Universidad Nacional de Ingeniería

Facultad de Ciencias y Sistemas

IMPORTANCIA DEL DESCONOCIMIENTO DE LA PRIVACIDAD Y SEGURIDAD EN LAS REDES WIFI PUBLICAS EN EL MUNICIPIO DE CIUDAD SANDINO.

Trabajo Monográfico para optar al título de Ingeniero de Sistemas.

Elaborado por:

Br. Roberto Eduardo López Pereira.
Carnet: 2020-0279I

Br. Anthony Brandon Guevara Morales.
Carnet: 2020 – 0289I

Br. Martin Eduardo Janns Martínez
Carnet: 2017 – 0670I

Tutor:

Msc. Ing. Mario José Selva Mendoza

Noviembre, 2023
Managua, Nicaragua

Universidad Nacional de Ingeniería

Contenido

Universidad Nacional de Ingeniería

I. Introducción

La evolución de la tecnología ha transformado la forma en que buscamos información y nos comunicamos en Ciudad Sandino. En la actualidad, la mayoría de la población recurre a Internet como su principal fuente de conocimiento, desplazando a las tradicionales bibliotecas y librerías que solían ser los puntos de referencia para la adquisición de información y transferencia de datos. Este cambio ha sido impulsado por una serie de ventajas que ofrece el acceso a la red, como la rapidez en la búsqueda de información, la capacidad de transferir grandes cantidades de datos con facilidad, la diversidad de temas disponibles y la economía de no tener que adquirir material impreso.

El acceso a Internet se ha convertido en una herramienta indispensable en nuestras vidas cotidianas, brindando la posibilidad de estar al tanto de las últimas noticias, investigar temas de interés y acceder a recursos educativos de manera eficiente. La comodidad y la inmediatez que ofrecen las redes Wi-Fi públicas en Ciudad Sandino han contribuido significativamente a esta transformación, permitiendo a los ciudadanos conectarse desde lugares públicos como parques y plazas. Sin embargo, a medida que aumenta la dependencia de estas redes, también surgen preocupaciones importantes relacionadas con la privacidad y la seguridad de los usuarios.

Es crucial abordar de forma proactiva la cuestión de la privacidad y seguridad en las redes Wi-Fi públicas de Ciudad Sandino. A medida que avanzamos hacia una sociedad cada vez más interconectada, es imperativo asegurar que los ciudadanos puedan disfrutar plenamente de los beneficios de Internet sin exponer su información personal ni comprometer su seguridad digital.

II. Antecedentes

En los últimos años una de las tecnologías que más ha evolucionado son las Redes de área local inalámbricas (Wireless Local Área Networks), las cuales tienen la funcionalidad de brindar conexión a una Red de computadoras local o a internet sin necesidad de una conexión física, como sucedía con las redes cableadas. Sin embargo, desde su estandarización uno de los grandes retos que presentó fue la seguridad, puesto que son más difíciles de proteger debido a que utilizan ondas de radio y por tanto el espacio libre como medio de transmisión.

Para enfrentar esta problemática de las redes inalámbricas el instituto de Ingenieros Eléctricos y Electrónicos (Institute of Electrical and Electronics Engineers, IEEE) manifestó mecanismos de encriptación y autenticación en su estándar 802.11, en 1999. Sin embargo, en 2001 fueron publicados una serie de documentos que evidenciaban vulnerabilidades en este mecanismo de encriptación y ponían en duda la seguridad de las redes WiFi, puesto que el método de autenticación del estándar 802.11 no era el más seguro.

Para solucionar esta problemática y las necesidades de seguridad en redes inalámbricas el IEEE público su estándar certificado 802.11i en 2004, el cual presentaba mejoras significativas para la seguridad, como era la incorporación de una capa de seguridad especifica.

Siendo la seguridad uno de los grandes inconvenientes en las comunicaciones inalámbricas no ha sido un obstáculo para el crecimiento en masa que ha tenido la

tecnología WiFi en los últimos años y se estima que siga en crecimiento, puesto que los equipos portátiles representan una amplia facilidad de movilidad y estabilidad.

III. Planteamiento de problema

El acceso a Internet en el Municipio de Ciudad Sandino representa una herramienta esencial para el desarrollo socioeconómico y la participación ciudadana. Sin embargo, se enfrenta a una serie de desafíos relacionados con la privacidad, seguridad y la accesibilidad que requieren una atención inmediata.

Ciudad Sandino, al igual que muchas otras localidades, experimenta problemas significativos en relación con sus redes Wi-Fi públicas. La falta de seguridad y privacidad en estas redes expone a los usuarios a riesgos potenciales, incluyendo la interceptación de datos sensibles y el acceso no autorizado. Además, la accesibilidad a estas redes es limitada, lo que reduce su utilidad para la comunidad.

En este contexto, surgen preguntas fundamentales que deben abordarse para buscar una solución óptima:

Pregunta Principal:

¿Cuánto desconocimiento tiene la población del municipio acerca de la falta de privacidad y seguridad en las redes públicas?

Subpreguntas:

1. ¿Cuál es la mejor forma de informar a la población municipal del riesgo que corren al desconocer estos tipos de robos a su privacidad?
2. ¿Cuál es el impacto que tendrá esta información en el resto de la población?

IV. Objetivos

4.1. Objetivo general

- Analizar el nivel de desconocimiento de la privacidad y seguridad en las redes Wi-Fi públicas del Municipio de Ciudad Sandino.

4.2. Objetivos específicos

- Realizar un diagnóstico con el método de observación directa del uso promedio de las redes wifi públicas.
- Encuestar a cierta población acerca de los riesgos del uso de las redes wifi públicas.
- Dar a conocer los resultados obtenidos de la encuesta.

V. Justificación

Este estudio se fundamenta en la imperiosa necesidad de abordar la seguridad y privacidad en las redes Wi-Fi públicas del Municipio de Ciudad Sandino, reconociendo el papel fundamental que desempeña el acceso a Internet en la vida cotidiana de sus habitantes. En la era actual, el Internet no solo representa una herramienta de comunicación, sino también un medio esencial para la obtención de información, formacióny participación en la sociedad digital. En este contexto, la propuesta sobre la privacidad y seguridad en las redes Wi-Fi públicas surge como una respuesta crucial a los desafíos emergentes relacionados con la integridad de los datos y la confidencialidad de la información en un entorno cada vez más conectado.

La creciente dependencia de la conectividad online en Ciudad Sandino ha revelado la existencia de vulnerabilidades en las redes Wi-Fi públicas, exponiendo a los ciudadanos ariesgos de seguridad y pérdida de privacidad. Este estudio se justifica en la urgente necesidad de proteger la información sensible de los usuarios y garantizar un entorno digital seguro para la comunidad. Además, se considera esencial abordar estos desafíos enel marco de la promoción del acceso equitativo a la información y los servicios en línea, reconociendo el Internet como una herramienta clave para el desarrollo socioeconómico ycultural del municipio.

El análisis de la seguridad y privacidad en las redes Wi-Fi públicas no solo responde a la actualidad, sino que también anticipa las demandas futuras de una sociedad cada vez másconectada. En este sentido, el presente trabajo

investigativo busca proporcionar soluciones pertinentes y prácticas que no solo mitiguen los riesgos actuales, sino que también sienten las bases para un desarrollo digital sostenible en Ciudad Sandino.

VI. Marco de Referencia

6.1. Metodología Top-Down Network.

"La metodología Top-Down se centra en el análisis de requisitos y en la definición de la seguridad y privacidad en las redes WiFi públicas antes de la selección de componentes específicos para construir la infraestructura física de la red." (J G, 2012, pág. 28).

Esta metodología presenta las siguientes fases:

6.1.2. Fase 1: Análisis de Requisitos de Seguridad

- Identificar y comprender los requisitos de seguridad específicos para la red WiFi pública.
- Determinar las regulaciones y estándares de seguridad que deben cumplirse.

6.1.3. Fase 2: Evaluación de Riesgos

- Realizar una evaluación de riesgos para identificar posibles amenazas y vulnerabilidades en la red.
- Clasificar los riesgos según su impacto y probabilidad.

6.1.4. Fase 3: Definición de Políticas de Seguridad

- Establecer políticas de seguridad claras y específicas para la red WiFi pública.
- Incluir políticas relacionadas con la autenticación, autorización, encriptación y control de acceso.

6.1.5. Fase 4: Implementación de Controles de Acceso

- Configurar medidas de control de acceso para garantizar que solo usuarios autorizados puedan acceder a la red.
- Utilizar autenticación robusta, como WPA3, y considerar el uso de certificados digitales.

6.1.6. Fase 5: Encriptación de Datos

- Implementar protocolos de encriptación fuertes, como WPA3-Enterprise, para proteger la confidencialidad de los datos transmitidos.
- Asegurarse de que las comunicaciones estén protegidas mediante VPN (Redes Privadas Virtuales) si es necesario.

6.1.7. Fase 6: Monitoreo Continuo

- Establecer un sistema de monitoreo continuo para detectar y responder rápidamente a cualquier actividad sospechosa.
- Utilizar herramientas de análisis de tráfico para identificar patrones anómalos.

6.1.8. Fase 7: Educación y Concientización

- Proporcionar educación continua a los usuarios sobre prácticas seguras en redes WiFi públicas.
- Informar sobre posibles amenazas y cómo evitar caer en trampas de seguridad.

6.1.9. Fase 8: Actualizaciones y Mantenimiento

- Mantener actualizados todos los dispositivos y sistemas relacionados con la red WiFi.
- Aplicar parches de seguridad y actualizaciones de firmware de manera regular.

6.1.10 Fase 9: Respuesta a Incidentes

- Establecer un plan de respuesta a incidentes para abordar cualquier violación de seguridad de manera eficiente.
- Documentar procedimientos para mitigar y recuperarse de incidentes de seguridad.

6.2. Conceptos propios

6.2.1. Las Redes

Según (Limones, 2021) nos menciona que "Una red informática es la unión de dos dispositivos o algo tan complejo como millones de dispositivos conectados entre sí. Se define como un conjunto de nodos conectados directa o indirectamente, haciendo uso de algún medio de comunicación para intercambiar datos, compartir archivos y recursos, por cada uno de los equipos o máquinas (móviles, PCs, tablets.) que forman parte de la red."

También (Limones, 2021) nos dice que "Con la creación de una red informática se puede compartir información, datos, equipos (hardware) y aplicaciones (software). De esta forma, estarán disponibles para todos los nodos de la red que lo soliciten siempre y cuando se les otorguen los permisos necesarios para poder acceder a ellos. Además de lo anterior, permitirá un ahorro económico y se tendrá acceso en tiempo real a la información, lo que provocará un aumento de la producción, una mejora en la toma de decisiones e incluso un incremento del rendimiento del personal de las empresas."

6.2.2. Aplicaciones de las redes LAN

Según (tanenbaum & Wetherall, 2012, pág. 12) nos dicen que "Las redes de área local, generalmente llamadas LAN (Local Área Networks), son redes de propiedad privada que operan dentro de un solo edificio, como una casa, oficina o fábrica. Las redes LAN se utilizan ampliamente para conectar computadoras personales y electrodomésticos con el fin de compartir recursos (por ejemplo, impresoras) e intercambiar información. Cuando las empresas utilizan redes LAN se les conoce como redes empresariales".

Según (NetCloudEngineering, 2019) Nos plantea que una red LAN "Es una red que conecta uno o más ordenadores dentro de un ámbito pequeño y limitado. Se puede encontrar a través de **cable Ethernet**, lo que

significa que todos *los dispositivos se interconectan mediante un router*. Si se hace a través de ondas de radio hablamos de **WLAN**, lo que nos permite eliminar todo el problema de los cables."

6.2.3. Seguridad en Redes WIRELESS

Según (Sánchez, 2012) "Las redes inalámbricas constan de dos elementos clave: las estaciones y los puntos de acceso, la comunicación puede realizarse entre estaciones o a través de puntos de acceso. Un punto de acceso transmite señales de gestión periódicamente, una estación después de recibir esta señal inicia la autenticación mediante el envío de una trama. Una vez realizada la autenticación se produce la asociación entre los dos equipos."

6.2.4. IEEE 8.2.11.

Según (Kurose & Ross, 2017, pág. 440) nos mencionan lo siguiente que "Los estándares presentan algunas diferencias importantes en la capa física. Los dispositivos 802.11 operan en dos rangos de frecuencia distintos: 2,4–2,4835 GHz (al que se hace referencia como rango de 2,4 GHz) y 5,1 – 5,8 GHz (el rango de 5 GHz). El rango de 2,4 GHz es una banda de frecuencias sin licencia, en la que los dispositivos 802.11 pueden competir por el espectro de frecuencias con los hornos microondas y teléfonos a 2,4 GHz. A 5 GHz, las redes LAN 802.11 proporcionan una distancia de transmisión más corta para un determinado nivel de potencia y se ven más afectadas por la propagación multica mino."

Sistema abierto:

Primeramente, se explicará de las llamadas redes abiertas, estas redes se caracterizan por no implementar ningún sistema de autenticación o cifrado, las comunicaciones entre terminal y AP (punto de acceso) viajan en texto plano (sin cifrar) y no se necesita ningún dato para acceder a la red.

Claves Compartidas:

En este servicio de autenticación existen claves que son compartidas entre el AP y la terminal.

En este tipo de servicio se sigue una serie de pasos:

- El AP pide a la terminal que se autentique mediante el envío de una trama de datos.
- Una vez recibida, la terminal debe codificar dicha trama y reenviarla al AP.
- El AP decodificará la trama retransmitida por la terminal.
- Si la trama es igual a la original, el AP permitirá a la terminal establecer una asociación, en caso contrario se niega el acceso.

6.2.5. Riesgo en las Redes Wifi

Según (J G, 2012) nos plantean que “El utilizar el espacio libre como medio de transmisión en un factor que pone en riesgola información confidencial. Hay ataques dirigidos a la seguridad de una red inalámbrica, entre los cuales se mencionan:

- Romper Access control Lista basados en MAC: entre las primeras medidas de seguridad usadas en redes wireless fue el filtrado de conexiones por dirección MAC. para ello se crea una lista de direcciones MAC en el AP indicando solo las direcciones que podrán tener acceso permitido o denegado. este método es poco seguro debido a la sencillez de cambiar la dirección MAC de nuestra tarjeta por otra valida previamente obtenida mediante un sniffer.
- Ataque de denegación de servicio: conocido como ataque DoS, el objetivo de este ataque consiste en impedir la comunicación entre un terminal y un AP, para lograr esto solo debemos hacernos pasar por el AP poniéndonos su dirección MAC (obtenida con un sniffer) y negar la conmutación al terminal mediante el envío continuo de notificaciones de desasociación.
- Suplantación: se hace creer a la terminal victima que el atacante es el AP, y al mismo tiempo, convencer al AP que el atacante es el cliente. se usa un sniffer para obtener los siguientes datos necesarios:
    - El ESSID de la red
    - La dirección MAC del AP
    - La dirección MAC de la terminal

Conociendo estos datos se emplea la misma técnica del ataque DoS para romper la conexión entre terminal y AP, tras la ruptura la tarjeta de la terminal comenzara a buscar un nuevo AP empleando su MAC y ESSID en un canal diferente, de manera paralela el atacante ha de suplantar la identidad de la terminal con el AP empleando para esto la dirección MAC de la terminal, de esta manera ni AP ni terminal se dan cuenta de la infiltración.”

Como se mencionó en la sección de “seguridad de redes”, las medidas de seguridad que se implementaban se centran en impedir el acceso a la red a usuarios no autorizados. Sin embargo, ninguna de las medidas anteriores se emplea para evitar la obtención de información intercambiada entre el AP y las terminales.

Para solucionar esto se implementa el cifrado de las comunicaciones de tal forma que si alguien captura las comunicaciones entre una terminal y el AP no pueda acceder a la información concreta enviada.

6.2.6. Algoritmo WEP

Según (J G, 2012) nos mencionan que “La Privacidad Equivalente al Cableado WEP fue el primer mecanismo de seguridadque se implementó bajo el estándar 802.11 aprobado por la IEEE y opera en la capa dos delmodelo OSI. Este algoritmo permite codificar los datos que se transfieren a través de una red inalámbrica y autenticar los dispositivos móviles que se conectan al AP.”

Asi como también (J G, 2012) nos dicen que “La seguridad ofrecida por WEP tiene como pilar fundamental el uso de una clavecompartida entre todas las terminales y el AP la cual se emplea para cifrar los datos enviados, lo que reduce en gran medida la seguridad que puede ofrecer este sistema.”

6.2.7. Debilidades

Según (J G, 2012) nos dicen lo siguiente “La encriptación WEP no cubre las transmisiones desde el principio hasta el final, solamente protege la información de los paquetes de datos, pero no protege a nivel físico.Esto implica que datos de control necesarios para gestionar la red pueden ser capturados por dispositivos móviles extraños.”

Tambien (J G, 2012) nos plantean que una “WEP emplea claves de cifrado estáticas, las cuales son configuradas manualmente y deben ser cambiadas periódicamente. Un intruso puede acumular grandes cantidades de texto cifrado con la misma clave e intentar un ataque por fuerza bruta.”

6.2.8. Topología básica de red.

Segun (Buettrich & Pascual) nos dicen que **“**La topología de una red representa la disposición de los enlaces que conectan los nodos de una red. Las redes pueden tomar muchas formas diferentes dependiendo de cómo están interconectados los nodos. Hay dos formas de describir la topología de una red: física o lógica.”

También (Buettrich & Pascual) nos dicen lo siguiente “La topología física se refiere a la configuración de cables, antenas, computadores y otros dispositivos de red, mientras la topología lógica hace referencia a un nivel más abstracto, considerando por ejemplo el método y flujo de la información transmitida entre nodos.” (Buettrich & Pascual)

6.2.9. Seguridad de la Red

Según (Chavez, 2023) nos dice que “La seguridad de la red es toda aquella actividad, proceso, tecnología o política que busca proteger los recursos digitales de un individuo u organización de amenazas a su confidencialidad y disponibilidad.”

También (Chavez, 2023) nos menciona que “Su principal objetivo es evitar que ataques maliciosos logren acceder a redes internas de ordenadores u otros dispositivos, protegiendo así los datos, sistemas y dispositivos donde estos se almacenan. Esto asegura que la información que entra y sale de los dispositivos, se conserve solo entre ellos y sus destinatarios, permaneciendo confidenciales y alejados de terceros.”

Asi como también (Chavez, 2023) nos menciona “Las principales razones por las que un hacker podría atacar son: robo de información o identidad, manipulación de datos e interrupción del servicio.”

6.6 Teorías.

6.6.1 Teoría de la comunicación.

La página Tesis y Masters nos dice que “Podemos definir a la teoría de la comunicación como un estudio que se especializa en la investigación y análisis de la capacidad que tienen los individuos de tener relaciones con otros. Esto por medio del intercambio de información y el buen entendimiento a la hora de establecer el proceso comunicativo.” (Masters, 2021)

También nos plantea que “La historia de la teoría de la comunicación no arranca sino hasta la concepción misma de la sociedad de la comunicación, en el final Siglo XIX. Este proceso se originó como resultado de los continuos procesos urbanos e industriales de la época. De ahí, la comunicación comenzó a enriquecerse más y más. Desde ese punto, podemos llegar a lo que se conoce como el nacimiento de la teoría de la comunicación, en el Siglo XX, más puntualmente en el año 1920.” (Masters, 2021)

La teoría nos dice que “Claude Shannon, era considerado el padre de la teoría de la información, señaló que e instaló el concepto de “ruido” como una parte fundamental para que la comunicación sea efectiva. Eso es algo que, de manera totalmente lógica, se mantiene incluso a día de hoy, al menos en la comunicación verbal.” (Masters, 2021)

“En el año 1948, Shannon indicó que había encontrado la manera más óptima de cifrar la información que era expuesta por el emisor. Claramente, teniendo en cuenta ese último concepto que te marcamos, se destacó por ser él quien desarrolló e ideó los elementos que participan en los procesos comunicativos de la teoría de la comunicación.” (Masters, 2021).

6.6.2 Teoría de la información.

La revista Aladro Vico Eva da a entender que “La teoría de la Información es una disciplina mapa, tal y como la definió en su día el profesor Valbuena de la Fuente (1997:18). Su objetivo fundamental es orientar y

situar el conocimiento en torno a la comunicación, con una dirección concreta específica para investigar la información.” (Aladro Vico, 2011)

“La Teoría de la Información nació de una Teoría del Periodismo, y posteriormente de una Teoría de la Noticia (vid. Ángel Benito 1982). La dificultad extrema de estudiar los procesos profesionales informativos y los fenómenos sociales y psicológicos asociados a ellos, que surgió con esos orígenes, ha hecho que el ánimo de dinamismo sea grande en esta disciplina, teniendo que adaptarse a los diversos enfoques y cambios de contexto que han ido surgiendo en la vida social informativa.” (Aladro Vico, 2011)

“En cierta etapa, la Teoría de la Información se adaptó a las teorizaciones matemáticas y cibernéticas que se estaban dando de los fenómenos comunicativos. En otro momento, el estudio sociológico abrió esta disciplina al análisis de los medios de masas y sus efectos y contextos. En otro, los descubrimientos psicosociales obligaron a la Teoría de la Información a absorber conocimientos del campo cognitivo y psicológico, y en otro, las metodologías de análisis del mensaje abrieron la disciplina al análisis cultural más amplio” (Aladro Vico, 2011)

VII. Diseño Metodológico

7.1. Tipo de Diseño

El tipo de diseño a desempeñar es Cualitativo, ya que nos permite analizar e interpretar datos obtenidos de fuentes electrónicas y/o audiovisuales sin la necesidad de aplicar análisis estadísticos.

La investigación cualitativa se abstiene de establecer, al principio, un concepto claro de lo que se estudia y de formular hipótesis para someterlas a prueba. Por el contrario, los conceptos o hipótesis se desarrollan y mejoran en el proceso de investigación. La investigación cualitativa parte de la idea de que los métodos y las teorías deben ser apropiadas para lo que se estudia. Sí los métodos existentes no encajan con un problema o campo concreto, de adapta o se desarrollan nuevos métodos o enfoques.

Una parte fundamental de la investigación cualitativa, desde las notas de campo y las transcripciones hasta las descripciones e interpretaciones y la presentación de los hallazgos y de la investigación entera, se basa en el texto y en la escritura. Por consiguiente, los problemas de transformar situaciones sociales complejas en el texto son preocupaciones fundamentales de la investigación cualitativa.

7.2. Tipo de Estudio

El estudio se realizará de forma descriptiva transversal con el instrumento de Entrevista, de esta forma los datos a obtener estarán mas dirigidos a encontrar la problemática de interés del proyecto.

Un estudio descriptivo es aquél en que la información es recolectada sin cambiar el entorno (es decir, no hay manipulación). En ocasiones se conocen como estudios “correlacionales” o “de observación.” También se define un estudio descriptivo como

"cualquier estudio que no es verdaderamente experimental." Los estudios descriptivos también se llevan a cabo para demostrar las asociaciones o relaciones entre las cosas en el entorno.

Los estudios descriptivos pueden implicar una interacción en una sola ocasión con grupos de personas (estudio transversal) o puede seguir a algunos individuos a lo largo del tiempo (estudio longitudinal). Los estudios descriptivos en que el investigador interacciona con el participante pueden involucrar encuestas o entrevistas para recolectar la información necesaria.

7.3. Descripción de fuentes de información.

Las fuentes de información juegan un papel fundamental al proporcionarnos datos que nos permiten reconstruir eventos. Estas fuentes son herramientas esenciales para el conocimiento, la investigación y el acceso a datos. La clasificación de estas fuentes varía según el nivel de información que ofrecen y la credibilidad respaldada por sus autores o instituciones.

7.3.1. Fuentes primarias.

Las fuentes primarias en esta investigación se refieren a aquellos recursos que contienen información original y no han sido modificados, interpretados o analizados; en otras palabras, se mantienen inalterados desde su creación.

Estadísticas y Reportes del Municipio de Ciudad Sandino: Informes oficiales del municipio o de organismos gubernamentales locales que puedan proporcionar datos sobre el uso de redes WiFi públicas, incidentes de seguridad o violaciones de privacidad.

Entrevistas con Usuarios Locales: Entrevistas directas con personas que utilicen redes WiFi públicas en Ciudad Sandino. Sus experiencias y perspectivas pueden ofrecer información valiosa sobre los desafíos de

seguridad y privacidad que enfrentan.

Informes de Organizaciones de Seguridad Cibernética: Informes publicados por organizaciones especializadas en seguridad cibernética. Estas fuentes pueden proporcionar análisis detallados de amenazas y vulnerabilidades en las redes WiFi públicas, así como sugerencias para mejorar la seguridad.

7.3.2. Fuentes secundarias.

La fuente secundaria es un recurso que proporciona información ampliada basada en la fuente primaria original. En este contexto, la fuente secundaria podría ser un análisis, una valoración o cualquier contenido que se derive de la fuente primaria. Es importante destacar que la fuente secundaria no presenta directamente los resultados o datos originales, sino que los interpreta, resume o contextualiza de alguna manera.

- **Páginas de las webs informativas, documentos y libros pdf** relacionados al tema de investigación.

- **Tesis Monográficas** con temas relacionados al tema de investigación, encontradas en los distintos repositorios institucionales de otras universidades, así como los obtenidos del repositorio de la UNI.
- **Revisión exhaustiva** de la situación de la seguridad y privacidad en las redes WiFi públicas en el municipio.

7.3 Cronograma de Actividades

Cronograma de Investigación Monográfica			
Tarea	**Duración**	**Comienzo**	**Fin**
Presentación del protocolo a la Facultad CyS	1 día	05/12/2023	05/12/2023
Revisión n°1 del protocolo	7 días	05/12/2023	10/12/2023
Incorporación de las sugerencias y recomendaciones	7 días	11/12/2023	18/12/2023
Aprobación por el tutor n°1	1 día	18/12/2023	19/12/2023
Envío para aprobación y revisión n°1	1 día	20/12/2023	21/12/2023
Revisión n°2 del protocolo	7 días	22/12/2023	29/12/2023
Incorporación de las sugerencias y recomendaciones	7 días	30/12/2023	06/01/2024
Aprobación por el tutor n°2	1 día	07/01/2024	08/01/2024
Envío para aprobación y revisión n°2	1 día	09/01/2024	10/01/2024
Aprobación a la Facultad CyS	3 días	11/01/2024	13/01/2024
Desarrollo Capítulo 1	30 días	14/01/2024	13/02/2024
Revisión del tutor	2 días	14/02/2024	16/02/2024
Corrección del capítulo	3 días	17/02/2024	20/02/2024
Envío de capítulo actualizado	1 día	21/02/2024	22/02/2024
Aprobación del capítulo	2 días	23/02/2024	25/02/2024
Desarrollo Capítulo 2	30 días	26/02/2024	26/03/2024
Revisión del tutor	2 días	27/03/2024	29/03/2024
Corrección del capítulo	1 día	30/03/2024	31/03/2024
Corrección del capítulo	7 días	01/04/2024	07/04/2024
Aprobación del capítulo	1 día	08/04/2024	09/04/2024
Desarrollo Capítulo 3	30 días	10/04/2024	10/05/2024
Revisión del tutor	3 días	11/05/2024	14/05/2024
Corrección del capítulo	3 días	15/05/2024	18/05/2024

Envío de capítulo actualizado	1 día	19/05/2024	20/05/2024
Aprobación del capítulo	1 día	21/05/2024	22/05/2024
Elaboración del informe final	10 día	23/05/2024	03/06/2024
Incorporación de todos los capítulos al documento final	5 día	04/06/2024	09/06/2024
Redacción de informe preliminar según normativa	2 días	10/06/2024	11/06/2024
Revisión del informe preliminar por el tutor	5 días	12/06/2024	17/06/2024
Corrección del informe final	4 días	18/06/2024	22/06/2024
Envío del informe final actualizado	1 día	23/06/2024	24/06/2024
Aval técnico del tutor para la pre defensa	1 día	25/06/2024	26/06/2024
Entrega del informe final para pre defensa	1 día	27/06/2024	28/06/2024
Pre defensa monográfica	1 día	29/06/2024	30/06/2024
Incorporación de las sugerencias y recomendaciones al informe Final	5 días	01/07/2024	06/07/2024
Envío de correcciones del informe final al tutor	1 día	07/07/2024	08/07/2024
Aval técnico del tutor para el empastado y defensa	1 día	09/07/2024	10/07/2024
Envío de los tres empastados a la FCYS	1 día	11/07/2024	12/07/2024
Programación de la defensa	1 día	13/07/2024	14/07/2024

7.4. Diagrama de Gantt

Diagrama de Gantt								
Actividades	Fechas							
	15-ago	30-ago	15-sep	30-sep	15-oct	30-oct	15-nov	25-nov
Portada								
Indice								
Introduccion								
Antecedentes								
Planteamiento del problema								
Objetivos								
Justificación								
Marco Teorico								
Diseño Metodologico								
Cronograma de Actividades								
Bibliografia								
Anexos								

Universidad Nacional de Ingeniería

IX. Bibliografía

Aladro Vico, E. (2011). La Teoría de la Información ante las nuevas tecnologías de la comunicación. *Radalyc, vol.16 83-93*, 12.

Buettrich, S., & Pascual, A. E. (s.f.). *Unidad 04: Topología e Infraestructur estructura Básica.* Obtenido de https://www.unac.edu.pe/images/inventario/documentos/manuales/topologia-e-infraestructura_guia_v02.pdf

Chavez, J. J. (3 de Octubre de 2023). *Delta Project*. Obtenido de https://www.deltaprotect.com/blog/seguridad-de-la-red

Cisco. (2014). *Cisco.*

J G, O. (2012). *J G.*

Kurose, J. F., & Ross, K. W. (2017). *Redes de computadoras Un enfoque descendente 7ma edicion.* PEARSON EDUCACION, S.A.

Limones, E. (15 de Marzo de 2021). *OpenWebinars*. Obtenido de https://openwebinars.net/blog/que-son-las-redes-informaticas-y-que-tipos-existen/

Masters, T. y. (2021). *Tesis y Masters*. Obtenido de https://tesisymasters.com.ar/teoria-de-la-comunicacion/

NetCloudEngineering. (19 de Septiembre de 2019). *NetCloudEngineering*. Obtenido de https://netcloudengineering.com/funcionamiento-redes-lan/

Sánchez, J. A. (2012). *SEMINARIO DE GRADUACIÓN.* Obtenido de https://repositorio.unan.edu.ni/5389/1/93586.pdf

tanenbaum, & Wetherall. (2012). *Redes de computadoras 5ta edicion.*

Universidad Nacional de Ingeniería

X. Anexos