UNIVERSIDAD ESTATAL DE BOLÍVAR

FACULTAD DE CIENCIAS ADMINISTRATIVAS, GESTIÓN EMPRESARIAL E INFORMÁTICA

CARRERA DE SOFTWARE

TRABAJO DE INTEGRACIÓN CURRICULAR
PREVIO A LA OBTENCIÓN DEL TÍTULO DE
INGENIERO EN SOFTWARE

FORMA: PROYECTO DE INVESTIGACIÓN

TEMA:

VULNERABILIDADES EN REDES WI-FI DE LA UNIVERSIDAD ESTATAL DE BOLÍVAR, EN EL AÑO 2025

AUTOR:

CRISTIAN JOSUE GARÓFALO YÁNEZ

DIRECTOR:

ING. RODRIGO DEL POZO DURANGO

GUARANDA – ECUADOR

2025

TEMA DEL PROYECTO DE INVESTIGACIÓN

VULNERABILIDADES EN REDES WI-FI DE LA UNIVERSIDAD ESTATAL DE BOLÍVAR, EN EL AÑO 2025

AGRADECIMIENTO

Expreso mi agradecimiento al Ingeniero Rodrigo Del Pozo, director de este trabajo de investigación, cuya experiencia fueron fundamentales durante cada etapa del proyecto.

De manera muy especial, agradezco al Ingeniero Edgar Rivadeneira, quien se consolidó como un pilar clave en este proceso. Su paciencia, dedicación constante y compromiso para orientarme marcaron una gran diferencia en la construcción de este trabajo. Su apoyo incondicional fue esencial para superar cada dificultad.

También quiero reconocer a la Ingeniera Galuth García, cuya influencia trasciende lo académico. Ella me enseñó que, a pesar de cualquier obstáculo, rendirse no es una opción y que siempre debemos dar el 100% de nosotros mismos. Sus lecciones de perseverancia y fortaleza quedaron grabadas en mí y fueron un motor crucial para culminar este reto.

Igualmente, extiendo mi agradecimiento al Ingeniero Cristian Barragán, quien no solo aportó sus conocimientos y sugerencias académicas, sino que fue una constante fuente de motivación. Sus palabras de aliento y su confianza me impulsaron a mantenerme firme en mis metas.

Cristian Garófalo Yánez

DEDICATORIA

Dedico este trabajo, en primer lugar, a mi Padre Celestial, por guiarme, fortalecerme y brindarme la sabiduría necesaria para llegar hasta aquí.

A mi madre, Cruz Yánez, y a mi padre, Gonzalo Garófalo, por su esfuerzo, constancia y sacrificio, que han sido fundamentales para alcanzar esta meta. Sin su apoyo incondicional, este logro no habría sido posible. A mi tía, Liliana Yánez, quien se ha convertido en una segunda madre para mí, y cuyo cariño, consejos y presencia han sido un gran respaldo a lo largo de este camino.

A mis hermanos, en especial a mi hermanita Juley por estar siempre ahí, brindándome ánimo y compañía en los momentos que más lo necesité.

Y, por último, a mi fiel compañero, mi gato Naruto, quien con su silenciosa compañía estuvo a mi lado en los momentos más difíciles, recordándome que incluso en la soledad, nunca estuve solo.

Cristian Garófalo Yánez

CERTIFICADO DE VALIDACIÓN

UNIVERSIDAD ESTATAL DE BOLIVAR

FACULTAD DE CIENCIAS ADMINISTRATIVAS, GESTIÓN EMPRESARIAL E INFORMÁTICA

CERTIFICADO DE VALIDACIÓN

Ing. Rodrigo del Pozo, Lic. Edgar Rivadeneira e Ing. Christian Barragán, en su orden Director y Pares Académicos del Trabajo de Integración Curricular "VULNERABILIDADES EN REDES WI-FI DE LA UNIVERSIDAD ESTATAL DE BOLÍVAR, EN EL AÑO 2025" desarrollado por el señor Cristian Josue Garófalo Yánez.

CERTIFICAN

Que, luego de revisado el Trabajo de Integración Curricular en su totalidad, cumple con las exigencias académicas de la carrera SOFTWARE, por lo tanto, autorizamos su presentación y defensa.

Guaranda, 25 de agosto del 2025

Rodrigo Humberto Del Pozo Durango
Time Stamping Security Data
Ing. Rodrigo del Pozo
Director

EDGAR PATRICIO RIVADENEIRA RAMOS
Lic. Edgar Rivadeneira
Par Académico

CHRISTIAN FERNANDO BARRAGAN QUIZHPE
Ing. Christian Barragán
Par Académico

Dirección: Av. Ernesto Che Guevara y Gabriel Secaira
Guaranda-Ecuador
Teléfono: (593) 3220 6059
www.ueb.edu.ec

DERECHOS DE AUTOR

UEB | UNIVERSIDAD ESTATAL DE BOLIVAR

BIBLIOTECA GENERAL

DERECHOS DE AUTOR

Yo **Cristian Josue Garófalo Yánez** portador de la Cédula de Identidad **0250308228** en calidad de autor y titular de los derechos morales y patrimoniales del Trabajo de Titulación: **Vulnerabilidades en redes Wi-Fi de la Universidad Estatal de Bolívar, en el año 2025**, modalidad **Proyecto de Investigación**, de conformidad con el Art. 114 del CÓDIGO ORGÁNICO DE LA ECONOMÍA SOCIAL DE LOS CONOCIMIENTOS, CREATIVIDAD E INNOVACIÓN, concedemos a favor de la Universidad Estatal de Bolívar, una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos. Conservamos a mi/nuestro favor todos los derechos de autor sobre la obra, establecidos en la normativa citada.

Así mismo, autorizo a la Universidad Estatal de Bolívar, para que realice la digitalización y publicación de este trabajo de titulación en el Repositorio Digital, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

El autor declara que la obra objeto de la presente autorización es original en su forma de expresión y no infringe el derecho de autor de terceros, asumiendo la responsabilidad por cualquier reclamación que pudiera presentarse por esta causa y liberando a la Universidad de toda responsabilidad.

Cristian Josue Garófalo Yánez
C.I: 0250308228

Dirección: Av. Ernesto Che Guevara y Gabriel Secaira
Guaranda-Ecuador
Teléfono: (593) 3220 6059
www.ueb.edu.ec

ÍNDICE DE CONTENIDO

TEMA DEL PROYECTO DE INVESTIGACIÓN i

AGRADECIMIENTO ii

DEDICATORIA iii

CERTIFICADO DE VALIDACIÓN iv

DERECHOS DE AUTOR v

ÍNDICE DE CONTENIDO vi

ÍNDICE DE TABLAS ix

ÍDICE DE FIGURAS x

INTRODUCCIÓN 1

RESUMEN 3

SUMILLA 4

ABSTRACT 5

CAPÍTULO I 6

FORMULACIÓN GENERAL DEL PROYECTO 6

1.1. Descripción del Problema 6

1.2. Formulación del Problema 7

1.3. Preguntas de Investigación 7

1.4. Justificación 7

1.5. Objetivos: 8

1.6. Idea a Defender 8

CAPÍTULO II 9

MARCO TEÓRICO 9

2.1. Antecedentes 9

2.2. Científico 10

2.3. Conceptual 11

2.4. Legal 14
2.5. Georreferencial 21
CAPITULO III 22
METODOLOGÍA 22
3.1. Tipo de Investigación 22
3.2. Enfoque de la investigación 22
3.3. Métodos de Investigación 22
3.4. Técnicas e instrumentos de recopilación de datos 23
3.5. Universo, Población y Muestra 24
3.6. Procesamiento de la Información 24
CAPITULO IV 26
RESULTADOS Y DISCUSIÓN 26
4.1. Análisis entrevista no estructurada 26
4.2. Análisis encuesta 28
4.3. Discusión de Resultados 47
CAPITULO V 54
PROPUESTA 54
PLAN DE MITIGACIÓN DE VULNERABILIDADES EN LA RED WI-FI DE LA UNIVERSIDAD ESTATAL DE BOLÍVAR 54
5.1. Introducción 54
5.2. Objetivos 54
5.2.1. Objetivo General 54
5.2.2. Objetivos Específicos 55
5.3. Metodología 55
5.3.1. Fases del proyecto 55
5.3.2. Estándares y Marcos de Referencia 56

5.3.3. Herramientas y Técnicas de Análisis 57
5.4. Plan de Mitigación Detallado..... 57
5.7. Indicadores Clave de Rendimiento (KPIs)..... 73
5.8. Conclusiones 75
5.9. Recomendaciones..... 75
CONCLUSIONES 76
RECOMENDACIONES 77
BIBLIOGRAFÍA..... 78
ANEXOS..... 82

ÍNDICE DE TABLAS

Tabla 1 Distribución de protocolos IP en la red institucional 28

Tabla 2 Protocolos de encriptación Wi-Fi implementados en la Universidad Estatal de Bolívar 29

Tabla 3 Implementación de segmentación VLAN en la red Wi-Fi institucional.. 30

Tabla 4 Sistemas operativos implementados en los puntos de acceso Wi-Fi universitarios 31

Tabla 5 Implementación de Client Isolation en la red Wi-Fi institucional 33

Tabla 6 métodos de autenticación empleado para el acceso a la red Wi-Fi..... 35

Tabla 7 filtración por direcciones MAC en la red..... 36

Tabla 8 red Wi-Fi separada para visitantes 39

Tabla 9 frecuencia de intentos de intrusión en la red Wi-Fi 40

Tabla 10 herramientas para registrar o gestionar incidentes de seguridad..... 41

Tabla 11 auditorías de seguridad Wi-Fi 42

Tabla 12 ataques detectados o posibles en la red Wi-Fi 44

Tabla 13 Capacitación del personal técnico en seguridad Wi-Fi..... 46

ÍDICE DE FIGURAS

Gráfico 1 Distribución de protocolos IP en la red institucional 28

Gráfico 2 Protocolos de encriptación Wi-Fi implementados en la Universidad Estatal de Bolívar 29

Gráfico 3 Implementación de segmentación VLAN en la red Wi-Fi institucional30

Gráfico 4 Sistemas operativos implementados en los puntos de acceso Wi-Fi universitarios 32

Gráfico 5 Implementación de Client Isolation en la red Wi-Fi institucional 34

Gráfico 6 método de autenticación empleado para el acceso a la red Wi-Fi 35

Gráfico 7 filtración por direcciones MAC en la red 36

Gráfico 8 red Wi-Fi separada para visitantes 39

Gráfico 9 frecuencia de intentos de intrusión en la red Wi-Fi 40

Gráfico 10 herramientas para registrar o gestionar incidentes de seguridad 41

Gráfico 11 auditorías de seguridad Wi-Fi 42

Gráfico 12 ataques detectados o posibles en la red Wi-Fi 44

Gráfico 13 Capacitación del personal técnico en seguridad Wi-FI 46

INTRODUCCIÓN

En la era digital actual, la conectividad se ha consolidado como un pilar fundamental para el funcionamiento y desarrollo de las instituciones educativas. La Universidad Estatal de Bolívar, como centro de conocimiento y formación, depende en gran medida de sus infraestructuras de red, siendo las redes Wi-Fi un componente crítico para el acceso a la información, la comunicación académica y la gestión administrativa. Sin embargo, esta dependencia inherente a la tecnología conlleva una exposición significativa a riesgos de ciberseguridad, lo que hace imperativo evaluar y mitigar las vulnerabilidades presentes en sus sistemas.

La proliferación de dispositivos conectados y la creciente sofisticación de las amenazas cibernéticas exigen un enfoque proactivo en la protección de la infraestructura de red. En este contexto, la presente investigación se enfoca en identificar y analizar las vulnerabilidades existentes en las redes Wi-Fi de la Universidad Estatal de Bolívar durante el año 2025. El interés de este estudio radica en la necesidad imperante de salvaguardar la integridad de los datos institucionales, la privacidad de la comunidad universitaria y la continuidad de los servicios educativos esenciales, frente a posibles ciberataques que podrían comprometer la reputación y las operaciones de la institución.

Para abordar esta problemática, la investigación empleará una metodología que permita diagnosticar el estado actual de la seguridad de las redes Wi-Fi, identificar las brechas de seguridad y proponer soluciones efectivas. El propósito principal es proporcionar un análisis exhaustivo de las vulnerabilidades y, a partir de este diagnóstico, plantear estrategias de mitigación que permitan fortalecer la infraestructura de red de la Universidad, asegurando un entorno digital más resiliente y seguro.

El presente documento se estructura en cinco capítulos:

En el **Capítulo I**, se establece el problema de investigación, se justifica su relevancia, y se definen tanto el objetivo general como los objetivos específicos que guían el estudio.

El **Capítulo II** presenta el marco teórico, donde se abordan los antecedentes relevantes, los conceptos clave relacionados con la seguridad de redes Wi-Fi y las normativas de seguridad aplicables.

En el **Capítulo III**, se detalla la metodología de investigación empleada, incluyendo el tipo y enfoque del estudio, así como las técnicas de recolección y procesamiento de datos utilizadas.

El **Capítulo IV** expone el diagnóstico de las vulnerabilidades identificadas en las redes Wi-Fi de la Universidad Estatal de Bolívar y presenta el análisis de los resultados obtenidos.

Finalmente, en el **Capítulo V**, se proponen las estrategias y recomendaciones específicas para la mitigación de las vulnerabilidades detectadas, orientadas a fortalecer la seguridad de la red Wi-Fi de la institución.

RESUMEN

En el presente estudio se analizan las vulnerabilidades en las redes Wi-Fi de la Universidad Estatal de Bolívar, proyectadas para el año 2025. A pesar de su uso generalizado, estas redes presentan vulnerabilidades inherentes que las convierten en un objetivo frecuente de ciberataques. Los problemas recurrentes incluyen el empleo de protocolos de seguridad obsoletos (como WEP y WPA), configuraciones incorrectas que utilizan contraseñas débiles o predeterminadas, y la falta de actualización del firmware de los puntos de acceso, exponiendo así los dispositivos a vulnerabilidades conocidas. La creciente interconexión de dispositivos IoT con medidas de seguridad inadecuadas amplía significativamente la superficie de ataque. En entornos educativos y organizacionales, la situación se agrava por la implementación de redes abiertas o mal configuradas, vulnerables a ataques como sniffing, phishing y man-in-the-middle, que facilitan la interceptación de información sensible. La ausencia de concienciación en los usuarios, la obsolescencia de hardware y software sin actualizaciones regulares, y la falta de auditorías periódicas y políticas de seguridad robustas contribuyen a un entorno inseguro, anticipando que la Universidad Estatal de Bolívar enfrentará desafíos similares, como el uso de cifrados anticuados, auditorías irregulares y la carencia de políticas de seguridad claras, lo que expondría a sus usuarios al robo de credenciales o ataques de intermediarios.

SUMILLA

Kay yachaypi rikurishka Wi-Fi ñetukunapa chinkaykuna, Universidad Estatal de Bolívarpi, 2025 watapi llankakushkakuna. Wi-Fi ñetukunaka, achka llaktakunapi usaykushka kashka karpi, chaykunapi wakin chinkaykuna charikushkan, chaymanta chaykunaka ciberataque ñawpak alli rikchaykuna tukurinkapakmi kashkan.

Rikurirkani wakin chinkaykunaka: seguridad ñawpak runashka protocolos (WEP, WPA) ñawpa shimikunawan llankay, mana allilla kamachishka, shimikuna llulla llankaywan, firmware mana kunanllami rurakushka puntos de acceso ñawpak. Kaymana, aparatokuna chay chinkaykuna rikcharinkapakmi kashkan.

IoT aparatokunaka, seguridad mana sinchilla charishka, ñawpak attacke rikcharinanta killkan. Yachay wasipi o institucionespi, chay ñetukunaka mana allilla configurashka kashkakuna, ñawpa riksishka attackekunawan: sniffing, phishing, man-in-the-middle, chaykunamanta allpa ñawpak shimikunata mana yaykuna runakuna chaskinkapakmi.

Runakunapika mana yuyaykuymi kashkan seguridadpi, wakin aparatomi ñawpa kashka, softwaremi mana kunankama rurashka. Mana kashkachu auditoría chaskikuna, mana kashkachu kamachiy sinchi ruraykuna. Chaymanta Universidad Estatal de Bolívarmi kunan watakunapi shuk kikinka chinkaykuna rikuchinkapakmi kashkan: cifrado ñawpa usay, mana siempre riksishka auditoríakunaka, mana kashkachu seguridad ñawpak kamachikuna. Kaykuna chaypi rurakunata chinkaymanta, chinkaykuna shimikunata llutakuyta, intermediario attacketa chaskinkapakmi chaskishkan.

ABSTRACT

Wi-Fi networks, despite their widespread use, exhibit inherent vulnerabilities that make them frequent targets for cyberattacks. Recurring issues include the employment of outdated security protocols (such as WEP and WPA), misconfigurations utilizing weak or default passwords, and the lack of firmware updates for access points, thereby exposing devices to known vulnerabilities. The increasing interconnection of IoT devices with inadequate security significantly broadens the attack surface. In educational and organizational settings, the situation is exacerbated by the implementation of open or poorly configured networks, vulnerable to attacks like sniffing, phishing, and man-in-the-middle, which facilitate the interception of sensitive information. The absence of user awareness, obsolete hardware and software lacking regular updates, and the lack of periodic audits and robust security policies contribute to an insecure environment. This study analyzes these conditions, anticipating that the Bolívar State University will face similar challenges, such as the use of antiquated encryption, irregular audits, and the lack of clear security policies, which would expose its users to credential theft or man-in-the-middle attacks.

CAPÍTULO I

FORMULACIÓN GENERAL DEL PROYECTO

1.1.Descripción del Problema

Las redes Wi-Fi, a pesar de ser una tecnología ampliamente utilizada en todo el mundo, tiene varias vulnerabilidades, que las convierten en un objetivo frecuente para ciberataques. Mora Zambrano (2024), uno de los principales problemas es el uso de protocolos de seguridad obsoletos, como WEP (Wired Equivalent Privacy) y WPA (Wi-Fi Protected Access), que son altamente vulnerables a ataques de sniffing y cracking. Estos protocolos permiten a los atacantes interceptar el tráfico de red y acceder a información sensible, como contraseñas, datos personales y comunicaciones confidenciales. Además, muchas redes Wi-Fi están mal configuradas, con contraseñas predeterminadas o débiles que pueden ser descifradas fácilmente mediante herramientas de fuerza bruta. Según Mora Zambrano (2024) señala que la falta de actualización en el firmware de los routers y puntos de acceso agrava el problema; los dispositivos quedan expuestos a vulnerabilidades conocidas que podrían ser corregidas con parches de seguridad. A esto se suma la creciente conectividad de dispositivos IoT (Internet de las Cosas), muchos de los cuales carecen de medidas de seguridad adecuadas, ampliando la superficie de ataque.

Las redes Wi-Fi, especialmente en entornos educativos y organizacionales, enfrentan desafíos en materia de seguridad cibernética debido a la implementación de protocolos de seguridad obsoletos, como WEP, y la proliferación de red abiertas o mal configurado son altamente vulnerables a ataques como:sniffing, phishing y de intermediario (man-in-the-middle), lo que permite a los atacantes interceptar información sensible, como credenciales de acceso, datos personales y comunicaciones confidenciales. Además, la falta de concienciación entre los usuarios, quienes a menudo priorizan la comodidad sobre la seguridad, agrava el problema, ya que muchos se conectan a redes inseguras sin utilizar medidas de protección como redes privadas virtuales (VPN) o autenticación de dos factores. El uso de hardware y software obsoleto, que no recibe actualizaciones regulares, exponiendo a las redes a vulnerabilidades conocidas que pueden ser explotadas por ciberdelincuentes. La ausencia de auditorías periódicas y políticas de seguridad

robustas también contribuye a crear un entorno inseguro, aumentando el riesgo de brechas de seguridad y comprometiendo la privacidad de los usuarios y la reputación de las instituciones.

En la Universidad Estatal Bolívar, es probable que las redes Wi-Fi se enfrenten a desafíos similares a los observados en otras instituciones educativas de la región. Es posible que las redes utilicen protocolos de cifrado anticuados o que no se lleven a cabo auditorías periódicas para identificar y corregir vulnerabilidades. La falta de políticas de seguridad claras y la posible ausencia de una autenticación sólida podrían exponer a los usuarios a riesgos como los ataques de intermediarios o el robo de credenciales.

1.2.Formulación del Problema

¿Cuáles son las principales vulnerabilidades en redes Wi-Fi de la Universidad Estatal de Bolívar?

1.3.Preguntas de Investigación

¿Qué tipos de vulnerabilidades son las más propensas en las redes Wi-Fi de la Universidad Estatal de Bolívar?

¿Qué protocolos de seguridad se aplican en la red Wi-Fi de la Universidad Estatal de Bolívar?

¿Qué medidas de seguridad se pueden aplicar para mitigar las vulnerabilidades identificadas en la Universidad Estatal de Bolívar?

1.4.Justificación

Las instituciones educativas, como las universidades, las redes Wi-Fi se han convertido en una infraestructura esencial para el desarrollo académico, la investigación y la gestión administrativa. Sin embargo, como señalan Espinosa, García & Llanos (2018), el uso masivo de redes inalámbricas en entornos universitarios ha generado nuevas oportunidades para accesos no autorizados, robo de información sensible e interrupciones del servicio, lo que representa un riesgo significativo para la integridad de los datos y la privacidad de la comunidad universitaria. Por ello, es fundamental implementar metodologías de seguridad avanzadas que permitan proteger estas redes y garantizar su funcionamiento óptimo.

La investigación de Mero Lino et al. (2021) destaca que, mediante el análisis de seguridad y la aplicación de protocolos y normas adecuadas, es posible mejorar la integridad de los datos y la protección de la información en redes inalámbricas. En el ámbito universitario, esto se traduce en un entorno más seguro para estudiantes, docentes y personal administrativo, quienes dependen de estas redes para acceder a recursos académicos, plataformas de aprendizaje y sistemas de gestión. Además, la implementación de prácticas como el hacking ético y auditorías de redes permite identificar vulnerabilidades

y proponer soluciones efectivas, contribuyendo a la creación de un ecosistema digital confiable.

Por otro lado, Carhuaz Malpartida (2021) resalta la importancia de utilizar herramientas y mecanismos de seguridad, como la encriptación avanzada y la autenticación robusta, para proteger las redes inalámbricas en entornos abiertos y de alto tráfico, como los campus universitarios. La adopción de estas medidas no solo mitiga riesgos, sino que también fomenta una cultura de seguridad entre los usuarios, promoviendo buenas prácticas como el uso de contraseñas seguras y la verificación de redes confiables.

línea de investigación:

1.5.Objetivos:

General

Identificar las vulnerabilidades en redes Wi-Fi en la Universidad Estatal de Bolívar.

Específicos

1. Evaluar el nivel de exposición a ataques externos e internos.
2. Proponer medidas de mejora para fortalecer la seguridad de la red Wi-Fi.

1.6.Idea a Defender

"Las redes Wi-Fi en entornos universitarios, como las de la Universidad Estatal de Bolívar, suelen enfrentar desafíos de seguridad que serían mitigados mediante la implementación de protocolos de seguridad avanzados y buenas prácticas de gestión de redes."

CAPÍTULO II

MARCO TEÓRICO

2.1. Antecedentes

En la actualidad, la seguridad informática en entornos laborales, educativos y otros ambientes es frecuentemente vulnerada debido a la complejidad de los sistemas y la diversidad de amenazas que pueden surgir en cualquier momento y lugar. Como señala Cataño García (2021) en su monografía Análisis y modelado de vulnerabilidades en redes inalámbricas, los sistemas informáticos son altamente complejos, y la responsabilidad de protegerlos se distribuye entre múltiples actores, a menudo con intereses en conflicto. Esto dificulta la implementación de medidas de seguridad efectivas y coherentes. Uno de los principales desafíos a nivel global es la seguridad en redes Wi-Fi, que dependen de ondas de radio electromagnéticas para transmitir datos. Estas redes son vulnerables a ataques que explotan puertos abiertos y protocolos de seguridad obsoletos, como WEP. Cataño García (2021) destaca que, mediante técnicas como el pentesting (pruebas de penetración), es posible identificar vulnerabilidades en etapas tempranas y diseñar métodos de prevención para blindar los sistemas de información. Sin embargo, la falta de concienciación y la proliferación de dispositivos inalámbricos mal configurados aumentan el riesgo de ataques como el sniffing, la interceptación de datos y la explotación de vulnerabilidades en protocolos de comunicación.

Además, el autor enfatiza la importancia de realizar un análisis detallado y diagnóstico de vulnerabilidades en comunicaciones inalámbricas, con el fin de identificar, proteger, detectar y responder a incidentes de seguridad. Este enfoque proactivo es esencial para garantizar la confidencialidad, integridad y disponibilidad de los datos transmitidos a través de redes Wi-Fi, especialmente en entornos donde la conectividad inalámbrica es fundamental, como en instituciones educativas y empresas.

En el contexto ecuatoriano, la seguridad de las redes Wi-Fi en instituciones educativas es un tema de creciente preocupación. Análisis de la vulnerabilidad del sistema de conexión a la red Wi-Fi genérica de un Instituto Educativo, muchos centros académicos del país ofrecen redes Wi-Fi abiertas sin sistemas de autenticación robustos, lo que expone a estudiantes, docentes y personal

administrativo a riesgos significativos, como la fuga de información y la suplantación de identidad.

Las redes Wi-Fi en entornos universitarios enfrentan desafíos comunes que pueden comprometer la seguridad de la información y la privacidad de los usuarios. Aunque no se cuenta con información específica sobre la infraestructura de red y las políticas de seguridad de la Universidad Estatal de Bolívar, es posible identificar problemas recurrentes en instituciones educativas similares, como la falta de actualización en los protocolos de seguridad, el uso de hardware obsoleto y la ausencia de auditorías periódicas. Estos problemas no solo exponen a la comunidad universitaria a riesgos como el robo de información, la interceptación de comunicaciones y los ataques de intermediario (man-in-the-middle), sino que también pueden tener consecuencias graves para la reputación de la institución y la confianza de los usuarios en sus sistemas.

2.2. Científico

Seguridad Informática

La seguridad informática es una disciplina esencial en el mundo digital actual, encargada de proteger los sistemas de cómputo y los datos que manejan. Según Cristiá (2021), en su tesis sobre seguridad informática, esta se define como "la rama de la informática que se encarga de estudiar cómo preservar la confidencialidad, integridad y disponibilidad de datos y programas en sistemas de cómputo" (p. 3). Estos tres atributos, conocidos como el modelo CID (Confidencialidad, Integridad, Disponibilidad), son la base de cualquier estrategia de seguridad.

Confidencialidad: Preservar la confidencialidad de los datos significa que solo los usuarios autorizados puedan ver dichos datos. Esto es especialmente relevante en redes Wi-Fi, donde la transmisión de datos a través de ondas de radio puede ser interceptada por atacantes si no se implementan medidas de encriptación adecuadas (Cristiá,2021, p. 3).

Integridad: Preservar la integridad de los datos y programas implica que solo los usuarios autorizados, y solo por los mecanismos autorizados, puedan modificar dichos datos y programas. En el contexto de redes, esto implica proteger los datos transmitidos contra modificaciones maliciosas, como las que ocurren en ataques de intermediario (man-in-the-middle) (Cristiá,2021, p. 3).

Disponibilidad: Preservar la disponibilidad de datos y programas significa que los usuarios autorizados puedan usar los datos y programas cada vez que los necesiten. En redes Wi-Fi, esto puede verse comprometido por ataques de denegación de servicio (DoS) que saturan la red y la hacen inaccesible (Cristiá,2021, p. 3).

1. Modelo de Gestión de Riesgos en Redes Inalámbricas

La seguridad en redes inalámbricas surge como una respuesta a la necesidad de proteger la información y los sistemas de posibles amenazas y vulnerabilidades. Cifuentes Rodríguez, (2017) en su investigación sobre la gestión de riesgos en redes inalámbricas, las empresas deben implementar metodologías adecuadas para reducir los riesgos asociados con el uso de estas tecnologías. Esto es especialmente relevante en entornos empresariales, donde la información es un activo crítico que debe protegerse contra accesos no autorizados, pérdidas o robos.

2. Hacking Ético:

El hacking ético es una práctica que se enmarca dentro de un movimiento más amplio dedicado a la producción de software libre y de código abierto (F/OSS, por sus siglas en inglés). Según Coleman (2019), en su libro Coding Freedom, los hackers no son simplemente individuos que explotan vulnerabilidades técnicas, sino que forman parte de una comunidad con valores éticos y políticos bien definidos. Esta comunidad se dedica a promover la libertad en el desarrollo de software, cuestionando las restricciones impuestas por las leyes de propiedad intelectual y defendiendo principios como la transparencia, la meritocracia y el acceso abierto al conocimiento.

2.3.Conceptual

Ataque de intermediario (Man-in-the-Middle, MITM): Técnica en la que un atacante intercepta y manipula la comunicación entre dos partes sin su conocimiento. En redes Wi-Fi, esto puede ocurrir cuando un usuario se conecta a una red falsa (evil twin) creada por el atacante (Ataques Man-in-the-Middle (MitM) y autenticación RADIUS).

Auditoría de seguridad: Evaluación sistemática de una red para identificar vulnerabilidades y proponer medidas correctivas. Incluye el uso de herramientas de análisis y pruebas de penetración (pentesting) (Transformación digital en Latinoamérica - OT Latam).

Autenticación: Proceso de verificar la identidad de un usuario o dispositivo antes de permitir el acceso a una red. Puede incluir métodos como contraseñas, certificados digitales o autenticación de dos factores (2FA) (¿Qué es la autenticación? Definición y métodos | Seguridad de Microsoft).

Cracking de contraseñas: Proceso de descifrar contraseñas mediante técnicas como la fuerza bruta o el uso de diccionarios. Las contraseñas débiles o predeterminadas son especialmente vulnerables a este tipo de ataques (¿Qué es un ataque de fuerza bruta? | Tipos y cómo funciona| Fortinet).

Encriptación: Proceso de convertir datos en un formato ilegible (cifrado) para protegerlos durante la transmisión. Solo los usuarios autorizados pueden descifrar la información utilizando una clave de encriptación. Ejemplos comunes incluyen AES y TKIP (Temporal Key Integrity Protocol) (Encriptación de datos: Métodos para la seguridad de la información).

Evil Twin (Gemelo Maligno): Red Wi-Fi falsa creada por un atacante para imitar una red legítima. Los usuarios que se conectan a esta red pueden ser víctimas de robo de información o ataques MITM (¿Qué es el ataque del gemelo malvado? Explicación del gemelo malvado de Wi-Fi).

Firewall: Sistema de seguridad que monitorea y controla el tráfico de red entrante y saliente, basado en reglas predefinidas. Ayuda a prevenir accesos no autorizados (Que es un Firewall - TI Rescue).

Hacking ético: Práctica de identificar vulnerabilidades en sistemas y redes con el permiso del propietario, con el objetivo de mejorar la seguridad. Es una herramienta clave en la auditoría de redes (¿Qué es el Hacking Ético? - TI Rescue).

MAC Address Filtering (Filtrado por Dirección MAC): Técnica de seguridad que permite o deniega el acceso a una red basándose en las direcciones MAC (Media Access Control) de los dispositivos. Sin embargo, esta medida puede ser eludida mediante técnicas de spoofing (Para qué sirve y cómo configurar el filtrado MAC en el router Wi-Fi).

Protocolo de seguridad: Conjunto de reglas y estándares diseñados para proteger la información transmitida a través de una red (Seguridad de Wi-Fi: WEP, WPA y WPA2). Los protocolos comunes en redes Wi-Fi incluyen:

- **WEP (Wired Equivalent Privacy):** Protocolo obsoleto y vulnerable a ataques de sniffing y cracking.
- **WPA (Wi-Fi Protected Access):** Mejora sobre WEP, pero aún presenta vulnerabilidades.
- **WPA2 (Wi-Fi Protected Access 2):** Introduce encriptación AES (Advanced Encryption Standard) y es más seguro que WPA.
- **WPA3 (Wi-Fi Protected Access 3):** Protocolo más reciente que ofrece encriptación avanzada y protección contra ataques de fuerza bruta.

Redes Wi-Fi (Wireless Fidelity): Tecnología que permite la conexión inalámbrica de dispositivos a una red local o a internet, utilizando ondas de radio para transmitir datos. Es ampliamente utilizada en entornos domésticos, empresariales y educativos debido a su facilidad de instalación y uso (¿Qué es el wifi?).

Rogue Access Point (Punto de Acceso No Autorizado): Dispositivo de red instalado en una infraestructura Wi-Fi sin autorización, que puede ser utilizado por atacantes para interceptar tráfico o realizar ataques (Puntos de Acceso Falsos: La Amenaza Invisible que Atraviesa el Aire - TI Rescue).

Sniffing: Técnica utilizada por atacantes para capturar y analizar el tráfico de red con el fin de obtener información sensible, como contraseñas o datos personales (¿Qué es un sniffer? Características y riesgos del sniffing).

SSID (Service Set Identifier): Nombre de una red Wi-Fi que permite a los usuarios identificarla y conectarse. Ocultar el SSID es una medida de seguridad básica, aunque no infalible (SSID de red: qué es, cómo encontrar el tuyo y cómo cambiarlo).

VPN (Red Privada Virtual): Tecnología que crea una conexión segura y encriptada entre un dispositivo y una red, protegiendo la información transmitida de posibles interceptaciones. Es especialmente útil en redes Wi-Fi públicas (¿Qué es una conexión VPN, para qué sirve y qué ventajas tiene?).

Vulnerabilidad: Debilidad o fallo en un sistema, red o dispositivo que puede ser explotado por un atacante para comprometer la seguridad. En el contexto de redes Wi-Fi, las vulnerabilidades pueden incluir protocolos obsoletos, contraseñas débiles o configuraciones incorrectas (Tipos de Vulnerabilidades y Amenazas informáticas).

2.4.Legal

No existe ningún impedimento que dificulte u obstaculice el avance de este proyecto de investigación.

CONSTITUCIÓN DE LA REPÚBLICA 2008

De acuerdo a la Constitución de la República del Ecuador (2008), se establece lo siguiente:

Artículo 16.- Todas las personas, en forma individual o colectiva, tienen derecho a:

1. Una comunicación libre, intercultural, incluyente, diversa y participativa, en todos los ámbitos de la interacción social, por cualquier medio y forma, en su propia lengua y con sus propios símbolos.
2. El acceso universal a las tecnologías de información y comunicación.
3. La creación de medios de comunicación social, y al acceso en igualdad de condiciones al uso de las frecuencias del espectro radioeléctrico para la gestión de estaciones de radio y televisión públicas, privadas y comunitarias, y a bandas libres para la explotación de redes inalámbricas.
4. El acceso y uso de todas las formas de comunicación visual, auditiva, sensorial y a otras que permitan la inclusión de personas con discapacidad.
5. Integrar los espacios de participación previstos en la Constitución en el campo de la comunicación;

Artículo 66.- Se reconoce y garantiza a las personas: (...)

19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley. (…)
21. El derecho a la inviolabilidad y al secreto de la correspondencia física y virtual; ésta no podrá ser retenida, abierta ni examinada, excepto en los casos previstos en la ley, previa intervención judicial y con la obligación de guardar el secreto de los asuntos ajenos al hecho que motive su examen. Este derecho protege cualquier otro tipo o forma de comunicación;

CÓDIGO ORGÁNICO INTEGRAL PENAL (COIP)

De acuerdo con el Código Orgánico Integral Penal (2014), los siguientes artículos abordan delitos relacionados con la tecnología y la información:

Artículo 178.- Violación a la intimidad. - La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años.

No son aplicables estas normas para la persona que divulgue grabaciones de audio y vídeo en las que interviene personalmente, ni cuando se trata de información pública de acuerdo con lo previsto en la ley;

Artículo 190.- Apropiación fraudulenta por medios electrónicos.- La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años. La misma sanción se impondrá si la infracción se comete con inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas o encriptadas, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes;

Artículo 194.- Comercialización ilícita de terminales móviles. - La persona que comercialice terminales móviles con violación de las disposiciones y procedimientos previstos en la normativa emitida por la autoridad competente de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años;

Artículo 229.- Revelación ilegal de base de datos. - La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros,

archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años. Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años;

Artículo 232.- Ataque a la integridad de sistemas informáticos. - La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años.

Con igual pena será sancionada la persona que:

1. Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo.
2. Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general.

Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad;

Artículo 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.- La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas

proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años;

LEY ORGANIZA DE PROTECCIÓN DE DATOS PERSONALES 2021

La Ley Orgánica de Protección de Datos Personales (2021) establece los siguientes principios y normativas:

Artículo 10.- Principios.

Sin perjuicio de otros principios establecidos en la Constitución de la República, los instrumentos internacionales ratificados por el Estado u otras normas jurídicas, la presente Ley se regirá por los principios de:

a) Juridicidad: El tratamiento de datos personales debe cumplir con la normativa vigente.

b) Lealtad y transparencia: Los datos personales deben ser tratados de manera clara y comprensible para sus titulares.

c) Seguridad de datos personales: Se deben implementar medidas técnicas y organizativas adecuadas para proteger los datos frente a cualquier riesgo, amenaza o vulnerabilidad.

Artículo 11.- Violación de datos personales.

Se considera una violación de datos personales cualquier incidente de seguridad que provoque su acceso no autorizado, alteración, pérdida o divulgación ilícita.

Artículo 17.- Responsabilidad en el tratamiento de datos.

Las entidades que procesan datos personales en redes Wi-Fi deben garantizar su protección y confidencialidad. Se deben aplicar medidas de ciberseguridad adecuadas para evitar el acceso indebido.

Artículo 25.- Seguridad en el tratamiento de datos.

Los responsables del tratamiento deberán aplicar medidas que garanticen la confidencialidad, integridad y disponibilidad de los datos almacenados y transmitidos en redes Wi-Fi, evitando posibles vulnerabilidades o ataques cibernéticos.

Artículo 34.- Derechos de los titulares frente a la seguridad de la información.

Toda persona tiene derecho a exigir que sus datos personales sean tratados con altos estándares de seguridad y a ser informada sobre cualquier vulnerabilidad que pueda comprometer su privacidad.

Artículo 50.- Sanciones por incumplimiento de medidas de seguridad.

El incumplimiento de normas de seguridad en el tratamiento de datos personales, incluyendo fallos en redes Wi-Fi que permitan accesos no autorizados, será sancionado de acuerdo con la gravedad del incidente.

LEY ORGÁNICA DE GESTIÓN DE LA IDENTIDAD Y DATOS CIVILES

De acuerdo con la Ley Orgánica de Gestión de la Identidad y Datos Civiles (2016),la normativa tiene los siguientes objetivos principales:

Artículo 3.- Objetivos. La presente Ley tiene como objetivos:

1. Asegurar el ejercicio del derecho a la identidad de las personas.
2. Precautelar la situación jurídica entre el Estado y las personas naturales dentro de sus relaciones de familia.
3. Proteger el registro de los hechos y actos relativos al estado civil de las personas.
4. Proteger la confidencialidad de la información personal.
5. Evitar el subregistro o carencia de datos en registro de una persona.
6. Proteger la información almacenada en archivos y bases de datos de los hechos y actos relativos al estado civil de las personas.
7. Propender a la simplificación, automatización e interoperabilidad de los procesos concernientes a los hechos y actos relativos al estado civil de las personas, de conformidad a la normativa legal vigente para el efecto

LEY ORGÁNICA DE TELECOMUNICACIONES

De acuerdo con la Ley Orgánica de Telecomunicaciones (2022), la normativa establece lo siguiente en sus disposiciones relacionadas con la seguridad y la privacidad:

Artículo 76.- Medidas técnicas de seguridad e invulnerabilidad. - Las y los prestadores de servicios ya sea que usen red propia o la de un tercero, deberán adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad de sus servicios y la invulnerabilidad de la red y garantizar el secreto de las comunicaciones y de la información transmitida por sus redes. Dichas medidas garantizarán un nivel de seguridad adecuado al riesgo existente;

Artículo 77.- Interceptaciones. - únicamente se podrán realizar interceptaciones cuando exista orden expresa de la o el Juez competente, en el marco de una investigación de un delito o por razones de seguridad pública y del Estado, de conformidad con lo que establece la ley y siguiendo el debido proceso;

Artículo 78.- Derecho a la intimidad. - para la plena vigencia del derecho a la intimidad, establecido en el artículo 66, numeral 20 de la Constitución de la República, las y los prestadores de servicios de telecomunicaciones deberán garantizar, en el ejercicio de su actividad, la protección de los datos de carácter personal. Para tal efecto, las y los prestadores de servicios de telecomunicaciones deberán adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad de su red con el fin de garantizar la protección de los datos de carácter personal de conformidad con la ley;

Artículo 79.- Deber de información. - en caso de que exista un riesgo particular de violación de la seguridad de la red pública o del servicio de telecomunicaciones, el prestador de servicios de telecomunicaciones deberá informar a sus abonados, clientes y usuarios sobre dicho riesgo y sobre las medidas a adoptar;

Artículo 82.- Uso comercial de datos personales. - Las y los prestadores de servicios no podrán usar datos personales, información del uso del servicio, información de tráfico o el patrón de consumo de sus abonados, clientes o usuarios para la promoción comercial de servicios o productos, a menos que el abonado o usuario al que se refieran los datos o tal información, haya dado su consentimiento previo y expreso. Los usuarios o abonados dispondrán de la posibilidad clara y fácil

de retirar su consentimiento para el uso de sus datos y de la información antes indicada. Tal consentimiento deberá especificar los datos personales o información cuyo uso se autorizan, el tiempo y su objetivo específico;

Artículo 84.- Entrega de información. - Las y los prestadores de servicios, entregarán a las autoridades competentes la información que les sea requerida dentro del debido proceso, con el fin de investigación de delitos. La Agencia de Regulación y Control de las Telecomunicaciones establecerá los mecanismos y procedimientos que sean necesarios;

Artículo 140.- Rectoría del sector. - El Ministerio encargado del sector de las Telecomunicaciones y de la Sociedad de la Información es el órgano rector de las telecomunicaciones y de la sociedad de la información, informática, tecnologías de la información y las comunicaciones y de la seguridad de la información. A dicho órgano le corresponde el establecimiento de políticas, directrices y planes aplicables en tales áreas para el desarrollo de la sociedad de la información, de conformidad con lo dispuesto en la presente Ley, su Reglamento General y los planes de desarrollo que se establezcan a nivel nacional. Los planes y políticas que dicte dicho Ministerio deberán enmarcarse dentro de los objetivos del Plan Nacional de Desarrollo y serán de cumplimiento obligatorio tanto para el sector público como privado.

2.5.Georreferencial



- **Latitud:** -1.5703384059520988
- **Longitud:** -79.00774104337646

CAPITULO III

METODOLOGÍA

3.1. Tipo de Investigación

La investigación no experimental descriptiva es un tipo de estudio que se enfoca en observar y describir fenómenos sin manipular variables. Su objetivo es analizar situaciones reales en su contexto natural, identificando características, comportamientos o problemas específicos. Este enfoque es ideal para investigaciones que buscan comprender un fenómeno tal como ocurre, sin intervenir en él.

En este estudio, se utiliza para describir las vulnerabilidades presentes en las redes Wi-Fi de la Universidad Estatal de Bolívar. No se realizan experimentos ni se manipulan variables, sino que se observa y analiza la situación actual de la red para identificar sus debilidades y proponer mejoras basadas en la evidencia recopilada.

3.2. Enfoque de la investigación

El enfoque mixto (cualitativo y cuantitativo) combina métodos de investigación cualitativos y cuantitativos para obtener una comprensión más completa del fenómeno estudiado. El enfoque cualitativo se centra en comprender contextos, percepciones y experiencias, mientras que el cuantitativo se basa en el análisis de datos numéricos para identificar patrones y tendencias.

En este estudio, el enfoque cualitativo se utiliza para analizar las percepciones, opiniones y criterios del personal de TI (Tecnologías de la Información), así como para revisar documentos relacionados con la seguridad de la red. El enfoque cuantitativo se emplea para obtener datos numéricos relacionados con estadísticas de vulnerabilidades o resultados de pruebas técnicas. La combinación de ambos enfoques permite un análisis completo y enriquecedor, integrando la profundidad del análisis cualitativo con la precisión de los datos cuantitativos.

3.3. Métodos de Investigación

Los métodos **inductivo y deductivo** son enfoques de razonamiento utilizados en investigación. El método inductivo parte de observaciones específicas para llegar a conclusiones generales, mientras que el deductivo aplica teorías o principios generales a casos específicos.

Como se aplicará dentro de la investigación

- **Inductivo:** Se parte de la observación de vulnerabilidades específicas en la red Wi-Fi de la universidad para llegar a conclusiones generales sobre las medidas de seguridad necesarias.
- **Deductivo:** Se aplican conceptos generales de ciberseguridad, como el modelo CID (Confidencialidad, Integridad, Disponibilidad), al caso específico de la Universidad Estatal de Bolívar. Esto permite evaluar si las prácticas actuales cumplen con los estándares de seguridad.

3.4. Técnicas e instrumentos de recopilación de datos

Las técnicas de recopilación de datos son herramientas y procedimientos utilizados para obtener información relevante para la investigación. Estas incluyen observación, encuestas y revisión documental.

Observación directa: Se analiza el comportamiento y desempeño de la red Wi-Fi de la universidad utilizando una lista de verificación (checklist) para identificar aspectos técnicos como protocolos implementados, políticas de contraseñas y configuraciones básicas de red, sin realizar pruebas intrusivas.

Entrevistas no estructuradas: Se realizan conversaciones abiertas con el Técnico responsable del área de redes, permitiendo explorar aspectos cualitativos, experiencias personales y desafíos no documentados en la gestión de la red Wi-Fi.

Encuestas: Se aplica un cuestionario estructurado al personal del área de redes y técnico de cada facultad para evaluar el funcionamiento actual de la red en cuanto a: seguridad implementada, infraestructura tecnológica y políticas aplicadas. El instrumento utilizado es un formulario estandarizado.

Revisión documental: Se examinan documentos institucionales oficiales como:

- Políticas de seguridad actuales
- Informes técnicos de configuración
- Protocolos de red establecidos
- Estándares de ciberseguridad adoptados

3.5. Universo, Población y Muestra

El universo se refiere al conjunto total de elementos que son objeto de estudio. La población es un subconjunto del universo que comparte características específicas, y la muestra es una selección representativa de la población.

- **Aplicación en la investigación:**
  - **Población:** El personal de TI responsable de la gestión y seguridad de las redes Wi-Fi, según el siguiente detalle:

Funciones	*Número*
Director de TIC´s	1
Área de redes	2
Responsables en facultad	5
Total	8

  - **Muestra**: al tratarse de una población sumamente pequeña, no es necesario la determinación de una muestra.

3.6. Procesamiento de la Información

El procesamiento de la información se realiza mediante las siguientes técnicas:

1. **Análisis cualitativo**: Se examinan en profundidad las respuestas obtenidas en las encuestas (incluyendo las preguntas abiertas) y la entrevista no estructurada realizada al técnico especialista del área de redes de TICs, mediante técnicas de análisis de contenido. Este proceso permite identificar percepciones, experiencias y recomendaciones clave sobre la seguridad de la red Wi-Fi desde la perspectiva del personal operativo. Se analizan las respuestas abiertas y los testimonios para detectar patrones comunes, preocupaciones recurrentes y sugerencias de mejora, proporcionando una comprensión detallada de los aspectos humanos y organizacionales de la seguridad informática en la universidad.

2. **Análisis cuantitativo**: Los datos numéricos de las encuestas se procesan mediante herramientas estadísticas para obtener mediciones precisas. Se calculan frecuencias, porcentajes y correlaciones básicas que permiten cuantificar el nivel de conocimiento en seguridad informática, el grado de

implementación de protocolos y las áreas que requieren mayor atención. Los resultados se presentan en tablas y gráficos que facilitan la visualización de tendencias y la comparación entre diferentes facultades o áreas de la universidad.

3. **Análisis documental**: Se realiza una revisión exhaustiva y crítica de toda la documentación institucional relacionada con la seguridad de redes. Este proceso compara las políticas escritas, protocolos técnicos y registros históricos con los estándares actuales de ciberseguridad. El análisis identifica discrepancias entre lo establecido en los documentos y las mejores prácticas del sector, destacando áreas donde la universidad cumple con los requisitos y aquellas que necesitan actualización o mejora.

4. **Evaluación técnica no intrusiva**: Mediante métodos de observación pasiva, se analiza la configuración actual de la red Wi-Fi sin interferir con su funcionamiento. Esta evaluación examina los protocolos de seguridad activos, las políticas de contraseñas, los sistemas de autenticación y otros parámetros técnicos relevantes. El proceso detecta posibles vulnerabilidades de configuración y verifica el cumplimiento de los estándares básicos de seguridad, proporcionando una evaluación objetiva del estado técnico de la infraestructura de red.

CAPITULO IV

RESULTADOS Y DISCUSIÓN

4.1. Análisis entrevista no estructurada

Se presentan los resultados obtenidos mediante la entrevista no estructurada realizada al Ingeniero Patricio Pachala responsable del área de redes de TIC´s de la Universidad Estatal de Bolívar. Este análisis cualitativo revela información crítica sobre la situación actual de la infraestructura tecnológica y los desafíos operativos que enfrenta la institución.

Infraestructura tecnológica obsoleta

El entrevistado confirmó que la universidad cuenta con puntos de acceso Aruba con más de 8-10 años de antigüedad, superando ampliamente su vida útil recomendada. Esta situación genera dos problemas principales: imposibilidad de recibir actualizaciones de firmware críticas para la seguridad e incompatibilidad con protocolos modernos como WPA3. Adicionalmente, se identificó que el Data Center opera con equipos Cisco y Huawei, aunque se quiere plan de migración completa a Huawei por consideraciones de costos.

Gestión de seguridad y dependencia tecnológica

El análisis reveló que Fortinet constituye el principal y casi único mecanismo de defensa de la red universitaria, cumpliendo funciones esenciales como firewall y prevención de intrusiones. Sin embargo, se evidenciaron dos vulnerabilidades operativas clave: la dependencia exclusiva de esta solución y los altos costos de licenciamiento que limitan su mantenimiento óptimo. Preocupa especialmente la ausencia de un plan de contingencia o solución redundante que mitigue el riesgo en caso de fallos del sistema principal.

Capacidad operativa y limitaciones humanas

La estructura del equipo técnico presenta serias limitaciones, con solo tres personas responsables de toda la infraestructura de red universitaria. Esta situación genera una sobrecarga operativa crítica, agravada por la falta de protocolos documentados para la gestión de incidentes y la ausencia total de planes de mitigación ante escenarios de crisis. Los técnicos por facultad tienen roles limitados, enfocados

únicamente en reportar fallas básicas sin capacidad para intervenciones técnicas complejas.

Falta de estandarización y planificación

Se detectó una marcada heterogeneidad en la infraestructura de red, donde la sede principal opera con equipos Aruba y Fortinet, mientras los campus periféricos mantienen configuraciones independientes y no unificadas. Esta disparidad tecnológica dificulta la implementación de políticas de seguridad consistentes y multiplica los vectores de ataque potenciales. Paralelamente, se confirmó la ausencia de planes de contingencia para escenarios críticos, brecha que quedó en evidencia durante la pandemia.

Brecha entre políticas y realidad operativa

Uno de los hallazgos más relevantes fue la significativa discrepancia entre las políticas de seguridad documentadas y su implementación práctica. El entrevistado confirmó que muchas normativas quedan en el plano teórico debido a limitaciones presupuestarias y técnicas no consideradas en la planificación, situación que se agrava por la ausencia de mecanismos de mitigación efectivos.

4.2. Análisis encuesta

Se presentan los datos y en análisis de la información recabada a través de la encuesta aplicada al personal técnico del área de redes y de la dirección de Tics de la Universidad Estatal de Bolívar.

Pregunta 1: ¿Qué tipo de protocolo IP predomina en la red institucional?

Tabla 1 Distribución de protocolos IP en la red institucional

Opción	***Frecuencia***	***Porcentaje***
IPV4	*7*	*87,5%*
IPV6	*0*	*0%*
Ambos por igual	*1*	*12,5%*
No estoy seguro	*0*	*0%*
Total	*8*	*100%*

Fuente: *Encuesta a técnicos del área de redes Universidad Estatal de Bolívar, 2025*

Elaboración: *Garófalo, C*

Gráfico 1 Distribución de protocolos IP en la red institucional



Fuente: *Encuesta a técnicos del área de redes Universidad Estatal de Bolívar, 2025*

Elaboración: *Garófalo, C*

Interpretación: Los resultados reflejan que IPv4 es el protocolo dominante en la red institucional (87,5%), mientras que IPv6 no muestra implementación. El 12,5% que menciona "ambos por igual" podría corresponder a un técnico de facultad que, por desconocimiento de la red central, no tiene claridad sobre su funcionamiento

real. Esto confirma que la universidad opera principalmente con IPv4, sin una adopción significativa de IPv6.

Pregunta 2: ¿Qué protocolos de encriptación utiliza actualmente la red Wi-Fi de la Universidad Estatal de Bolívar?

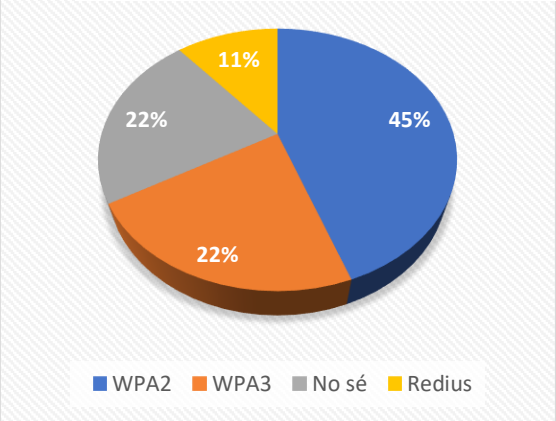
Tabla 2 Protocolos de encriptación Wi-Fi implementados en la Universidad Estatal de Bolívar

Opción	***Frecuencia***	***Porcentaje***
WPA2	*4*	*44,5%*
WPA3	*2*	*22.2%*
No sé	*2*	*22,5%*
Radius	*1*	*11,5%*
Total	*9*	*100%*

Fuente: *Encuesta a técnicos del área de redes Universidad Estatal de Bolívar, 2025*

Elaboración: *Garófalo, C*

Gráfico 2 Protocolos de encriptación Wi-Fi implementados en la Universidad Estatal de Bolívar



Fuente: *Encuesta a técnicos del área de redes Universidad Estatal de Bolívar, 2025*

Elaboración: *Garófalo, C*

Interpretación: Los resultados muestran que WPA2 es el protocolo más reportado (44,5%), donde los 3 técnicos del área de redes confirmaron su uso, mientras que el cuarto caso probablemente corresponde a personal de otras facultades que supone su implementación. La mención de Radius (11,5%) -aunque no es protocolo de encriptación- vendría de un técnico que conoce su uso para autenticación, pero lo confundió al responder. El 22,5% que indicó "No sé" evidencia el desconocimiento

del personal técnico periférico, reflejando falta de capacitación sobre la operación real de la red institucional. Esto revela una clara brecha entre quienes gestionan la red centralmente y los técnicos de facultades que trabajan con información limitada o supuestos.

Pregunta 3: ¿La red Wi-Fi institucional está segmentada mediante VLANs?

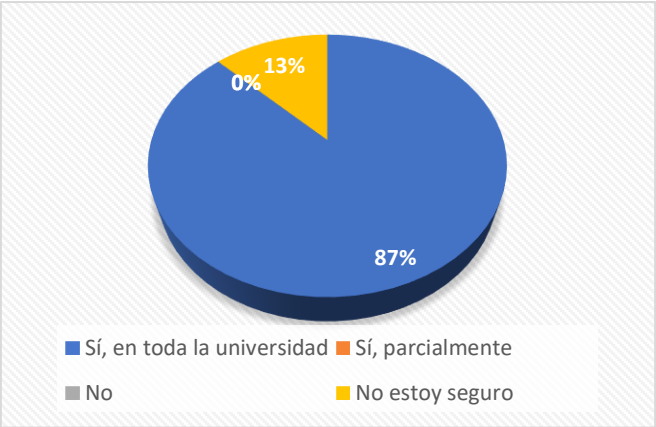
Tabla 3 Implementación de segmentación VLAN en la red Wi-Fi institucional

Opción	***Frecuencia***	***Porcentaje***
Sí, en toda la universidad	*7*	*87,5%*
Sí, parcialmente	*0*	*0%*
No	*0*	*0%*
No estoy seguro	*1*	*12,5*
Total	*8*	*100%*

Fuente: *Encuesta a técnicos del área de redes Universidad Estatal de Bolívar, 2025*

Elaboración: *Garófalo, C*

Gráfico 3 Implementación de segmentación VLAN en la red Wi-Fi institucional



Fuente: *Encuesta a técnicos del área de redes Universidad Estatal de Bolívar, 2025*

Elaboración: *Garófalo, C*

Interpretación: Los resultados muestran que el 87.5% de los técnicos confirma que la red Wi-Fi institucional está completamente segmentada mediante VLANs en toda la universidad, mientras que el 12.5% restante no proporcionó respuesta en

esta encuesta. Este alto porcentaje de consenso indica que la implementación de VLANs es una práctica generalizada y bien establecida en la infraestructura de red, gestionada centralmente por el área de TIC. La ausencia total de respuestas que mencionen una implementación parcial o desconocimiento del tema refuerza que esta característica de la red es claramente reconocida por el personal técnico, a diferencia de otros aspectos donde se evidenciaron vacíos de conocimiento. El pequeño porcentaje sin respuesta podría corresponder a técnicos de facultades con menor involucramiento en la configuración de red.

Pregunta 4: ¿Qué sistemas operativos utilizan los puntos de acceso Wi-Fi?

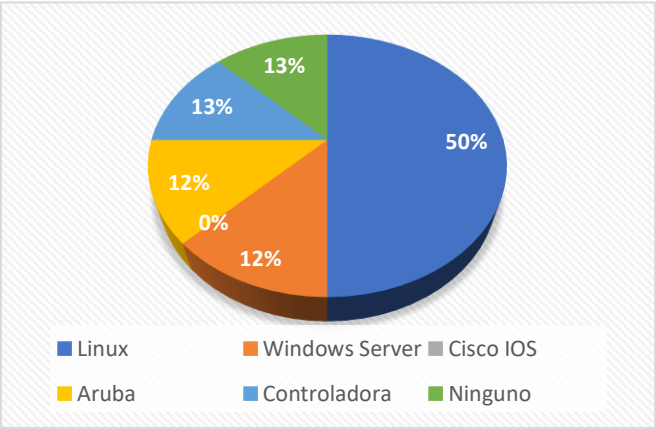
Tabla 4 Sistemas operativos implementados en los puntos de acceso Wi-Fi universitarios

Opción	***Frecuencia***	***Porcentaje***
Linux	*4*	*50%*
Windows Server	*1*	*12,5%*
Cisco IOS	*0*	*0%*
Aruba	*1*	*12,5%*
controladora	*1*	*12,5%*
Ninguno	*1*	*12,5%*
Total	*8*	*100%*

Fuente: *Encuesta a técnicos del área de redes Universidad Estatal de Bolívar, 2025*

Elaboración: *Garófalo, C*

Gráfico 4 Sistemas operativos implementados en los puntos de acceso Wi-Fi universitarios



Fuente: *Encuesta a técnicos del área de redes Universidad Estatal de Bolívar, 2025*

Elaboración: *Garófalo, C*

Interpretación: Los resultados muestran que el 50% de los encuestados reporta Linux como sistema operativo en los puntos de acceso Wi-Fi, lo que probablemente corresponde a los 3 técnicos del área de redes que conocen la configuración real, mientras que las otras respuestas (Windows Server 12.5%, Aruba 12.5%, "controladora" 12.5% y "Ninguno" 12.5%) parecen reflejar suposiciones o confusiones por parte del personal técnico de facultades que no tiene acceso directo a esta información. Esta dispersión en las respuestas, con menciones a sistemas poco probables para puntos de acceso (como Windows Server) o términos ambiguos ("controladora"), evidencia una clara brecha entre el conocimiento centralizado del equipo de redes y el desconocimiento del personal periférico, lo que sugiere la necesidad de mejorar los canales de comunicación y capacitación técnica a nivel institucional para homogenizar el entendimiento de la infraestructura de red.

Pregunta 5: ¿Qué puertos suelen estar abiertos en los puntos de acceso Wi-Fi?

Interpretación:

Las respuestas muestran una clara división en el conocimiento técnico: mientras los 2 miembros del área de redes afirman que "ningún" puerto está abierto (lo que

indicaría una configuración segura), el director de TIC responde que "eso no se puede decir", sugiriendo posibles políticas de confidencialidad o complejidad técnica. Por otro lado, las diversas respuestas de los técnicos de facultades (mencionando puertos como 80, 43, 3389, 21, 5590 y 5900, o indicando "no tengo idea") revelan un preocupante desconocimiento sobre la configuración real de la red. Esta dispersión de respuestas evidencia dos problemas críticos:

a) falta de comunicación clara entre el área central de TIC y las facultades necesidad urgente de capacitación técnica estandarizada, ya que el personal periférico parece trabajar con información incompleta o errónea sobre aspectos fundamentales de seguridad de red. La mención de puertos potencialmente vulnerables (como FTP o RDP) por parte de algunos técnicos podría indicar riesgos de seguridad si estas suposiciones reflejan prácticas reales en algunas áreas de la universidad.

Pregunta 6: ¿Se encuentra habilitado el aislamiento de clientes (Client Isolation) en la red Wi-Fi?

Tabla 5 Implementación de Client Isolation en la red Wi-Fi institucional

Opción	***Frecuencia***	***Porcentaje***
Sí, en todas las redes	*3*	*37,5%*
Solo en redes de invitados	*3*	*37,5%*
No	*2*	*25%*
No sé	*0*	*0%*
Total	*8*	*100%*

Fuente: *Encuesta a técnicos del área de redes Universidad Estatal de Bolívar, 2025*

Elaboración: *Garófalo, C*

Gráfico 5 Implementación de Client Isolation en la red Wi-Fi institucional



Fuente: *Encuesta a técnicos del área de redes Universidad Estatal de Bolívar, 2025*

Elaboración: *Garófalo, C*

Interpretación: Los resultados revelan una alarmante falta de estandarización en la configuración del aislamiento de clientes, evidenciada por las respuestas contradictorias incluso entre los técnicos especializados de redes: mientras 1 técnico central afirma su implementación total (respaldado por 2 técnicos de facultad, sumando 37.5%), otro del área de redes asegura que solo aplica a redes de invitados (coincidiendo con 2 técnicos periféricos, totalizando otro 37.5%), y el tercer especialista junto a un técnico de facultad (25%) niegan su existencia. Esta divergencia crítica demuestra: (1) la ausencia de documentación oficial sobre políticas de red, (2) la implementación arbitraria de configuraciones según áreas sin supervisión centralizada, y (3) el peligroso desconocimiento que obliga al personal periférico a operar mediante suposiciones. La situación expone vulnerabilidades graves en la seguridad de la red institucional, donde la falta de protocolos unificados y comunicación efectiva entre TIC y facultades compromete tanto la integridad de los datos como la gestión eficiente de la infraestructura tecnológica.

Pregunta 7: ¿Qué métodos de autenticación se emplea para el acceso a la red Wi-Fi?

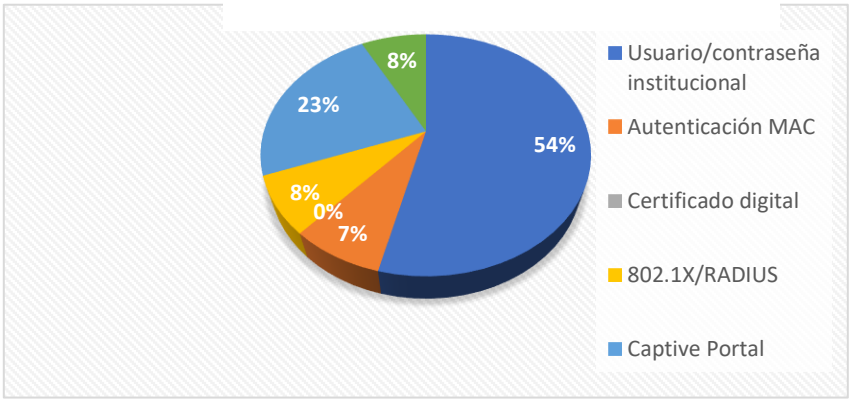
Tabla 6 métodos de autenticación empleado para el acceso a la red Wi-Fi

Opción	*Frecuencia*	*Porcentaje*
Usuario/contraseña institucional	*7*	*53,8%*
Autenticación MAC	*1*	*7,7%*
Certificado digital	*0*	*0%*
802.1X/RADIUS	*1*	*7,7%*
Captive Portal	*3*	*23,3%*
Contraseña	*1*	*7,7%*
Total	*13*	*100*

Fuente: *Encuesta a técnicos del área de redes Universidad Estatal de Bolívar, 2025*

Elaboración: *Garófalo, C*

Gráfico 6 método de autenticación empleado para el acceso a la red Wi-Fi



Fuente: *Encuesta a técnicos del área de redes Universidad Estatal de Bolívar, 2025*

Elaboración: *Garófalo, C*

Interpretación: Los resultados muestran que el método de autenticación predominante en la red Wi-Fi es el usuario/contraseña institucional (53.8%), lo que indica que la mayoría de los accesos se gestionan mediante credenciales centralizadas. El Captive Portal aparece como segunda opción (23.3%), sugiriendo su uso para redes de invitados o acceso temporal. Otros métodos como autenticación MAC, 802.1X/RADIUS y contraseña simple tienen una presencia marginal (7.7% cada uno), mientras que el certificado digital no se

emplea (0%). Esta distribución revela una estrategia de autenticación basada principalmente en credenciales tradicionales, con un enfoque secundario en soluciones para usuarios temporales (Captive Portal). La ausencia de métodos más seguros como certificados digitales y el bajo uso de 802.1X/RADIUS podrían indicar oportunidades para fortalecer la seguridad de la red. La pequeña presencia de "contraseña" (7.7%) sin contexto institucional sugiere posibles configuraciones locales no estandarizadas.

Pregunta 8: ¿Existe filtrado por direcciones MAC en la red?

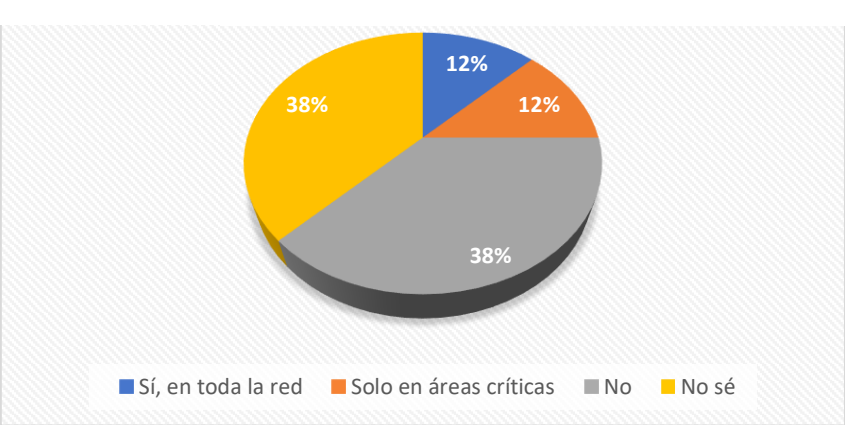
Tabla 7 filtración por direcciones MAC en la red

Opción	***Frecuencia***	***Porcentaje***
Sí, en toda la red	*1*	*12,5%*
Solo en áreas críticas	*1*	*12,5%*
No	*3*	*37,5%*
No sé	*3*	*37,5%*
Total	*8*	*100%*

Fuente: *Encuesta a técnicos del área de redes Universidad Estatal de Bolívar, 2025*

Elaboración: *Garófalo, C*

Gráfico 7 filtración por direcciones MAC en la red



Fuente: *Encuesta a técnicos del área de redes Universidad Estatal de Bolívar, 2025*

Elaboración: *Garófalo, C*

Interpretación:

Los resultados muestran una clara discrepancia en la implementación del filtrado MAC. De los tres técnicos especializados del área de TIC, dos (37.5% del total) afirman que no existe este filtrado, coincidiendo con un técnico de facultad, mientras que el tercer técnico de TIC (12.5%) indica que solo se aplica en áreas críticas. Por otro lado, un técnico de facultad (12.5%) supone que el filtrado está implementado en toda la red, y tres técnicos periféricos (37.5%) manifiestan desconocer esta configuración.

Pregunta 9: ¿Cómo se gestiona el acceso de dispositivos personales a la red Wi-Fi?

Interpretación: Los resultados revelan una clara falta de estandarización en la gestión de dispositivos personales en la red Wi-Fi. Los tres técnicos del área de TIC presentan respuestas similares pero con variaciones: uno menciona "Mediante usuarios del SAC", otro "mediante usuario y contraseña" y el tercero "Usuario y Clave del SAC", lo que sugiere que aunque usan el Sistema de Acceso Centralizado (SAC), no existe una nomenclatura unificada ni protocolos claramente documentados.

Las respuestas de los técnicos de facultades muestran mayor dispersión:

- Algunos mencionan métodos similares (contraseñas, usuario/clave)
- Otros proponen mecanismos distintos (Radius, correo institucional)
- Un caso indica desconocimiento ("NO SE")
- Otro sugiere un proceso manual ("CON EL DEPARTAMENTO DE REDES")

Pregunta 10: ¿Qué tipo de restricciones de acceso o uso están implementadas en la red Wi-Fi?

Interpretación: Los resultados revelan graves inconsistencias en el conocimiento de las restricciones de la red Wi-Fi, a pesar de ser una red unificada. Los tres técnicos del área de TIC responsables de la configuración presentan respuestas contradictorias: dos mencionan bloqueo de contenido específico (pornografía, juegos, descargas de música y videos y sitios no seguros), mientras que el tercero se refiere a mecanismos técnicos (contraseñas, redes de invitados y autenticación RADIUS). Esta divergencia entre los propios especialistas evidencia la falta de protocolos documentados. Paralelamente, las respuestas de los técnicos de facultades -que van desde "NO SE" hasta suposiciones como "Control de ancho de Banda"- demuestran un preocupante desconocimiento sobre las políticas reales de la red. La situación crítica surge no por diferencias reales en la implementación, sino por la ausencia total de comunicación y capacitación formal desde el área central, lo que exige urgentemente la documentación y socialización oficial de estas restricciones a todo el personal técnico institucional.

Pregunta 11: ¿Existe una red Wi-Fi separada para visitantes?

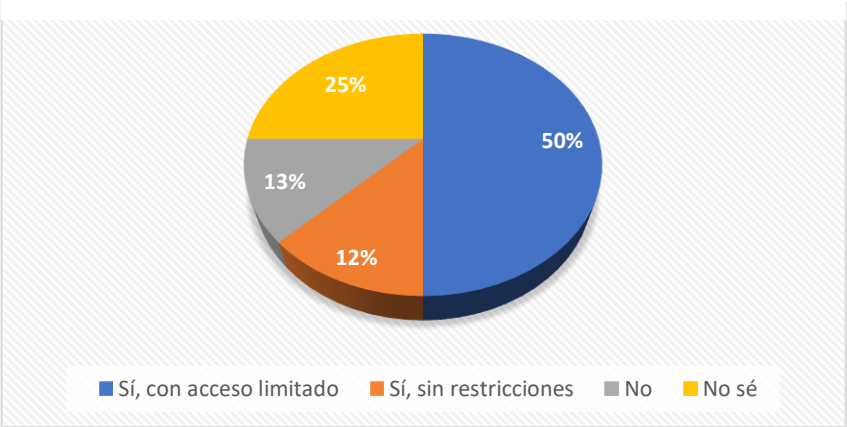
Tabla 8 red Wi-Fi separada para visitantes

Opción	*Frecuencia*	*Porcentaje*
Sí, con acceso limitado	*4*	*44,4%*
Sí, sin restricciones	*2*	*22,2%*
No	*1*	*11,1%*
No sé	*2*	*22,2%*
Total	*9*	*100%*

Fuente: *Encuesta a técnicos del área de redes Universidad Estatal de Bolívar, 2025*

Elaboración: *Garófalo, C*

Gráfico 8 red Wi-Fi separada para visitantes



Fuente: *Encuesta a técnicos del área de redes Universidad Estatal de Bolívar, 2025*

Elaboración: *Garófalo, C*

Interpretación: Los resultados muestran que el 44.4% de los encuestados (incluyendo 2 técnicos del área de redes y 2 técnicos de facultad) afirma que existe una red Wi-Fi para visitantes con acceso limitado, mientras que el 11.1% (un técnico del área de redes) niega su existencia. Por otro lado, el 22.2% (técnicos de facultad) cree que el acceso es sin restricciones, y otro 22.2% (técnicos de facultad) desconoce la política. Esta discrepancia evidencia una falta de estandarización en la implementación y comunicación de las configuraciones de red, donde incluso el personal técnico especializado no coincide en su percepción, lo que podría generar

vulnerabilidades de seguridad al no aplicarse uniformemente las restricciones de acceso.

Pregunta 12: ¿Con qué frecuencias se detectan intentos de intrusión en la red Wi-Fi?

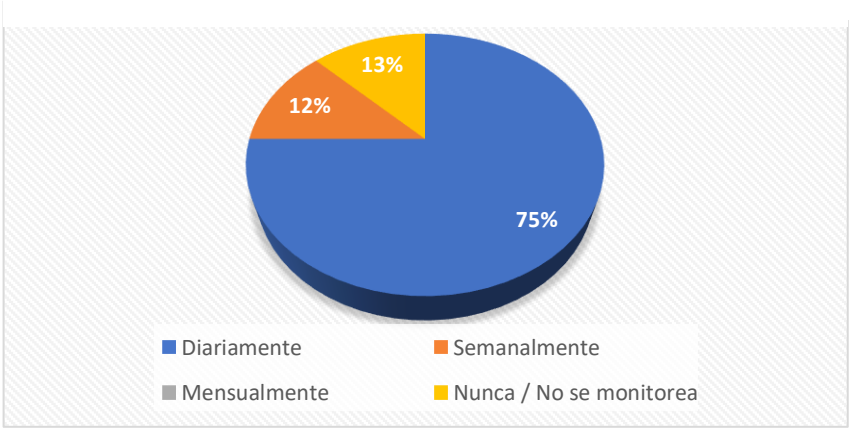
Tabla 9 frecuencia de intentos de intrusión en la red Wi-Fi

Opción	***Frecuencia***	***Porcentaje***
Diariamente	*6*	*66,7%*
Semanalmente	*2*	*22,2%*
Mensualmente	*0*	*0%*
Nunca / No se monitorea	*1*	*11,1%*
Total	*9*	*100%*

Fuente: *Encuesta a técnicos del área de redes Universidad Estatal de Bolívar, 2025*

Elaboración: *Garófalo, C*

Gráfico 9 frecuencia de intentos de intrusión en la red Wi-Fi



Fuente: *Encuesta a técnicos del área de redes Universidad Estatal de Bolívar, 2025*

Elaboración: *Garófalo, C*

Interpretación: Los resultados muestran que el 66.7% de las respuestas indican detección diaria de intrusiones, incluyendo dos técnicos del área de redes TIC y cuatro técnicos de facultades. El 22.2% corresponde a reportes de detección semanal provenientes de los encargados del área de redes TIC. Finalmente, el 11.1% afirma no realizar monitoreo. Esta distribución revela una discrepancia crítica dentro del equipo central de redes TIC, donde algunos técnicos reportan

detección diaria mientras otros indican frecuencia semanal. Además, se identifica una brecha de seguridad en al menos una facultad que no realiza monitoreo.

Pregunta 13: ¿Qué herramientas se utilizan para registrar o gestionar incidentes de seguridad?

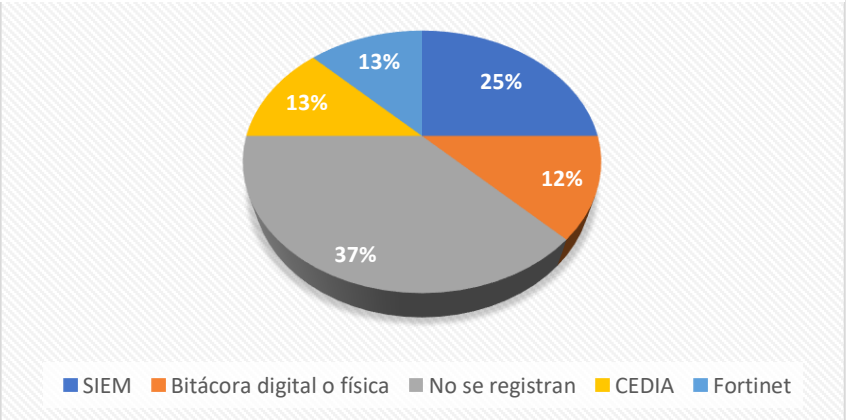
Tabla 10 herramientas para registrar o gestionar incidentes de seguridad

Opción	***Frecuencia***	***Porcentaje***
SIEM	*2*	*25%*
Bitácora digital o física	*1*	*12,5%*
No se registran	*3*	*37,5*
CEDIA	*1*	*12,5%*
Fortinet	*1*	*12,5%*
Total	*8*	*100%*

Fuente: *Encuesta a técnicos del área de redes Universidad Estatal de Bolívar, 2025*

Elaboración: *Garófalo, C*

Gráfico 10 herramientas para registrar o gestionar incidentes de seguridad



Fuente: *Encuesta a técnicos del área de redes Universidad Estatal de Bolívar, 2025*

Elaboración: *Garófalo, C*

Interpretación: Los resultados revelan una grave falta de estandarización en la gestión de incidentes de seguridad, donde los técnicos del área de redes TIC presentan tres enfoques distintos: un 12.5% utiliza Fortinet (solución profesional), otro 12.5% emplea bitácora manual (método obsoleto) y un 12.5% no registra incidentes (omisión crítica). Por otro lado, entre los técnicos de facultades, un 25%

usa SIEM (sistema avanzado), un 12.5% utiliza CEDIA y un 25% tampoco registra incidentes. Esta fragmentación expone vulnerabilidades críticas: el 37.5% del personal no documenta incidentes (incluyendo técnicos clave de TIC), coexisten cuatro sistemas incompatibles sin integración, y persisten métodos manuales obsoletos en el núcleo técnico. Urge implementar un SIEM institucional unificado, eliminar las bitácoras físicas, y establecer políticas obligatorias de registro para todo el personal, priorizando la capacitación del equipo de redes TIC para garantizar una gestión coherente y profesional de la seguridad universitaria.

Pregunta 14: ¿Se realizan auditorías de seguridad Wi-Fi?

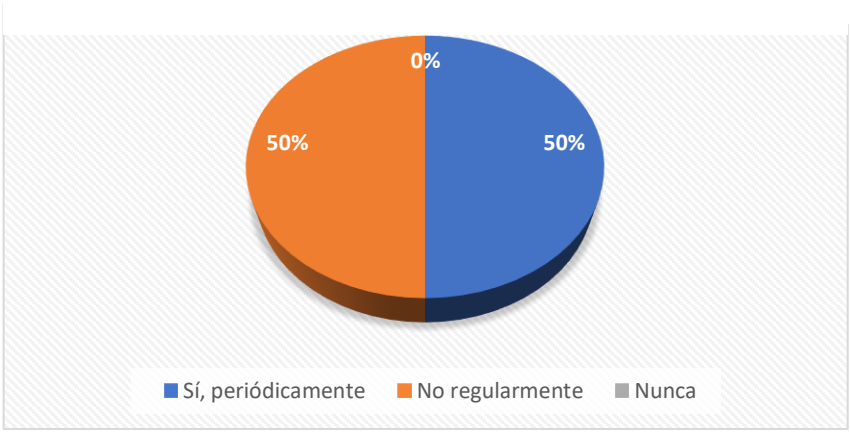
Tabla 11 auditorías de seguridad Wi-Fi

Opción	***Frecuencia***	***Porcentaje***
Sí, periódicamente	*4*	*50%*
No regularmente	*4*	*50%*
Nunca	*0*	*0%*
Total	*8*	*100%*

Fuente: *Encuesta a técnicos del área de redes Universidad Estatal de Bolívar, 2025*

Elaboración: *Garófalo, C*

Gráfico 11 auditorías de seguridad Wi-Fi



Fuente: *Encuesta a técnicos del área de redes Universidad Estatal de Bolívar, 2025*

Elaboración: *Garófalo, C*

Interpretación: Los resultados muestran contradicciones críticas en el equipo de redes TIC, donde dos técnicos confirman auditorías periódicas mientras un tercero

reporta irregularidades, evidenciando falta de estandarización en los procesos de seguridad. Por otro lado, las facultades presentan respuestas divididas (40% periódicas vs 60% irregulares) que, al no gestionar directamente estas auditorías, probablemente reflejan suposiciones más que datos concretos. Esta situación revela graves fallas en la implementación y comunicación de los protocolos de seguridad, donde incluso el equipo central responsable muestra inconsistencias operativas. Urge documentar y formalizar un cronograma obligatorio de auditorías, asegurando que todo el personal técnico, especialmente el área de redes TIC, cumpla con los mismos estándares y comunique los resultados a las facultades para eliminar discrepancias.

Pregunta 15: ¿Existe un protocolo documentado de respuesta ante incidentes de seguridad Wi-Fi en la institución?

Interpretación: La respuesta del director de tics indicando "No lo sé" sobre la existencia de protocolos documentados para incidentes de seguridad Wi-Fi es sumamente preocupante, evidenciando una grave falla en la gobernanza de ciberseguridad. Esta situación crítica se amplifica al confirmar que el 100% del equipo de redes TIC (3/3) desconoce estos protocolos, incluyendo respuestas como "ninguna" y "no" de los técnicos de redes de tics. Entre los técnicos de facultades, solo uno afirma su existencia, pero no puede validarlo técnicamente al no pertenecer al área competente, mientras que los demás respondieron "Desconozco", "No" o "NO LO SE", demostrando un desconocimiento generalizado.

Pregunta 16: ¿Qué tipos de ataques ha detectado o considera posibles en la red Wi-Fi?

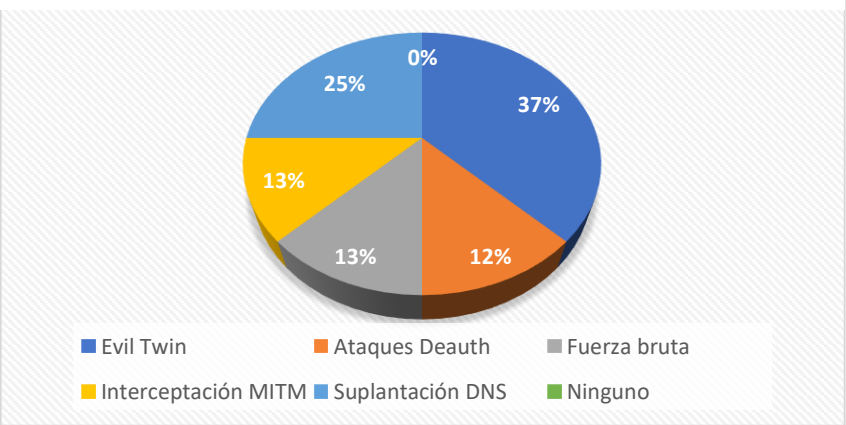
Tabla 12 ataques detectados o posibles en la red Wi-Fi

Opción	*Frecuencia*	*Porcentaje*
Evil Twin	*3*	*37,5%*
Ataques Deauth	*1*	*12,5%*
Fuerza bruta	*1*	*12,5%*
Interceptación MITM	*1*	*12,5%*
Suplantación DNS	*2*	*25%*
Ninguno	*0*	*0*
Total	*8*	*100%*

Fuente: *Encuesta a técnicos del área de redes Universidad Estatal de Bolívar, 2025*

Elaboración: *Garófalo, C*

Gráfico 12 ataques detectados o posibles en la red Wi-Fi



Fuente: *Encuesta a técnicos del área de redes Universidad Estatal de Bolívar, 2025*

Elaboración: *Garófalo, C*

Interpretación: Los resultados muestran que el 37.5% de los técnicos (3/8) no identificó ningún ataque ("Ninguno"), incluyendo respuestas tanto del área de redes TIC como de facultades. Entre quienes reportaron amenazas específicas, se observa que el 25% (2/8 técnicos de facultades) mencionó "Suplantación DNS", el 12.5% (1/8 técnico de redes TIC) detectó "Ataques Deauth", otro 12.5% (1/8 técnico de redes TIC) señaló "Fuerza bruta", y un 12.5% adicional (1/8 técnico de facultades) indicó "Interceptación MITM". Es importante destacar que las respuestas de los

técnicos de facultades podrían basarse en suposiciones, ya que, al no estar directamente involucrados en el área de redes, no tienen forma de verificar si estos ataques realmente ocurren o no. Esta situación revela una disparidad en la percepción de amenazas, donde el personal técnico directamente responsable de la seguridad (TIC) muestra mayor conocimiento específico, mientras que las facultades podrían estar mencionando riesgos teóricos más que incidentes confirmados.

Pregunta 17: ¿Qué dispositivos IoT están actualmente conectados a la red Wi-Fi institucional?

Interpretación: Los resultados muestran inconsistencias significativas en el conocimiento sobre dispositivos IoT conectados a la red Wi-Fi institucional. Entre los técnicos del área de redes TIC (responsables directos de la gestión de red), las respuestas varían considerablemente: un técnico reporta "relojes de control de personal" (12.5%), otro menciona "ninguno" (12.5%), y un tercero indica "Sistema de Video vigilancia" (12.5%). Esta falta de consenso dentro del equipo central es preocupante, ya que revela que no existe un inventario unificado de dispositivos IoT. Por otro lado, las respuestas de los técnicos de facultades - que incluyen "Consola" (12.5%), "todos los dispositivos que tengan wifi" (12.5%) y dos casos de "NO LO SE" (25%) - deben considerarse como meras suposiciones, dado que estos técnicos no están directamente involucrados en la administración de la red.

Pregunta 18: ¿El personal técnico recibe capacitación específica en seguridad Wi-Fi?

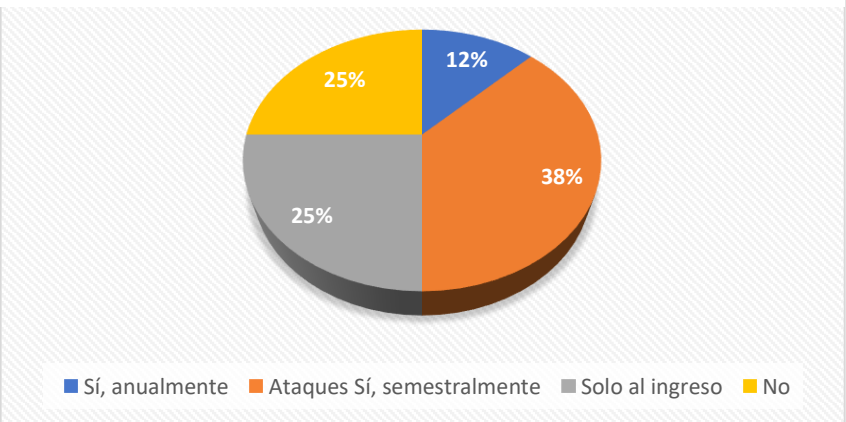
Tabla 13 Capacitación del personal técnico en seguridad Wi-Fi

Opción	***Frecuencia***	***Porcentaje***
Sí, anualmente	*1*	*12,5%*
Sí, semestralmente	*3*	*37,5%*
Solo al ingreso	*2*	*25%*
No	*2*	*25%*
Total	*8*	*100%*

Fuente: *Encuesta a técnicos del área de redes Universidad Estatal de Bolívar, 2025*

Elaboración: *Garófalo, C*

Gráfico 13 Capacitación del personal técnico en seguridad Wi-FI



Fuente: *Encuesta a técnicos del área de redes Universidad Estatal de Bolívar, 2025*

Elaboración: *Garófalo, C*

Interpretación: Los resultados revelan una grave falta de estandarización en la capacitación sobre seguridad Wi-Fi. En el área de redes TIC (3 técnicos), las respuestas son inconsistentes: 1 reporta capacitación semestral, 1 solo al ingreso y 1 afirma no recibir formación, demostrando que incluso el equipo central carece de un programa unificado. Por otro lado, en las facultades (5 técnicos) la situación es igualmente dispersa: 2 mencionan capacitación semestral, 1 anual, 1 solo al ingreso y 1 no recibe entrenamiento. Esta disparidad evidencia que la formación depende completamente de circunstancias individuales (como fecha de ingreso o iniciativas

aisladas) y no de un plan institucional. La ausencia de coordinación del área de redes TIC - donde coexisten técnicos con formación semestral con otros sin capacitación alguna - es particularmente preocupante, ya que impide establecer protocolos de seguridad consistentes. Urge implementar un programa obligatorio con frecuencia mínima semestral para todo el personal técnico, priorizando la alineación del equipo de redes TIC como responsable de su cumplimiento.

Pregunta 19: ¿Qué herramientas considera necesarias para mejorar la seguridad de la red Wi-Fi?

Interpretación: Los técnicos del área de redes TIC presentan respuestas divergentes sobre herramientas de seguridad: dos mencionan específicamente "licencias actualizadas en Fortinet" (66.6%), mientras que el tercero (director de TIC) enumera múltiples elementos (firewall, antivirus, VPN) sin priorización clara (33.3%), revelando falta de coordinación interna. Por su parte, los técnicos de facultades muestran un panorama fragmentado: desde sugerencias técnicas avanzadas (balanceador de carga, SIEM - 40%) hasta medidas básicas (cambio de contraseñas, WPA2 - 40%) y respuestas genéricas ("ataques externos"), lo que evidencia desconocimiento de los protocolos institucionales.

4.3. Discusión de Resultados

La combinación de la **entrevista no estructurada** al responsable del área de redes de TIC's y la **encuesta aplicada al personal técnico** revela una serie de hallazgos críticos sobre el estado de la seguridad Wi-Fi en la Universidad Estatal de Bolívar. A continuación, se discuten los resultados más relevantes, contrastando ambas fuentes de información y analizando sus implicaciones.

1. Infraestructura tecnológica obsoleta y falta de actualización

Entrevista:

- El responsable de redes confirmó que los **puntos de acceso Aruba tienen entre 8 y 10 años de antigüedad**, lo que impide:
  - ❖ La instalación de actualizaciones de firmware críticas para la seguridad.
  - ❖ La implementación de protocolos modernos como **WPA3**.

- El **Data Center** opera con equipos **Cisco y Huawei**, pero no hay un plan claro de migración.

Encuesta:

- El **87.5%** de los técnicos reportó que la red opera principalmente con **IPv4**, mientras que **IPv6 no está implementado**.
- Solo **22.2%** mencionó el uso de **WPA3**, mientras que **44.5%** sigue utilizando **WPA2**, un protocolo con vulnerabilidades conocidas.

Análisis:

- La **falta de inversión en infraestructura** genera riesgos significativos, ya que los equipos antiguos no soportan medidas de seguridad modernas.
- La **ausencia de IPv6** limita la capacidad de la universidad para adoptar mejores prácticas de seguridad y escalabilidad.

2. Gestión de seguridad: dependencia de una única solución y falta de documentación

Entrevista:

- La seguridad de la red depende casi exclusivamente de **Fortinet** (firewall y prevención de intrusiones), lo que genera:
    - **Alto costo de licenciamiento**.
    - **Falta de redundancia** (si falla, no hay respaldo).
- No existen **protocolos documentados** para la gestión de incidentes.
- Solo **tres personas** administran toda la red universitaria, lo que genera sobrecarga operativa.

Encuesta:

- **37.5%** de los técnicos admitió que **no se registran incidentes de seguridad**.

- **50%** afirmó que las auditorías de seguridad se realizan **periódicamente**, mientras que el otro **50%** dijo que son **irregulares**.
- **Ningún técnico** pudo describir un **protocolo de respuesta ante incidentes**.

Análisis:

- La **dependencia de un único sistema de seguridad (Fortinet)** es un **punto crítico de fallo**.
- La **falta de documentación y estandarización** en auditorías y respuesta a incidentes incrementa el riesgo de brechas de seguridad.
- El **personal insuficiente** y la **falta de capacitación continua** dificultan una gestión proactiva de la seguridad.

3. Configuraciones inconsistentes y falta de segmentación adecuada

Entrevista:

- Existen **redes independientes en campus periféricos** sin unificación con la sede central.
- No hay un **plan de contingencia** ante fallos masivos.

Encuesta:

- **37.5%** afirmó que el **Client Isolation** está habilitado en todas las redes, mientras que otro **37.5%** dijo que solo en redes de invitados.
- **87.5%** confirmó el uso de **VLANs**, pero no está claro si la segmentación es óptima.
- **53.8%** utiliza **usuario/contraseña institucional** para autenticación, pero solo **7.7%** emplea **802.1X/RADIUS** (más seguro).

Análisis:

- Las **contradicciones en las respuestas** sugieren que **no hay una política clara de configuración**.

- La **falta de autenticación robusta (como RADIUS)** facilita ataques como **credenciales robadas o fuerza bruta**.
- La **segmentación con VLANs** es positiva, pero la inconsistencia en **Client Isolation** podría permitir ataques internos.

4. Amenazas detectadas y falta de monitoreo

Entrevista:

- Se reportan **intentos de intrusión frecuentes**, pero no hay un sistema centralizado de monitoreo.
- No se realizan **pruebas de penetración (pentesting)** periódicas.

Encuesta:

- **66.7%** de los técnicos detecta intentos de intrusión **diariamente**.
- Los ataques más mencionados fueron:
  - **Evil Twin (37.5%)**
  - **Suplantación DNS (25%)**
  - **Ataques Deauth (12.5%)**
- **37.5%** no registra incidentes, y las herramientas de gestión son inconsistentes (**SIEM, Fortinet, bitácoras manuales**).

Análisis:

- La **alta frecuencia de intentos de intrusión** confirma que la red es un **blanco constante**.
- La **falta de un SIEM unificado** impide una respuesta rápida ante incidentes.
- La **ausencia de pentesting** significa que las vulnerabilidades no se identifican proactivamente.

5. Capacitación insuficiente del personal técnico

Entrevista:

- No hay un **programa formal de capacitación en ciberseguridad**.
- Los técnicos de facultades tienen **poco conocimiento sobre la configuración central de la red**.

Encuesta:

- **25%** del personal técnico **no recibe capacitación** en seguridad Wi-Fi.
- **37.5%** tiene entrenamiento **semestral**, pero es inconsistente.
- Las respuestas sobre herramientas necesarias fueron **muy variadas**, lo que indica falta de alineación.

Análisis:

- La **falta de capacitación estandarizada** explica las **contradicciones en las respuestas**.
- Sin un **entrenamiento continuo**, el personal no puede implementar medidas de seguridad avanzadas.

Hallazgos principales y análisis profundo

a) **Infraestructura obsoleta que impide actualizaciones de seguridad**

La investigación reveló que los puntos de acceso Aruba con más de 8-10 años de operación representan un riesgo crítico, al carecer de soporte para actualizaciones de firmware y protocolos modernos como WPA3. Esta obsolescencia técnica no solo limita la implementación de medidas de seguridad avanzadas, sino que también incrementa exponencialmente la superficie de ataque, ya que los equipos contienen vulnerabilidades conocidas sin parches disponibles. La situación se agrava por la falta de un plan de renovación tecnológica documentado, lo que perpetúa el uso de infraestructura insegura.

b) **Dependencia excesiva de Fortinet sin redundancia**

El análisis demostró que la universidad ha desarrollado una peligrosa dependencia monocultural hacia la solución Fortinet, generando un único punto de falla crítico. Si bien Fortinet ofrece capacidades robustas, su implementación como única barrera de seguridad - sumado a los altos costos de licenciamiento que limitan su mantenimiento óptimo - viola el principio básico de defensa en profundidad. Esta situación se torna más preocupante al no existir sistemas redundantes o planes de contingencia que mitiguen el impacto de posibles fallos en esta plataforma.

c) **Falta de documentación y protocolos para gestión de incidentes**

Se identificó una alarmante ausencia de protocolos estandarizados y documentados para la gestión de incidentes de seguridad, evidenciado por las respuestas contradictorias del personal técnico (37.5% admite no registrar incidentes). Esta carencia organizacional impide respuestas ágiles y coordinadas ante brechas de seguridad, aumentando el tiempo de exposición a ataques y dificultando el análisis forense posterior. La falta de documentación también obstaculiza la capacitación del personal y la transferencia de conocimiento institucional.

d) **Configuraciones inconsistentes (VLANs, Client Isolation, autenticación**

El estudio detectó graves inconsistencias en la implementación de medidas básicas de seguridad como VLANs (87.5% afirma usarlas, pero sin estandarización), Client Isolation (37.5% no lo aplica) y autenticación (53.8% usa solo usuario/contraseña). Estas discrepancias configuracionales, particularmente preocupantes en una red unificada, crean vectores de ataque internos y externos, además de demostrar falta de gobernanza en la administración de la infraestructura tecnológica. La situación sugiere una ausencia de políticas de hardening de red institucionalmente adoptadas.

e) **Ataques frecuentes sin un sistema de monitoreo unificado**

Los datos revelan que 66.7% del personal técnico detecta intentos de intrusión diarios (incluyendo Evil Twin, MITM y suplantación DNS), pero

sin herramientas centralizadas para su correlación y análisis. Esta falta de visibilidad unificada impide la detección temprana de patrones de ataque complejos y la respuesta coordinada ante incidentes. La dependencia de métodos manuales y dispersos (37.5% usa bitácoras físicas) aumenta el riesgo de que ataques sofisticados pasen desapercibidos por largos períodos.

f) **Capacitación insuficiente del personal técnico**

Se evidenció una grave fragmentación en la capacitación del personal, donde 25% no recibe ningún entrenamiento en seguridad Wi-Fi y solo 37.5% tiene formación semestral. Esta brecha de conocimiento explica las respuestas contradictorias sobre configuraciones básicas y la incapacidad para implementar medidas avanzadas. La ausencia de un programa institucional de capacitación continua perpetúa prácticas inseguras y limita la adopción de tecnologías modernas, dejando la red vulnerable ante técnicas de ataque actualizadas.

CAPITULO V

PROPUESTA
PLAN DE MITIGACIÓN DE VULNERABILIDADES EN LA RED WI-FI DE LA UNIVERSIDAD ESTATAL DE BOLÍVAR

5.1. Introducción

En la era actual de transformación digital, las instituciones académicas como la Universidad Estatal de Bolívar se han convertido en ecosistemas complejos, donde la conectividad y el acceso a la información son pilares fundamentales. Sin embargo, esta dependencia tecnológica conlleva una exposición creciente a amenazas de ciberseguridad. El diagnóstico previo (Capítulo IV) ha revelado vulnerabilidades críticas en la infraestructura de red Wi-Fi de la UEB, que ponen en riesgo la **integridad de los datos institucionales**, la **privacidad de la comunidad universitaria** y la **continuidad de los servicios académicos** esenciales.

Este capítulo presenta un **Plan Integral de Mitigación de Vulnerabilidades** diseñado específicamente para la red Wi-Fi de la Universidad Estatal de Bolívar. La propuesta va más allá de soluciones reactivas, adoptando un enfoque proactivo y holístico que integra la modernización tecnológica (incluyendo la planificación para la migración a WiFi 7), una gobernanza de seguridad robusta, una gestión de riesgos sistemática y programas de capacitación escalonados y continuos. El objetivo es transformar la red Wi-Fi de la UEB en un entorno seguro, resiliente y preparado para los desafíos futuros.

5.2. Objetivos

5.2.1. Objetivo General

Implementar un modelo de seguridad basado en el **Esquema Gubernamental de Seguridad de la Información del Ecuador (EGSI)** en la infraestructura Wi-Fi de la Universidad Estatal de Bolívar, integrando tecnologías de última generación y mejores prácticas de ciberseguridad para garantizar la **confidencialidad, integridad y disponibilidad** de todos los servicios de red y la protección de los activos de información.

5.2.2. Objetivos Específicos

- **Modernizar la infraestructura de conectividad:** Adquirir e implementar equipos de red inalámbrica compatibles con el estándar **WiFi 7 (802.11be)**, aprovechando las bandas de 6GHz y la tecnología Multi-Link Operation (MLO) para optimizar el rendimiento, la capacidad y la eficiencia en entornos de alta densidad de usuarios.

- **Fortalecer los controles de acceso y autenticación:** Migrar los protocolos de seguridad Wi-Fi a **WPA3-Enterprise** con autenticación **802.1X**, y desplegar un sistema de **Control de Acceso a la Red (NAC)** adaptativo para asegurar una autenticación robusta y una autorización granular basada en el rol y el estado de seguridad de cada dispositivo y usuario.

- **Establecer una gobernanza de seguridad y monitoreo continuo:** Desarrollar e implementar un **Sistema de Gestión de Seguridad de la Información (ISMS)** basado en ISO/IEC 27001, e integrar un **Sistema de Información y Gestión de Eventos de Seguridad (SIEM)** para el monitoreo en tiempo real, la detección temprana de amenazas y la automatización de protocolos de respuesta a incidentes.

- **Desarrollar y fortalecer las capacidades humanas:** Implementar un programa de capacitación certificada para el personal técnico en áreas clave de redes y seguridad Wi-Fi (ej., **CWNP, CIEH**), y realizar simulaciones periódicas de ciberataques y ejercicios de mesa para mejorar la resiliencia operativa y la capacidad de respuesta del equipo ante incidentes.

5.3. Metodología

La elaboración e implementación de este plan de mitigación se basa en una metodología estructurada y en la aplicación de marcos de referencia reconocidos internacionalmente, garantizando un enfoque sistemático y eficaz.

5.3.1. Fases del proyecto

a) **Diagnóstico y análisis de brechas (completado en capítulo iv):** Evaluación de la situación actual de la infraestructura, identificación de

vulnerabilidades, análisis de la capacidad operativa y el nivel de conocimiento del personal.

b) **Diseño del plan de mitigación (presente capítulo):** Definición de objetivos, selección de tecnologías, diseño de arquitecturas de seguridad, desarrollo de iniciativas y establecimiento de métricas.

c) **Implementación y despliegue:** Ejecución de las iniciativas planificadas, adquisición e instalación de equipos, configuración de sistemas, migración de servicios y puesta en marcha de programas de capacitación.

d) **Monitoreo, evaluación y mejora continua:** supervisión constante del rendimiento y la seguridad de la red, evaluación de la efectividad de las medidas implementadas, identificación de nuevas amenazas y adaptación del plan según sea necesario.

5.3.2. Estándares y Marcos de Referencia

- **ISO/IEC 27001 (Sistema de Gestión de Seguridad de la Información - ISMS):** Servirá como guía para establecer, implementar, mantener y mejorar continuamente la gestión de la seguridad de la información en la red Wi-Fi.
- **NIST Cybersecurity Framework (NIST CSF):** Se utilizará para organizar y gestionar el riesgo de ciberseguridad, cubriendo las funciones de Identificar, Proteger, Detectar, Responder y Recuperar.
- **NIST Special Publication 800-30 (Guía para la Evaluación de Riesgos):** Se aplicará para la identificación, análisis y priorización de los riesgos de seguridad asociados a las vulnerabilidades detectadas.
- **Esquema Gubernamental de Seguridad de la Información (EGSI):** Se adoptará como el marco rector de seguridad a nivel nacional, estableciendo los principios y directrices para la protección de la información en las instituciones del sector público ecuatoriano.

5.3.3. Herramientas y Técnicas de Análisis

- **Análisis FODA (Fortalezas, Oportunidades, Debilidades, Amenazas):** Para comprender el entorno interno y externo de la UEB en relación con la ciberseguridad de su red Wi-Fi.
- **Análisis de Brechas (Gap Analysis):** Comparación entre el estado actual de la seguridad de la red y el estado deseado según los estándares y objetivos definidos.
- **Modelado de Costo Total de Propiedad (TCO):** Evaluación de los costos directos e indirectos asociados a la implementación y mantenimiento del plan a lo largo de su ciclo de vida.

5.4. Plan de Mitigación Detallado

El plan se estructura en cuatro ejes estratégicos, cada uno con iniciativas específicas diseñadas para abordar las vulnerabilidades identificadas.

Eje Estratégico 1: Modernización y fortalecimiento de la infraestructura wi-fi

Problema Abordado: Infraestructura tecnológica obsoleta, falta de estandarización, limitaciones de rendimiento y seguridad.

Iniciativa	Fundamentación técnica	Proceso de implementación	Kpis	Mecanismos de control	Análisis estratégico
1.1. Adquisición e implementación de puntos de acceso wifi 7 (802.11be)	Los APs actuales (Aruba 8-10 años) son obsoletos, carecen de actualizaciones de firmware y no soportan WPA3. WiFi 7 ofrece mayor capacidad (6GHz), menor latencia (MLO) y eficiencia, esencial para alta densidad de usuarios y aplicaciones modernas.	1. Evaluación de proveedores (Cisco, Huawei, Aruba). 2. Diseño de cobertura y capacidad. 3. Adquisición de APs y controladoras. 4. Instalación y configuración inicial. 5. Pruebas de rendimiento y seguridad.	% de APs WiFi 7 implementados. Tasa de throughput promedio. Latencia de red.	Reportes de inventario. Monitoreo de rendimiento (NMS). Auditorías de configuración.	**Movimiento estratégico clave.** No es solo una actualización, es una inversión a largo plazo que prepara a la UEB para futuras tecnologías (AR/VR, IoT masivo) y asegura que la infraestructura no se vuelva obsoleta pronto.
1.2. Actualización de la infraestructura	Equipos de Data Center (Cisco, Huawei) requieren un plan de migración y	1. Auditoría de equipos actuales. 2. Diseño de arquitectura de red	% de equipos core actualizados.	Registros de configuración.	**Absolutamente necesario.** Sin esto, los nuevos APs WiFi 7

de red core (switches, routers)	actualización para soportar las nuevas capacidades de WiFi 7 y las demandas de seguridad (VLANs, 802.1X).	escalable. 3. Adquisición de equipos compatibles con WiFi 7 y Zero Trust. 4. Implementación gradual y migración de servicios.	Disponibilidad de la red core.	Pruebas de carga y estrés.	serían como tener un auto de Fórmula 1 atascado en el tráfico. El Core es la autopista que debe soportar la nueva velocidad y seguridad.
1.3. Implementación de gestión centralizada de aps	La heterogeneidad y la falta de unificación en la gestión dificultan la aplicación de políticas de seguridad. Una controladora centralizada simplifica la configuración, el monitoreo y la aplicación de políticas.	1. Selección de solución de gestión (controladora física/virtual o basada en la nube). 2. Integración con los nuevos APs. 3. Configuración de perfiles y políticas unificadas.	Tiempo de despliegue de políticas. Consistencia de configuración entre APs.	Dashboards de gestión centralizada. Logs de configuración.	**Fundamental para la eficiencia y la seguridad.** Permite una gestión unificada y coherente, eliminando errores humanos y asegurando que las políticas de seguridad se apliquen de forma homogénea en toda la red.

1.4. Migración a ipv6 (dual stack)	El predominio de IPv4 limita la escalabilidad y la adopción de nuevas tecnologías. La implementación de IPv6 (en modo Dual Stack) es crucial para el crecimiento futuro y la compatibilidad con IoT.	1. Planificación de direccionamiento IPv6. 2. Configuración de routers y switches para Dual Stack. 3. Habilitación de IPv6 en servidores y servicios clave. 4. Pruebas de conectividad IPv6.	% de dispositivos/servicios con IPv6 habilitado. Tráfico IPv6 en la red.	Monitoreo de tráfico (NetFlow/sFlow). Auditorías de configuración de red.	**Visión de futuro.** Aunque no resuelve un problema de seguridad inmediato y visible, es crucial para la escalabilidad a largo plazo. Abordarlo ahora evita problemas mayores en el futuro.

Eje Estratégico 2: Implementación de controles de acceso y seguridad avanzados

Problema Abordado: Dependencia de Fortinet, protocolos de encriptación desactualizados, falta de estandarización en aislamiento de clientes y filtrado MAC, gestión de dispositivos personales inconsistente.

Iniciativa	Fundamentación técnica	Proceso de implementación	Kpis	Mecanismos de control	Análisis estratégico
2.1. Implementación de wpa3-enterprise y 802.1x	WPA2 es vulnerable. WPA3-Enterprise con 802.1X y un servidor RADIUS proporciona autenticación robusta basada en credenciales, cifrado individual (SAE) y protección contra ataques.	1. Configuración de servidor RADIUS. 2. Integración con directorio de usuarios (LDAP/AD). 3. Configuración de APs para WPA3-Enterprise/802.1X. 4. Despliegue de certificados. 5. Pruebas.	% de redes Wi-Fi usando WPA3-Enterprise. Tasa de éxito de autenticación.	Logs de RADIUS. Auditorías de seguridad Wi-Fi.	**El estándar de oro.** Esto eleva la seguridad de "una contraseña para todos" a "cada usuario/dispositivo se autentica individualmente". Es el pilar de un acceso a la red seguro y moderno.
2.2. Despliegue de un sistema de	Permite un control granular del acceso basado en identidad,	1. Selección de solución NAC. 2. Definición de políticas de acceso	% de dispositivos gestionados por NAC. % de	Reportes de NAC. Alertas del SIEM.	**El cerebro del control de acceso.** El NAC es lo que permite aplicar

control de acceso a la red (nac)	tipo de dispositivo, estado de seguridad y rol, aplicando el principio de Zero Trust.	basadas en roles. 3. Integración con 802.1X y SIEM. 4. Pruebas de cumplimiento y cuarentena.	accesos no autorizados bloqueados.		inteligencia al acceso: un estudiante no puede acceder a la red administrativa, y un dispositivo sin antivirus es puesto en cuarentena. Es la implementación práctica de "Confianza Cero".
2.3. Microsegmentación de la red wi-fi (vlans dinámicas)	La microsegmentación va más allá, aislando el tráfico entre dispositivos incluso dentro de la misma VLAN o SSID, reduciendo la superficie de ataque.	1. Diseño de políticas de microsegmentación. 2. Configuración de APs y switches para VLANs dinámicas (integrado con NAC). 3. Pruebas de aislamiento de tráfico.	Número de segmentos de red implementados. % de tráfico aislado.	Pruebas de penetración internas. Monitoreo de flujos de tráfico.	**Táctica de seguridad avanzada.** Impide el movimiento lateral de un atacante. Si un dispositivo es comprometido, la microsegmentación limita el daño al evitar que se comunique con otros dispositivos innecesariamente.

2.4. Implementación de filtrado de contenido y aplicaciones	Para controlar el acceso a sitios y aplicaciones no deseados o maliciosos, mejorando la seguridad y el uso eficiente del ancho de banda.	1. Evaluación de soluciones de filtrado (NGFW, proxy). 2. Definición de políticas de filtrado. 3. Implementación y monitoreo.	% de tráfico malicioso/no deseado bloqueado.	Reportes del firewall/proxy. Retroalimentación de usuarios.	**Control y protección perimetral.** Es una capa de defensa esencial para proteger a los usuarios de amenazas externas (malware, phishing) y para asegurar que los recursos de la red se usen para fines académicos.
2.5. Gestión de dispositivos iot (inventario y segmentación)	El desconocimiento sobre los dispositivos IoT conectados es una vulnerabilidad. Es crucial identificarlos, inventariarlos y aislarlos en segmentos de red específicos.	1. Descubrimiento y registro de IoT. 2. Creación de VLANs dedicadas para IoT. 3. Implementación de políticas de seguridad específicas.	% de dispositivos IoT inventariados. % de dispositivos IoT segmentados.	Inventario de activos. Monitoreo de tráfico en VLANs IoT.	**Controlar el caos.** Los dispositivos IoT son notoriamente inseguros. Esta iniciativa aborda proactivamente un vector de ataque creciente, aislando estos dispositivos para que no puedan comprometer la red principal.

Eje Estratégico 3: Gobernanza, monitoreo y respuesta a incidentes

Problema Abordado: Dependencia exclusiva de Fortinet, ausencia de plan de contingencia, falta de protocolos documentados para incidentes, gestión inconsistente, auditorías irregulares.

Iniciativa	Fundamentación técnica	Proceso de implementación	Kpis	Mecanismos de control	Análisis estratégico
3.1. Establecimiento de un isms (iso 27001)	Proporciona un marco para gestionar la seguridad de manera sistemática, incluyendo políticas, procedimientos y controles.	1. Definición del alcance. 2. Evaluación de riesgos. 3. Desarrollo de políticas. 4. Implementación de controles. 5. Auditoría.	% de cumplimiento con ISO 27001. Número de políticas documentadas.	Auditorías internas y externas. Revisiones de la dirección.	**Formaliza la seguridad.** Transforma la ciberseguridad de un conjunto de tareas técnicas a un proceso de negocio gestionado, medible y continuamente mejorado, alineado con el EGSI.
3.2. Implementación de un siem	Centraliza y correlaciona los logs de seguridad de todos los dispositivos, facilitando la detección	1. Selección de solución SIEM. 2. Integración de logs. 3. Configuración de reglas de correlación y alertas.	Tiempo de detección de incidentes (MTTD). Número de falsos positivos.	Reportes del SIEM. Ejercicios de detección de amenazas.	**Ojos y oídos de la red.** Un SIEM proporciona la visibilidad necesaria para detectar ataques que de otro modo pasarían

	temprana de anomalías e intrusiones.				desapercibidos. Es la base de un centro de operaciones de seguridad (SOC) moderno.
3.3. Desarrollo de protocolos de respuesta a incidentes	Se necesitan procedimientos estandarizados para identificar, contener, erradicar y recuperar.	1. Creación de un equipo de respuesta (CSIRT). 2. Desarrollo de planes de respuesta. 3. Documentación y socialización.	Tiempo promedio de respuesta (MTTR). % de incidentes resueltos según protocolo.	Simulacros de respuesta. Auditorías de cumplimiento.	**El plan de acción para el "día malo".** Sin un protocolo, la respuesta a un incidente es caótica e ineficaz. Este plan asegura una respuesta coordinada, rápida y que minimiza el daño.
3.4. Realización de auditorías de seguridad wi-fi periódicas	Se deben realizar pruebas de penetración y evaluaciones de vulnerabilidad de forma sistemática.	1. Cronograma de auditorías. 2. Contratación de expertos externos. 3. Realización de escaneos. 4. Seguimiento de remediaciones.	Frecuencia de auditorías. Número de vulnerabilidades críticas remediadas.	Informes de auditoría. Planes de acción correctiva.	**Verificación independiente.** Permite que un tercero experto encuentre las debilidades antes que los atacantes. Es un control de calidad esencial para todo el programa de seguridad.

3.5. Implementación de un plan de contingencia y recuperación (drp)	Se deben definir procedimientos para la continuidad del negocio ante interrupciones prolongadas.	1. Identificación de servicios críticos. 2. Diseño de redundancia y backup. 3. Documentación del DRP. 4. Pruebas periódicas.	Tiempo de recuperación objetivo (RTO). Punto de recuperación objetivo (RPO).	Informes de pruebas de DRP.	**Garantiza la resiliencia.** Mientras que la respuesta a incidentes se enfoca en el ataque, el DRP se enfoca en mantener la operación de la universidad. Asegura que los servicios esenciales puedan continuar a pesar de un desastre.

Eje Estratégico 4: Desarrollo de capacidades humanas y concientización

Problema Abordado: Limitaciones humanas, sobrecarga operativa, falta de capacitación estandarizada, desconocimiento del personal periférico.

Iniciativa	Fundamentación técnica	Proceso de implementación	Kpis	Mecanismos de control	Análisis estratégico
4.1. Programa de capacitación certificada para técnicos (cwnp, ccna security)	Las certificaciones especializadas garantizan un nivel de conocimiento y habilidades estandarizado para el personal técnico.	1. Identificación de necesidades. 2. Selección de cursos y certificaciones. 3. Inscripción y seguimiento. 4. Evaluación de aplicación.	% de técnicos certificados. Puntuaciones en exámenes.	Registros de capacitación. Evaluaciones de desempeño.	**Invierte en el equipo.** Profesionaliza al personal técnico, asegurando que tienen las competencias para gestionar la nueva tecnología y responder a incidentes. Es una inversión directa en la calidad del servicio.
4.2. Simulacros periódicos de ciberataques	La práctica es clave para mejorar la capacidad de respuesta. Permiten ensayar los protocolos	1. Diseño de escenarios. 2. Ejecución de ejercicios de mesa. 3. Realización de simulacros técnicos. 4.	Tiempo de contención en simulacros.	Informes de simulacros.	**Entrenamiento para el combate.** Es como un simulacro de incendio para los ciberataques. Pone a prueba los

	en un entorno controlado.	Análisis y lecciones aprendidas.	Número de errores críticos.	Planes de mejora.	protocolos y al personal, revelando debilidades en un entorno seguro antes de que ocurra un incidente real.
4.3. Programa de concientización para usuarios	Educar a toda la comunidad universitaria sobre las amenazas y las mejores prácticas de seguridad.	1. Desarrollo de materiales. 2. Campañas de concientización (phishing simulado). 3. Inclusión de módulos de seguridad.	% de participación. % de usuarios que reportan phishing.	Encuestas de conocimiento. Reportes de campañas simuladas.	**El firewall humano.** Esta es una de las iniciativas de mayor impacto. Convierte al eslabón más débil (el usuario) en la primera y más grande línea de defensa de la organización.
4.4. Fomento de la cultura de reporte de incidentes	Promover que cualquier miembro de la comunidad se sienta seguro para reportar actividades sospechosas.	1. Establecimiento de canales claros. 2. Comunicación de la importancia del reporte. 3. Reconocimiento y retroalimentación.	Número de reportes de usuarios. Tiempo promedio de reporte.	Registros de incidentes. Encuestas de percepción.	**Crea una red de sensores humanos.** Una cultura donde reportar no es castigado, sino incentivado, aumenta exponencialmente la capacidad de detección temprana de la universidad.

Cronograma

Fase	Duración estimada	Hitos clave	Análisis estratégico
Fase 1: planificación y diseño detallado	2 meses	Formación de equipos, selección de proveedores, diseño de arquitecturas, elaboración de políticas.	Una planificación sólida al inicio es crucial para evitar sobrecostos y retrasos. Esta fase define el éxito del proyecto.
Fase 2: adquisición y preparación	3 meses	Compra de equipos, preparación de infraestructura física y lógica.	Fase logística clave. La gestión de la cadena de suministro y los tiempos de entrega de los proveedores será el principal desafío aquí.
Fase 3: implementación core y piloto	4 meses	Instalación y configuración central, despliegue piloto de WPA3/NAC, integración inicial de SIEM.	El enfoque en un piloto es una excelente práctica de gestión de riesgos. Permite probar y ajustar en un entorno controlado.
Fase 4: despliegue extendido y migración	6 meses	Despliegue progresivo en todo el campus, migración completa, implementación de microsegmentación.	La fase más larga y compleja, que requiere una excelente coordinación para minimizar el impacto en los usuarios finales.

Fase 5: gobernanza y capacitación inicial	3 meses	Establecimiento del ISMS, capacitación a técnicos, primeros simulacros, lanzamiento de concientización.	Se enfoca en los pilares de procesos y personas, asegurando que la nueva tecnología sea bien gestionada y utilizada.
Fase 6: monitoreo y mejora continua	Continuo	Operación del SIEM, auditorías periódicas, actualizaciones, capacitación continua.	Reconoce que la seguridad no es un proyecto con un fin, sino un proceso cíclico y permanente de adaptación.

Presupuesto

Categoría	Descripción	Estimación (usd)	Análisis estratégico
Hardware de red	APs WiFi 7, Controladoras, Switches, Routers, Servidores.	$150,000 - $300,000	La mayor inversión de capital inicial. La selección de proveedores aquí impactará los costos de soporte futuros.
Software y licencias	Licencias de NAC, SIEM, Firewall, EDR, Certificados.	$80,000 - $150,000 (anual)	Costo recurrente significativo (OPEX). Es crucial entender los modelos de licenciamiento (por usuario, por dispositivo, etc.).
Servicios de consultoría e implementación	Diseño, integración, pentesting, auditorías.	$50,000 - $100,000	Esencial para asegurar que la implementación se haga correctamente, especialmente con tecnologías complejas como NAC y SIEM.
Capacitación y certificación	Cursos, exámenes, talleres, materiales.	$30,000 - $60,000	Una de las inversiones con mayor retorno. Un equipo bien capacitado maximiza el valor de todo el hardware y software.

Mantenimiento y soporte	Contratos de soporte para hardware y software.	$40,000 - $80,000 (anual)	Costo recurrente necesario para garantizar la continuidad operativa, actualizaciones de seguridad y soporte técnico.
Contingencia (10-15%)	Fondo para imprevistos.	$35,000 - $80,000	Una práctica de gestión de proyectos prudente y necesaria que demuestra madurez en la planificación financiera.
Total estimado (primer año)		**$385,000 - $770,000**	Un rango realista que refleja la complejidad y la escala del proyecto. La cifra final dependerá de la negociación con los proveedores.

Nota: Estas son estimaciones generales y deben ser detalladas con cotizaciones de proveedores específicos.

5.7. Indicadores Clave de Rendimiento (KPIs)

Un plan sin métricas es solo una intención. Esta selección de KPIs es excelente porque es equilibrada y cubre los tres pilares del proyecto: la infraestructura, la seguridad y las personas. Permiten medir de forma objetiva el retorno de la inversión y el éxito del plan.

Categoría	**Indicador clave de rendimiento (kpi)**	**Análisis estratégico / relevancia**
Infraestructura	Porcentaje de Cobertura WiFi 7	Mide directamente el progreso del despliegue físico y el alcance de la modernización. Es un indicador de cumplimiento del proyecto.
Infraestructura	Tasa de Throughput Promedio	Traduce la inversión en hardware en un beneficio tangible para el usuario: la velocidad. Responde a la pregunta: "¿La red es realmente más rápida?".
Infraestructura	Latencia Promedio	Crítico para aplicaciones modernas (videoconferencias, streaming, etc.). Una baja latencia es sinónimo de una red de alta calidad y una buena experiencia de usuario.
Seguridad	Porcentaje de Dispositivos con WPA3-Enterprise	Mide la tasa de adopción del control de seguridad más fundamental de la red inalámbrica. Un 100% es el objetivo para eliminar vulnerabilidades de protocolos antiguos.
Seguridad	Porcentaje de Cumplimiento de Políticas NAC	Es el termómetro del modelo Zero Trust. Mide qué tan efectivamente se están aplicando las políticas de seguridad en los dispositivos antes de permitir su acceso.
Seguridad	Tiempo Promedio de Detección (MTTD)	Un KPI de ciberseguridad estándar en la industria. Mide la eficacia del SIEM y del equipo de monitoreo. Un MTTD bajo significa que las amenazas se descubren rápidamente.

Seguridad	Tiempo Promedio de Respuesta (MTTR)	Complementa al MTTD. Mide la eficiencia de los protocolos de respuesta a incidentes y del equipo técnico. Un MTTR bajo minimiza el impacto de un ataque.
Seguridad	Número de Vulnerabilidades Críticas Remediadas	Demuestra el valor de las auditorías periódicas y la capacidad del equipo para cerrar brechas de seguridad de alto riesgo de manera proactiva.
Capacidades humanas	Porcentaje de Técnicos Certificados	Cuantifica la inversión en el personal. Mide el aumento del nivel de competencia y especialización del equipo de TIC.
Capacidades humanas	Puntuación Promedio en Simulacros	Es la métrica más clara sobre la preparación práctica del equipo. Mide la capacidad de ejecutar los planes de respuesta bajo presión, no solo en teoría.
Capacidades humanas	Porcentaje de Participación en Concientización	Mide el alcance y la efectividad de las campañas para fortalecer el "firewall humano". Una alta participación es un indicador de una cultura de seguridad en desarrollo.

5.8. Conclusiones

- Coherencia Estratégica: Conecta exitosamente la implementación técnica (WiFi 7, NAC) con conceptos de alto nivel como "modelo Zero Trust" y "seguridad proactiva y resiliente". Esto es ideal para audiencias directivas.
- Visión Integral: Recalca de forma efectiva la sinergia entre la tecnología, la gobernanza y la capacitación, demostrando una comprensión holística del desafío de la ciberseguridad.
- Proyección a Futuro: Finaliza con una nota de visión a largo plazo, posicionando el plan no como un gasto para solucionar problemas pasados, sino como una inversión fundamental que habilita el futuro y posiciona a la UEB como un "referente" nacional. Es un cierre contundente que justifica la inversión.

5.9. Recomendaciones

- Compromiso Institucional y Presupuesto Recurrente: Esta es la recomendación más importante. Transforma la ciberseguridad de un proyecto finito (CapEx) a una función operativa continua y prioritaria (OpEx). Sin un presupuesto recurrente, la inversión inicial se degradará con el tiempo.
- Fomento de la Colaboración Interinstitucional: Una recomendación muy inteligente. La ciberseguridad no se gana en solitario. La colaboración y el intercambio de inteligencia sobre amenazas son multiplicadores de fuerza que permiten a la universidad anticiparse a ataques que ya han afectado a otras instituciones.
- Evaluación y Adaptación Continua: Refuerza el principio de que la seguridad es un ciclo, no una línea recta. Esta recomendación asegura que el plan se mantenga relevante y efectivo frente a amenazas en constante evolución, alineándose perfectamente con el marco ISO 27001.
- Fortalecimiento del Equipo de TIC: Aborda directamente el factor humano desde la perspectiva operativa. Reconoce que la tecnología más avanzada es inútil si el equipo que la gestiona está sobrecargado. Es una recomendación clave para garantizar la sostenibilidad y la proactividad del programa.

CONCLUSIONES

- **Infraestructura Wi-Fi al límite de su vida útil:** El diagnóstico realizado expone una realidad operativa riesgosa: la universidad depende de puntos de acceso Aruba con más de ocho años de servicio, equipos que han superado su ciclo de vida útil. Esta obsolescencia no es solo un problema técnico, sino un impedimento estratégico que bloquea la implementación de parches de seguridad críticos y protocolos modernos como WPA3, manteniendo a la red en un estado de vulnerabilidad permanente frente a amenazas conocidas.
- **Falta de un gobierno unificado de seguridad:** Más allá de los problemas técnicos, el estudio revela una desconexión operativa crítica. La ausencia de protocolos documentados, las configuraciones inconsistentes entre campus (como el aislamiento de clientes) y las respuestas contradictorias del personal técnico no son fallas aisladas, sino síntomas de una falta de gobernanza centralizada. Esto resulta en una gestión fragmentada donde cada área opera con criterios distintos, debilitando la postura de seguridad general.
- **Exposición constante sin capacidad de respuesta ágil:** El verdadero problema yace en la incapacidad institucional para responder de manera coordinada. La dependencia de herramientas dispersas y la falta de un sistema centralizado de monitoreo (SIEM) dejan a los técnicos reaccionando de forma aislada, sin una visión global que permita anticipar o contener amenazas de manera efectiva.
- **Desconexión entre el conocimiento central y la periferia:** Se identificó una brecha profunda en las competencias técnicas. Mientras el equipo central de TIC maneja información parcialmente actualizada, el personal técnico de las facultades opera con conocimiento limitado o desactualizado. Esta disparidad, agravada por la falta de un programa de capacitación continuo, explica las inconsistencias en la configuración de la red y perpetúa un modelo de gestión reactiva, donde las soluciones se aplican sobre la marcha y sin estandarización.

- **Control de acceso débil y superficie de ataque expandida:** La seguridad de la red descansa principalmente en el uso de credenciales institucionales (usuario/contraseña), un método vulnerable frente a técnicas como la fuerza bruta. A esto se suma la falta de un inventario confiable de dispositivos IoT y la gestión no regulada de equipos personales, lo que amplía indiscriminadamente la superficie de ataque. La escasa implementación de autenticación robusta (802.1X/RADIUS) refleja una postura permisiva que incrementa el riesgo de accesos no autorizados y movimientos laterales dentro de la red.

RECOMENDACIONES

- **Asignar un presupuesto urgente para renovar el núcleo de la red:** La universidad debe destinar recursos inmediatos para reemplazar los puntos de acceso obsoletos por equipos que soporten estándares modernos como Wi-Fi 6/7 y WPA3. Esta inversión no es un lujo, sino un requisito mínimo para eliminar vulnerabilidades críticas conocidas y sentar las bases de una red estable. Un plan de financiamiento escalonado (por fases o facultades) podría hacer viable esta transición.
- **Crear un manual único de operaciones y seguridad:** Es fundamental desarrollar y hacer cumplir un conjunto claro de políticas de configuración para toda la red universitaria. Este manual, accesible para todo el personal técnico, debe especificar cómo configurar aspectos críticos como el aislamiento de clientes, las VLANs y el filtrado MAC, acabando con las prácticas arbitrarias y fragmentadas que existen actualmente.
- **Centralizar la visión de la red con una herramienta de monitoreo unificada:** La adquisición e implementación de un sistema SIEM es prioritaria para dejar de depender de reportes manuales y desconectados. Esta plataforma permitirá correlacionar eventos de seguridad en tiempo real, detectar patrones de ataque y medir el desempeño de la red desde una consola central, transformando la gestión de reactiva a proactiva.
- **Institucionalizar la capacitación técnica con un plan concreto:** Más que "capacitar", se propone establecer un programa formal y obligatorio con ciclos semestrales. Este programa debe cerrar la brecha de conocimiento entre el

equipo central y los técnicos de facultad, enfocándose en la configuración estandarizada de la red y la respuesta coordinada a incidentes, utilizando los mismos manuales y herramientas que usan en su trabajo diario.

- **Migrar de las contraseñas simples a una autenticación robusta y segmentada:** Se debe abandonar progresivamente la dependencia de la autenticación por usuario/contraseña. La implementación de un sistema NAC (Control de Acceso a la Red) junto con 802.1X/RADIUS permitirá un control granular sobre quién y qué se conecta a la red, automatizando la segmentación de dispositivos (estudiantes, personal, IoT) y reduciendo drásticamente el riesgo de movimientos laterales en caso de una brecha.

BIBLIOGRAFÍA

Asamblea Nacional. (2008). *Constitución del Ecuador (2008)*.

Asamblea Nacional. (2021). *LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES*. www.lexis.com.ec

Asamblea Nacional. (2022). *LEY ORGÁNICA DE TELECOMUNICACIONES*.

Asamblea Nacional. (2024). *LEY ORGANICA DE GESTION DE LA IDENTIDAD Y DATOS CIVILES*. www.lexis.com.ec

Ataques Man-in-the-Middle (MitM) y autenticación RADIUS. (s/f). Recuperado el 16 de marzo de 2025, de https://www.splashtop.com/es/blog/man-in-the-middle-and-radius?srsltid=AfmBOor1v3ZwbF3gLGGXlf-eIHFxTvWrpGYyFkTPBsX9amOwhPDSTfcG

Carhuaz Malpartida, K. F. (2021). *La seguridad en redes inalámbricas*. Universidad Nacional de Educación Enrique Guzman y Valle. https://repositorio.une.edu.pe/handle/20.500.14039/5393

Cataño García, D. S. (2021, enero 1). *Método para la prevención y mitigación de vulnerabilidades en redes WI-FI*. https://repository.unad.edu.co/handle/10596/44590

Cifuentes Rodríguez, J. J. (2017, agosto 1). *Diseño de un modelo de gestión de seguridad en redes de comunicación inalámbricas aplicado a pequeñas*

empresas del sector privado de la ciudad de Bogotá. https://repository.unad.edu.co/handle/10596/12862

Coleman, E. G. (2019). Coding Freedom. *Coding Freedom*. https://doi.org/10.1515/9781400845293/HTML

Comisión de Justicia y Estructura del Estado. (2014). *CÓDIGO ORGÁNICO INTEGRAL PENAL, COIP*. www.lexis.com.ec

Cristiá, M., Nacional, U., & Rosario -Argentina, R. (2021). *Apunte de clase Seguridad Informática*.

Encriptación de datos: Métodos para la seguridad de la información. (s/f). Recuperado el 16 de marzo de 2025, de https://tuatara.co/blog/software/encriptacion-de-datos-seguridad-de-informacion/

Mero Lino, E. A., Ortíz Hernández, M. M., Yanangómez Zambrano, J. M., & Rodríguez, A. (2021). Análisis de seguridad de las redes inalámbricas en la carrera de Tecnologías de Información. *Serie Científica de la Universidad de las Ciencias Informáticas, ISSN-e 2306-2495, Vol. 14, Nº. 9, 2021 (Ejemplar dedicado a: : Septiembre), págs. 139-147*, *14*(9), 139–147. https://dialnet.unirioja.es/servlet/articulo?codigo=8590648&info=resumen&idioma=ENG

Mora Zambrano, E. R. (2024). Análisis de vulnerabilidades en redes inalámbricas: métodos y soluciones. *INSTA MAGAZINE*, *7*(1), 33–36. http://186.69.149.245/index.php/instamagazine/article/view/66/100

Para qué sirve y cómo configurar el filtrado MAC en el router Wi-Fi. (s/f). Recuperado el 19 de marzo de 2025, de https://www.redeszone.net/tutoriales/configuracion-routers/configurar-filtrado-mac-router/

Puntos de Acceso Falsos: La Amenaza Invisible que Atraviesa el Aire - TI Rescue. (s/f). Recuperado el 19 de marzo de 2025, de https://tirescue.com/puntos-de-acceso-falsos-la-amenaza/

¿Qué es el ataque del gemelo malvado? Explicación del gemelo malvado de Wi-Fi. (s/f). Recuperado el 16 de marzo de 2025, de https://latam.kaspersky.com/resource-center/preemptive-safety/evil-twin-attacks?srsltid=AfmBOoo_hTwA8jCJOzenbupQkLWCgE_UcJ-3H9XgpFO-SQwPj1CeiyRY

¿Qué es el Hacking Ético? - TI Rescue. (s/f). Recuperado el 16 de marzo de 2025, de https://tirescue.com/que-es-el-hacking-etico/

¿Qué es el wifi? - Tipos de conexiones wifi y seguridad | Proofpoint ES. (s/f-a). Recuperado el 15 de marzo de 2025, de https://www.proofpoint.com/es/threat-reference/wifi?utm_source=chatgpt.com

¿Qué es el wifi? - Tipos de conexiones wifi y seguridad | Proofpoint ES. (s/f-b). Recuperado el 15 de marzo de 2025, de https://www.proofpoint.com/es/threat-reference/wifi?utm_source=chatgpt.com

¿Qué es la autenticación? Definición y métodos | Seguridad de Microsoft. (s/f). Recuperado el 19 de marzo de 2025, de https://www.microsoft.com/es-es/security/business/security-101/what-is-authentication

¿Qué es un ataque de fuerza bruta? | Tipos y cómo funciona| Fortinet. (s/f). Recuperado el 16 de marzo de 2025, de https://www.fortinet.com/lat/resources/cyberglossary/brute-force-attack

Que es un Firewall - TI Rescue. (s/f). Recuperado el 16 de marzo de 2025, de https://tirescue.com/que-es-un-firewall/

¿Qué es un sniffer? Características y riesgos del sniffing. (s/f). Recuperado el 16 de marzo de 2025, de https://ecuador.unir.net/actualidad-unir/que-es-sniffer-red/

¿Qué es una conexión VPN, para qué sirve y qué ventajas tiene? (s/f). Recuperado el 19 de marzo de 2025, de https://www.xataka.com/basics/que-es-una-conexion-vpn-para-que-sirve-y-que-ventajas-tiene

Sánchez Espinosa, F., Vivero García, J., & Llanos, D. B. (2018). *Aplicación de una metodología de seguridad avanzada en redes inalámbricas*.

Seguridad de Wi-Fi: WEP, WPA y WPA2. (s/f). Recuperado el 15 de marzo de 2025, de https://www.avast.com/es-es/c-wep-vs-wpa-or-wpa2?utm_source=chatgpt.com

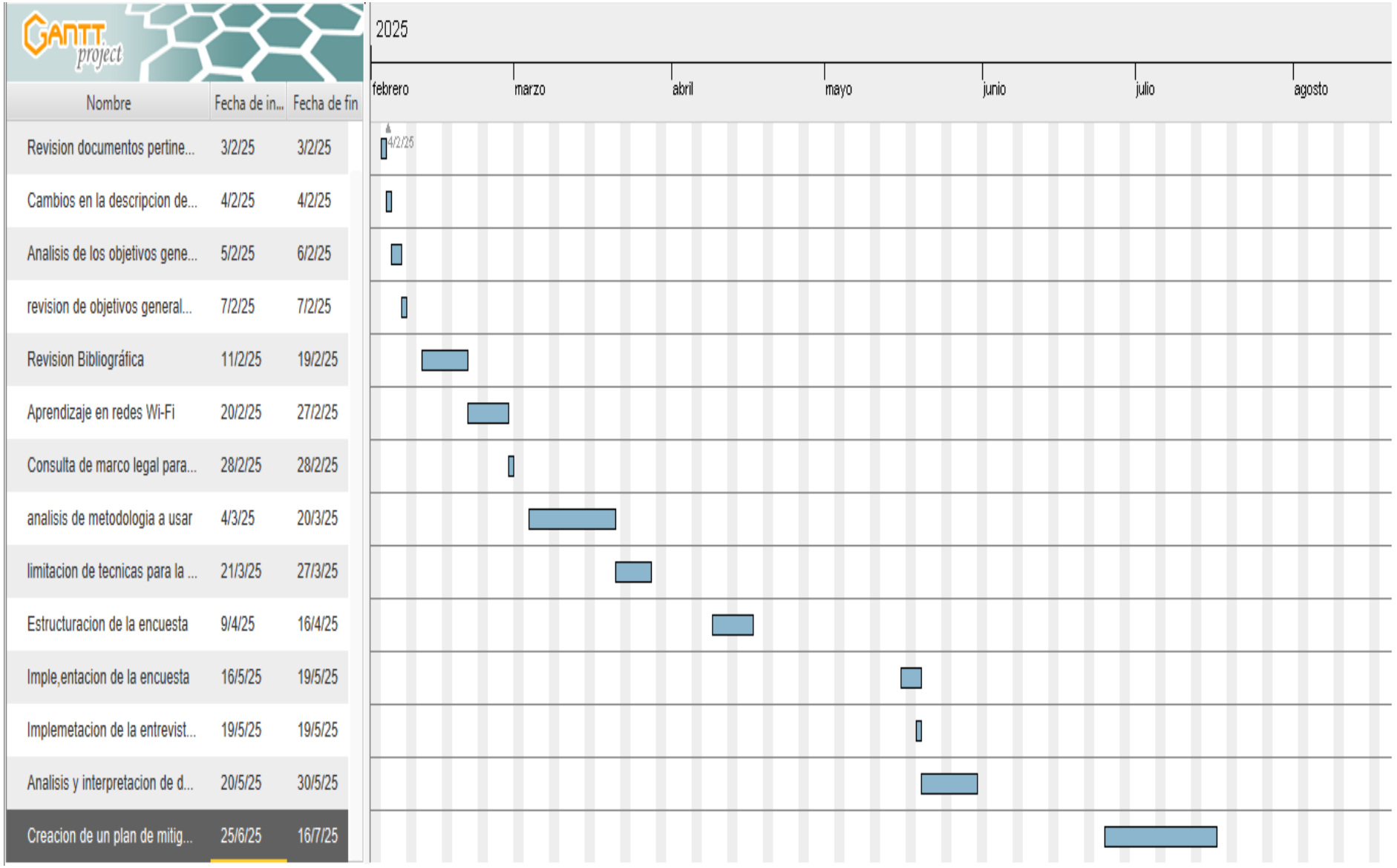
SSID de red: qué es, cómo encontrar el tuyo y cómo cambiarlo. (s/f). Recuperado el 19 de marzo de 2025, de https://www.xataka.com/basics/ssid-red-que-como-encontrar-tuyo-como-cambiarlo

Tipos de Vulnerabilidades y Amenazas informáticas. (s/f). Recuperado el 16 de marzo de 2025, de https://www.ambit-bst.com/blog/tipos-de-vulnerabilidades-y-amenazas-inform%C3%A1ticas

Transformación digital en Latinoamérica - OT Latam. (s/f). Recuperado el 16 de marzo de 2025, de https://ot-latam.com/?utm_source=google&utm_medium=cpc&utm_campaign=campana-ciber-trafico&utm_id=trafico&utm_term=ciberseguridad&utm_content=anuncio1&gad_source=1&gclid=Cj0KCQjwkN--BhDkARIsAD_mnIrBODUchxYRbMItJlNBUlcfPeUEY8f4XFrguRA2nGxOP1eabd0SHjoaArzmEALw_wcB

ANEXOS

ANEXOS 1:
Cronograma (Gantt)


GANTT project
2025
febrero
marzo
abril
mayo
junio
julio
agosto
Nombre
Fecha de in...
Fecha de fin
Revision documentos pertine... 3/2/25 3/2/25
Cambios en la descripcion de... 4/2/25 4/2/25
Analisis de los objetivos gene... 5/2/25 6/2/25
revision de objetivos general... 7/2/25 7/2/25
Revision Bibliográfica 11/2/25 19/2/25
Aprendizaje en redes Wi-Fi 20/2/25 27/2/25
Consulta de marco legal para... 28/2/25 28/2/25
analisis de metodologia a usar 4/3/25 20/3/25
limitacion de tecnicas para la ... 21/3/25 27/3/25
Estructuracion de la encuesta 9/4/25 16/4/25
Imple,entacion de la encuesta 16/5/25 19/5/25
Implemetacion de la entrevist... 19/5/25 19/5/25
Analisis y interpretacion de d... 20/5/25 30/5/25
Creacion de un plan de mitig... 25/6/25 16/7/25

ANEXOS 2:
Presupuesto Ejecutado

Tabla Presupuesto

Concepto	*Cantidad*	*Tiempo*	*Descripción*	*Costo*
Tecnología hardware y software	1	5 meses	Laptop, Internet	$850
Costos operativos	1	5 meses	Transporte	$240
Costos de utilería	1	5 meses	Impresiones, anillado y empastado	$150
Contingente	1	5 meses	Imprevistos durante el desarrollo del trabajo de investigación	$120
	Total			$1360

Fuente: Elaboración propia

ANEXOS 3:

Instrumentos de recopilación de datos (entrevista no estructurada, encuesta)

ENTREVISTA NO ESTRUCTURADA

Proyecto de investigación: *"Vulnerabilidades en Redes Wi-Fi de la Universidad Estatal de Bolívar en el año 2025"*
Fecha de la entrevista:
Lugar:
Nombre del entrevistador:
Cargo o área del entrevistado:
Confidencialidad:
Esta entrevista tiene fines exclusivamente académicos. La información proporcionada será tratada con estricta confidencialidad y no se divulgarán nombres ni datos personales.
Tema central:
Gestión integral de la seguridad en redes Wi-Fi institucionales: infraestructura, mantenimiento de firmware, detección de amenazas, políticas de acceso, capacitación técnica y asignación presupuestaria

Patricio Pachala



ENCUESTA

"VULNERABILIDADES EN REDES WI-FI DE LA UNIVERSIDAD ESTATAL DE BOLÍVAR EN EL AÑO 2025"

Fecha:16/05/2025

Objetivo:

Esta encuesta busca recopilar información técnica sobre las medidas de seguridad implementadas en las redes Wi-Fi de la Universidad Estatal de Bolívar, como parte de la investigación "Vulnerabilidades en Redes Wi-Fi de la UEB en el año 2025". Sus respuestas permitirán:

- Identificar debilidades en protocolos, hardware y políticas de seguridad.
- Proponer mejoras basadas en evidencia técnica.

Confidencialidad:

- Los datos proporcionados serán utilizados **exclusivamente con fines académicos**.

Preguntas:

1. Infraestructura y configuración de red

1. ¿Qué tipo de protocolo IP predomina en la red institucional?
   ☐ IPv4

   ☐ IPv6

   ☐ Ambos por igual

   ☐ No estoy seguro

2. ¿Qué protocolo de encriptación utiliza actualmente la red Wi-Fi de la Universidad Estatal de Bolívar?
   ☐ WPA2

   ☐ WPA3

   ☐ Otro: _____ (Especifique)

   ☐ No sé

3. ¿La red Wi-Fi institucional está segmentada mediante VLANs?
   ☐ Sí, en toda la universidad

   ☐ Sí, parcialmente

   ☐ No

☐ No estoy seguro

4. ¿Qué sistemas operativos utilizan los puntos de acceso Wi-Fi? (Puede marcar más de uno)
   ☐ Linux

   ☐ Windows Server

   ☐ Cisco IOS

   ☐ Otro: _____ (Especifique)

5. ¿Qué puertos suelen estar abiertos en los puntos de acceso Wi-Fi?

---

6. ¿Se encuentra habilitado el aislamiento de clientes (Client Isolation) en la red Wi-Fi?
   ☐ Sí, en todas las redes

   ☐ Solo en redes de invitados

   ☐ No

   ☐ No sé

---

2. Autenticación y control de acceso

7. ¿Qué métodos de autenticación se emplea para el acceso a la red Wi-Fi?
   ☐ Usuario/contraseña institucional

   ☐ Autenticación MAC
   ☐ Certificado digital

   ☐ 802.1X/RADIUS

   ☐ Captive Portal
   ☐ Otro: _____ (Especifique)

8. ¿Existe filtrado por direcciones MAC en la red?
   ☐ Sí, en toda la red

   ☐ Solo en áreas críticas

   ☐ No

   ☐ No sé

9. ¿Cómo se gestiona el acceso de dispositivos personales a la red Wi-Fi?

10. ¿Qué tipo de restricciones de acceso o uso están implementadas en la red Wi-Fi?

---

11. ¿Existe una red Wi-Fi separada para visitantes?
    ☐ Sí, con acceso limitado

    ☐ Sí, sin restricciones

    ☐ No

    ☐ No sé

---

3. Monitoreo, auditoría y gestión de incidentes

12. ¿Con qué frecuencia se detectan intentos de intrusión en la red Wi-Fi?
    ☐ Diariamente

    ☐ Semanalmente

    ☐ Mensualmente

    ☐ Nunca / No se monitorea

13. ¿Qué herramientas se utilizan para registrar o gestionar incidentes de seguridad?
    ☐ SIEM

    ☐ Bitácora digital o física

    ☐ No se registran
    ☐ Otro: _____ (Especifique)

14. ¿Se realizan auditorías de seguridad Wi-Fi?
    ☐ Sí, periódicamente

    ☐ No regularmente

    ☐ Nunca

15. ¿Existe un protocolo documentado de respuesta ante incidentes de seguridad Wi-Fi?
    ☐ Sí → Describa brevemente: _____
    ☐ No

    ☐ No estoy seguro

4. Amenazas y dispositivos conectados

15. ¿Qué tipos de ataques ha detectado o considera posibles en la red Wi-Fi? (Marque los que correspondan)
    ☐ Evil Twin
    ☐ Ataques Deauth
    ☐ Fuerza bruta
    ☐ Interceptación MITM
    ☐ Suplantación DNS
    ☐ Ninguno
16. ¿Con qué frecuencia se actualiza el firmware de los puntos de acceso Wi-Fi para corregir vulnerabilidades?
    ☐ Siempre que el fabricante lanza una nueva versión
    ☐ De forma periódica (mensual/trimestral)
    ☐ Solo cuando hay incidentes de seguridad
    ☐ No se actualiza regularmente
    ☐ No sé
17. ¿Qué dispositivos IoT están actualmente conectados a la red Wi-Fi institucional?

---

5. Recursos humanos y presupuesto

18. ¿El personal técnico recibe capacitación específica en seguridad Wi-Fi?
    ☐ Sí, anualmente
    ☐ Sí, semestralmente
    ☐ Solo al ingreso
    ☐ No
19. ¿Qué herramientas considera necesarias para mejorar la seguridad de la red Wi-Fi?

ANEXOS 4:
Certificado Antiplagio

ING. RODRIGO DEL POZO EN CALIDAD DE DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR,

CERTIFICA

Que el trabajo de integración curricular denominado "**VULNERABILIDADES EN REDES WI-FI DE LA UNIVERSIDAD ESTATAL DE BOLÍVAR, EN EL AÑO 2025**", presentado por Cristian Josue Garófalo Yánez estudiantes de la **carrera de Software** pasó el análisis de coincidencia no accidental en la herramienta TURNITIN, reflejando un **porcentaje de similitud del 4%**, como se puede evidenciar en el documento adjunto.

Guaranda, 25 de agosto del 2025

Atentamente,

Ing. Rodrigo Del Pozo
Director

Firmado electrónicamente por:
RODRIGO HUMBERTO
DEL POZO DURANGO
Validar únicamente con FirmaEC

Tesis Garofalo Final.docx

My Files
My Files
Universidad Estatal de Bolivar

Detalles del documento

Identificador de la entrega
trn:oid:::3117:477529560

Fecha de entrega
31 jul 2025, 8:20 a.m. GMT-5

Fecha de descarga
31 jul 2025, 10:45 a.m. GMT-5

Nombre de archivo
Tesis Garofalo Final.docx

Tamaño de archivo
3.6 MB

99 Páginas

17.707 Palabras

104.885 Caracteres

turnitin Página 1 of 103 - Portada Identificador de la entrega trn:oid:::3117:477529560

4% Similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para ca...

Filtrado desde el informe

- Bibliografía
- Texto citado
- Texto mencionado
- Coincidencias menores (menos de 16 palabras)

Exclusiones

- N.º de fuentes excluidas
- N.º de coincidencias excluidas

Fuentes principales

2% Fuentes de Internet
0% Publicaciones
4% Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.º de alerta de integridad para revisión

Texto oculto
153 caracteres sospechosos en N.º de páginas
El texto es alterado para mezclarse con el fondo blanco del documento.

Los algoritmos de nuestro sistema analizan un documento en profundidad para buscar inconsistencias que permitirían distinguirlo de una entrega normal. Si advertimos algo extraño, lo marcamos como una alerta para que pueda revisarlo.

Una marca de alerta no es necesariamente un indicador de problemas. Sin embargo, recomendamos que preste atención y la revise.

ANEXOS 5:

Link del repositorio digital de biblioteca donde fue subido el proyecto