seres queridos. A mis padres Adalberto y Judith por haberme enseñado los valores de la vida, luchar por los sueños y anhelos fijados por salir adelante pese a los obstáculos que la vida misma nos pone. Gracias Padre por su apoyo inquebrantable durante el crecimiento profesional.

A mi esposa Anabely por ser mi compañera incondicional de vida, con quien juntos hemos venido construyendo nuestra vida con fe de lucha de una manera inquebrantable y con resiliencia.

A mis hermanos Paola y Roberto, a pesar de la distancia, en todo momento han estado con su apoyo incondicional para seguir alcanzando juntos la felicidad y éxitos.

Xavier Fabricio Abarca Chávez

AGRADECIMIENTO

Quiero expresar mi agradecimiento a la Universidad Técnica del Norte por brindarme la oportunidad de formar parte de la comunidad y adquirir los conocimientos y valores éticos que me permiten ser un mejor ser humano al servicio de la sociedad.

Agradezco especialmente a todos mis maestros que han sido parte de este proceso de aprendizaje, en particular al Magíster Alex Guevara, Coordinador de la Maestría; al Msc. Iván Patricio Ortíz Garcés, Director de Tesis; y al PhD. Antonio Quiña Merao, Asesor. Su experiencia y conocimientos han sido fundamentales para que pueda alcanzar este objetivo académico.

Xavier Fabricio Abarca Chávez

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE FOTOGRAFÍAS

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

PROGRAMA DE MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA

Autor: Xavier Fabricio Abarca Chávez

Director: Mgt. Iván Ortíz

Año: 2025

RESUMEN

La investigación aborda la problemática de las vulnerabilidades en redes inalámbricas Wi-Fi en instituciones públicas, específicamente en un GAD Parroquial de la provincia de Imbabura, donde la falta de medidas de seguridad robustas expone información sensible a riesgos de ciberataques. El objetivo general fue desarrollar un plan integral de seguridad para proteger la confidencialidad, integridad y disponibilidad de la información, garantizando la continuidad de los servicios y el cumplimiento normativo. Se utilizó un enfoque mixto, combinando análisis cualitativo y cuantitativo, mediante pruebas de penetración con herramientas como AirCrack, Wireshark y NESSUS, entrevistas y revisión documental. Los resultados revelaron vulnerabilidades críticas, como contraseñas débiles y ausencia de segmentación de red, lo que permitió accesos no autorizados. La propuesta incluye una arquitectura de seguridad basada en segmentación de red, autenticación robusta, uso de firewalls, sistemas IDS/IPS y políticas de seguridad, además de un plan de capacitación para el personal. Entre los aportes destacados, se identificaron medidas efectivas para mitigar riesgos, como la implementación de contraseñas seguras, cifrado de datos y un plan de

respuesta ante incidentes, contribuyendo a fortalecer la seguridad informática y la confianza ciudadana en la gestión institucional.

Palabras clave: Ciberseguridad, Redes Wi-Fi, Instituciones públicas, Vulnerabilidades, Seguridad informática.

ABSTRACT

The research addresses the issue of vulnerabilities in Wi-Fi wireless networks in public institutions, specifically in a Parish GAD in the province of Imbabura, where the lack of robust security measures exposes sensitive information to cyberattack risks. The general objective was to develop a comprehensive security plan to protect the confidentiality, integrity, and availability of information, ensuring service continuity and regulatory compliance. A mixed approach was used, combining qualitative and quantitative analysis through penetration testing with tools such as AirCrack, Wireshark, and NESSUS, interviews, and document review. The results revealed critical vulnerabilities, such as weak passwords and lack of network segmentation, which allowed unauthorized access. The proposal includes a security architecture based on network segmentation, robust authentication, the use of firewalls, IDS/IPS systems, and security policies, in addition to a training plan for staff. Among the highlighted contributions, effective measures were identified to mitigate risks, such as implementing secure passwords, data encryption, and an incident response plan, contributing to strengthening IT security and citizens' trust in institutional management.

Keywords: Cybersecurity, Wi-Fi networks, Public institutions, Vulnerabilities, IT security.

CAPÍTULO I

El PROBLEMA

1.1 Problema de Investigación

El uso de redes inalámbricas se ha vuelto un tema de máxima relevancia en el contexto actual, transformando nuestras formas de conexión y comunicación. Su facilidad de instalación y uso ha llevado a una adopción masiva por parte de individuos, organizaciones y gobiernos. Sin embargo, esta conveniencia también implica una serie de riesgos asociados, puesto que la transmisión de información a través de ondas de radio las hace vulnerables a ataques maliciosos. Los protocolos de seguridad disponibles actualmente ya no se consideran completamente eficaces, lo que aumenta la vulnerabilidad de estas redes (Hernández et al., 2017).

A nivel global, el informe del Centro de Denuncias de Delitos en Internet (IC3) (2023) pone de manifiesto que durante 2023 se registraron más de 3,200 violaciones de datos, que impactaron a millones de personas en diversos países. Esta tendencia es preocupante, ya que el incremento en el uso de dispositivos móviles y redes Wi-Fi ha comprometido la seguridad de la información personal. Al conectarse a redes inseguras sin las debidas precauciones, los usuarios se colocan en riesgo (Statista, 2023). Se estima que el costo de los ciberataques podría alcanzar los 10.5 billones de dólares anuales para 2025, reflejando el considerable impacto económico derivado de las brechas de seguridad en redes inalámbricas (Deloitte, 2023). Este peligro es aún más acentuado en comparación con las redes de conexión fija, que suelen ofrecer una mayor robustez ante ciberamenazas (Moreno, 2024).

En Ecuador, la pandemia de 2020 actuó como catalizador para el aumento del uso de internet, resultando en un 7.7% más de hogares con acceso a la red (Chuquitarco y Romero, 2018). No obstante, el crecimiento de la conectividad también ha traído consigo nuevas vulnerabilidades y amenazas. La falta de educación en ciberseguridad impide que muchos

usuarios adopten las medidas necesarias para protegerse, y la insuficiencia de recursos para implementar mecanismos de protección incrementa la exposición a ciberataques, lo que puede traducirse en pérdidas económicas significativas, especialmente en un entorno donde muchas empresas dependen de redes inalámbricas (Salazar et al., 2023).

Particularmente en el ámbito de las instituciones públicas, la seguridad de las redes Wi-Fi emerge como un desafío crítico, sobre todo para los gobiernos autónomos descentralizados (GAD). Estas entidades no solo realizan funciones esenciales, sino que también gestionan información sensible que atañe a la ciudadanía, incluidos datos personales, presupuestos municipales y planificación territorial. Según Ávila (2024), a pesar de los esfuerzos del gobierno nacional para reforzar la ciberseguridad, muchas instituciones públicas enfrentan desafíos para implementar protocolos robustos para proteger sus redes inalámbricas, exponiéndolos a riesgos como accesos no autorizados y robo de información.

En la provincia de Imbabura, los GAD parroquiales enfrentan retos considerables para mejorar su ciberseguridad. Entre las principales limitaciones se encuentran la falta de infraestructura tecnológica adecuada y la escasa capacitación del personal en materia de ciberseguridad. En muchos municipios, las redes Wi-Fi institucionales no cuentan con medidas avanzadas de protección, tales como firewalls efectivos, cifrado actualizado o autenticación multifactor. La falta de inversión en seguridad, la obsolescencia de los equipos y la carencia de políticas adecuadas y capacitación en ciberseguridad son obstáculos persistentes. Esta vulnerabilidad deja a las instituciones expuestas a posibles ciberataques, que podrían resultar en la exfiltración de datos, interrupciones en servicios públicos esenciales y daños a la reputación institucional, lo que impacta negativamente la confianza de la ciudadanía en su gestión y en el cumplimiento de sus atribuciones.

1.2 Interrogantes de la Investigación

RQ: ¿Cuáles son los riesgos de ciberseguridad en la red WIFI la Institución Pública, que permita la identificación y propuesta de medidas efectivas de protección y mitigación?

A partir de la pregunta anterior, surgen las siguientes interrogantes que nos llevan a examinar los problemas específicos:

- ¿Qué medidas de seguridad deben implementarse en la red Wi-Fi de la institución para mitigar las vulnerabilidades existentes?
- ¿Cómo garantizar la confidencialidad de los datos y asegurar la continuidad de los servicios, en cumplimiento con las normativas vigentes?
- ¿Cuál es el nivel de madurez de la gestión de seguridad de la red Wi-Fi de la institución?
- ¿Qué vulnerabilidades técnicas y de configuración existen en la infraestructura de red?
- ¿Cuál es la efectividad de las medidas de seguridad implementadas actualmente?
- ¿Qué factores organizacionales y culturales influyen en la seguridad de la red?
- ¿Qué recomendaciones se pueden hacer para mejorar la seguridad de la red a corto y largo plazo?

1.3 Objetivos de la Investigación

1.3.1 Objetivo General

Desarrollar un plan integral de seguridad para la red Wi-Fi de una institución pública con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, garantizando la continuidad de los servicios y cumplimiento del marco normativo aplicable.

1.3.1 Objetivos Específicos

Realizar un análisis exhaustivo de la seguridad de la red Wi-Fi, identificando vulnerabilidades, evaluando riesgos y analizando el cumplimiento normativo.

Proponer soluciones técnicas y organizacionales para fortalecer la seguridad de la red, incluyendo la implementación de políticas de seguridad, el uso de protocolos de seguridad modernos y la capacitación del personal.

Elaborar un plan detallado de políticas para responder a incidentes de seguridad, incluyendo la recuperación de datos y la continuidad de los servicios.

Evaluar la efectividad de las políticas propuestas sobre los riesgos de ciberseguridad en la red WIFI de la Institución, como medidas de protección y mitigación.

1.4 Hipótesis del Trabajo

El análisis exhaustivo de los riesgos y vulnerabilidades de ciberseguridad en la red WIFI de la institución pública permitirá identificar y proponer medidas efectivas de protección y mitigación.

1.5 Justificación

La presente investigación se justifica ante la creciente necesidad de abordar las vulnerabilidades de las redes inalámbricas, un aspecto crítico en el ámbito de la ciberseguridad, especialmente en el contexto de las instituciones públicas en Imbabura. La expansión del uso de tecnologías inalámbricas ha transformado fundamentalmente la manera en que los Gobiernos Autónomos Descentralizados (GAD) gestionan información sensible y ofrecen servicios a la ciudadanía. Esta transformación hace imperativa la identificación y la mitigación de los riesgos asociados a estas tecnologías, que, de no ser atendidos, pueden comprometer tanto la seguridad de la información como la confianza pública.

Proteger la información personal y sensible es esencial para salvaguardar la privacidad de los ciudadanos y la integridad de las instituciones. De acuerdo con Ávila (2024), las instituciones públicas son considerablemente más vulnerables a los riesgos cibernéticos, lo que subraya la necesidad de implementar estrategias efectivas que fortalezcan la seguridad de sus redes. Además, Morán (2021) destaca que el incremento de los ataques a la seguridad informática obliga a estas instituciones a diseñar medidas robustas que prevengan la pérdida de recursos estatales y salvaguarden la información privada y sensible.

En respuesta a estas necesidades, el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL) (2021) establece la Estrategia Nacional de Ciberseguridad, aplicable a todo el país. Esta estrategia reconoce que la creciente dependencia de las tecnologías digitales, junto con la sofisticación de las amenazas cibernéticas, exige que las organizaciones fortalezcan sus capacidades para identificar, gestionar y mitigar los riesgos de ciberseguridad. Garantizar la protección de la información y los activos digitales es vital no solo para la continuidad operativa y la competitividad, sino también para preservar la confianza de los ciudadanos y la reputación de las instituciones en un entorno digital cada vez más vulnerable.

En este contexto, es fundamental que las instituciones públicas, incluidos los GAD que manejan datos sensibles y desempeñan funciones cruciales para la ciudadanía, adopten medidas preventivas y correctivas. Por ello, la presente investigación tiene como objetivo identificar las principales vulnerabilidades y riesgos que presenta la red inalámbrica de un GAD Parroquial en la Provincia de Imbabura, proponiendo soluciones adaptadas a la realidad de estos actores. Lo que es relevante debido a la escasez de estudios específicos sobre la seguridad de las redes Wi-Fi en instituciones públicas en Ecuador. Los resultados obtenidos permitirán llenar este vacío de conocimiento y proporcionar una guía práctica para mejorar la seguridad cibernética en este tipo de organizaciones.

El desarrollo de la propuesta de mejora de la seguridad inalámbrica también fomentará una cultura de ciberseguridad y la capacitación necesaria entre el personal de la institución pública. La educación en ciberseguridad es crucial para empoderar a empleados y usuarios, permitiéndoles reconocer y prevenir potenciales amenazas. Según Catota et al., (2019) la implementación de programas de formación y concienciación en ciberseguridad resulta fundamental no solo para reducir vulnerabilidades, sino también para aumentar la resiliencia institucional ante incidentes.

Adicionalmente, se evidencia una carencia de investigaciones que aborden específicamente las problemáticas de ciberseguridad en el ámbito de los GAD en Ecuador. Por lo que esta investigación llena un vacío en la literatura existente y proporciona un marco teórico y práctico que pueda ser utilizado para mejorar las políticas de ciberseguridad en las instituciones públicas del país.

Finalmente, esta investigación se alinea con los Objetivos de Desarrollo Sostenible (ODS) establecidos por la Organización de las Naciones Unidas (ONU) en 2015, en particular con el ODS 9, que se refiere a Industria, innovación e infraestructura. Al fortalecer la seguridad de la red inalámbrica, se contribuye a la resiliencia de la infraestructura tecnológica de la institución, lo cual es esencial para operar de manera eficiente y segura. Además, concurre con el ODS 16, que promueve la paz, la justicia y el fortalecimiento de instituciones, asegurando así la protección de la información sensible y previniendo el acceso no autorizado. Esto fortalece la confianza pública en dichas instituciones y en su capacidad para manejar los datos de manera segura.

CAPÍTULO II

MARCO REFERENCIAL

2.1 Marco teórico

2.1.1 Introducción a Redes

La Organización Internacional de Normalización (ISO/IEC 7498) (1994) establece que una red informática es un sistema de computadoras interconectadas que brinda a sus usuarios diversos servicios relacionados con la comunicación y el acceso a la información. Estas redes pueden operar tanto de forma inalámbrica como a través de sistemas cableados, permitiendo la coexistencia de ambas tecnologías en una infraestructura unificada. Cisco Systems (2019) sugiere que, a través de esta interconexión, es posible enlazar distintos dispositivos o terminales móviles asociados a la red, tales como:

- **WWAN/MAN (Wireless Wide Area Network/Metropolitan Area Network)**: Redes de área amplia o metropolitana que facilitan la conectividad en grandes extensiones geográficas.
- **WLAN (Wireless Local Area Network)**: Redes inalámbricas de área local utilizadas en espacios como oficinas, hogares o instituciones.
- **WPAN (Wireless Personal Area Network)**: Redes personales inalámbricas diseñadas para la interconexión de dispositivos a corta distancia.

2.1.2 Fundamentos de Redes Inalámbricas (Wi-Fi)

Según Cisco (2025), una red inalámbrica es una red informática que utiliza ondas electromagnéticas para conectar dispositivos, lo que posibilita la conexión de dispositivos sin la necesidad de cables físicos. Las redes Wi-Fi emplean ondas de radio para ofrecer conexiones inalámbricas de red e internet de alta velocidad a dispositivos ubicados dentro de un área de

cobertura determinada (Teltonika 2024). Los puntos de acceso extienden la cobertura de la señal Wi-Fi, permitiendo que los dispositivos mantengan su conexión a la red incluso si están alejados del router. Al acceder a una red Wi-Fi en lugares como cafeterías, hoteles, aeropuertos u otros espacios públicos, los usuarios se conectan a la infraestructura inalámbrica disponible en ese entorno.

Salazar (2016) afirma que las redes inalámbricas tienen múltiples aplicaciones. En algunos casos, reemplazan a las redes cableadas, mientras que en otros facilitan el acceso remoto a datos corporativos. Su implementación suele ser más económica en comparación con las redes tradicionales con cableado. Sin embargo, la reducción de costos no es el único beneficio. Brindar a una comunidad acceso más asequible y sencillo a la información genera un impacto positivo, ya que permite aprovechar mejor los recursos disponibles en Internet. El acceso eficiente a la información ahorra tiempo y esfuerzo, lo que contribuye al desarrollo local al aumentar la productividad. Además, las redes inalámbricas permiten la conexión de dispositivos sin importar la distancia, ya sea a pocos metros o a varios kilómetros, sin la necesidad de realizar instalaciones complejas con cables o conectores. Estas ventajas han impulsado su adopción y crecimiento acelerado

Las redes inalámbricas, basadas en la tecnología Wi-Fi, se han convertido en un componente esencial de la infraestructura de comunicaciones moderna, permitiendo la conectividad a Internet y a recursos de red sin la necesidad de cables físicos (Curay 2023). A continuación, se proporciona una visión general de los principios fundamentales de las redes Wi-Fi, incluyendo sus estándares, arquitecturas y componentes.

2.1.3 Arquitectura de Redes inalámbricas (Wi-Fi)

De acuerdo con Salazar (2016) existen dos modos para configurar la arquitectura de una red inalámbrica: ad hoc e infraestructura. En el modo ad hoc, los dispositivos transmiten

directamente punto a punto, mientras que en el modo infraestructura, los dispositivos se comunican a través de un punto de acceso que sirve de puente a otras redes.

Modo Ad hoc: Según Salazar (2016), en el modo ad hoc todos los dispositivos de la red inalámbrica interactúan entre sí de forma directa y equitativa, siguiendo un esquema de comunicación punto a punto. Este tipo de red no posee una estructura fija ni puntos de conexión establecidos, y no se requiere un punto de acceso para que los dispositivos se comuniquen. Esta modalidad es ideal para grupos pequeños de dispositivos que se encuentren físicamente próximos. Sin embargo, el rendimiento de la red puede verse afectado al aumentar el número de dispositivos. Una de las limitaciones de este modo es la posibilidad de desconexiones aleatorias y la dificultad en la gestión de la red. Además, sin la implementación de gateways especiales, las redes en modo ad hoc no pueden conectarse a una red de área local cableada, lo que impide el acceso a Internet. No obstante, el modo ad hoc puede ser efectivo en entornos pequeños, siendo la opción más sencilla y económica para configurar una red inalámbrica.

En este sentido, las ventajas del modo ad hoc son: a) facilidad de configuración y b) ausencia de requerimientos de infraestructura adicional. Por otro lado, las desventajas incluyen: a) alcance limitado, b) menor seguridad y c) complejidad en la gestión en redes de mayor tamaño.

Modo infraestructura: Al considerar el modo infraestructura, Salazar (2016) señala que, en esta configuración, todos los dispositivos se conectan a la red a través de un punto de acceso (AP). Estos puntos de acceso suelen ser routers o switches que convierten los datos de la red inalámbrica en datos compatibles con una conexión Ethernet cableada, funcionando como un enlace entre la red local cableada y los dispositivos inalámbricos. La conexión de múltiples puntos de acceso mediante una red troncal Ethernet puede ampliar aún más la cobertura de la red inalámbrica, permitiendo que los dispositivos móviles se desplacen fuera del rango de un

punto de acceso y se conecten a otro. De esta manera, los clientes inalámbricos pueden moverse libremente entre los dominios de diferentes puntos de acceso manteniendo una conexión estable.

Los beneficios del modo infraestructura incluyen: a) mayor alcance y cobertura, b) gestión centralizada de la red y c) mayor seguridad. Sin embargo, sus desventajas son: a) la necesidad de instalar y configurar puntos de acceso y b) la dependencia de un punto de acceso central.

2.1.4 Componentes de una Red Inalámbrica (Wi-Fi)

De acuerdo con Rodríguez (2025), una red Wi-Fi estándar está compuesta por varios elementos fundamentales que trabajan juntos para proporcionar conectividad inalámbrica:

Puntos de Acceso (APs): Estos dispositivos son fundamentales en una red Wi-Fi de infraestructura ya que actúan como intermediarios entre la red inalámbrica y la cableada. Permiten que los dispositivos de conexión inalámbrica accedan a recursos como Internet, servidores de archivos e impresoras. Los APs pueden existir como unidades independientes o estar integrados en routers. Su posicionamiento estratégico es esencial para maximizar tanto la cobertura como el rendimiento de la red.

Clientes: Este término hace referencia a los dispositivos que se conectan a la red Wi-Fi, incluyendo laptops, smartphones, tablets y otros aparatos capaces de conectarse de manera inalámbrica. Cada uno de estos dispositivos necesita contar con una tarjeta de red inalámbrica (NIC) para poder establecer la conexión con la red.

Routers: Estos dispositivos son responsables de gestionar el flujo de datos entre distintas redes, como la red local (LAN) y la red de Internet (WAN). En muchos hogares y pequeñas oficinas, los routers también funcionan como puntos de acceso Wi-Fi, ofreciendo

conectividad tanto inalámbrica como cableada en un solo aparato. Además, suelen integrar funciones de seguridad, como firewalls y la traducción de direcciones de red (NAT).

Estos componentes trabajan conjuntamente para garantizar una conectividad inalámbrica eficiente y segura en diversos entornos.

2.1.5 Amenazas y Vulnerabilidades en Redes Inalámbricas

El Centro de Criminología Nacional de España (CN-CERT) (2024) menciona que las redes inalámbricas Wi-Fi están expuestas a riesgos y amenazas como:

Contraseñas Débiles: El empleo de contraseñas que son fáciles de adivinar o predecibles representa una de las vulnerabilidades más serias. Los atacantes pueden aprovechar herramientas de cracking para descifrar rápidamente estas contraseñas y conseguir acceso a la red. Por lo tanto, es crucial que las contraseñas sean complejas, combinando letras mayúsculas y minúsculas, números y símbolos, con una longitud mínima de 12 caracteres.

Configuraciones Inseguras: Las configuraciones predeterminadas en routers y puntos de acceso suelen ser vulnerables y necesitan ser ajustadas para aumentar la seguridad. Algunas de las configuraciones inseguras más comunes son:

- **SSID Predeterminado:** Mantener el SSID (nombre de la red) en su configuración original facilita a los atacantes identificar el tipo de dispositivo y sus vulnerabilidades.
- **Contraseña de Administración Predeterminada:** Dejar la contraseña de administración del router o punto de acceso en su estado predeterminado permite a los atacantes acceder a la configuración del dispositivo y realizar modificaciones no autorizadas.
- **WEP:** La utilización del protocolo de seguridad WEP (Wired Equivalent

Privacy) es obsoleta y fácilmente quebrantable.

- **WPS (Wi-Fi Protected Setup):** Tener activado el WPS, que presenta vulnerabilidades conocidas, puede permitir a los atacantes obtener la contraseña de la red.

Falta de Actualizaciones: No mantener actualizados los firmwares de los routers y puntos de acceso representa una vulnerabilidad significativa. Las actualizaciones de firmware suelen incluir parches de seguridad que corrigen fallos conocidos. Ignorar estas actualizaciones expone los dispositivos a ataques que pueden aprovechar dichas vulnerabilidades.

Vulnerabilidades de Software: Los dispositivos clientes que se conectan a la red Wi-Fi también pueden ser susceptibles a ataques. El software desactualizado, los sistemas operativos sin parches y las aplicaciones inseguras pueden ser explotados por individuos malintencionados para obtener acceso a la red o robar información confidencial.

Falta de Segmentación de Red: No dividir la red en distintas zonas (por ejemplo, una para invitados y otra para empleados) puede incrementar el riesgo de que un ataque se propague a través de toda la red.

Falta de Autenticación Robusta: No implementar métodos de autenticación de dos factores (2FA) o depender de métodos de autenticación débiles, como solo contraseñas, facilita que los atacantes consigan acceso no autorizado a la red.

2.1.6 Ataques en las redes inalámbricas (Wi-Fi)

Según Fortinet (2025) un ataque informático se refiere a una acción diseñada para apuntar a una computadora o a cualquier elemento de un sistema de información computarizado para cambiar, destruir o robar datos, así como explotar o dañar una red. Los ciberataques han ido en aumento, en sincronía con la digitalización de negocios que se ha vuelto cada vez más

popular en los últimos años. Las redes inalámbricas están expuestas a una variedad de ataques que pueden comprometer la confidencialidad, la integridad y la disponibilidad de la información.

De acuerdo con El Instituto Nacional de Ciberseguridad de España (INCIBE) (2021) los ataques en redes tienen más procedencia en ser atacados por fuentes maliciosas, ya sea por falla en el software, hardware e incluso en el personal que se encuentra en el área informática, con el objetivo de causar daño en la información, archivos de la víctima. Estos ataques se los divide en dos categorías: pasivos, cuando un intruso obstruye los datos de red que viajan a través de ello y se limitan a registrar el uso de los recursos del sistema y activos, cuando el intruso utiliza sus técnicas de comandos para alterar el funcionamiento de sus recursos del sistema.

Valderrama (2017) menciona que ningún tipo de red es completamente segura; incluso las redes cableadas pueden ser objeto de ataques. Sin embargo, las redes inalámbricas tienden a ser más susceptibles a vulneraciones, ya que su señal puede ser captada desde múltiples direcciones. A continuación, se presentan los principales tipos de ataques que él identifica:

Suplantación de Punto de Acceso (Access Point Spoofing): Este ataque ocurre cuando un ciberdelincuente se hace pasar por un punto de acceso legítimo, engañando a los usuarios para que se conecten a una red falsa. Al hacerlo, el atacante puede interceptar datos y afectar el rendimiento de la red en el dispositivo víctima. Este tipo de vulnerabilidad es especialmente frecuente en redes ad-hoc, donde los dispositivos se conectan libremente entre sí sin un punto de acceso central.

Suplantación de Dirección MAC (MAC Spoofing): Este tipo de amenaza se basa en la falsificación de una dirección MAC dentro de una red, permitiendo que un atacante se haga pasar por un usuario autorizado. Como consecuencia, se compromete la seguridad del sistema y se facilita el ingreso de amenazas o fallos en la infraestructura de red.

Envenenamiento de ARP (ARP Poisoning): En esta técnica, el atacante manipula la tabla de direcciones ARP en una red local para interceptar y redirigir el tráfico de datos. Esta alteración puede generar congestión en la red, interferencias en las comunicaciones e incluso el robo de información confidencial, como credenciales de acceso, cookies o mensajes intercambiados en correos electrónicos y aplicaciones de mensajería.

Escaneo de Redes WLAN: Según Valderrama (2017), este método consiste en monitorear y detectar redes inalámbricas activas con el propósito de analizarlas y evaluar posibles vulnerabilidades de seguridad.

Wardriving y Warchalking: El wardriving es una práctica en la que los atacantes recorren diferentes ubicaciones para identificar redes Wi-Fi accesibles utilizando dispositivos con adaptadores inalámbricos. Por otro lado, el warchalking consiste en marcar físicamente las ubicaciones donde se han detectado redes vulnerables, facilitando que otros posibles atacantes puedan explotarlas.

Eavesdropping (Escucha Indebida): Este ataque consiste en interceptar y leer el tráfico de red transmitido de forma inalámbrica. Un atacante puede utilizar herramientas de software especializadas (como Wireshark) para capturar paquetes de datos y analizar su contenido. Si la red no está correctamente encriptada, el atacante puede obtener información confidencial como contraseñas, nombres de usuario, datos bancarios y otros datos sensibles. El eavesdropping es especialmente peligroso en redes Wi-Fi públicas no protegidas.

Man-in-the-Middle (Ataque de Intermediario): En este tipo de ataque, el atacante se posiciona entre el cliente y el punto de acceso, interceptando y modificando la comunicación entre ambos. El atacante puede utilizar técnicas como ARP spoofing o DNS spoofing para redirigir el tráfico del cliente a través de su propio dispositivo. Esto le permite al atacante robar información confidencial, insertar malware o manipular la información

transmitida. El ataque Evil Twin es una forma común de ataque Man-in-the-Middle en redes Wi-Fi.

Ataques de Denegación de Servicio (DoS): Estos ataques buscan interrumpir o degradar el servicio de la red inalámbrica, haciéndola inaccesible para los usuarios legítimos. Los ataques DoS pueden tomar varias formas, como:

- **Jamming:** Consiste en interferir con la señal de radiofrecuencia utilizada por la red Wi-Fi, inundando el área con ruido o señales falsas para impedir la comunicación.
- **Deauthentication Attack:** Consiste en enviar repetidamente paquetes de desautenticación a los clientes de la red, desconectándolos del punto de acceso y obligándolos a intentar reconectarse continuamente.
- **Flooding:** Consiste en inundar la red con un gran volumen de tráfico para sobrecargar los recursos del punto de acceso y hacerlo inaccesible.

Password Cracking (Descifrado de Contraseñas): Los atacantes pueden intentar descifrar la contraseña de la red Wi-Fi utilizando técnicas como:

- **Brute-Force Attack:** Consiste en probar todas las combinaciones posibles de contraseñas hasta encontrar la correcta.
- **Dictionary Attack:** Utiliza una lista predefinida de contraseñas comunes (un diccionario) para intentar adivinar la contraseña.
- **Rainbow Table Attack:** Utiliza tablas precalculadas de hashes de contraseñas para acelerar el proceso de descifrado.

Wardriving: Es la práctica de buscar redes Wi-Fi mientras se está en movimiento, generalmente en un vehículo, utilizando un ordenador portátil o dispositivo móvil con una antena Wi-Fi. Aunque no es un ataque en sí mismo, el wardriving permite a los atacantes

identificar redes vulnerables y recopilar información sobre ellas.Protocolos y Mecanismos de Seguridad en Redes Wi-Fi

2.1.7 Protocolos y Mecanismos de Seguridad en Redes Inalámbricas (Wi-Fi)

De acuerdo con Halbouni et al., (2023), la seguridad de las redes Wi-Fi está íntimamente ligada a la aplicación de protocolos y mecanismos de seguridad robustos. Estos métodos están diseñados para salvaguardar la confidencialidad, integridad y disponibilidad de tanto la red como de los datos que se transmiten a través de ella.

En el ámbito de las redes inalámbricas, es esencial mantener un nivel elevado de seguridad para proteger la información del acceso no autorizado. Esto conlleva la implementación de estándares y protocolos de cifrado efectivos. Cada uno de estos estándares presenta características, ventajas y limitaciones específicas que deben ser consideradas al seleccionar el más adecuado para una red en particular.

A continuación, se describen algunos de los protocolos de seguridad más relevantes en el contexto de redes Wi-Fi (tabla 1), así como sus características:

WEP (Wired Equivalent Privacy): Aunque fue uno de los primeros protocolos de seguridad utilizados en redes Wi-Fi, se considera obsoleto debido a sus vulnerabilidades. WEP utiliza una clave de cifrado de 40 bits, lo que lo hace susceptible a ataques de decodificación.

WPA (Wi-Fi Protected Access): Este protocolo fue introducido para mejorar la seguridad en comparación con WEP. Utiliza un método de cifrado más fuerte y es más resistente a ataques. WPA se basa en un sistema de autenticación llamado TKIP (Temporal Key Integrity Protocol).

WPA2: Considerado como el estándar más robusto antes de la introducción de WPA3, WPA2 utiliza el protocolo de cifrado AES (Advanced Encryption Standard). Ofrece una mayor

seguridad y es ampliamente utilizado en la mayoría de las redes inalámbricas actuales.

WPA3: El más reciente de los protocolos de seguridad, WPA3 asegura mejor la autenticación y el cifrado. Introduce características como la autenticación de contraseña más fuerte y protección contra ataques de fuerza bruta, proporcionando una seguridad notablemente mejorada.

De acuerdo con Ghimiray (2022) los anteriores protocolos de seguridad son los más utilizados para proteger las redes Wi-Fi. Cada protocolo ha sido diseñado para superar las deficiencias de sus predecesores, ofreciendo niveles crecientes de seguridad. No obstante, el protocolo WEP (Wired Equivalent Privacy) fue uno de los primeros intentos de proteger las redes Wi-Fi. Utilizaba el algoritmo de cifrado RC4 y una clave estática de 64 o 128 bits. Si bien representó una mejora inicial en comparación con la ausencia de seguridad, pronto se descubrieron vulnerabilidades significativas. El algoritmo RC4 resultó ser susceptible a varios ataques, y la clave estática facilitaba la captura y el descifrado de paquetes. En la actualidad, WEP se considera obsoleto y no debe utilizarse bajo ninguna circunstancia, ya que se puede romper con herramientas disponibles públicamente en cuestión de minutos.

Tabla 1. *Estimación de tiempo para vulnerar protocolos*

Protocolo	Tiempo estimado para romper la seguridad
WEP	5 minutos a 1 hora
WPA	2 a 10 horas
WPA2	1 a 2 días (puede ser más si se usa AES)
WPA3	Más de 10 años (actualmente considerado seguro)

Nota: Basada en los análisis de (Irei, 2023)

Según Coria (2024), la evolución de los protocolos de seguridad en redes Wi-Fi ha

buscado solucionar las vulnerabilidades presentes en versiones anteriores (tabla 2), mejorando la protección de la información transmitida.

Tabla 2. *Comparativa de protocolos de seguridad inalámbrica*

ASPECTO	WEP	WPA	WPA2	WPA3
Año de Introducción	1999	2003	2004	2018
Tipo de Cifrado	RC4	TKIP (Temporal Key Integrity Protocol)	AES (Advanced Encryption Standard)	AES-GCMP (Galois/Counter Mode Protocol)
Autenticación	Claves WEP	Claves pre compartidas (PSK)	Claves pre compartidas (PSK)	SAE (Simultaneous Authentication of Equals)
Fortaleza del Cifrado	Débil	Moderado	Fuerte	Muy Fuerte
Vulnerabilidades Conocidas	Sí, numerosas	Sí, pero mejor que WEP	Algunas, pero menos que WPA	Algunas (Dragonblood, parcheadas)
Seguridad de Contraseña	Baja	Mejorada que WEP	Mejorada que WPA	Mejorada que WPA2
Soporte Empresarial	Rara vez utilizado	Utilizado, pero menos robusto que WPA2	Ampliamente utilizado	Ampliamente utilizado (cifrado hasta 192 bits)
Seguridad Pública (Open)	No recomendado	No recomendado	No recomendado	Recomendado (OWE: Opportunistic Wireless Encryption)
Protocolo de Configuración Rápida (WPS)	No presente	Presente, pero inseguro	Presente, pero inseguro	No presente
Vulnerabilidades Relacionadas con WPS	–	Sí, ataques PIN y de fuerza bruta	Sí, ataques PIN y de fuerza bruta	–
Seguridad en Redes Públicas	No recomendado	No recomendado	No recomendado	Recomendado (OWE)
Compatibilidad con Dispositivos Antiguos	No aplica	No aplica	No aplica	Modo de transición WPA2/WPA3
Nivel de Seguridad Actual	Insuficiente	Aceptable, pero no ideal	Satisfactorio	Muy alto
Uso Recomendado	Desaconsejado	Uso temporal, reemplazado por WPA2/WPA3	Recomendado para la mayoría	Recomendado para máxima seguridad

Nota: No se ha lanzado oficialmente ningún protocolo de seguridad inalámbrica nuevo después de WPA3. Fuente: (Vadavo, 2024)

2.1.8 Autenticación

Según ESET (2022), la autenticación es un elemento crucial para asegurar que solo los usuarios o dispositivos autorizados puedan acceder a una red. Existen diversas modalidades de autenticación, cada una con diferentes niveles de seguridad y aplicabilidad:

Contraseñas (PSK - Pre-Shared Key): Este es uno de los métodos más frecuentemente empleados en redes domésticas y pequeñas empresas. Requiere que los usuarios introduzcan una clave previamente establecida para conectarse a la red. Aunque su implementación es sencilla, la seguridad depende de la fortaleza de la contraseña utilizada. Las claves débiles pueden ser vulnerables a ataques de diccionario y fuerza bruta; por lo tanto, se aconseja emplear contraseñas complejas y actualizarlas regularmente.

Certificados digitales: Utilizados en entornos corporativos, este método se integra en protocolos como WPA2/WPA3-Enterprise. Verifica la identidad de los usuarios a través de un certificado válido, lo que dificulta su falsificación y proporciona un mayor nivel de seguridad en comparación con las contraseñas tradicionales. Sin embargo, su implementación requiere contar con una infraestructura de clave pública (PKI) para gestionar los certificados eficientemente.

Autenticación de dos factores (2FA): Este mecanismo exige que el usuario valide su identidad mediante dos elementos diferentes, como una contraseña y un código generado en una aplicación móvil. Esta técnica refuerza la seguridad, ya que, incluso si un atacante obtiene la contraseña, necesitaría también el segundo factor para acceder a la red. No obstante, su implementación requiere la configuración de un sistema 2FA y la colaboración activa de los usuarios.

2.1.9 Cifrado

Según Buxton (2024), el cifrado es el mecanismo que transforma los datos en un formato que no puede ser leído fácilmente, lo que ayuda a proteger la confidencialidad de la información que se transmite a través de redes Wi-Fi. Dentro de los algoritmos de cifrado, se destacan los siguientes:

AES (Advanced Encryption Standard): Este es un algoritmo de cifrado simétrico que goza de gran popularidad y se considera extremadamente seguro. AES se utiliza en los protocolos WPA2 y WPA3 junto con el método de cifrado CCMP. Su diseño le permite resistir la mayoría de los ataques conocidos y está disponible tanto en hardware como en software, lo que asegura un rendimiento eficiente. Hasta la fecha, no se han identificado debilidades significativas en AES.

TKIP (Temporal Key Integrity Protocol): Este protocolo fue implementado en WPA como solución provisional para abordar las vulnerabilidades de WEP. Aunque emplea el algoritmo RC4 y le agrega mejoras, se considera que TKIP es más seguro que WEP, pero sigue siendo susceptible a ciertos ataques. Debido a estas vulnerabilidades, TKIP ahora se clasifica como obsoleto.

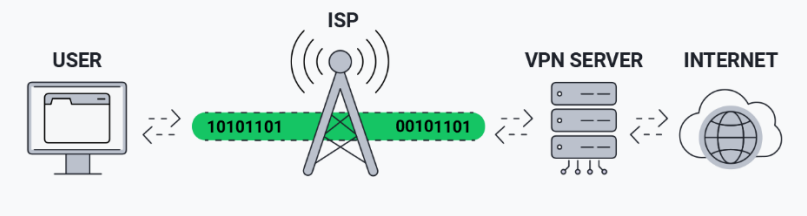
2.1.10 VPNs y Túneles Seguros para Acceso Remoto

Según Burrell (2024), las Redes Privadas Virtuales (VPN) y los túneles seguros son herramientas esenciales para garantizar un acceso remoto protegido a una red. Las VPN (Virtual Private Network) establecen una conexión cifrada entre el dispositivo del usuario y la red, lo que impide que terceros intercepten la información transmitida. En la figura 1 se muestra el proceso de conexión a través de un VPN. Gracias a esto, los usuarios pueden conectarse de manera segura a recursos internos desde cualquier ubicación. No obstante, su implementación requiere la instalación y configuración de software tanto en el dispositivo del usuario como en la red.

Por otro lado, los túneles seguros, como el tunelado SSH (SSH Tunneling), utilizan el protocolo Secure Shell (SSH) para crear un canal encriptado que protege el tráfico de red. Este método permite un acceso seguro a determinados servicios dentro de la red y resulta sencillo de configurar en sistemas operativos como Linux y macOS. Sin embargo, a diferencia de una

VPN, el túnel SSH solo protege la información que circula a través de él y no todo el tráfico de la red.

Figura 1. *Proceso de Conexión a Internet a través de un VPN*



Nota: Obtenido de AntiVirus Guard (AVG), 2025)

2.1.11 Normativa y Estándares de Seguridad

De acuerdo con el Instituto Nacional de Estándares y Tecnología (INET) (2018) La seguridad de las redes Wi-Fi no solo depende de la implementación de protocolos y mecanismos técnicos, sino también del cumplimiento de la normativa y los estándares de seguridad relevantes. Estos marcos proporcionan directrices y requisitos para proteger la información y los sistemas de información de las organizaciones.

GDPR (General Data Protection Regulation): Es el Reglamento General de Protección de Datos de la Unión Europea (2016) sobre la protección de datos y la privacidad. Aplica a cualquier organización que procese datos personales de ciudadanos de la UE, independientemente de su ubicación. La GDPR exige que las organizaciones implementen medidas de seguridad adecuadas para proteger los datos personales, incluyendo el cifrado, el control de acceso y la prevención de la pérdida de datos. En el contexto de las redes Wi-Fi, esto implica garantizar la seguridad de la red para proteger los datos personales transmitidos a través de ella. En la figura 2 se muestran los principios básicos de un GDPR que guían el tratamiento responsable de la información personal.

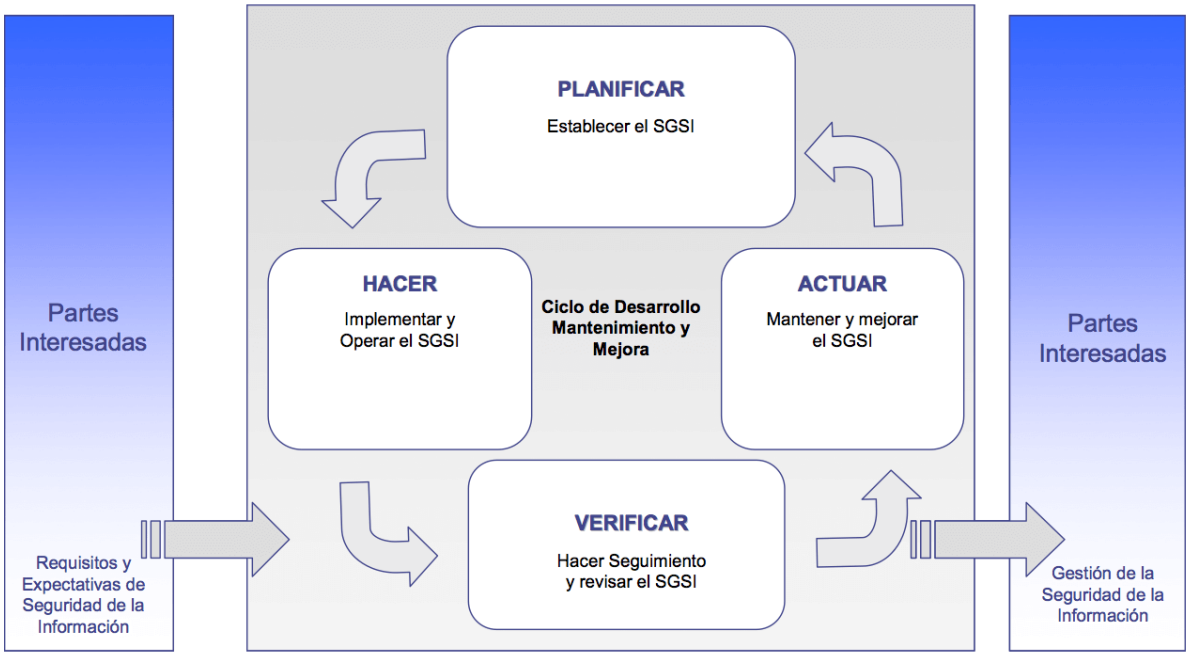
Figura 2. *Los principios básicos de GDPR*

Nota: Este gráfico ilustra los siete principios fundamentales del GDPR, que guían el tratamiento responsable y ético de los datos personales. Fuente: Consejo de la Unión Europea (2016).

International Organization for Standardization (ISO) 27001: La ISO 21001 (2022) se enfoca en la Seguridad de la información, ciberseguridad y protección de la privacidad. Esta normativa proporciona un marco para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información (SGSI). ISO 27001 ayuda a las organizaciones a identificar, evaluar y gestionar los riesgos de seguridad de la información, incluyendo los relacionados con las redes Wi-Fi. La certificación ISO 27001 demuestra el compromiso de una organización con la seguridad de la información. La implementación de un SGSI basado en ISO 27001 puede mejorar la seguridad de las redes Wi-Fi y proteger la información confidencial. En la figura 3 se muestra el ciclo de mejora continua que establece

el Sistema de Gestión de la seguridad de la información, que contempla las fases de planificación, hacer, actuar y verificar.

Figura 3. *Ciclo de mejora continua para el SGSI.*



Nota: El ciclo PDCA (Plan-Do-Check-Act) es una herramienta eficaz para fomentar la mejora continua en sistemas de gestión, promoviendo la adaptación y optimización de procesos organizativos. Fuente: (NovaSec, 2024).

Estándares IEEE 802.11 (a/b/g/n/ac/ax): De acuerdo con la Institute of Electrical and Electronics Engineers (IEE) los estándares IEEE 802.11 son un conjunto de especificaciones que definen cómo funcionan las redes inalámbricas Wi-Fi (IEE, s.f.). Cada estándar representa una evolución tecnológica que busca mejorar la velocidad, el alcance, la seguridad y la eficiencia de las redes Wi-Fi.

- **802.11a:** Uno de los primeros estándares, lanzado en 1999. Utiliza la banda de frecuencia de 5 GHz y ofrece velocidades de hasta 54 Mbps. Sin embargo, su alcance es limitado y sufre más interferencias que otros estándares.
- **802.11b:** También lanzado en 1999, opera en la banda de frecuencia de 2.4 GHz y ofrece

velocidades de hasta 11 Mbps. Es más económico y tiene un mayor alcance que 802.11a, pero es susceptible a interferencias de otros dispositivos que utilizan la misma banda (ej., microondas, teléfonos inalámbricos).

- **802.11g:** Introducido en 2003, combina las ventajas de 802.11a y 802.11b. Opera en la banda de 2.4 GHz y ofrece velocidades de hasta 54 Mbps. Es compatible con dispositivos 802.11b, lo que facilitó su adopción.
- **802.11n:** Lanzado en 2009, utiliza múltiples antenas (MIMO - Multiple Input Multiple Output) para mejorar el rendimiento y el alcance. Puede operar en las bandas de 2.4 GHz y 5 GHz, y ofrece velocidades teóricas de hasta 600 Mbps (aunque en la práctica suele ser menor).
- **802.11ac:** Introducido en 2013, opera exclusivamente en la banda de 5 GHz y utiliza tecnologías como MIMO multiusuario (MU-MIMO) y canales más amplios para ofrecer velocidades significativamente mayores que 802.11n, alcanzando velocidades teóricas de hasta varios gigabits por segundo.
- **802.11ax (Wi-Fi 6):** El estándar más reciente, lanzado en 2019, está diseñado para mejorar la eficiencia y el rendimiento en entornos con alta densidad de dispositivos. Utiliza tecnologías como OFDMA (Orthogonal Frequency Division Multiple Access) y MU-MIMO para permitir que varios dispositivos compartan el mismo canal simultáneamente. Opera tanto en la banda de 2.4 GHz como en la de 5 GHz, y ofrece velocidades teóricas aún mayores que 802.11ac.

En la siguiente tabla 3, se presenta un análisis comparativo de los principales estándares de conexión WLAN, destacando sus bandas de frecuencia, velocidades máximas teóricas, y las respectivas ventajas y desventajas de cada uno. Este resumen permite entender las características clave de cada estándar y cómo se adaptan a diferentes entornos y necesidades de conexión.

Tabla 3. *Comparativa de Estándares IEEE 802.11*

Estándar	Banda de Frecuencia	Velocidad Máxima Teórica	Ventajas	Desventajas
802.11a	5 GHz	54 Mbps	Mayor inmunidad a interferencias en comparación con 802.11b.	Alcance limitado.
802.11b	2.4 GHz	11 Mbps	Mayor alcance y menor costo.	Susceptible a interferencias. Velocidad relativamente baja.
802.11g	2.4 GHz	54 Mbps	Compatibilidad con 802.11b. Velocidad mejorada en comparación con 802.11b.	Susceptible a interferencias.
802.11n	2.4/5 GHz	600 Mbps	Mayor velocidad y alcance gracias a MIMO.	El rendimiento real puede variar dependiendo de las condiciones del entorno.
802.11ac	5 GHz	Varios Gbps	Velocidades muy altas gracias a MU-MIMO y canales más amplios.	Solo opera en la banda de 5 GHz, lo que puede limitar el alcance en algunos entornos.
802.11ax	2.4/5 GHz	Aún mayores que 802.11ac	Mayor eficiencia en entornos densos. Mejor gestión de la energía de los dispositivos.	El hardware compatible con 802.11ax puede ser más costoso. El rendimiento óptimo requiere dispositivos cliente y puntos de acceso compatibles con 802.11ax. La mejora significativa se nota más en entornos con muchos dispositivos simultáneamente conectados.

Nota: La tabla resume las principales características de los estándares de redes inalámbricas, destacando sus bandas de frecuencia, velocidades máximas teóricas, así como sus ventajas y desventajas. La elección del estándar adecuado dependerá de las necesidades específicas de uso, el entorno y el presupuesto disponible. Fuente: (IEE, 2025).

2.1.12 Buenas Prácticas de Seguridad para Redes Inalámbricas

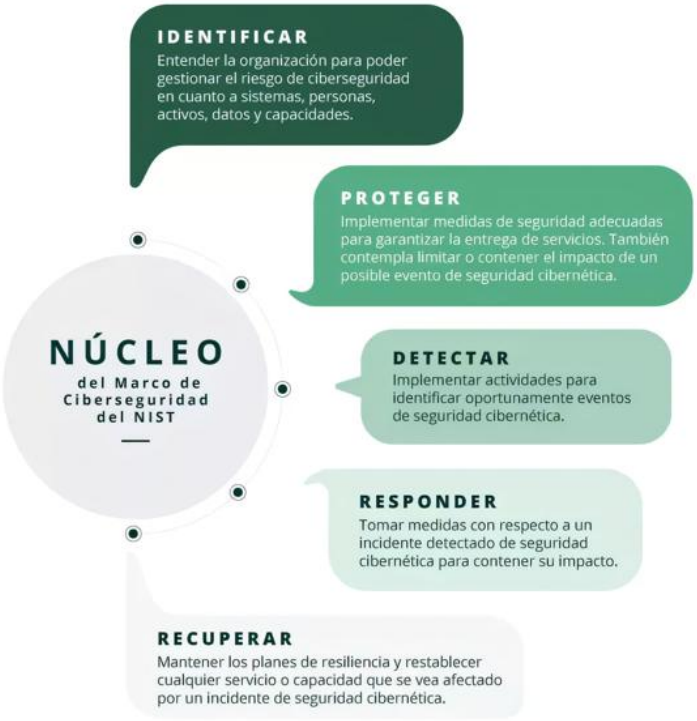
Además de la normativa, existen una serie de buenas prácticas recomendadas por organizaciones como NIST (National Institute of Standards and Technology) y OWASP (Open Web Application Security Project) para proteger las redes inalámbricas:

NIST (National Institute of Standards and Technology) es una agencia del gobierno de los Estados Unidos que desarrolla estándares y directrices para la seguridad de la información. NIST publica una serie de documentos sobre la seguridad de las redes inalámbricas, que incluyen recomendaciones sobre la configuración segura de los puntos de

acceso (figura 4), la autenticación de usuarios y el cifrado de datos. Algunos ejemplos son NIST Special Publication 800-48: Wireless Network Security y NIST Special Publication 800-153: Guidelines for Securing Wireless Local Area Networks (WLANs) (Scarfone et al., 2008).

En la figura 4 se muestra el marco de ciberseguridad del NIST, en el cual se presentan las funciones críticas: identificar, proteger, detectar, responder y recuperar.

Figura 4. *Marco de Ciberseguridad del NIST*



Nota: Funciones críticas del Marco de Ciberseguridad del NIST. Fuente: (Jiménez, 2021).

OWASP (Open Web Application Security Project) OWASP se define como una comunidad en constante evolución que se dedica a la identificación y mitigación de riesgos de seguridad presentes en aplicaciones web. Según la información proporcionada por el sitio oficial de OWASP (2021), su conjunto de directrices es considerado como un estándar de sensibilización dirigido tanto a desarrolladores como a profesionales de la seguridad de aplicaciones web. Estas directrices representan un amplio consenso acerca de los riesgos de

seguridad más críticos asociados a las aplicaciones web. Es importante resaltar que OWASP no mantiene ninguna afiliación con empresas de tecnología, aunque respalda el uso informado de tecnologías de seguridad comerciales. La comunidad genera diversos tipos de materiales de manera colaborativa, transparente y abierta (OWASP, 2021).

OWASP (2021) maneja el Top 10 de las vulnerabilidades más críticas y comunes en aplicaciones web. Esta lista es actualizada periódicamente y tiene como objetivo concienciar a los desarrolladores, arquitectos y organizaciones sobre los principales riesgos de seguridad en sus aplicaciones. A continuación, se enumeran las Top 10.

- **A01:2021-Control de acceso roto** sube del quinto al primer lugar; el 94% de las aplicaciones fueron evaluadas por alguna forma de este problema. Las 34 Enumeraciones de Debilidades Comunes (CWEs) asociadas al control de acceso roto tuvieron más ocurrencias en aplicaciones que cualquier otra categoría.
- **A02:2021-Fallas criptográficas** asciende una posición al segundo lugar, anteriormente conocido como Exposición de Datos Sensibles, que era un síntoma amplio en lugar de una causa raíz. El enfoque renovado aquí se centra en las fallas relacionadas con la criptografía, que a menudo conducen a la exposición de datos sensibles o a la compromisión del sistema.
- **A03:2021-Inyección** desciende al tercer lugar. El 94% de las aplicaciones fueron probadas por algún tipo de inyección, y las 33 CWEs asociadas a esta categoría tienen la segunda mayor cantidad de ocurrencias en aplicaciones. El Cross-site Scripting ahora forma parte de esta categoría en esta edición.
- **A04:2021-Diseño inseguro** es una nueva categoría para 2021, enfocándose en los riesgos relacionados con fallas de diseño. Si realmente queremos "movernos a la izquierda" como industria, esto requiere un mayor uso de modelado de amenazas, patrones y principios de diseño seguro, y arquitecturas de referencia.

- **A05:2021-Misconfiguración de seguridad** sube del sexto lugar en la edición anterior; el 90% de las aplicaciones fueron evaluadas por algún tipo de misconfiguración. Con el aumento de software altamente configurable, no es sorprendente ver este ascenso. La categoría anterior de Entidades Externas XML (XXE) ahora forma parte de esta categoría.
- **A06:2021-Componentes vulnerables y desactualizados** anteriormente se titulaba Uso de Componentes con Vulnerabilidades Conocidas y ocupa el segundo lugar en la encuesta de la comunidad del Top 10, pero también tuvo suficientes datos para entrar en el Top 10 a través del análisis de datos. Esta categoría sube del noveno lugar en 2017 y es un problema conocido que seguimos luchando por evaluar y probar. Es la única categoría sin Vulnerabilidades y Exposiciones Comunes (CVEs) mapeadas a las CWEs incluidas, por lo que se consideran pesos de explotación e impacto predeterminados de 5.0 en sus puntajes.
- **A07:2021-Fallas de identificación y autenticación** anteriormente se conocía como Autenticación Rota y desciende del segundo lugar, ahora incluye CWEs más relacionadas con fallas de identificación. Esta categoría sigue siendo una parte integral del Top 10, pero la disponibilidad creciente de marcos estandarizados parece estar ayudando.
- **A08:2021-Fallas de integridad del software y los datos** es una nueva categoría para 2021, que se enfoca en hacer suposiciones relacionadas con actualizaciones de software, datos críticos y pipelines de CI/CD sin verificar su integridad. Uno de los impactos más altos en el puntaje se relaciona con datos de CVE/CVSS mapeados a las 10 CWEs en esta categoría. La deserialización insegura de 2017 ahora forma parte de esta categoría más amplia.
- **A09:2021-Fallas en el registro y monitoreo de seguridad** anteriormente se conocía

como Registro y Monitoreo Insuficientes y se añadió a partir de la encuesta de la industria (#3), subiendo del décimo lugar anterior. Esta categoría se amplía para incluir más tipos de fallas, es difícil de probar y no está bien representada en los datos de CVE/CVSS. Sin embargo, las fallas en esta categoría pueden impactar directamente en la visibilidad, las alertas de incidentes y la forense.

- **A10:2021-Falsificación de solicitudes del lado del servidor**, los datos muestran una tasa de incidencia relativamente baja con una cobertura de pruebas superior a la media, junto con calificaciones superiores a la media en cuanto a potencial de explotación e impacto. Esta categoría representa un escenario en el que los miembros de la comunidad de seguridad nos indican que es importante, aunque no se refleje en los datos en este momento.

2.2 Marco legal

2.2.1 Ley de protección de datos personales

En Ecuador, la protección de datos personales está regida por la Ley Orgánica de Protección de Datos Personales (LOPD) (2021) y su Reglamento General. Estas normativas definen los principios, derechos y responsabilidades pertinentes a la protección de los datos de los ciudadanos ecuatorianos. La ley impone a las organizaciones la responsabilidad de salvaguardar los datos personales de sus usuarios, incluyendo la implementación de medidas de seguridad informática adecuadas para evitar vulnerabilidades y ciberataques. A través de la Ley de Protección de Datos Personales, se busca proteger a los titulares de la información, permitiéndoles decidir a quién entregan su información personal, fomentando así la confianza en los proveedores de servicios digitales.

2.2.2 Acuerdo Nro. MINTEL-MINTEL-2024-0003

De acuerdo con el MINTEL, mediante Acuerdo Ministerial No. MINTEL-MINTEL-

2024-0003 expide el Esquema Gubernamental de Seguridad de la Información (EGSI), es de implementación obligatoria en el sector público ecuatoriano. Este esquema busca proteger la confidencialidad, integridad y disponibilidad de la información, promoviendo la gestión de riesgos y la mejora continua. La Contraloría General del Estado, mediante sus normas de control interno, contribuye al marco jurídico de ciberseguridad, orientando la implementación de un Sistema de Gestión de Seguridad de la Información.

El EGSI promueve la mejora continua a través de la revisión constante de políticas y procedimientos, adaptándose a las nuevas amenazas y desafíos de ciberseguridad. Se enfoca en la gestión de riesgos, la evaluación de vulnerabilidades y la implementación de controles de seguridad, incluyendo políticas de acceso, gestión de incidentes y seguridad de redes. El cumplimiento se monitorea y evalúa, garantizando la protección efectiva de los activos de información. (MINTEL 2024). Además, el esquema establece controles organizacionales, de personas y físicos, así como controles técnicos para proteger los sistemas de información. Se incluyen políticas de seguridad, gestión de acceso, protección contra malware y gestión de vulnerabilidades. La gestión de incidentes, la continuidad del negocio y el cumplimiento legal son aspectos clave. La revisión independiente y el monitoreo continuo aseguran la efectividad de las medidas implementadas.

CAPÍTULO III

MARCO METODOLÓGICO

3.1 Descripción del área de estudio del GAD Parroquial de Imbabura

Debido a la sensibilidad de la información relacionada con la seguridad de la red Wi-Fi y en cumplimiento de las políticas de confidencialidad, la identidad específica de la institución pública Gobierno Autónomo Descentralizado Parroquial GADP en la provincia de Imbabura, se mantendrá anónima a lo largo de este documento. Sin embargo, a continuación, se proporciona una descripción general de las características relevantes para el análisis de seguridad.

3.1.1 Contexto Organizacional

Se trata de un Gobierno Autónomo Descentralizado Parroquial (GADP), responsable de la administración y gestión de los servicios públicos en una parroquia de la provincia de Imbabura, Ecuador. El Orgánico de Organización Territorial, Autonomía y Descentralización (COOTAD) (2010) establece que los GAD Parroquiales son una figura clave en el sistema de organización territorial en Ecuador, destinados a promover el desarrollo sustentable y garantizar el bienestar de la comunidad en su circunscripción territorial. Tienen un rol fundamental en la gestión del desarrollo local y la participación ciudadana.

Según el artículo 64 del COOTAD (2010) el GAD Parroquial Rural abarcan una serie de responsabilidades fundamentales para el desarrollo local. En primer lugar, el GAD Parroquial debe promover el desarrollo sustentable de su circunscripción, lo que implica diseñar e impulsar políticas de inclusión que aseguren el acceso equitativo a oportunidades y recursos. Además, es indispensable implementar sistemas de participación ciudadana que faciliten el ejercicio de los derechos de los habitantes, fomentando así una gestión democrática efectiva.

Asimismo, el GAD Parroquial tiene la obligación de elaborar y ejecutar planes de desarrollo que atiendan las necesidades de la comunidad, así como ejecutar las competencias reconocidas por la ley. También es fundamental vigilar la calidad de los servicios públicos para garantizar que las obras y los servicios sean proporcionados de manera eficiente. Además, debe fomentar el desarrollo económico, impulsando actividades que beneficien a la economía local y patrocinar la cultura y el deporte para enriquecer la vida comunitaria. Por último, se espera que preste los servicios que le sean delegados y que coordine con la Policía Nacional para garantizar la seguridad ciudadana.

Por otro lado, el artículo 65 del COTAD (2010) establece que las competencias exclusivas de un GAD Parroquial Rural incluyen la planificación y ordenamiento territorial, la gestión de infraestructura, el mantenimiento de la vialidad, la promoción de actividades productivas y la preservación del ambiente. Asimismo, es responsable de la administración de los servicios públicos, promover la organización ciudadana, gestionar la cooperación internacional, y supervisar la ejecución de obras y servicios, consolidando así su papel esencial en la gobernanza local.

Estas instituciones son cruciales para garantizar derechos en las comunidades, enfocándose en mejorar el acceso a servicios de salud, promover espacios públicos de calidad, facilitar el acceso a viviendas seguras y prevenir la violencia contra las personas adultas mayores.

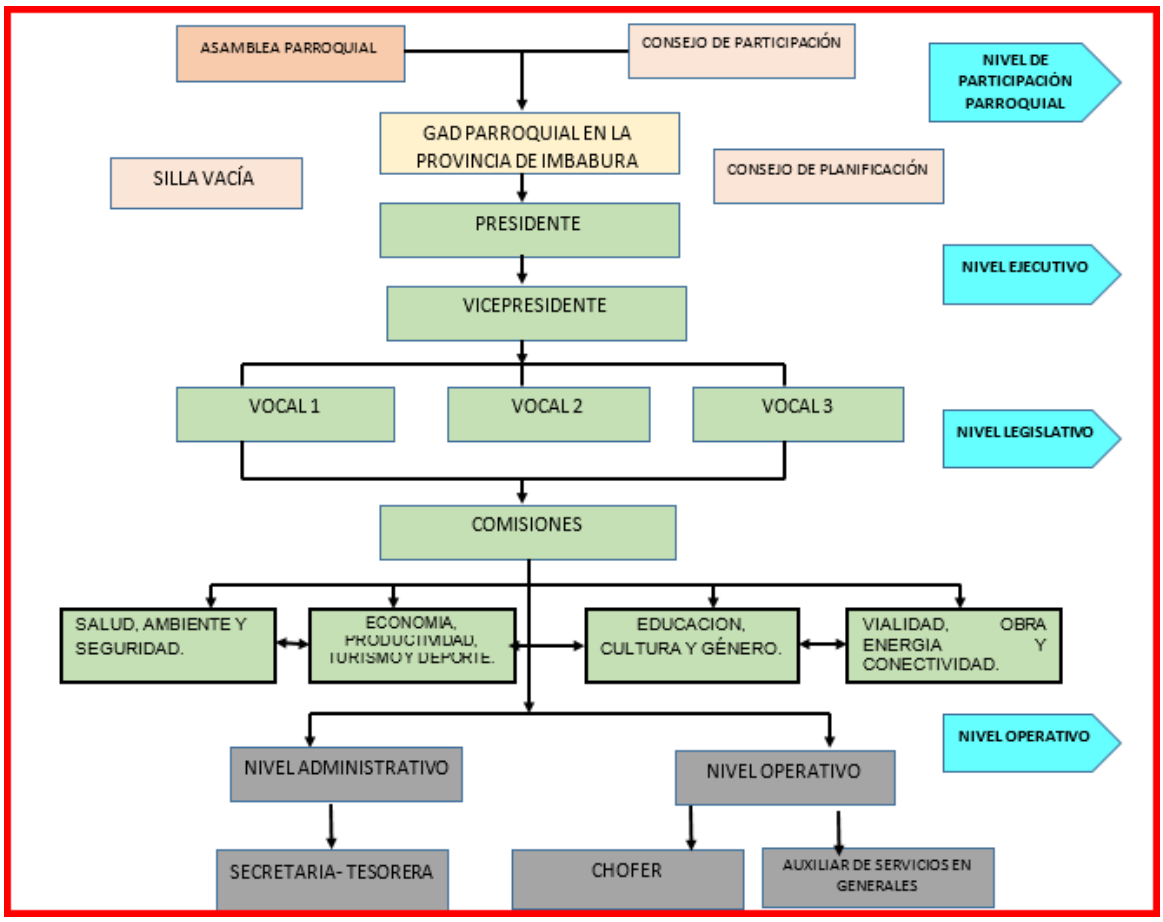
3.1.2 Dependencia de la Red Inalámbrica Wi-Fi.

La red Wi-Fi es esencial para el funcionamiento diario de la institución y se utiliza para los siguientes propósitos:

- Acceso a internet por empleados y funcionarios.
- Comunicación interna efectiva.

- Acceso a sistemas de información gubernamentales y aplicaciones web.
- Atención al público, ofreciendo acceso Wi-Fi para ciudadanos en algunas áreas

Figura 5. *Organigrama del GAD Parroquial de Imbabura*



Nota. El organigrama de la institución determina la organización. Fuente: Cortesía del GAD Parroquial de Imbabura.

3.1.3 Población

La población está conformada por el personal que trabaja en el Gobierno Autónomo Descentralizado Parroquial (GADP), como se muestra la (figura 5).

3.1.4 Muestra

La muestra está compuesta por 20 funcionarios, incluyendo al presidente, vicepresidente, vocales, así como los representantes de salud, ambiente y seguridad,

economía, productividad, turismo y deporte, educación, género, y viabilidad, obra, energía y conectividad.

3.2 Enfoque de la investigación

La presente investigación tiene un enfoque mixto, ya que se analizaron datos cualitativos y cuantitativos. El cualitativo fundamentado en la recolección y análisis de datos estadísticos con el objetivo de identificar las vulnerabilidades y amenazas a la red inalámbrica (Wi-Fi) del GAD Parroquial de Imbabura. Mientras que el cuantitativo debido al análisis de entrevistas realizadas a la autoridad del GAD Parroquial.

3.3 Tipo de investigación

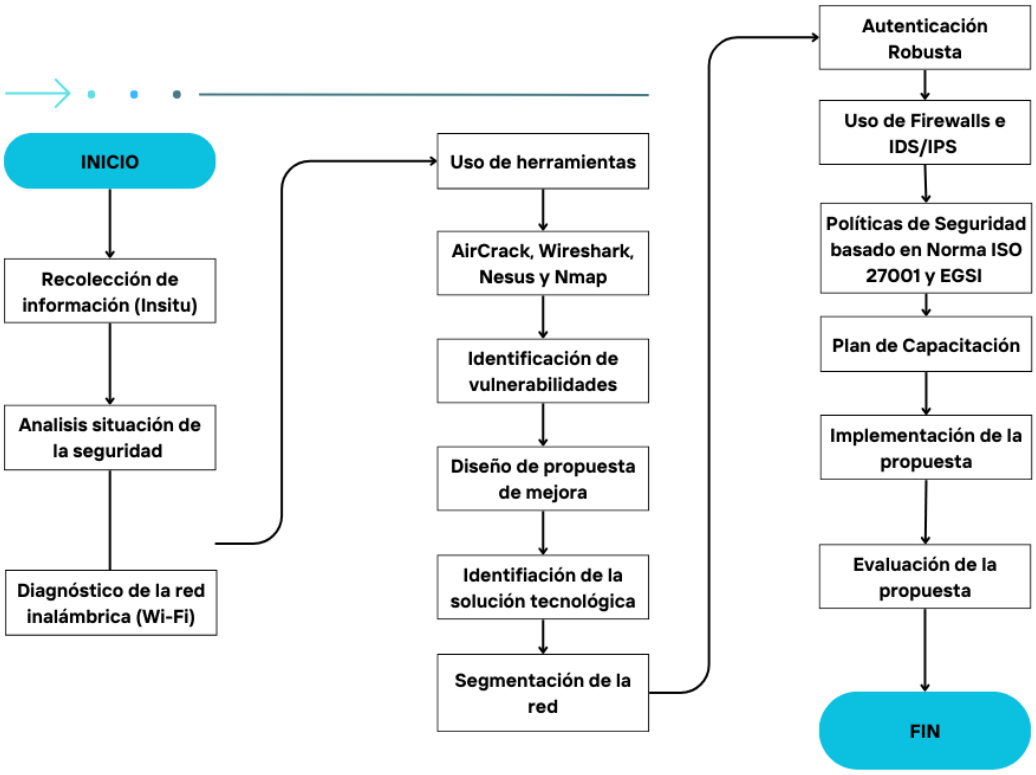
La presente investigación se estructura en torno a tres tipos de indagación: Se trata de una investigación descriptiva, ya que se analizó la información recopilada para caracterizar las diversas vulnerabilidades y amenazas presentes en la red Wi-Fi. Además, es una investigación de campo, dado que se recopilaron datos directamente en el lugar de estudio a través de análisis prácticos y pruebas de penetración (pentest). Esto permitió obtener información específica sobre las condiciones reales de la red, revelando así sus vulnerabilidades. Finalmente, también se trata de una investigación es documental, ya que se complementaron los hallazgos de campo con una revisión de la literatura existente, así como de normas de seguridad y protocolos recomendados en ciberseguridad. Este enfoque proporciona un respaldo teórico a los datos empíricos y enriquece la comprensión del problema.

3.3 Procedimiento de investigación

El flujograma de la (figura 6) detalla un proceso sistemático para mejorar la seguridad de la red inalámbrica. Comienza con la recolección de información en el sitio y un análisis de la situación actual, lo que permite un diagnóstico claro de la red Wi-Fi y una comprensión de

las vulnerabilidades existentes. A continuación, se utilizan herramientas especializadas como AirCrack, Wireshark, Nessus y Nmap para identificar debilidades. Con los hallazgos, se formula una propuesta de mejora que incluye la segmentación de la red, autenticación robusta, firewalls y políticas de seguridad en línea con la Norma ISO 27001. El proceso culmina con un plan de capacitación para el personal, seguido de la implementación de la propuesta y su posterior evaluación. Este enfoque holístico asegura que la red se adapte a las nuevas amenazas y mantenga un nivel óptimo de protección.

Figura 6. *Flujo de procesos para la ejecución del proyecto de investigación.*



Fuente: Elaboración del autor.

CAPÍTULO IV

RESULTADOS Y DISCUSIÓN

3.1 Situación Actual de la Infraestructura y Seguridad Informática

La infraestructura tecnológica del GAD Parroquial de Imbabura se encuentra incompleta, ya que carece de un cableado estructurado certificado y de un switch que permita multiplexar los puntos de acceso para que los usuarios se conecten a la red y a Internet. Esta deficiencia limita la capacidad de ampliar la configuración de más equipos de acceso a la red inalámbrica (access points).

Además, la institución no cuenta con un router propio, lo que dificulta la administración efectiva de la red inalámbrica y compromete su seguridad. La ausencia de este dispositivo impide llevar a cabo acciones esenciales, como el cambio periódico de contraseñas y el control de usuarios autorizados para acceder a la red (listas de control de acceso). Se ha observado que los funcionarios de la institución no poseen una conciencia adecuada sobre la importancia de la seguridad de la información y el impacto que podría tener la pérdida de datos a causa de un ataque informático. Esta falta de concienciación se ve agravada por la ausencia de personal especializado en tecnologías de la información y la falta de capacitación en estos temas.

Finalmente, la entidad pública enfrenta restricciones financieras que limitan la adquisición de recursos necesarios y la contratación de consultorías que podrían mejorar la seguridad de la red inalámbrica, protegiendo así la información sensible. La infraestructura tecnológica del GAD Parroquial de Imbabura se encuentra incompleta debido a que no cuenta con un cableado estructurado certificado ni con un switch que permita multiplexar puntos de acceso a los usuarios para que accedan a la red y conexión internet (Foto 1). Así mismo esto limita la ampliación de configuración de más equipos de acceso a la red inalámbrico (acces point). Además, la institución no cuenta con un router de su propiedad, por lo que no pueden

mantener una administración adecuada que posibilite la seguridad de la red inalámbrica como: el cambio periódico de contraseñas, el control de usuarios que tienen acceso a la conexión a la red inalámbrica (listas de control de acceso).

Foto 1. *Router proveedor de internet*

Nota: Fotografía del autor.

3.2 Diagnóstico de la Red Inalámbrica (Wi-Fi) en el GAD Parroquial de Imbabura

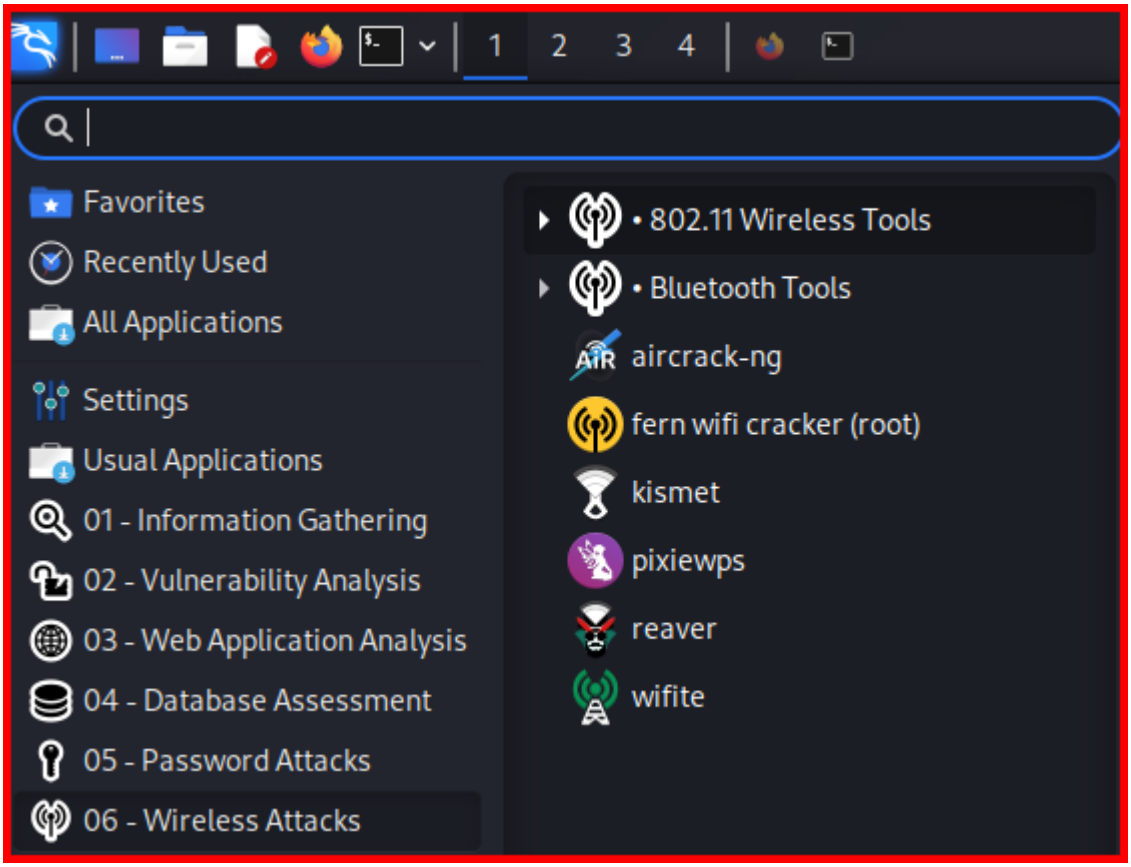
3.2.1 Pruebas de penetración a la red inalámbrica (Wi-Fi) con AirCrack

Mediante el uso de la herramienta AirCrack sin tener la clave de la red inalámbrica identificada como “GAD Imbabura”, se realizó un ataque ético que permita obtener la clave de acceso a la red inalámbrica. El objetivo fue identificar vulnerabilidades en la seguridad de la red, específicamente verificando la fortaleza de la contraseña utilizada. Se realizó el siguiente proceso:

Equipamiento utilizado: Adaptador Wi-Fi compatible con modo monitor (D-Link

Corp. DWA-123 Wireless N 150 Adapter (rev.D1). En la (figura 7) se muestra el Sistema operativo Kali Linux, que incluye la suite Aircrack-ng preinstalada.

Figura 7. *Sistema Operativo Kali Linux*

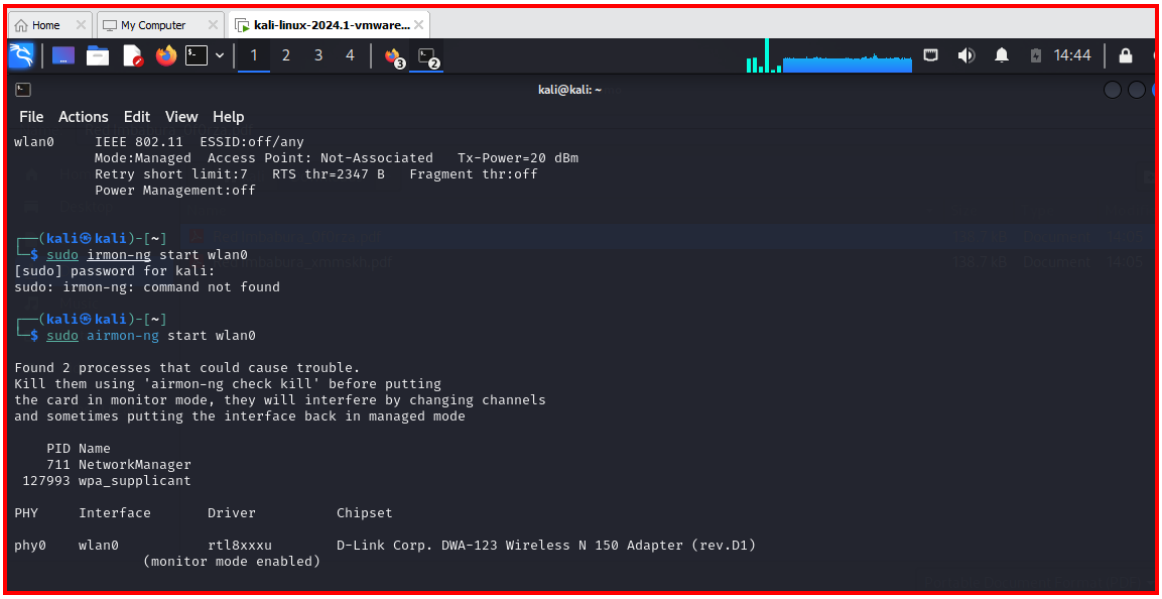


Fuente: Elaboración del autor.

Configuración de la red: Asegurarse de que el adaptador Wi-Fi esté correctamente configurado para funcionar en modo monitor.

Activación del Modo Monitor: En la (figura 8) se muestra que se activó el modo monitor con el siguiente comando: sudo airmon-ng start wlan0. Esto permitió que el adaptador escuche el tráfico de red en lugar de solo enviar y recibir datos en una conexión específica.

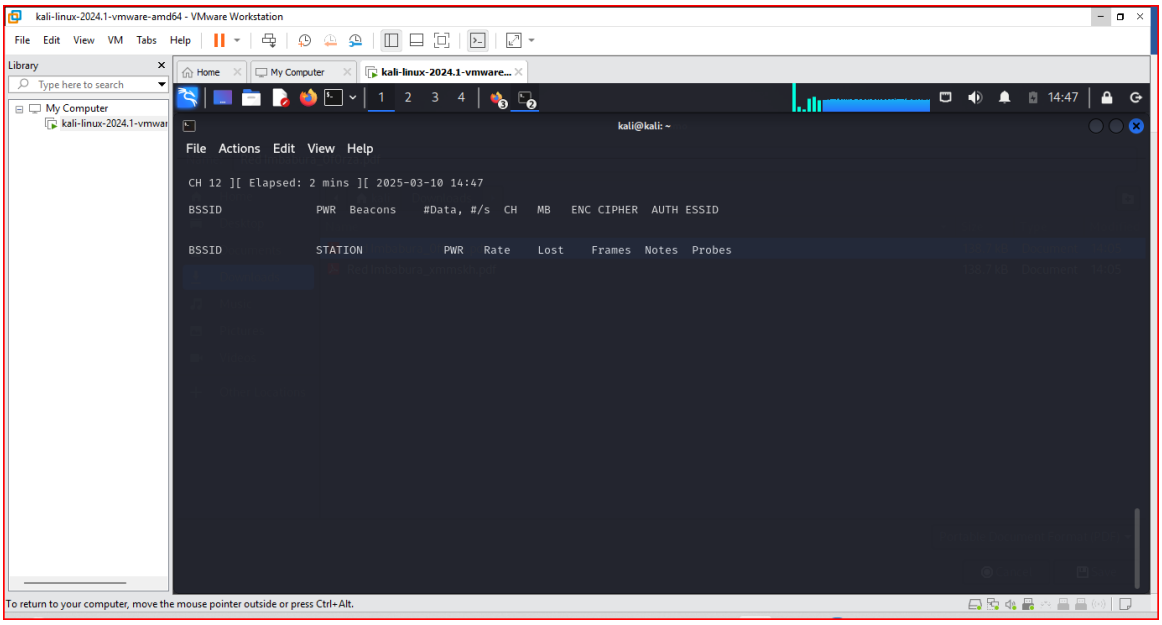
Figura 8. *Activación del modo monitor.*



Nota: Elaboración del autor.

Captura de Tráfico de Red: Como se muestra en la (figura 9) se utilizó la herramienta airodump-ng para identificar redes disponibles y comenzar la captura de paquetes: sudo airodump-ng wlan0mon.

Figura 9. *Captura del tráfico de red.*



Nota: Elaboración del autor.

Se identificó la red “GAD Imbabura” junto con su BSSID y el canal de operación (Channel). Una vez localizado el objetivo, comenzamos a capturar paquetes específicos de esa red: sudo airodump-ng --bssid GADImbabura -c 6 -w captura wlan0mon. GADImbabura: Dirección MAC del punto de acceso (AP) de “GAD Imbabura”.

Desautenticación de un cliente: Una vez localizado el objetivo se procedió a obtener el handshake (intercambio de llaves) de la red, se utilizó el siguiente comando para desautenticar a un usuario conectado, obligándole a volver a autenticarse y, por lo tanto, enviar nuevamente el handshake: sudo aireplay-ng --deauth 10 -a [BSSID] wlan0mon. El número 10 especifica el número de paquetes de desautenticación que se envían.

Captura del handshake: Una vez realizado el procedimiento anterior, se logró capturar el handshake que se almacenó en el archivo de captura especificado anteriormente. Se verificó que el handshake se capturó con éxito.

Ruptura de la contraseña WPA: Se utilizó aircrack-ng para intentar descifrar la contraseña de la red: aircrack-ng -w [ruta/diccionario.txt] captura-01.cap [ruta/diccionario.txt]: Ruta hacia un archivo de diccionario que contiene posibles contraseñas. Durante el proceso, se encontró que la contraseña utilizada por la red “GAD Imbabura” era simple, lo que permitió obtener acceso a la red rápidamente.

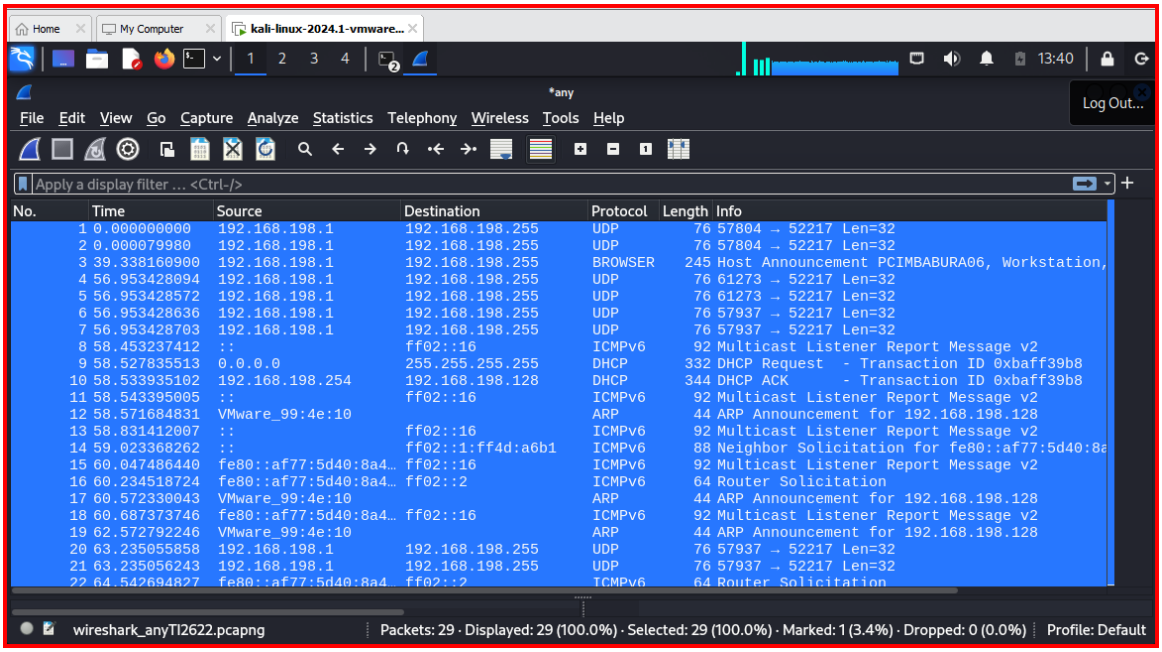
Se accedió a la red “GAD Imbabura” usando la contraseña extraída del usuario, la contraseña identificada no cumplía con los parámetros de complejidad, por lo que fue de fácil acceso. La red utilizaba WPA (Wi-Fi Protected Access) como protocolo de seguridad, sin embargo, la simplicidad de la contraseña comprometió la seguridad de la red.

3.2.2 Análisis de Tráfico en la Red Inalámbrica mediante Wireshark

Como muestra la (figura 10) se realizó la captura de paquetes con Wireshark, lo que permitió

obtener una lectura de la red local.

Figura 10. *Análisis de Tráfico en la Red mediante Wireshark*



Hallazgos identificados

Direcciones IP en uso:

192.168.198.1: Esta dirección IP parece ser el gateway (router) de la red local.

192.168.198.255: Esta es la dirección de broadcast para la red 192.168.198.0/24.

192.168.198.128: Este parece ser un cliente en la red.

0.0.0.0 y 255.255.255.255: Son direcciones de broadcast.

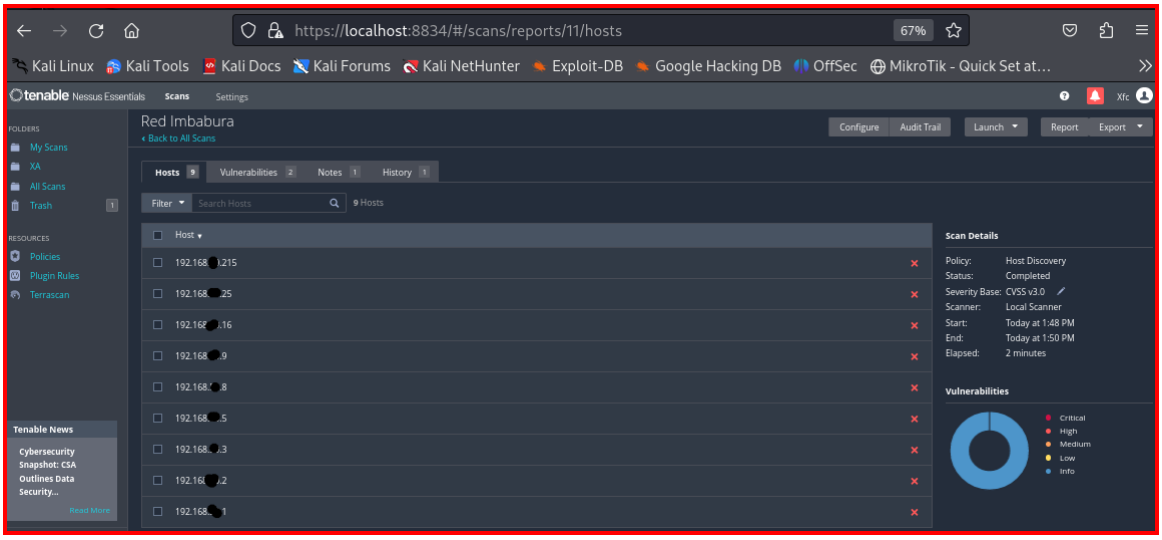
Protocolos involucrados

- **UDP:** Se observa que varios paquetes utilizan UDP, lo que podría indicar servicios que operan sobre este protocolo (por ejemplo, servicios de descubrimiento o notificaciones).
- **BROWSER:** Indica que hay anuncios de máquinas como parte del protocolo de NetBIOS para la identificación de dispositivos en la red.
- **DHCP:** Se observan solicitudes y respuestas de DHCP, lo que indica asignación de direcciones IP en la red.
- **ARP:** Protocolo de resolución de direcciones que se usa para descubrir las direcciones MAC a partir de las direcciones IP.

3.2.3 Escaneo a computadores y dispositivos activos mediante NESSUS

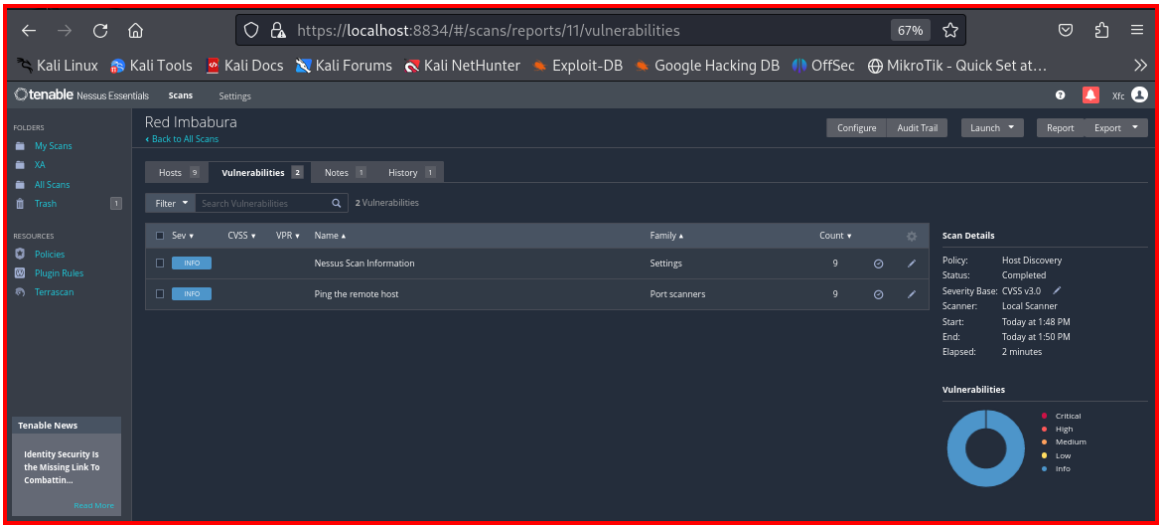
Para realizar este análisis se usó la aplicación NESSUS permitió tener una lectura real de los equipos activos para identificar vulnerabilidades. Toda vez estando dentro del aplicativo, se parametrizó un nuevo escaneo llamado XA, como se muestra en la (figura 11). Gracias a esto, se obtuvo como resultados la información de 9 hosts, indicando 2 alertas de vulnerabilidades, como muestra la (figura 12).

Figura 11. *Escaneo a computadores usando XA.*



Nota: Elaboración propia.

Figura 12. *Resultados del escaneo*



Nota: Elaboración propia.

El informe de Nessus Essentials mostró los resultados de un escaneo realizado en varias direcciones IP dentro del rango 192.168.x.x: 192.168.X.1, 192.168.X.2, 192.168.X.3, 192.168.X.5, 192.168.X.8, 192.168.X.9, 192.168.X.16, 192.168.X.25, y 192.168.X.215.

Resultados de Vulnerabilidades:

- Para cada dirección IP, se encontraron dos elementos informativos (INFO).
- No se identificaron vulnerabilidades de severidad CRÍTICA, ALTA, MEDIA o BAJA.

Tipos de Vulnerabilidades Identificadas (INFO):

- **Nessus Scan Information (Plugin ID 19506)**: Este plugin proporciona información general sobre el escaneo en sí.

- **Ping the remote host (Plugin ID 10180)**: Este plugin simplemente verifica si el host remoto está respondiendo a los pings.

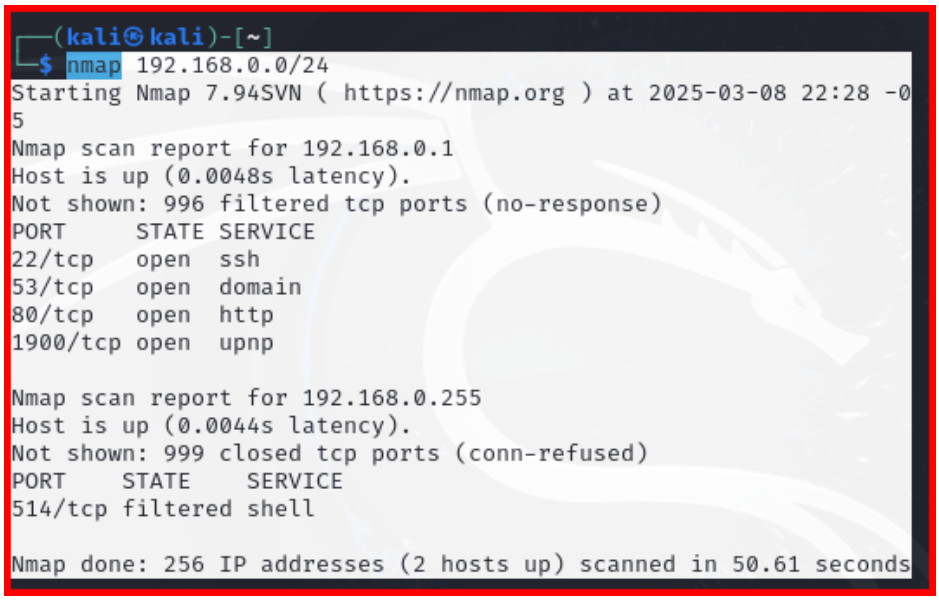
El informe indica que los hosts escaneados no presentan vulnerabilidades críticas, altas, medias o bajas según el escaneo realizado.

3.2.4 Descubrimiento de la red

Mediante la utilización de la herramienta Nmap (escaneo de la red) se identificaron las computadoras activas y los servicios que se ejecutan en tiempo real. Esto reveló información de vulnerabilidades en las estaciones de trabajo. Como primer paso escaneó a toda la red 192.168.X.0/24 con el comando Nmap en un Kali Linux.

Como se puede observar (figura 13) el resultado del escaneo de Nmap a la red 192.168.X.0/24 revela la siguiente información:

Figura 13. *Escaneo de puertos*



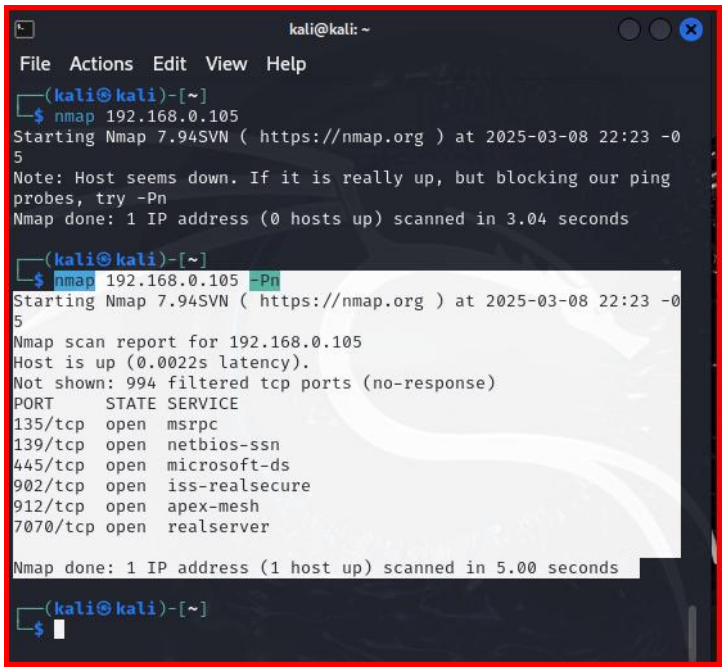
Nota: Es escaneo de Nmap a la red 192.168.X.0/24. Fuente: El autor.

- **192.168.X.1:** Este host está activo. Los puertos 22 (SSH), 53 (DNS/domain), 80 (HTTP) y 1900 (UPnP) están abiertos. Esto sugiere que este host podría ser un router, un servidor o un dispositivo que ofrece servicios web, resolución de nombres de dominio y/o funcionalidades UPnP.
- **192.168.X.255:** Este host está activo. El puerto 514 (shell) está filtrado. Este puerto generalmente se asocia con el servicio de shell remoto (rsh). El estado "filtrado" indica que Nmap no pudo determinar si el puerto está abierto o cerrado porque los paquetes de prueba fueron filtrados por un firewall u otro dispositivo de red.

El escaneo exploró 256 direcciones IP en el rango 192.168.X.0/24, encontrando solo 2 hosts activos (192.168.X.1 y 192.168.X.255). Los puertos filtrados indican que existen reglas de firewall que impiden la determinación del estado de los puertos.

Posteriormente se realizó un escaneo a una computadora activa dentro de la red 192.168.X.0 con el comando 192.168.X.105 -Pn.

Figura 14. *Escaneo Nmap al host*



Nota: El escaneo Nmap al host 192.168.X.105 revela que los puertos 135, 139, 445, 902, 912 y 7070 están abiertos. Fuente: El autor.

El escaneo Nmap al host 192.168.X.105, como se aprecia en la (figura 14), revela que los puertos 135, 139, 445, 902, 912 y 7070 están abiertos. El resto de los puertos (994) están filtrados y no responden. Aquí hay un desglose de los puertos abiertos y sus posibles servicios:

- **135/tcp (msrpc):** Microsoft RPC Endpoint Mapper. Este servicio es utilizado para la comunicación entre componentes en un entorno Windows.
- **139/tcp (netbios-ssn):** NETBIOS Session Service. Este servicio se utiliza para el intercambio de datos en la red y para compartir archivos e impresoras en redes Windows.
- **445/tcp (microsoft-ds):** Microsoft Directory Services. Este puerto también se utiliza para compartir archivos e impresoras en redes Windows y es el puerto utilizado por SMB (Server Message Block).
- **902/tcp (iss-realsecure):** VMware ESXi. Este puerto es utilizado para la

comunicación con servidores VMware ESXi.

- **912/tcp (apex-mesh):** apex-mesh. No encontré información específica sobre este servicio. Es posible que sea un servicio propietario o menos común.
- **7070/tcp (realserver):** RealServer. Este puerto está asociado con RealNetworks RealServer, un servidor de transmisión de medios.

El hecho de que estos puertos están abiertos indica que el host 192.168.X.105 está ejecutando servicios que utilizan estos puertos. El escaneo también muestra que el host está activo y respondiendo a las solicitudes de red. El parámetro "-Pn" en el comando Nmap indica que no se realizó un ping al host antes del escaneo de puertos. Posteriormente en una nueva fecha, se realiza un nuevo escaneo para obtener más resultados de equipo conectados a la red con los siguientes resultados:

Figura 15. *Uso de herramienta Nmap.*

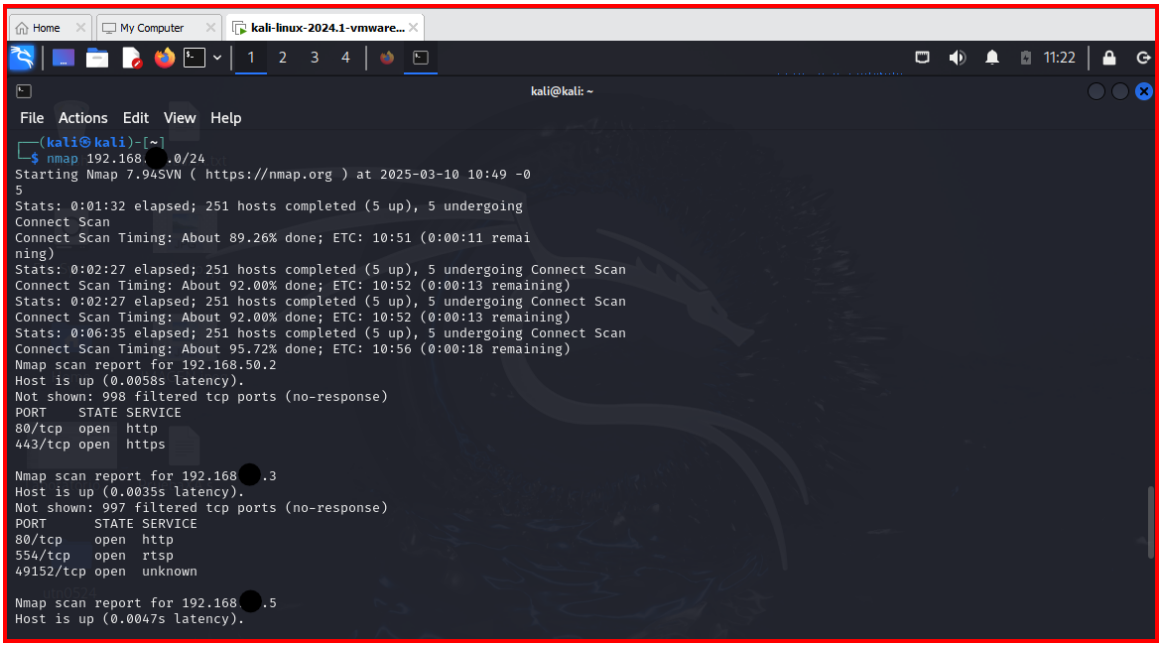
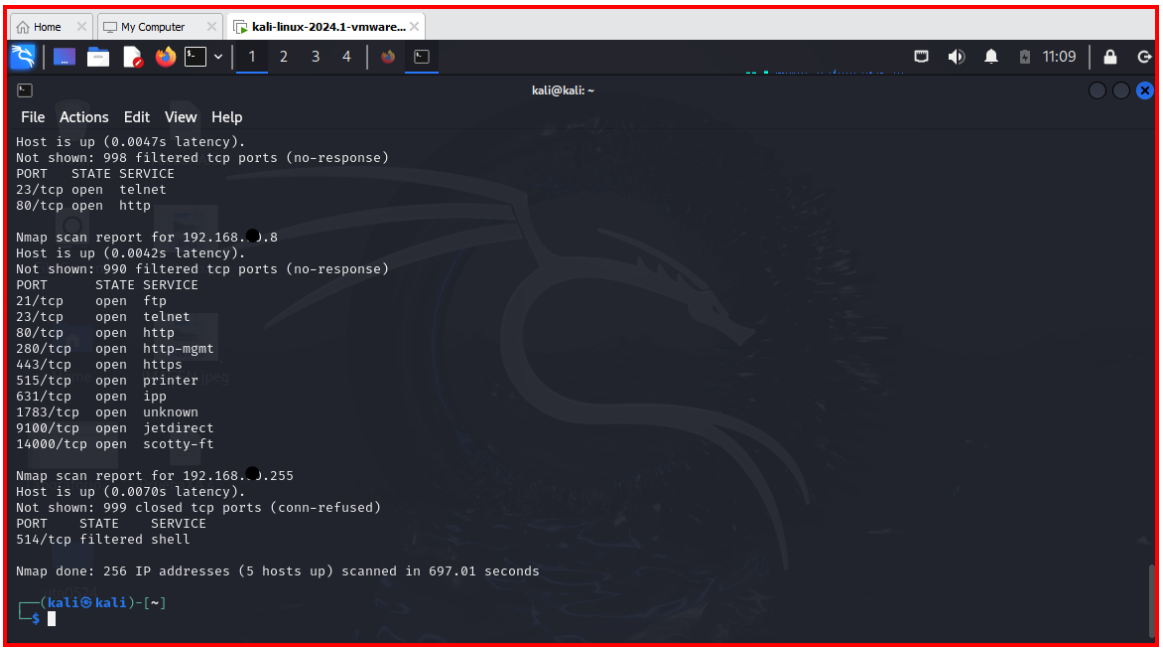


Figura 16. *Escaneo de hosts activos.*

Figura 17. *Hosts activos en tiempo real.*



Se escanearon 256 direcciones IP en total (Figuras 15, 16 y 17). Se identificaron 5 hosts activos en la red, lo que sugiere que la mayoría de los dispositivos en el rango están apagados o no son accesibles. Se detectaron 995 puertos TCP filtrados, lo que indica que

muchos de los dispositivos están configurados con firewalls o sistemas de protección que evitan respuestas a ciertos puertos.

Como se muestra en la tabla 4 se detectaron 5 hosts activos, además de los puertos y la descripción de cada uno de ellos.

Tabla 4. *Detección de hosts activos*

Hosts activo	Puertos abiertos	Descripción
192.168.X.2	80 (http) y 443 (https)	Este es un server web, accesible a través de los protocolos http y https.
192.168.X.8	21 (ftp), 23 (telnet), 80 (http), 280 (http-mgmt), 443 (https), 515 (printer), 631 (ipp), 1783 (unknown), 9100 (jetdirect), 14000 (scotty-ft)	Este host tiene múltiples servicios funcionando, incluyendo FTP, Telnet, varios puertos HTTP, servicio de impresión, y uno para manejo de impresoras IPP. Es la máquina con más servicios expuestos, lo que puede ser tanto un recurso útil como un riesgo de seguridad.
192.168.X.255	514 (filtered shell)	Esta dirección se utiliza generalmente como broadcast. El puerto 514 está filtrado, indicando que podría haber medidas de seguridad implementadas
192.168.X.8	21 (ftp), 23 (telnet), 80 (http), 280 (http-mgmt), 443 (https), 515 (printer), 631 (ipp), 1783 (unknown), 9100 (jetdirect), 14000 (scotty-ft)	Este host tiene múltiples servicios funcionando, incluyendo FTP, Telnet, varios puertos HTTP, servicio de impresión, y uno para manejo de impresoras IPP. Es la máquina con más servicios expuestos, lo que puede ser tanto un recurso útil como un riesgo de seguridad.
192.168.X.255	514 (filtered shell)	Esta dirección se utiliza generalmente como broadcast. El puerto 514 está filtrado, indicando que podría haber medidas de seguridad implementadas

Nota: Elaboración del autor.

En este contexto, el diagnóstico de la red inalámbrica permitió acceder fácilmente a todos los equipos activos en ese momento. Esto sugiere que la red carece de seguridad, ya que se trata de una red plana que no implementa segmentación (VLAN). La ausencia de esta

segmentación compromete los principios fundamentales de la seguridad de la información, que son la confidencialidad, la integridad y la disponibilidad.

3.2.5 Identificación de Vulnerabilidades

Mediante los análisis realizados con las herramientas Aircrack, Wireshark, NESSUS, Nmap se identificaron las siguientes vulnerabilidades. Como se muestra en la tabla 5 se menciona la vulnerabilidad identificada acompañada de la descripción y su impacto potencial.

Tabla 5. Vulnerabilidades Identificadas

Vulnerabilidad	Descripción	Impacto Potencial
Contraseñas débiles	Uso de contraseñas simples o predeterminadas.	Acceso no autorizado a la red.
Configuraciones predeterminadas	Uso de SSID predeterminado y WPS habilitado.	Facilita ataques de fuerza bruta y reconocimiento de red.
Falta de segmentación de red	Toda la red opera en un único segmento.	Propagación de ataques entre dispositivos conectados.
Falta de autenticación robusta	Uso de WPA sin autenticación avanzada.	Acceso no autorizado y exposición de datos sensibles.
Tráfico no cifrado	Datos transmitidos sin cifrado adecuado.	Intercepción de información sensible.
Vulnerabilidades en dispositivos IoT	Dispositivos conectados con configuraciones inseguras.	Compromiso de dispositivos y propagación de ataques.
Falta de actualizaciones de firmware	Dispositivos con firmware desactualizado.	Exposición a vulnerabilidades conocidas.

3.2.6 Evaluación de aspectos en seguridad informática

Se llevó a cabo una verificación mediante un checklist para evaluar los cumplimientos y riesgos presentes en la red inalámbrica del GAD Parroquial en la Provincia de Imbabura. El objetivo de este proceso fue analizar los aspectos que componen cada uno de estos elementos. Basándose en la norma ISO 27001, se definieron 10 aspectos que permitieron medir tanto el grado de cumplimiento como el nivel de riesgo que enfrentó la organización.

A través del uso de un checklist, como se muestra en la (tabla 6), se identificó que la organización no cumple con ninguno de los criterios establecidos, lo que implica una falta de

alineación con las mejores prácticas recomendadas por la norma ISO 27001. De los aspectos evaluados, se identificó que tres presentan un impacto medio y siete tienen un impacto alto en términos de riesgo

Tabla 6. *Matriz de verificación de cumplimiento en seguridad informática*

Aspecto	Cumple		Nivel de riesgo		
	Sí	No	Bajo	Medio	Alto
POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN					
El GAD cuenta con política de seguridad de la información		X		X	
CONCIENCIACIÓN Y CAPACITACIÓN DEL PERSONA					
Desarrolla sistemas de capacitación al personal referente a la seguridad informática		X		X	
El personal es consciente de la importancia de la seguridad informática		X		X	
CONTROLES DE SEGURIDAD					
Contraseña robusta		X			X
Configuraciones predeterminadas		X			X
Segmentación de la red		X			X
Autenticación robusta		X			X
Tráfico cifrado		X			X
Vulnerabilidades en dispositivos IoT		X			X
Falta de actualizaciones de firmware		X			X
TOTAL		10		3	7

La situación actual indica una necesidad de establecer políticas de seguridad y de implementar sistemas de capacitación para el personal, con el fin de mejorar la concienciación sobre la importancia de la seguridad informática. Sin estas acciones, el GAD Parroquial se encuentra en una posición vulnerable, lo cual podría tener graves repercusiones para la seguridad de la información y la confianza pública en sus operaciones.

La organización carece de una política formal de seguridad de la información. Esta ausencia de un marco normativo y directrices claras limita la capacidad para salvaguardar aspectos fundamentales de la información, tales como la confidencialidad, integridad y disponibilidad.

CAPÍTULO V

PROPUESTA DE MEJORA EN SEGURIDAD PARA LA RED WI-FI

La seguridad de la red Wi-Fi en la institución pública es fundamental para proteger la información sensible y mantener la confianza de los ciudadanos. A continuación, se presenta una propuesta integral de mejora en seguridad que incluye una serie de prácticas, políticas y un plan de capacitación para garantizar un entorno seguro y efectivo.

4.1 Diseño de la Arquitectura de Seguridad Propuesta

La seguridad de la red Wi-Fi en el GAD Parroquial es fundamental para proteger la información sensible y garantizar un servicio eficaz a la comunidad. Para alcanzar estos objetivos, se ha diseñado una arquitectura de seguridad integral que utiliza la solución UNIFI Cloud Key y tres puntos de acceso Ubiquiti, junto con un Switch Cloud Router CRS328-24P-4S+RM de Mikrotik (Foto 2). Esta solución proporciona la cobertura necesaria e incluye un portal cautivo y módulos adicionales de seguridad que contribuyen a la protección de la información en la red. A continuación, se detallan los componentes esenciales de esta arquitectura.

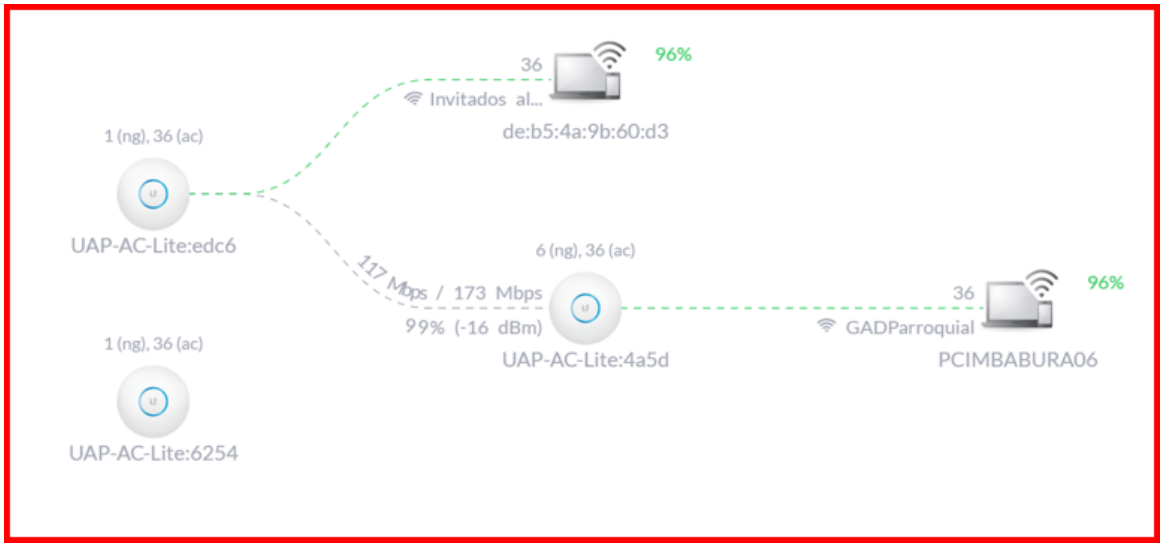
Foto 2. *Arquitectura de seguridad integral*

Fuente: Fotografía del autor.

4.1.1 Segmentación de la Red

La segmentación de la red es un componente vital para la seguridad y administración eficiente del tráfico. Con los puntos de acceso Ubiquiti gestionados por la UNIFI Cloud Key, se pueden establecer múltiples redes (SSIDs) que segmenten la red según diferentes grupos de usuarios y dispositivos, como se observa en la (figura 18).

Figura 18. *Estructura de la segmentación de red*



Nota: Este diagrama presenta la segmentación de la red Wi-Fi utilizando el Switch Cloud Router Switch CRS328-24P-4S+RM y puntos de acceso Ubiquiti. Fuente: El autor

La red está dividida en tres segmentos: administración e invitados, cada uno con políticas de seguridad y acceso específicas para garantizar la protección de la información sensible. El uso de un portal cautivo en la red de invitados controla el acceso de los usuarios y ayuda a recopilar información sobre su uso.

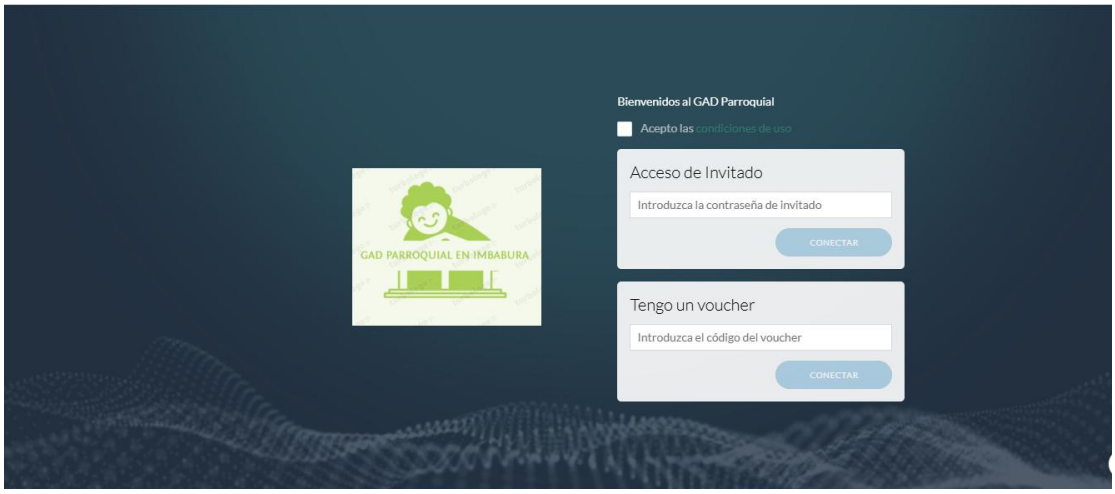
Redes Separadas: Se crearon diferentes redes para distintos grupos, incluyendo una red para el personal administrativo, una red para visitantes y otra para dispositivos IoT, como cámaras de seguridad y sensores. Esta segmentación limita el acceso a información sensible y reduce el riesgo de comprometer la red en su totalidad si se produce una brecha en un segmento

específico.

Control de Acceso entre Segmentos: UNIFI Cloud Key proporcionó la capacidad de implementar controles de acceso precisos entre los segmentos de la red. Por ejemplo, los dispositivos en la red de invitados no tienen acceso a recursos críticos de la red interna, garantizando un entorno seguro para los datos sensibles.

Portal Cautivo: Para mejorar la seguridad y la experiencia del usuario en la red de invitados, se utiliza un portal cautivo. Este sistema requiere que los visitantes se autentiquen antes de acceder a Internet, lo que no solo permite una mejor gestión de usuarios, sino que también ayuda a recolectar información relevante sobre ellos, como se observa en la (Figura 19). Esto facilita la supervisión y el control del acceso a la red.

Figura 19. *Proceso de autenticación para acceder a internet*



Nota: Elaboración propia

4.1.2. Implementación de Autenticación Robusta.

La autenticación es el primer y determinante paso en el proceso de acceso a la red. Esta propuesta incluye medidas robustas de autenticación para asegurar que solo los usuarios

autorizados puedan acceder a recursos críticos.

WPA2-Enterprise: Debido a que los equipos actuales soportan WPA2, se implementó este protocolo en los puntos de acceso Ubiquiti. WPA2-Enterprise ofrece estándares de seguridad y cifrado superiores en comparación con sus predecesores. Este protocolo proporciona autenticación individual para cada usuario, mejorando significativamente la seguridad de la red. Además, facilita la creación de certificados digitales, lo que aumenta la resistencia ante ataques y refuerza la integridad de las conexiones.

Módulos Adicionales de Seguridad: La solución UNIFI incluye módulos adicionales que facilitan la gestión de las credenciales de los usuarios y soportan la implementación de políticas de acceso. Esto garantiza que todos los accesos estén debidamente controlados y auditados, permitiendo un seguimiento efectivo de las actividades en la red.

Autenticación de Dos Factores (2FA): Se integró un sistema de autenticación de dos factores en el portal cautivo. De esta forma, los usuarios no solo ingresan su contraseña, sino que también verifican su identidad mediante un segundo método, mediante un código de acceso enviado a su dispositivo móvil. Esta capa adicional de seguridad previene accesos no autorizados incluso en caso de que las credenciales sean comprometidas.

4.1.3 Uso de Firewalls y Sistemas de Detección de Intrusiones (IDS/IPS)

Para fortalecer la defensa de la red Wi-Fi, es esencial implementar firewalls y sistemas de detección y prevención de intrusiones.

Firewalls Integrados: El Switch Cloud Router Switch CRS328-24P-4S+RM de Mikrotik incluye capacidades de firewall para filtrar el tráfico entre los diferentes segmentos de la red. Se configuró para permitir solo el tráfico necesario y bloquear acceso no autorizado, protegiendo así redes críticas de potenciales amenazas.

Sistemas de Detección y Prevención de Intrusiones (IDS/IPS): Emplearemos IDS/IPS para identificar y bloquear actividades maliciosas. Estos sistemas permiten mantener la supervisión constantemente el tráfico de la red, buscando patrones anómalos o intentos de acceso no autorizados, y responder automáticamente para mitigar cualquier amenaza detectada.

El diseño de la arquitectura de seguridad para la red inalámbrica Wi-Fi del GAD Parroquial de Imbabura, utilizando la solución UNIFI Cloud Key, tres puntos de acceso Ubiquiti y el Switch Cloud Router Switch CRS328-24P-4S+RM, está orientado a crear un entorno seguro, eficiente y fácil de gestionar. La segmentación de la red, la autenticación robusta, el uso de tecnologías de firewall y detección de intrusiones se combinaron para ofrecer múltiples capas de seguridad. La implementación de un portal cautivo y de módulos adicionales asegura una gestión adecuada de los accesos y la protección de la información crítica, garantizando que la institución pueda operar de manera segura y confiable.

4.2. Políticas de Seguridad Propuestas

Las políticas de seguridad son esenciales para establecer un marco claro de conducta en la administración de la red Wi-Fi, asegurando que todos los usuarios, empleados y visitantes entiendan las expectativas y responsabilidades que tienen al utilizar los recursos de la institución. A continuación, se presentan las políticas de seguridad propuestas que regirán el uso de la red Wi-Fi.

4.2.1. Política de Uso de la Red Wi-Fi

Esta política tiene como objetivo establecer las directrices para el uso seguro y responsable de la red Wi-Fi del GAD Parroquial en la Provincia de Imbabura. Se busca proteger la confidencialidad, integridad y disponibilidad de la información institucional, así como garantizar el cumplimiento de las leyes y regulaciones aplicables, incluyendo la Ley Orgánica

de Protección de Datos Personales. Esta política está alineada con el control 1.10 “Uso aceptable de la información y otros activos asociados” del EGSI MINTEL (Anexo A).

4.2.2. Política de Contraseñas Seguras

Esta política establece los requisitos para la creación, uso, almacenamiento y gestión de contraseñas para acceder a los sistemas de información y recursos del GAD Parroquial en la Provincia de Imbabura. El objetivo es proteger la confidencialidad, integridad y disponibilidad de la información institucional. Esta política está alineada con el control 1.17 “Información de autenticación” del EGSI MINTEL (Anexo B). Políticas de contraseñas.

4.2.3. Política de segmentación de la Red.

Esta política establece las directrices para la segmentación de la red del GAD Parroquial en la Provincia de Imbabura. El objetivo es mejorar la seguridad, el rendimiento y la gestión de la red, protegiendo la confidencialidad, integridad y disponibilidad de la información institucional. Esta política está alineada con el control 4.22 “Segmentación de redes” del EGSI (Anexo C).

4.2.4. Políticas de acceso remoto seguro.

Esta política establece los requisitos para el acceso remoto seguro a los sistemas de información y recursos del GAD Parroquial en la Provincia de Imbabura. El objetivo es proteger la confidencialidad, integridad y disponibilidad de la información institucional, así como garantizar el cumplimiento de las leyes y regulaciones aplicables, incluyendo la Ley Orgánica de Protección de Datos Personales. Esta política está alineada con el control 6.2.2 “Control de acceso seguro a la red” del EGSI (Anexo D).

4.2.5. Implementación de Medidas Técnicas

Considerando infraestructura específica del GAD Parroquial (computadoras de escritorio y portátiles, equipos de red limitados a un router del proveedor, un switch, puntos de acceso inalámbricos, y la información digital almacenada), y la implementación de una solución WiFi Ubiquiti Unifi con su controladora, se deben establecer los siguientes procedimientos para la gestión de la seguridad (Anexo E), con un enfoque particular en la seguridad de las redes inalámbricas.

4.3. Capacitación del Personal

El plan de capacitación del personal del GAD Parroquial de Imbabura está diseñado para fortalecer las habilidades y conocimientos del equipo encargado de la infraestructura de la red Wi-Fi, asegurando que todos los empleados comprendan la importancia de la seguridad informática y utilicen la red de manera segura. Con un total de aproximadamente 20 servidores públicos, incluyendo al presidente de la junta parroquial y la secretaria tesorera, es fundamental que todos estén alineados en las mejores prácticas para proteger la información y la infraestructura tecnológica de la entidad.

4.3.1. Concientización sobre Seguridad Informática

El objetivo de la capacitación en concientización sobre seguridad informática es educar a todo el personal sobre las amenazas cibernéticas y la importancia del cumplimiento de las políticas de seguridad.

Objetivos Generales:

- Fomentar una cultura de seguridad dentro de la organización.
- Informar a los empleados sobre las posibles amenazas a las que la red puede estar expuesta (como malware, phishing, ransomware y ataques de ingeniería social).

- Relacionar la seguridad informática con el trabajo diario de cada empleado y la protección de datos sensibles de la parroquia.

Contenido del Programa de Concientización

- **Tipos de Amenazas:** Capacitación sobre diferentes tipos de ciberamenazas que puede enfrentar la organización, incluyendo ejemplos específicos que podrían afectar a un GAD.
- **Mejores Prácticas de Seguridad:** Enseñar sobre la importancia de crear contraseñas seguras, el uso de autenticación de dos factores y el reconocimiento de intentos de phishing y otras técnicas de ingeniería social.
- **Protocolos de Reporte:** Instrucción sobre cómo identificar incidentes de seguridad y el procedimiento adecuado para reportarlos al presidente de la junta parroquial o a la secretaria tesorera.
- **Consecuencias del Incumplimiento:** Explicar las posibles consecuencias de no seguir las políticas de seguridad, tanto a nivel personal como institucional, para establecer la gravedad del asunto.

Formato de Capacitación:

- **Talleres Presenciales:** Realización de talleres periódicos donde se presenten casos prácticos y se realicen sesiones interactivas para facilitar el aprendizaje.
- **Materiales de Apoyo:** Creación de folletos, guías rápidas y videos informativos que se distribuyan al personal para facilitar el aprendizaje continuo y la referencia rápida.

4.3.2. Capacitación en el Uso Seguro de la Red Inalámbrica (Wi-Fi)

El objetivo de esta capacitación es proporcionar a los empleados del GAD Parroquial

las habilidades necesarias para utilizar la red Wi-Fi de manera segura, maximizando la protección de la infraestructura y la información.

Objetivos Generales:

- Asegurar que todo el personal sepa cómo conectarse a la red de manera segura.
- Proporcionar directrices sobre el comportamiento seguro en el uso de la red Wi-Fi.
- Capacitar en la identificación y el manejo de riesgos asociados al acceso y uso de la red.

Contenido del Programa de Concientización

- **Configuración de Dispositivos:** Instrucciones sobre cómo configurar de manera segura sus dispositivos (computadoras, teléfonos inteligentes y tabletas) para conectarse a la red Wi-Fi institucional.
- **Uso Correcto de Redes:** Directrices sobre cómo evitar conexiones a redes Wi-Fi no seguras y la importancia de utilizar la red institucional para fines de trabajo y no personales o no relacionados.
- **Acceso a Recursos Críticos:** Capacitación en cómo acceder a información sensible de la institución desde la red Wi-Fi, asegurando que se sigan los protocolos de autenticación y acceso.
- **Manejo de Incidencias:** Instrucciones sobre cómo responder ante situaciones inusuales mientras se utiliza la red, como recibir correos sospechosos o notar comportamientos extraños en la red.

Formato de capacitación

- **Sesiones de Capacitación en Línea:** Organizarlas mediante plataformas virtuales, que puede ser útil para personal que no pueda asistir a sesiones presenciales.

- **Simulaciones Prácticas:** Realizar simulaciones donde los empleados deban identificar un potencial ataque de phishing o una conexión no segura, brindando feedback inmediato sobre sus decisiones.

El plan de capacitación del personal del GAD Parroquial de Imbabura se centra en concientizar sobre la seguridad informática y proporcionar las habilidades para el uso seguro de la red Wi-Fi. Este enfoque permitirá no solo proteger la infraestructura tecnológica de la institución, sino también empoderar a los empleados para que se conviertan en defensores activos de la seguridad de la información. Con una capacitación continua y efectiva, el GAD podrá garantizar un entorno de trabajo más seguro y confiable para todos los servidores públicos y la comunidad a la que sirven.

4.4. Plan de respuesta ante incidentes

El Plan de Respuesta ante Incidentes es determinante para el GAD Parroquial de Imbabura, ya que permite actuar de manera rápida y eficaz ante situaciones de ciberseguridad que puedan comprometer la integridad de la red Wi-Fi y la seguridad de la información. Este plan incluye procedimientos claros para la recuperación de datos y la continuidad de los servicios, asegurando que la institución pueda minimizar el impacto de cualquier incidente. A continuación, se detallan ambos componentes.

4.4.1 Recuperación de datos

La recuperación de datos es un aspecto crítico en la respuesta ante incidentes, especialmente en el caso de ataques de ransomware, pérdidas de datos o fallos en el sistema. Un enfoque proactivo y organizado es esencial para garantizar que la información valiosa de la institución se pueda restaurar.

Objetivo: Minimizar la pérdida de datos y facilitar la restauración rápida de la información

crítica en caso de un incidente de seguridad.

Políticas de respaldo de datos

- **Frecuencia de Respaldo:** Establecer políticas que determinen que las copias de seguridad de los datos se realicen de forma regular, idealmente diariamente, y se almacenen en un medio seguro y fuera del servidor principal.
- **Verificación de Copias de Seguridad:** Implementar procedimientos para verificar periódicamente la integridad y disponibilidad de las copias de seguridad, asegurándose de que sean fácilmente recuperables cuando sea necesario.

Procedimiento de recuperación

- **Identificación de Pérdidas:** En caso de un incidente, se debe realizar una evaluación inicial para identificar qué datos se han perdido o comprometido y cuál es el alcance del impacto.
- **Activación del Plan de Recuperación:** Una vez que se identifique un incidente que afecta los datos, se activará un plan de recuperación que se detalla en un documento de procedimiento accesible a los responsables de TI. Este plan incluirá los pasos específicos para restaurar los datos desde las copias de seguridad.
- **Restauración de Sistemas:** Seguir el proceso diseñado para restaurar datos y recuperar sistemas afectados, verificando que los datos restaurados sean precisos y completos antes de volver a hacer que los sistemas estén en funcionamiento.

Documentación y aprendizaje

- **Registro de Incidentes:** Llevar un registro detallado de los incidentes, las acciones tomadas y su efectividad. Esto permitirá aprender y ajustar los planes de respuesta

futuros.

- **Revisión Post-Incidente:** Después de la recuperación, se llevará a cabo una revisión para evaluar la gestión del incidente y discutir posibles mejoras en el proceso.

Simulacros y entrenamientos

- **Pruebas de Continuidad:** Realizar simulacros de incidentes cada cierto tiempo para evaluar la efectividad del plan de continuidad de servicios. Este entrenamiento permite al personal practicar la respuesta coordinada y ajustarse a cualquier cambio necesario en el plan.
- **Revisión Continua:** A medida que cambian los servicios y las necesidades del GAD, se actualizará el plan de continuidad para reflejar estas realidades.

El Plan de Respuesta ante Incidentes del GAD Parroquial de Imbabura, que abarca tanto la recuperación de datos como la continuidad de los servicios, está diseñado para proporcionar un enfoque estructurado y proactivo ante cualquier eventualidad de seguridad. Establecer políticas claras y procedimientos para manejar incidentes no solo protege la infraestructura de la red Wi-Fi y la información de la instauración, sino que también asegura que los servicios esenciales para la comunidad continúen funcionando de manera óptima, incluso en situaciones adversas. Esto fomentará la confianza de los ciudadanos en la gestión del GAD, asegurando que la entidad pueda cumplir su misión de manera efectiva y segura.

4.5 Evaluación de cumplimiento

Tras la implementación de la propuesta de mejora para la red inalámbrica (Wi-Fi) del GAD Parroquial, se evaluaron diez aspectos fundamentales de seguridad informática. Como se aprecia en la (tabla 7), de estos, 8 aspectos cumplen la organización, mientras que con 2 aspectos no cumplen. Es importante destacar que los aspectos que no cumplen presentan un nivel de riesgo medio, mientras que aquellos que sí cumplen están asociados a un nivel de riesgo bajo.

Tabla 7. *Matriz de verificación de cumplimiento después de la implementación*

Aspecto	Cumple		Nivel de riesgo		
	Sí	No	Bajo	Medio	Alto
POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN					
El GAD cuenta con política de seguridad de la información	Sí		X		
CONCIENCIACIÓN Y CAPACITACIÓN DEL PERSONAL					
Desarrolla sistemas de capacitación al personal referente a la seguridad informática		X		X	
El personal es consciente de la importancia de la seguridad informática	X		X		
CONTROLES DE SEGURIDAD					
Contraseña robusta	X		X		
Configuraciones predeterminadas	X		X		
Segmentación de la red	X		X		
Autenticación robusta	X		X		
Tráfico cifrado	X		X		
Vulnerabilidades en dispositivos IoT	X		X		
Falta de actualizaciones de firmware	X		X		
TOTAL		10	9	1	

Nota: Elaboración del autor.

Los resultados posteriores a la implementación de la propuesta de mejora en el GAD Parroquial son alentadores, con 9 aspectos cumpliendo los requerimientos y solo 1 elementos quedando por mejorar. No obstante, es crucial que la organización enfoque sus esfuerzos en resolver aquellos aspectos que no cumplen, dado que representan un riesgo medio. Es necesario contar con personal capacitado en seguridad informática, una persona que esté a cargo de esta actividad en la organización. Abordar estas deficiencias no sólo fortalecerá la postura de seguridad del GAD, sino que también contribuirá a mantener la integridad y confidencialidad de la información gestionada. La mejora continua y la capacitación del personal siguen siendo elementos clave en este proceso, asegurando que la cultura de la seguridad informática se mantenga y fortalezca con el tiempo.

Antes de la implementación, El GAD tenía un 0% de cumplimiento en los 10 aspectos evaluados, lo que indica que no se cumplía ninguno de los requisitos establecidos. De estos aspectos, 3 presentaban un nivel de riesgo medio (30%) y 7 tenían un nivel de

riesgo alto (70%). Esto reflejaba una situación alarmante en términos de vulnerabilidad a amenazas de seguridad.

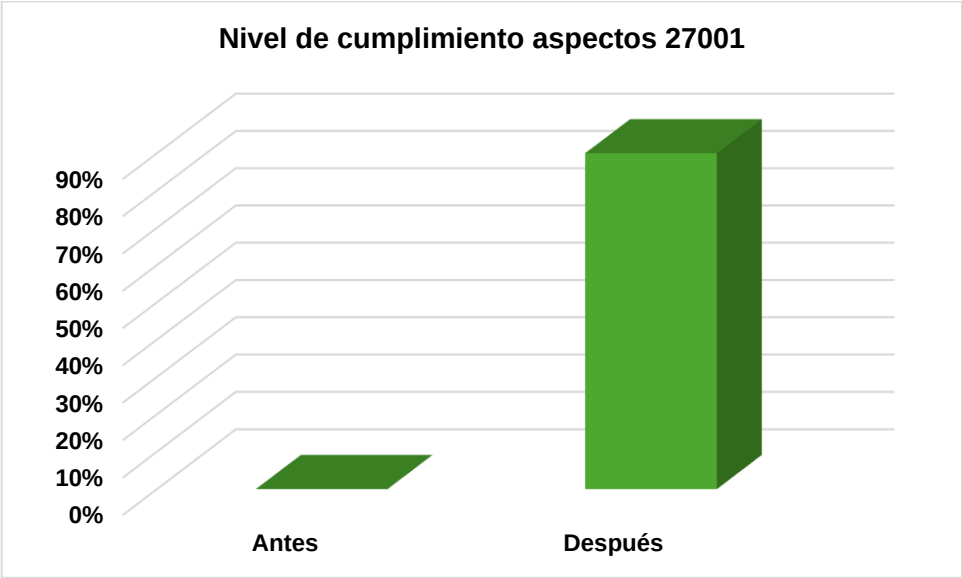
Este escenario indicaba una vulnerabilidad crítica, lo que podría resultar en serias implicaciones para la integridad y seguridad de la información gestionada. Mientras que después de la implementación la situación ha cambiado notablemente de forma positiva. Tras la implementación de la propuesta de mejora, el grado de cumplimiento se elevó a 9 de los 10 aspectos evaluados cumplen con los estándares requeridos. El aspecto que aún no cumplen, representa un 10%, y está clasificado como de nivel medio en términos de riesgo. Esto sugiere que, aunque se ha logrado un avance considerable, hay áreas que aún necesitan atención.

La situación actual del El GAD Parroquial de Imbabura tras la implementación de la propuesta de mejora presenta un avance fundamental en cuanto seguridad informática. Esto debido a que no presenta aspectos clasificados como de alto riesgo y solamente 1 aspecto con riesgo medio. Esta reducción en el riesgo resalta la efectividad de las medidas implementadas y el compromiso del GAD Parroquial hacia una gestión más segura de la información. El hecho de que la institución no cumpla con un aspecto se debe principalmente a que la organización no cuenta con una persona encargada de manejar las tecnologías de la información, no tienen a una persona rentada que desempeñe estas actividades, lo que limita la existencia de una capacitación continua en ciberseguridad.

En cuanto al grado de cumplimiento, la implementación de la propuesta de mejora a la seguridad de la red inalámbrica obtuvo un progreso de 0% a 90% en el cumplimiento, como se observa en la (figura 20). En contraste, después de la implementación de las mejoras, el nivel de cumplimiento se eleva significativamente, alcanzando prácticamente el máximo posible. Esto refleja una evolución positiva en la gestión de la seguridad de la información, lo que sugiere que las medidas adoptadas han sido efectivas para alinear la organización con los

estándares de seguridad requeridos por la norma ISO 27001.

Figura 20. *Comparación del nivel de cumplimiento de los aspectos de seguridad de la información según la Norma ISO 27001: antes y después de la implementación*



Nota: El nivel de cumplimiento antes de la implementación era nulo. Mientras que el actual equivale a un 80%. Fuente: Elaboración del autor.

Esto denota un compromiso por parte del GAD Parroquial para fortalecer su seguridad de la información. Aun así, es crucial que la organización continúe enfocándose en la mejora de los aspectos que aún no cumplen, ya que representan un nivel de riesgo que podría comprometer la integridad de los datos. El camino hacia la mejora continua es esencial para garantizar no solo que se mantenga este alto nivel de cumplimiento, sino que se reduzcan aún más los riesgos asociados a la seguridad de la información en el GAD Parroquial.

CONCLUSIONES Y RECOMENDACIONES

El análisis exhaustivo de la red Wi-Fi del GAD Parroquial de Imbabura permitió identificar múltiples vulnerabilidades críticas, como contraseñas débiles, configuraciones predeterminadas y la falta de segmentación de red. Estas deficiencias incrementan significativamente el riesgo de accesos no autorizados, comprometiendo la confidencialidad, integridad y disponibilidad de la información sensible. Además, se evidenció un bajo nivel de cumplimiento normativo en términos de ciberseguridad.

La implementación de soluciones técnicas, como la segmentación de la red mediante VLANs, el uso de protocolos de seguridad modernos como WPA2-Enterprise, junto con políticas organizacionales claras, demostró ser efectiva para mitigar los riesgos identificados. Estas medidas fortalecen la infraestructura de seguridad y establecen un marco organizacional para la gestión de la red Wi-Fi.

La implementación de políticas de seguridad y la mejora de la infraestructura de seguridad de la red inalámbrica han transformado significativamente la postura de la institución en relación con la seguridad de la información. Gracias a estas iniciativas, el grado de cumplimiento con respecto a la norma ISO 27001 ha aumentado en un 90%, lo que refleja un avance notable en el establecimiento de controles y prácticas de seguridad adecuadas. Además, este esfuerzo ha permitido que la institución pase de enfrentar un nivel de riesgo crítico a uno bajo, lo que representa un logro fundamental en la protección de datos y la minimización de vulnerabilidades.

La elaboración de un plan detallado para responder a incidentes de seguridad, incluyendo procedimientos para la recuperación de datos y la continuidad de los servicios,

garantiza una respuesta rápida y efectiva ante posibles ciberataques. Este plan es esencial para minimizar el impacto de los incidentes y proteger los activos digitales de la institución.

Las políticas propuestas, como el uso de contraseñas seguras, la segmentación de la red y la capacitación del personal, mostraron una reducción significativa en los riesgos de ciberseguridad. La implementación de estas políticas no solo mejora la protección de la red, sino que también fomenta una cultura de ciberseguridad dentro de la institución, empoderando al personal para actuar como defensores de la seguridad.

Se recomienda, en vista de la brecha de talento humano en la institución, contratar a un profesional externo que realice un mínimo de dos visitas al mes. Su labor consistirá en proporcionar soporte técnico para revisar y mitigar riesgos en la red inalámbrica WIFI y en la infraestructura tecnológica en general. Esta estrategia permitirá evaluar la efectividad de las medidas implementadas y realizar los ajustes necesarios para mantener un entorno seguro.

REFERENCIAS

Acuerdo Nro. MINTEL-MINTEL-2024-0003. (2024, 1 de marzo). Esquema Gubernamental de Seguridad de la Información – EGSI. Tercer Suplemento Nº 509 - Registro Oficial.https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2024/03Registro-Oficial-Acuerdo-Ministerial-No.-0003-2024-EGSI-version-3.0.pdf

Antivirus Guard [AVG]. (2025). *What is a VPN and why should you use one?* https://www.avg.com/es/signal/what-is-a-vpn-and-why-should-you-use-one

Ávila, A. A. (2024). Seguridad de la información en instituciones públicas: desafíos y buenas prácticas en el contexto ecuatoriano. *Innovación Social y Respuestas Económicas, 4*(2):140-156. https://doi.org/10.55813/gaea/jessr/v4/n2/96

Burrel, S. (2024). ¿Qué es un túnel VPN? Wray Castle. https://wraycastle.com/es/blogs/glossary/what-is-a-vpn-tunnel?srsltid=AfmBOorxtYgVlWUTZG5dlWWgurUf8MZqRgbs-gOe4Qxt-H0EHlzLmmmU

Buxton, O. (2024). *WEP, WPA, WPA2, and WPA3: Definitions and comparison.* Norton. https://us.norton.com/blog/wifi/wep-vs-wpa

Catota, F. E., Morgan, M. G. y Sicker, D. C. (2019). Cybersecurity education in a developing nation: the Ecuadorian environment. *Journal of Cybersecurity*, *00*(0), 1-19 https://repositorio.uisek.edu.ec/bitstream/123456789/3409/1/2057-2093%20CATOTA%20F.%202019-02-15.pdf

Centro Criptológico Nacional [CN-CERT]. (2021). *Recomendaciones de seguridad en redes Wi-Fi corporativas. Informe de buenas prácticas.* CCN-CERT BP/11. https://www.ccn-cert.cni.es/es/informes/informes-de-buenas-practicas-bp/3137-ccn-cert-bp-11-recomendaciones-redes-wifi-corporativas/file?format=html

Chuquitarco, M. y Romero, M. (2018). Diagnóstico de las vulnerabilidades en redes inalámbricas en el Ecuador. *INNOVA Research Journal*, *3*(2.1), 111-122. https://revistas.uide.edu.ec/index.php/innova/article/view/692/675

Cisco Systems, Inc. (2019). *Guía de redes para pequeñas empresas*. https://www.cisco.com/c/dam/global/es_mx/solutions/small-business/pdfs/smb-redes-mx.pdf

Cisco Systems, Inc. (2025.). *Introducción a las redes inalámbricas*. https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/networking/wireless-network.html#~introduction

Coria, C. (2024). *WPA3: El protocolo de seguridad más seguro para tu red wifi.* Seguridad de la Información. https://seguridad.cicese.mx/noticia/2195/WPA3:-el-protocolo-de-seguridad-m%C3%A1s-seguro-para-tu-red-Wifi

Curay Calucho, M. F. (2023). *Análisis de vulnerabilidades de redes inalámbricas domésticas utilizando pentesting en tungurahua*. [Tesis de pregrado, Universidad Técnica de Ambato (UTA)]. https://repositorio.uta.edu.ec/server/api/core/bitstreams/c02e1770-e65f-4a37-80be-4f66f0698dca/content

Deloitte. (2023). *Future of Cyber Survey*. Deloitte Future of Cyber. https://www.deloitte.com/global/en/services/consulting-risk/content/future-of-cyber.html

ESET. (2022). *Autenticación en dos pasos: qué es y por qué es clave para evitar el robo de cuentas. Cybersegurity pro.* https://www.eset.com/py/acerca-de-eset/sala-de-prensa/comunicados-de-prensa/articulos-de-prensa/black-friday-como-evitar-las-estafas-online-copy-100000000/

Fortinet. (2025). *Energía y servicios públicos seguros con Fortinet. Presentación de infraestructura crítica contra ciberataques*. https://www.fortinet.com/lat/solutions

/industries/power-utilities

Ghimiray, D. (2022). Seguridad de Wi-Fi: WEP frente a WPA o WPA2. Avast Academy. https://www.avast.com/es-es/c-wep-vs-wpa-or-wpa2

Halbouni, A., Ong, L.-Y. y Leow, L. M. (2023). Wireless security protocols WPA3: A systematic literature review. *IEEE Access, 11*, 1-1. https://doi.org/10.1109/ACCESS.2023.3322931

Hernández, M. C., Rodríguez, L. M. y Aguilar, M. (2017). Análisis de seguridad en redes inalámbricas de las MiPyME y propuesta de mejora. *Revista Iberoamericana de Producción Académica y Gestión Educativa*, *4*(7). https://www.pag.org.mx/index.php/PAG/article/view/647

Ley Orgánica de Protección de datos personales. (2021, 26 de mayo). Presidencia de la República del Ecuador. https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

Instituto Nacional de Ciberseguridad [INCIBE]. 2021. *Glosario de términos de ciberseguridad. Una guía de aproximación para el empresario* https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

Instituto Nacional de Estándares y Tecnología. [INET]. (2018). *Marco para la mejora de la seguridad cibernética en infraestructuras críticas.* Versión 1.1 https://www.nist.gov/system/files/documents/2018/12/10/frameworkesmellrev_20181102mn_clean.pdf

Institute of Electrical and Electronics Engineers (IEE). (2025.) Estándares de la IEEE 802.11 https://www.ieee.org/

Internet Crime Complaint Center (IC3). (2023). Federal Bureau of Investigation Internet Crime Report. https://www.ic3.gov/annualreport/reports/2023_ic3report.pdf

International Organization for Standardization [ISO/IEC JTC 1]. (1994). ISO/IEC 7498-1:1994 Information technology — Open Systems Interconnection — Basic Reference Model: The Basic Model (1st ed.). https://doi.org/10.3403/30302970

ISO/IEC 27001. (2022). Information security, cybersecurity and privacy protection — Information security management systems — Requirements. *ISO* https://www.iso.org/obp/ui/es/#iso:std:iso-iec:27001:ed-3:v1:en

Jiménez, M. M. (2021). *Conoce el Marco de Ciberseguridad del NIST*. https://www.piranirisk.com/es/blog/marco-ciberseguridad-nist-que-es

Ministerio de Telecomunicaciones y de la Sociedad de la Información [MINTEL]. (2021). Estrategia Nacional de Ciberseguridad del Ecuador.

Mora Zambrano, E. R. (2024). Análisis de vulnerabilidades en redes inalámbricas: métodos y soluciones. *Revista INSTA Magazine, 7*(1). https://dspace.itsjapon.edu.ec/jspui/handle/123456789/4669

Morán Maldonado, N. M. (2021). *Estado de la Ciberseguridad en las Empresas del Sector Público del Ecuador: Una Revisión Sistemática*. [Tesis de pregrado, Universidad Politécnica Salesiana del Ecuador]. http://dspace.ups.edu.ec/handle/123456789/20243

NovaSec. (2024). *ISO 27001 | Gestión Integral de la Seguridad de la Información | SGSI.* https://www.novasec.co/blog/62-gestion-integral-de-la-seguridad-de-la-informacio

Código Orgánico de Organización Territorial (COOTAD). (2010, 19 de octubre). Presidencia de la República del Ecuador. Registro Oficial Suplemento 303. https://www.defensa.gob.ec/wp-content/uploads/downloads/2016/01/dic15_CODIGO-ORGANICO-DE-ORGANIZACION-TERRITORIAL-COOTAD.pdf

Open Web Application Security Project [OWASP]. (2021). *OWASP top ten.* https://owasp.org/www-project-top-ten/

Organización de las Naciones Unidas [ONU]. (2015). *Objetivos de desarrollo sostenible*. https://www.un.org/sustainabledevelopment/es/objetivos-de-desarrollo-sostenible/

Ramos Secaira, Francisco Marcelo. 2023. Seguridad Cibernética en Empresas Ecuatorianas: Prácticas y Retos Actuales. *Educación y conocimiento científico, 2*(3). https://revistaczambos.utelvtsd.edu.ec/index.php/home/article/view/47

Rodríguez, A. (2025). *Descubre todos los componentes de redes.* Tokio School. https://www.tokioschool.com/noticias/componentes-de-redes/

Salazar, J. (2016). *Redes Inalámbricas.* České vysoké učení technické v Praze Fakulta elektrotechnická.https://upcommons.upc.edu/bitstream/handle/2117/100918/LM01_R_ES.pdf

Salazar, A. F., Barahona, D. A., Delgado, J. V. y Suárez, J. C. (2023). *Seguridades en Redes WIFI.* [Tesis de maestría, Universidad Internacional SEK Ecuador (UIDE)]. https://repositorio.uide.edu.ec/bitstream/37000/6106/1/UIDE-Q-TMCSE-2022-13.pdf

Scarfone, K., Dicoi, D., Sexton, M. y Tibbs, C. (2008). Guide to Securing Legacy IEEE 802.11 Wireless Networks. Special Publication (NIST SP) - 800-48 Rev 1, *National Institute of Standards and Technology*, https://doi.org/10.6028/NIST.SP.800-48r1 (Accessed March 20, 2025)

Statista. (2023). *Number of data breaches reported in the United States from 2005 to 2023*. https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/

Teltonika. (2024). *Qué elegir: Red por cable o inalámbrica.* https://teltonika-networks.com/es/newsroom/which-one-to-choose-wired-or-wireless-network

Consejo de la Unión Europea. (2016). Reglamento 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX :32016R0679&from=ES

Vadavo. (2024). *Protocolos de seguridad inalámbrica: WEP, WPA, WPA2 y WPA3.* https://www.vadavo.com/blog/protocolos-seguridad-inalambrica-wep-wpa-wpa2-wpa3/

Valderrama Guardia, J. E. (2017). *Pentesting "prueba de penetración" para la identificación de vulnerabilidades en la red de computadoras en la alcaldía del municipio de cantón del san pablo, departamento del chocó.* [Tesis de maestría, Universidad Nacional Abierta y a Distancia (UNAD), Quibdó -Colombia]. https://repository.unad.edu.co/bitstream/handle/10596/18049/1077436201.pdf?sequence=1&isAllowed=y

ANEXOS

Anexo A: Política de uso de la red WIFI

GAD Parroquial en la Provincia de Imbabura.

1. Introducción

Esta política define el uso aceptable y seguro de la red Wi-Fi del GAD Parroquial en la Provincia de Imbabura. Su objetivo es proteger la confidencialidad, integridad y disponibilidad de la información institucional, y asegurar el cumplimiento legal y regulatorio. Esta política está alineada con el control 1.10 "Uso aceptable de la información y otros activos asociados" del EGSI MINTEL.

2. Alcance

Aplica a todos los usuarios de la red Wi-Fi, incluyendo funcionarios, empleados, contratistas, consultores y visitantes.

3. Uso Aceptable

La red Wi-Fi se proporciona para:

- Acceso a información necesaria para las funciones laborales.
- Comunicación electrónica oficial.
- Investigación y desarrollo profesional relacionados con la Institución.

4. Prohibiciones

- Actividades ilegales.
- Acceso, descarga o distribución de material inapropiado (pornográfico, racista, etc.).
- Actividades que dañen o comprometan la seguridad de la red.
- Uso de la red para fines personales que impacten negativamente en la productividad.
- Compartir credenciales de acceso.
- Eludir medidas de seguridad.
- Acceder a información no autorizada.
- Enviar spam.
- Descarga de software no autorizado.
- Utilizar servicios de correo electrónico de libre uso tales como: Gmail, Hotmail, Yahoo, entre otros, para el envío de información sensible.

5. Seguridad

- Los usuarios son responsables de proteger sus credenciales.
- Reportar incidentes de seguridad al Presidente de la Junta Parroquial o a la Secretaria Tesorera.

- La Institución monitorea la red para asegurar el cumplimiento de esta política.
- Se implementan medidas de seguridad: firewalls, IDS/IPS, antivirus.
- Se utiliza WPA2 para la seguridad de la red inalámbrica.
- Se segmenta la red.
- Autenticación de dos factores (si es posible y aplicable).

6. Red Wi-Fi para Invitados

- Puede existir una red Wi-Fi separada para invitados, con términos y condiciones específicos y acceso restringido a recursos internos.
- El WIFI para invitados debe tener al menos las mismas restricciones que el WiFi para el personal, a fin de desalentar el uso del WiFi de invitados por parte del personal.

7. Monitoreo y Auditoría

La Institución se reserva el derecho de monitorear y auditar el uso de la red. El acceso a los contenidos monitoreados es potestad del Presidente de la Junta Parroquial o, en su ausencia, de la Secretaria Tesorera.

8. Cumplimiento

El incumplimiento puede resultar en la suspensión del acceso a la red y/o acciones disciplinarias.

9. Responsabilidades

- **Presidente de la Junta Parroquial:** Aprobación, implementación, mantenimiento y actualización de esta política; respuesta inicial a incidentes.
- **Secretaria Tesorera:** Colaboración en la implementación y mantenimiento de la política; respuesta a incidentes en ausencia del Presidente.
- **Usuarios:** Cumplimiento de la política; reporte de incidentes.

10. Revisiones

Esta política se revisará al menos anualmente o cuando sea necesario.

11. Aprobación

Aprobada por el Presidente de la Junta Parroquial el 14 de marzo de 2025.

_____	_____
Firma	Firma
Presidente de la Junta Parroquial	Secretaria Tesorera

Anexo B: Política de Contraseñas

GAD Parroquial de la Provincia de Imbabura.

1. Introducción

Esta política define los requisitos para la creación, uso y gestión de contraseñas en el GAD Parroquial de la Provincia de Imbabura. Su objetivo es proteger la confidencialidad, integridad y disponibilidad de la información. Esta política está alineada con el control 1.17 “Información de autenticación” del EGSI.

2. Alcance

Aplica a todos los usuarios de los sistemas de información de la Institución.

3. Requisitos de las Contraseñas

Complejidad:

- Longitud mínima: 16 caracteres.
- Caracteres de al menos tres de las siguientes categorías: mayúsculas, minúsculas, números, símbolos.
- No información personal fácil de obtener.
- No palabras del diccionario.

Unicidad

- No reutilizar contraseñas anteriores.
- No usar la misma contraseña en distintos sistemas.

4. Gestión de Contraseñas

- **Asignación Inicial:** Cambiar contraseñas predeterminadas inmediatamente. Verificar la identidad antes de proporcionar información de autenticación. Transmitir información de autenticación de manera segura.
- **Cambio Periódico:** Cambiar contraseñas al menos cada 90 días y si se sospecha compromiso.

- **Almacenamiento:** Almacenar contraseñas de forma protegida (cifrado y hashing).
- **Sistema de Gestión de Contraseñas:** Permitir seleccionar y cambiar contraseñas, aplicar contraseñas seguras, obligar a cambiar contraseñas en el primer inicio de sesión, evidenciar la responsabilidad de buen uso, evitar la reutilización, evitar contraseñas comunes, no mostrar contraseñas al ingresarlas.

5. Responsabilidades del Usuario

- Mantener la confidencialidad de la contraseña.
- Cambiar la contraseña si se sospecha compromiso.
- Seleccionar contraseñas seguras.
- No utilizar la misma contraseña en distintos sistemas.
- Evidenciar la responsabilidad de buen uso y que es secreta e intransferible

6. Sanciones

El incumplimiento puede resultar en la suspensión del acceso y/o acciones disciplinarias.

7. Excepciones

Requieren la aprobación del Presidente de la Junta Parroquial.

8. Revisión

Se revisará al menos anualmente.

9. Aprobación

Aprobada por el Presidente de la Junta Parroquial el [Fecha].

_____	_____
Firma	Firma
Presidente de la Junta Parroquial	Secretaria Tesorera

Anexo C: Política de Segmentación de la Red

GAD Parroquial en la Provincia de Imbabura

1. Introducción

Esta política define la segmentación de la red del GAD Parroquial. El objetivo es mejorar la seguridad, el rendimiento y la gestión de la red. Esta política está alineada con el control 4.22 "Separación en las redes" del EGSI.

2. Alcance

Aplica a todos los dispositivos, sistemas y usuarios conectados a la red de la Institución.

3. Principios de Segmentación

- Niveles de Confianza.
- Criticidad de la Información.
- Sensibilidad de la Información.
- Roles y Responsabilidades.
- Requisitos de Cumplimiento.

4. Dominios de Segmentación

- Dominio Público (Invitados).
- Dominio de Escritorio (Usuarios).
- Dominio de Servidores.

5. Métodos de Segmentación

- Redes Físicamente Separadas.
- Redes Lógicas (VLANs).
- Firewalls.
- Listas de Control de Acceso (ACLs).
- Autenticación y Autorización.

6. Control de Acceso entre Dominios

- Control en el perímetro mediante puerta de enlace (firewall, enrutador).
- Criterios basados en requisitos de seguridad y evaluación de riesgos.

7. Redes Inalámbricas

- Ajustar la cobertura de radio.
- Considerar tratar accesos inalámbricos como conexiones externas.
- Separar redes inalámbricas para invitados y personal.

8. Responsabilidades

- **Presidente de la Junta Parroquial:** Aprobación e implementación.
- **Secretaria Tesorera:** Colaboración en la implementación y mantenimiento.
- **Usuarios:** Cumplimiento y uso adecuado.

9. Cumplimiento

El incumplimiento puede resultar en la suspensión del acceso y/o acciones disciplinarias.

10. Revisión

Se revisará al menos anualmente.

11. Aprobación

Aprobada por el Presidente de la Junta Parroquial el 14 de marzo de 2025.

_____	_____
Firma	Firma
Presidente de la Junta Parroquial	Secretaria Tesorera

Anexo D: Política de Acceso Remoto Seguro

GAD Parroquial en la Provincia de Imbabura.

1. Introducción

Esta política define los requisitos para el acceso remoto seguro a los sistemas de información del GAD Parroquial. El objetivo es proteger la información institucional. Esta política está alineada con el control 6.2.2 "Control de acceso seguro a la red" del EGSI.

2. Alcance

Aplica a todos los usuarios que acceden remotamente a los sistemas de información de la Institución.

3. Requisitos Generales

- Autorización: Acceso solo para usuarios autorizados con necesidad legítima.
- Autenticación Fuerte: MFA (Autenticación Multifactor) requerida.
- Dispositivos Gestionados: Acceso solo desde dispositivos gestionados.
- Conexiones Seguras: Uso de VPN o protocolos cifrados.
- Principio de Mínimo Privilegio: Acceso solo a recursos necesarios.
- Registro y Monitoreo: Registro de la actividad de acceso remoto.

4. Dispositivos Permitidos

- Dispositivos Propiedad de la Institución: Antivirus, firewall personal, cifrado de disco, políticas de contraseñas, actualizaciones de seguridad.
- Dispositivos Personales (BYOD): Aceptar política BYOD, cumplir requisitos mínimos de seguridad, auditorías de seguridad.

5. Métodos de Acceso Remoto

- Red Privada Virtual (VPN): Requerida para acceso a la red interna, con protocolo de cifrado fuerte.
- Escritorio Remoto: Solo para aplicaciones específicas, con controles de acceso estrictos.
- Acceso Basado en Web: Solo a través de portales seguros y cifrados.

6. Políticas de Contraseñas

- Cumplir Política de Contraseñas de la Institución.
- Cambio periódico de contraseñas.
- Recomendación de administrador de contraseñas.

7. Seguridad de los Dispositivos

- Responsabilidad del usuario de proteger contra malware.
- Reportar incidentes de seguridad.
- Protección física contra robo o pérdida.
- Protección contra accesos no autorizados.

8. Responsabilidades

- **Presidente de la Junta Parroquial:** Aprobación e implementación.
- **Secretaria Tesorera:** Colaboración en la implementación y mantenimiento.
- **[Proveedor de Servicios de TI (si aplica)]:** Configuración y mantenimiento de la infraestructura.
- **Usuarios:** Cumplimiento y protección de dispositivos y credenciales.

9. Cumplimiento

El incumplimiento puede resultar en la suspensión del acceso y/o acciones disciplinarias.

10. Revisión

Se revisará al menos anualmente.

11. Aprobación

Aprobada por el Presidente de la Junta Parroquial el 14 de marzo de 2025.

_____	_____
Firma	Firma
Presidente de la Junta Parroquial	Secretaria Tesorera

Anexo E: Procedimientos de Gestión de la Seguridad de la Información y Redes Inalámbricas.

GAD Parroquial en la Provincia de Imbabura.

Objetivo: Establecer procedimientos claros y estandarizados para la gestión de la seguridad de la información y las redes inalámbricas en el GAD Parroquial, protegiendo los activos de información y minimizando los riesgos, especialmente aquellos relacionados con el acceso inalámbrico.

Alcance: Aplica a todos los equipos, sistemas y redes del GAD Parroquial, incluyendo computadoras de escritorio, laptops, equipos de red (router, switch, puntos de acceso Unifi) y la información digital almacenada.

Activos Clave:

- Computadoras de escritorio y portátiles (con información administrativa, financiera y de gestión).
- Equipos de red (router del proveedor, switch, puntos de acceso inalámbricos Ubiquiti Unifi).
- Información digital almacenada en estos equipos (documentos, etc.).
- Controladora Unifi (para la gestión de la red inalámbrica).

Procedimientos Específicos:

1. Seguridad de la Red Inalámbrica (Ubiquiti Unifi):

1.1. Configuración Inicial Segura:

- Cambiar las credenciales predeterminadas de la controladora Unifi y de los puntos de acceso.
- Habilitar el acceso HTTPS a la controladora Unifi.
- Configurar el firewall de la controladora Unifi para permitir solo el tráfico necesario.

1.2. Autenticación Robusta:

- Implementar WPA3 (si todos los dispositivos son compatibles) o WPA2-AES con una contraseña robusta (mínimo 14 caracteres, combinando mayúsculas, minúsculas, números y símbolos).
- Considerar la implementación de autenticación 802.1X con un servidor RADIUS para una autenticación más segura, especialmente para el personal. Esto permite la autenticación basada en credenciales de usuario individuales en lugar de una contraseña compartida.
- Para la red de invitados, utilizar un portal cautivo con autenticación mediante un código de acceso temporal o credenciales de redes sociales (con las debidas consideraciones de privacidad).

1.3. Segmentación de la Red Inalámbrica:

- Crear VLANs separadas para la red del personal y la red de invitados.
- Configurar reglas de firewall para restringir el acceso entre las VLANs. La red de invitados debe tener acceso limitado a los recursos internos.
- Utilizar la función de "Guest Control" de Unifi para aislar a los clientes de la red de invitados entre sí.

1.4. Control de Acceso Inalámbrico (NAC - Network Access Control):

Si la controladora Unifi lo permite, implementar políticas de NAC para verificar el estado de seguridad de los dispositivos antes de permitirles el acceso a la red. Esto puede incluir la verificación de la presencia de antivirus actualizado y la conformidad con las políticas de seguridad.

1.5. Monitoreo y Alertas:

- Configurar alertas en la controladora Unifi para detectar actividades sospechosas, como intentos de intrusión o conexiones no autorizadas.
- Revisar periódicamente los registros de la controladora Unifi para identificar posibles problemas de seguridad.

1.6. Actualizaciones de Firmware:

- Mantener el firmware de la controladora Unifi y de los puntos de acceso actualizados con las últimas versiones de seguridad.
- Programar las actualizaciones durante las horas de menor actividad para minimizar el impacto en los usuarios.

1.7. Control de Potencia de Transmisión:

Ajustar la potencia de transmisión de los puntos de acceso para cubrir solo el área necesaria, minimizando la señal que se extiende fuera del GAD Parroquial y reduciendo el riesgo de acceso no autorizado desde el exterior.

1.8. Deshabilitar Servicios Innecesarios:

Deshabilitar cualquier servicio innecesario en la controladora Unifi y en los puntos de acceso para reducir la superficie de ataque.

2. Configuración del Router del Proveedor:

2.1. Cambio de Credenciales Predeterminadas: Cambiar inmediatamente el nombre de usuario y la contraseña predeterminados del router proporcionado por el proveedor de servicios de Internet (ISP).

2.2. Firewall: Activar el firewall integrado en el router y configurar reglas básicas para permitir solo el tráfico necesario.

2.3. Actualizaciones de Firmware: Verificar regularmente si hay actualizaciones de firmware disponibles para el router y aplicarlas para corregir vulnerabilidades de seguridad.

2.4. Deshabilitar la Administración Remota: Deshabilitar la administración remota del router a menos que sea absolutamente necesario y se tomen medidas de seguridad adicionales.

2.5. DMZ (Zona Desmilitarizada): Evitar el uso de la DMZ a menos que sea absolutamente necesario. Si se utiliza, asegurarse de que solo se expongan los servicios estrictamente necesarios.

3. Seguridad de las Computadoras de Escritorio y Portátiles:

3.1. Antivirus y Anti-Malware: Instalar y mantener actualizado un software antivirus y anti-malware en todas las computadoras.

3.2. Firewall Personal: Activar el firewall personal en todas las computadoras.

3.3. Actualizaciones del Sistema Operativo y Software: Mantener el sistema operativo y todo el software actualizado con las últimas versiones de seguridad.

3.4. Políticas de Contraseñas: Implementar una política de contraseñas robusta (mínimo 12 caracteres, combinando mayúsculas, minúsculas, números y símbolos) y exigir el cambio periódico de contraseñas.

3.5. Cifrado de Disco: Habilitar el cifrado de disco completo en las computadoras portátiles para proteger los datos en caso de robo o pérdida.

3.6. Control de Acceso: Limitar los derechos de administrador a los usuarios que realmente los necesiten.

3.7. Concienciación y Formación: Proporcionar formación y concienciación sobre seguridad a todos los empleados, incluyendo la identificación de correos electrónicos de phishing, el uso seguro de la web y la protección de la información confidencial.

4. Gestión de la Información Digital:

4.1. Clasificación de la Información: Clasificar la información según su sensibilidad (pública, confidencial, etc.).

4.2. Control de Acceso a la Información: Implementar controles de acceso para restringir el acceso a la información confidencial solo a los usuarios autorizados.

4.3. Copias de Seguridad (Backups): Realizar copias de seguridad periódicas de la información crítica y almacenarlas en un lugar seguro, preferiblemente fuera de las instalaciones.

4.4. Destrucción Segura de la Información: Implementar procedimientos para la destrucción segura de la información que ya no es necesaria, utilizando métodos como la trituración de documentos o el borrado seguro de discos duros.

5. Monitorización y Respuesta a Incidentes:

5.1. Monitorización de la Red: Implementar herramientas de monitorización de la red para detectar actividades sospechosas.

5.2. Plan de Respuesta a Incidentes: Desarrollar un plan de respuesta a incidentes para abordar los incidentes de seguridad de forma rápida y eficaz.

5.3. Notificación de Incidentes: Establecer un procedimiento para que los empleados notifiquen los incidentes de seguridad.

6. Responsabilidades:

- Presidente del GAD Parroquial, secretaria tesorera y funcionarios.

7. Documentación:

- Documentar todos los procedimientos y configuraciones de seguridad.
- Mantener un registro de todos los incidentes de seguridad.

8. Revisión:

- Revisar los procedimientos de seguridad periódicamente para asegurar su efectividad.
- Actualizar los procedimientos de seguridad en respuesta a nuevas amenazas y vulnerabilidades.

_____	_____
Firma	Firma
Presidente de la Junta Parroquial	Secretaria Tesorera

Anexo F: Instructivo para Utilizar AIRCRACK _NG

Paso 1: Preparativos

1. Instala Aircrack-ng si aún no lo tienes instalado. Puedes hacerlo en sistemas basados en Debian/Ubuntu con:
2. sudo apt-get update
3. sudo apt-get install aircrack-ng
4. Verifica tu tarjeta de red ejecutando el comando:
5. iwconfig

Asegúrate de que tu tarjeta esté en modo monitor. Este modo es necesario para capturar paquetes de red.

Paso 2: Poner la interfaz en modo monitor

Reemplaza wlan0 con el nombre de tu interfaz de red. Puedes usar ifconfig o iwconfig para obtener el nombre correcto de tu interfaz.

sudo airmon-ng start wlan0

Esto creará una interfaz nueva (generalmente wlan0mon).

Paso 3: Escanear redes

Utiliza el siguiente comando para escanear las redes disponibles:

sudo airodump-ng wlan0mon

Esto mostrará una lista de redes WiFi y dispositivos asociados, incluyendo información sobre el BSSID (la dirección MAC del punto de acceso), el canal, la potencia de la señal, y el tipo de cifrado.

Paso 4: Ver detalles de una red específica

Identifica la red que deseas analizar y toma nota del BSSID y del canal. Luego, ejecuta el siguiente comando para capturar paquetes de esa red:

sudo airodump-ng --bssid <BSSID> -c <CANAL> -w <nombre_archivo> wlan0mon

Reemplaza <BSSID> por la dirección MAC de la red de interés, <CANAL> por el canal en el que opera la red, y <nombre_archivo> por el nombre del archivo en el que quieres guardar los datos capturados.

Paso 5: Capturar paquetes de autenticación (opcional)

Si tienes acceso al dispositivo y deseas intentar capturar el handshake (un proceso de autenticación), puedes intentar desautenticar a un cliente conectado a la red:

sudo aireplay-ng --deauth 10 -a <BSSID> wlan0mon

Esto enviará paquetes de desautenticación, provocando que el cliente se desconecte y se vuelva a conectar, lo que te permitirá capturar el handshake.

Paso 6: Uso de Aircrack-ng

Una vez que hayas capturado el handshake y lo hayas almacenado en un archivo, puedes usar Aircrack-ng para intentar descifrar la contraseña:

aircrack-ng <nombre_archivo>.cap -w <ruta/a/tu/diccionario.txt>

Reemplaza <nombre_archivo>.cap con el archivo guardado y <ruta/a/tu/diccionario.txt> con la ubicación del archivo de diccionario que deseas utilizar para el ataque.