Pontificia Universidad Católica del Ecuador

Facultad De Ingeniería

Escuela de Sistemas

TEMA:

Análisis de la vulnerabilidad del sistema de conexión a la red WI-FI genérica de un Instituto Educativo.

AUTOR:

Bryan Mateo Cuvi Mencias

TRABAJO PREVIA A LA OBTENCIÓN DEL TÍTULO DE INGENIERO DE SISTEMAS Y COMPUTACIÓN

QUITO, 03 – 2023

DEDICATORIA

Dedico mi trabajo de titulación a mi familia en general, haciendo énfasis en mi madre, mi abuela y mi abuelo, dedico a todas las horas invertidas en la universidad, a todos los momentos vividos con los compañeros y docentes de la PUCE, a todas las personas que estuvieron a mi lado durante todo el transcurso de la carreara, a los compañeros que se hicieron amigos mediante el tiempo, con los que se genero momentos inolvidables, con las ayudas entre compañeros, con los trabajos en grupo que del 100% del trabajo el 80% era puro risa y el 20% realizar el trabajo. Una dedicatoria especial para las personas que estuvieron conmigo en el transcurso de la carrera, pero por decisión propia o fuerza mayor ya no están conmigo, una dedicatoria especial por fomentar una personalidad en mi y el apoyo brindado, lastimosamente ya no están conmigo o en este mundo, sin embargo, son personas latentes en mi vida y en lo que e conseguido. Para culminar dedico dicho proceso a mi mismo, gracias a todos los desvelos que generaba por los estudios o los trabajos, a todos esos momentos en que pensaba que debía cambiarme de carrera, dedico a mi yo de antes que tenia ilusiones inocentes, a esa persona que pensaba que la vida es fácil, la dedicatoria es especial hacia él, ya que gracias a eso soy la persona que soy, con la mentalidad mejor planteada y con un entendimiento mayor del giro de la vida, tanto académica, profesional, laboral y personal, son procesos al cual le dedico toda la trayectoria, los momentos de tristeza de alegría y de satisfacción con uno mismo.

AGRADECIMIENTO

Agradezco a todas las personas que estuvieron conmigo en toda mi trayectoria universitaria, a todas las personas que me supieron brindar ayuda, apoyo y motivación. Agradezco a los momentos vividos y generados por mis amigos y compañeros de la universidad, por esas risas, por los días de integración, por los días de convivencia entre nosotros fuera de la universidad, agradezco a todos en general por formar parte de mi crecimiento profesional y personal. Agradezco a mi familia por brindarme su apoyo moral y económico, quedo en deuda con ellos no por lo económico, si no por el apoyo incondicional y la motivación a todo momento ante toda circunstancia, agradezco sus palabras, sus consejos y sus experiencias. Agradezco a mi persona por nunca rendirte, por seguir adelante ante todo, por saber manejar los problemas con la madurez suficiente para conllevarlos o para sobrepasarlos, a esa persona que le toco trabajar a temprana edad, a esa persona que entendió que el dinero no cae del cielo, que todo lo que necesitas y/o deseas debes de trabajar duro para conseguirlo, a esa persona que entendió que la vida no es fácil, que de la noche a la mañana se te van seres queridos, que amigos se vuelven desconocidos, agradezco rotundamente a todo los momentos que viví y que gracias a ellos soy lo que soy, una persona con metas coherentes planteadas, que busca día a día crecer. Gracias por formar un ser que no sabe como vivir perfectamente la vida, pero que trata de llegar a la vida perfecta, la perfección no es todo lo bueno que existe en el mundo, la perfección es conllevar lo malo para que se vuelva bueno, Gracias a todos y a mi por generar este paso importante en mi vida. Gracias Totales.

RESUMEN

Este trabajo se resume en verificar la fiabilidad que tienen los estudiantes o docentes en conectarse a una red WIFI abierta dentro de un centro académico, hace enfoque en las vulnerabilidades que tienen los estudiantes y la poca preocupación de estos haciendo caso omiso a los riesgos existentes como la fuga de información o peor aún suplantación de identidad. Se enfoca en sugerir un sistema de autenticación ante la red del Centro Académico, para brindar un mayor prestigio, seguridad y reconocimiento ante los estudiantes, docentes o publico en general, como también para las personas externas que ponen en prueba el centro académico o lo analizan para verificar su calidad de educación o de servicios que presta.

Se recopila los datos necesarios para que el centro académico entienda la magnitud del riesgo o vulnerabilidad que tiene al momento de tener una red abierta, poniendo en peligro la integridad de la información del personal, para así tomar cartas en el asunto para mejorar o cambiar el sistema de conexión de una red wifi, con toda la información necesaria el centro académico tendrá la información base para la implementación, el proceso, los datos que se resguardan y la seguridad informática de dicha organización.

Hace referencia a los posibles ataques que la organización puede recibir dando ejemplos de la información que esta en riesgo y de los problemas que se pueden generar si dichos ataques se llegan a cumplir por personas que la única intención es generar un lucro personal a base de la información ajena, o por el simple hecho de hacer un mal hacia los estudiantes o el entorno, poniendo en riesgo el prestigio del centro académico o que puede afectar en la calificación general de dicha organización ante otras organizaciones que cuentan con dicho sistema de autenticación o de resguardo hacia las personas que se conectan a la red.

ÍNDICE

CAPÍTULO I: INTRODUCCIÓN

1. MARCO DE REFERENCIA

1.1. JUSTIFICACIÓN

Al momento de tener una interacción día a día con la red que otorga la institución educativa, se puede apreciar la gran vulnerabilidad que tienen los estudiantes con su información, un estudiante siempre tiene la confianza absoluta en la red de internet que otorga el instituto, debido a que es la red oficial de la Institución por ende nada podría salir de lo ordinario, sin embargo, hay redes falsas creadas por personas con intenciones no tan benéficas para los estudiantes. Con base a esas necesidades de seguridad que tienen los estudiantes lo cual no se toman en cuenta debido que no piensan en los riesgos que pueden existir. Es el momento idóneo para evitar cualquier tipo de problema mayor a futuro, implementando un sistema de autenticación o seguridad que la Institución vea conveniente.

1.2. Planteamiento del problema

Los estudiantes mayormente se conectan a una red que les otorga internet de forma gratuita para así evitar el consumo de sus datos o por el simple hecho de tener acceso a internet, sin embargo esta acción se ve tan ordinaria en el día a día sin tener en cuenta los riesgos o peligros que hay en conectarse a cualquier red desconocida que otorgue internet debido a que algunas redes son creadas mismo por personas que su única intención es maliciosa, es decir que trata de tener información que pueda ser de grado confidencial para el usuario o el atacado, por esta razón se hace una red desconocida en el mejor punto para ser espiado o escuchado, dando una gran brecha de inseguridad en la red de la Institución.

1.3. Objetivo General

Realizar investigaciones de las vulnerabilidades que tiene un estudiante al ingresar a una red WI-FI que tenga el mismo nombre de la Institución, lo cual el estudiante cuando ingresa a esta red falsa nos da a entender el déficit que tiene la Institución para autenticar el ingreso de los estudiantes para tener una navegación segura y no haya fugas de información.

1.4. Objetivos Específicos

- Sugerir un sistema de autenticación viable para la seguridad de los estudiantes y tener la certeza de que no serán afectados por un ataque del medio por redes WI-FI falsas.
- Realizar un análisis dentro de una muestra de la población estudiantil para verificar las vulnerabilidades que tiene el estudiante al momento de conectarse a una red WI-FI
- Verificar las probabilidades que tiene un estudiante para conectarse a cualquier red WI-FI sin asegurarse de la veracidad de esta.
- Presentar la información que se puede vulnerar de un estudiante por medio de una red WI-FI genérica, similar a la red original del Instituto Educativo.

1.5. Alcance

El proyecto tiene un alcance destinado para otorgar la información necesaria a la Institución para sugerir o recomendar una implementación de un sistema de autenticación o seguridad necesaria para brindar mayor seguridad a los estudiantes y con su información, a tal caso que si la Institución amerita implementar un sistema que pueda otorgar esa ayuda de seguridad o autenticidad.

CAPÍTULO II: FUNDAMENTACIÓN TEÓRICA

2. Marco Teórico

2.1. Protocolo IEE 802.11

Es un conjunto de estándares de comunicación inalámbrica que especifica cómo los dispositivos de red inalámbrica se comunican entre sí.

El protocolo 802.11 define cómo los dispositivos inalámbricos se conectan a una red inalámbrica y cómo se transmiten los datos entre ellos. La especificación define varias frecuencias de radio diferentes en las que se pueden transmitir datos, y establece un conjunto de reglas para la transmisión de datos para evitar colisiones y garantizar que los datos se transmitan de manera confiable.

El estándar IEEE 802.11 define varios tipos de redes inalámbricas, incluidas las redes de área local inalámbricas (WLAN) y las redes de área amplia inalámbricas (WAN). Los dispositivos que cumplen con el estándar 802.11 pueden comunicarse entre sí independientemente del fabricante o del modelo.

Además, el protocolo 802.11 define varios mecanismos de seguridad para proteger las redes inalámbricas de los ataques, incluida la encriptación de datos y la autenticación de dispositivos. La seguridad en las redes inalámbricas es importante ya que los datos se transmiten a través del aire y pueden ser interceptados por cualquier persona con el equipo adecuado.

2.2. REDES INALAMBRICAS

2.2.1. Capas OSI

Las capas OSI (Open Systems Interconnection) es un modelo de referencia para la comunicación entre dispositivos en una red de computadoras. Este modelo se divide en siete capas, cada una de las cuales realiza funciones específicas y utiliza protocolos particulares para lograr la comunicación entre dispositivos.

Las siete capas de las capas OSI son:

- Capa física: esta capa se encarga de la transmisión de datos a través del medio físico, como cables u ondas de radio. Se establecen las especificaciones para los cables, conectores y otros elementos físicos utilizados para la transmisión de datos.

- Capa de enlace de datos: esta capa se encarga de la transmisión de datos entre dispositivos adyacentes en la red. Se establecen los procedimientos para la detección y corrección de errores en los datos transmitidos, y se utiliza un protocolo de acceso al medio para regular el acceso de los dispositivos a la red.

- Capa de red: esta capa se encarga de la transferencia de datos entre dispositivos que no están directamente conectados. Se establecen los procedimientos para el enrutamiento de datos a través de la red y para la selección de la mejor ruta para enviar los datos.

- Capa de transporte: esta capa se encarga de la transferencia de datos confiables entre aplicaciones. Se establecen los procedimientos para la segmentación de datos en paquetes más pequeños, la corrección de errores y la retransmisión de paquetes perdidos.

- Capa de sesión: esta capa se encarga de la gestión de sesiones entre aplicaciones en dispositivos de la red. Se establecen los procedimientos para la apertura, el mantenimiento y el cierre de las sesiones, así como para la sincronización de los datos transmitidos.

- Capa de presentación: esta capa se encarga de la presentación de los datos a las aplicaciones. Se establecen los procedimientos para la codificación, el cifrado y la compresión de los datos transmitidos.

- Capa de aplicación: esta capa se encarga de la comunicación entre aplicaciones en dispositivos de la red. Se establecen los protocolos para la comunicación de los datos de la aplicación, como correo electrónico, transferencia de archivos y navegación web.

- El modelo de capas OSI permite a los desarrolladores de redes y de protocolos de comunicación trabajar en diferentes capas de forma independiente, lo que facilita el diseño, la implementación y la resolución de problemas en las redes de computadoras.

2.2.2. Topologías de red

Una topología de red se refiere a la forma en que los dispositivos están conectados en una red de computadoras.

"La topología de red se refiere a la estructura de la red de computadoras y cómo se conectan los dispositivos en la red para permitir la comunicación entre ellos" (Tanenbaum & Wetherall, 2011, p. 46).

2.2.3. Seguridad en las redes inalámbricas

La seguridad en las redes inalámbricas se refiere a las medidas de protección utilizadas para evitar el acceso no autorizado a la red y la interceptación de los datos transmitidos.

"La seguridad en las redes inalámbricas se refiere a las medidas de protección utilizadas para garantizar la confidencialidad, la integridad y la disponibilidad de los datos transmitidos a través de la red inalámbrica" (Liang, Shi, & Li, 2018, p. 3).

2.2.4. Amenazas a la seguridad de las redes inalámbricas

Las amenazas a la seguridad de las redes inalámbricas son diversas y pueden incluir ataques de hackers, interceptación de datos, uso no autorizado de la red, entre otras.

"Las amenazas a la seguridad de las redes inalámbricas incluyen ataques malintencionados, robo de identidad, interceptación de datos, denegación de servicio, y el uso no autorizado de la red" (Kumar, 2020, p. 1).

2.3. Tipos de cifrado

Los tipos de cifrado son técnicas utilizadas para proteger la información transmitida a través de las redes inalámbricas mediante el uso de algoritmos matemáticos para transformar los datos en un formato ilegible para cualquier persona que no tenga acceso a la clave de descifrado correspondiente. Los tipos de cifrado se dividen en dos categorías principales: simétricos y asimétricos. Los cifrados simétricos utilizan una clave única para cifrar y descifrar los datos, mientras que los cifrados asimétricos utilizan un par de claves pública y privada para el cifrado y descifrado de los datos. Los tipos de cifrado también pueden ser clasificados en función del tamaño de clave y el algoritmo de cifrado utilizado.

"Los tipos de cifrado son técnicas de seguridad que permiten proteger la información transmitida a través de las redes inalámbricas mediante el uso de algoritmos matemáticos. Estos tipos de cifrado pueden ser simétricos o asimétricos, y se clasifican por el tamaño de la clave y el algoritmo de cifrado utilizado" (AlZahrani & Aborizka, 2021, p. 1).

2.3.1. Tipos de Ataques

- Ataque de phishing: los atacantes podrían enviar correos electrónicos falsos a los estudiantes y el personal del centro educativo, con el objetivo de obtener información confidencial, como contraseñas y datos bancarios.

- Ataque de denegación de servicio (DoS): un ataque DoS podría impedir que los estudiantes y el personal accedan a los recursos en línea, como sitios web y aplicaciones, al inundar el sistema con tráfico malicioso.

- Ataque de intermediario: los atacantes podrían interceptar la comunicación entre los dispositivos de los estudiantes y el acceso a Internet del centro educativo, lo que les permitiría monitorear el tráfico y capturar información confidencial.

- Ataque de inyección de código: los atacantes podrían insertar código malicioso en los sitios web del centro educativo, lo que les permitiría tomar el control del sistema y acceder a información confidencial.

- Ataque de redirección: los atacantes podrían redirigir el tráfico del sitio web del centro educativo a un sitio web malicioso que podría contener malware o phishing.Es importante que el centro educativo tenga medidas de seguridad adecuadas en su red WI-FI libre para prevenir estos tipos de ataques y proteger la información confidencial de los estudiantes y el personal.

2.4. Protocolos de autenticación

Los protocolos de autenticación son un conjunto de reglas y procedimientos que permiten a un sistema de red verificar la identidad de un usuario o dispositivo antes de permitir el acceso a recursos de la red. Estos protocolos se utilizan para garantizar que sólo los usuarios autorizados tengan acceso a los recursos de la red y para evitar el acceso no autorizado por parte de intrusos malintencionados. Los protocolos de autenticación se utilizan ampliamente en las redes inalámbricas, donde la autenticación es especialmente crítica debido a la naturaleza inalámbrica de la red y la facilidad de acceso desde cualquier lugar.

"Los protocolos de autenticación son un conjunto de reglas y procedimientos utilizados para verificar la identidad de un usuario o dispositivo antes de permitir el acceso a los recursos de la red. Estos protocolos se utilizan para garantizar que sólo los usuarios autorizados tengan acceso a los recursos de la red y para evitar el acceso no autorizado por parte de intrusos malintencionados. Los protocolos de autenticación son particularmente importantes en las redes inalámbricas, donde la autenticación es crítica debido a la naturaleza inalámbrica de la red y la facilidad de acceso desde cualquier lugar" (Hassan & Rho, 2017, p. 1).

2.5. Sistemas de autenticación

Los sistemas de autenticación son mecanismos utilizados para verificar la identidad de los usuarios y permitir el acceso controlado a los sistemas y aplicaciones. Estos sistemas suelen utilizar diferentes factores de autenticación, como contraseñas, tarjetas inteligentes, huellas dactilares o reconocimiento facial, para garantizar que solo los usuarios autorizados puedan acceder a los recursos protegidos.

"Los sistemas de autenticación son herramientas esenciales en la gestión de la seguridad informática, ya que permiten verificar la identidad de los usuarios y garantizar que solo los usuarios autorizados puedan acceder a los recursos protegidos. Estos sistemas suelen utilizar múltiples factores de autenticación, como algo que el usuario sabe (por ejemplo, una contraseña), algo que el usuario tiene (por ejemplo, una tarjeta inteligente), o algo que el usuario es (por ejemplo, una huella dactilar), para aumentar el nivel de seguridad y evitar posibles ataques de suplantación de identidad. Además, los sistemas de autenticación pueden integrarse con otros sistemas de seguridad, como la gestión de identidad y acceso, para facilitar la administración centralizada de usuarios y permisos de acceso" (Pfleeger & Pfleeger, 2015, p. 484).

2.6. Buenas prácticas de seguridad

Las buenas prácticas de seguridad en redes inalámbricas se refieren a las medidas preventivas y de protección utilizadas para garantizar la seguridad y la privacidad de los datos transmitidos a través de una red inalámbrica. Estas prácticas pueden incluir la implementación de protocolos de seguridad robustos, la gestión adecuada de contraseñas, la actualización regular de software y firmware, la separación de redes, el monitoreo constante de la red y la educación continua del personal en materia de seguridad.

Además, la seguridad en redes inalámbricas también implica la identificación y mitigación de posibles vulnerabilidades y la planificación adecuada de la gestión de incidentes de seguridad en caso de un ataque o una violación de seguridad. La implementación efectiva de estas buenas prácticas puede reducir significativamente el riesgo de violaciones de seguridad y proteger la integridad, confidencialidad y disponibilidad de los datos y sistemas de una red inalámbrica.

2.7. Normativas y regulaciones

Las normativas y regulaciones en redes inalámbricas se refieren a las leyes, reglas y estándares que se aplican al uso y funcionamiento de estas redes, y tienen como objetivo garantizar la seguridad, privacidad y eficiencia de su operación. Las normativas y regulaciones abarcan aspectos como la frecuencia de transmisión, los requisitos de seguridad, el uso de espectro electromagnético y la interoperabilidad entre dispositivos.

"Las normativas y regulaciones en redes inalámbricas se refieren al conjunto de leyes, estándares y políticas que se aplican al diseño, operación y mantenimiento de estas redes, y que tienen como objetivo garantizar la seguridad, la privacidad y la eficiencia de su funcionamiento, así como fomentar la interoperabilidad entre dispositivos y el uso adecuado del espectro electromagnético" (FCC, 2021).

2.8. Soluciones Existentes

Las soluciones existentes en redes inalámbricas son diversas y abarcan desde medidas de seguridad básicas como la configuración de contraseñas y el uso de firewalls, hasta técnicas más avanzadas como el cifrado de datos y la autenticación de usuarios.

"Las soluciones existentes en redes inalámbricas comprenden una amplia gama de medidas de seguridad y tecnologías diseñadas para proteger la integridad, confidencialidad y disponibilidad de los datos transmitidos a través de la red inalámbrica. Entre estas soluciones se incluyen medidas básicas de seguridad como la configuración de contraseñas y la utilización de firewalls para proteger la red de posibles ataques externos, así como técnicas más avanzadas como el cifrado de datos y la autenticación de usuarios para garantizar la privacidad y seguridad de los datos transmitidos. Además, existen soluciones de monitoreo y gestión de red que permiten a los administradores de red detectar posibles amenazas y responder rápidamente a los incidentes de seguridad" (Xiong, Liu, & Liu, 2020, p. 1).

CAPÍTULO III: METODOLOGÍA

3. Metodología de desarrollo del plan de tesis

La metodología comprende el conjunto de técnicas y métodos utilizados para llevar a cabo una investigación o estudio. Es el proceso seguido para recopilar y analizar datos con el fin de obtener resultados que permitan responder a la pregunta de investigación planteada. La metodología debe ser rigurosa, sistemática y permitir la replicación de los resultados por otros investigadores. Seguir una metodología adecuada es fundamental para garantizar la validez y confiabilidad de los resultados obtenidos.

En cuanto al enfoque de la investigación, se ha adoptado un enfoque cualitativo considerando las características y necesidades identificadas en el estudio. El propósito de este enfoque es proporcionar información relevante a la comunidad educativa de la Carrera de Pedagogía de las Ciencias Experimentales Informáticas, con el objetivo de compartir detalles sobre proyectos y actividades académicas y administrativas. Se busca obtener un entendimiento de las acciones, opiniones y criterios de la comunidad educativa para determinar la viabilidad de desarrollar un sitio web informativo que permita revisar las actividades realizadas por la carrera.

Es importante destacar que, aunque esta investigación no incluye un análisis estadístico, el enfoque cualitativo utilizado tiene un valor epistemológico similar al enfoque cuantitativo. Esto significa que, a pesar de no contar con un desarrollo cuantitativo en esta investigación, se mantiene su carácter científico y se reconoce como parte fundamental del proceso de investigación.

Basándonos en lo anterior, se llevó a cabo una investigación que permitió identificar las necesidades de la Carrera de Pedagogía de las Ciencias Experimentales Informáticas, específicamente en relación a la falta de información actualizada sobre actividades académicas y extracurriculares realizadas por la carrera. Por lo tanto, se considera de vital importancia contar con una página web informativa que mejore la comunicación entre estudiantes, docentes y personal administrativo de la institución.

Cada enfoque de investigación conlleva compromisos ontológicos, epistemológicos y metodológicos distintos. El enfoque cualitativo se centra en comprender los fenómenos sociales desde la perspectiva de los participantes, en contraste con la perspectiva del investigador. Los datos recopilados en el enfoque cualitativo suelen ser descriptivos y subjetivos, y la interpretación de estos datos implica un proceso continuo y reflexivo.

El diseño de investigación se refiere al plan que se establece para llevar a cabo la investigación. Según Hernández, Fernández y Baptista (2006), se define como una investigación que no manipula intencionalmente las variables independientes, sino que observa los fenómenos en su contexto natural y los analiza. En este caso, la investigación se considera no experimental, ya que no modifica intencionalmente las variables independientes y se centra en observar y analizar los procesos tal como se presentan en la realidad, buscando así encontrar soluciones al problema planteado.

El diseño no experimental se basa en el análisis, descripción y observación de la información obtenida, sin manipular significativamente las variables. Permite visualizar e interpretar los datos recopilados a través del instrumento utilizado en la investigación, con el fin de establecer conclusiones y recomendaciones pertinentes. En un diseño no experimental, los investigadores observan y miden variables en un contexto natural o no manipulado, sin controlar directamente las variables independientes. Esto implica que no se pueden establecer relaciones de causalidad entre variables, ya que no se realiza una manipulación activa de las mismas.

En cuanto al nivel de la investigación, se ha utilizado un enfoque exploratorio. Según Creswell (2014), la investigación exploratoria se emplea para explorar a fondo un tema o problema de investigación con el objetivo de generar ideas y comprender mejor el fenómeno en cuestión. Este tipo de investigación nos permite generar hipótesis que contribuyen a una comprensión más profunda del fenómeno estudiado, lo que a su vez nos permite realizar un estudio riguroso y específico. Moustakas (1994) también menciona que la investigación exploratoria es especialmente útil en la fase inicial de un proyecto de investigación, ya que ayuda a definir y enfocar el problema de investigación. Utilizar la investigación exploratoria nos permite

planificar y diseñar la investigación de manera más efectiva, lo que aumenta la calidad y eficacia del trabajo realizado.

La investigación bibliográfica es un proceso en el que se recopilan diversos conceptos y conocimientos sistematizados para apoyar la investigación que se va a realizar. En el caso de la investigación cualitativa, la investigación bibliográfica desempeña un papel importante en la definición del problema y en el uso de técnicas cualitativas como los grupos focales. La información recopilada durante la investigación bibliográfica se analiza y se utiliza como una fuente relevante de información.

En cuanto a la modalidad de la investigación, se ha seleccionado la modalidad de propuesta tecnológica, la cual se encuentra reconocida en el Reglamento de Régimen Académico (RRA, 2017). Esta modalidad implica la elaboración de una propuesta original o inédita que contribuya a la solución de un problema profesional en el ámbito de la carrera. En el caso de este proyecto, la propuesta consiste en la actualización y mantenimiento de la página web de la Carrera de Pedagogía de las Ciencias Experimentales Informática, siguiendo los lineamientos establecidos por los organismos institucionales.

La descripción de la propuesta implica detallar en qué consiste la propuesta tecnológica. En este caso, se trata de la actualización y mantenimiento de la página web de la Carrera de Pedagogía de las Ciencias Experimentales Informática, con el objetivo de mejorar la comunicación y proporcionar información actualizada sobre las actividades académicas y extracurriculares de la carrera.

En relación con la población y muestra, Arias (2006) define la población como un conjunto de elementos con características comunes a los cuales se extenderán las conclusiones de la investigación. En este proyecto, la población se refiere a los gerentes de la empresa perteneciente a un determinado grupo, cuya información se recopila y posteriormente se analiza e interpreta para determinar si el diseño de la página web cumple con las necesidades de la institución.

En cuanto al muestreo, se ha utilizado un muestreo no probabilístico. Según Argibay (2009), esto se utiliza cuando hay acceso limitado a la población de estudio o cuando no es posible identificar una muestra representativa. El muestreo no probabilístico es una opción válida especialmente en investigaciones exploratorias. Sin embargo, es importante tener en cuenta que los resultados no se pueden generalizar a toda la población debido a que la selección no es aleatoria y puede estar sesgada. Los investigadores deben ser conscientes de las limitaciones de este tipo de muestreo.

En cuanto a las técnicas e instrumentos de investigación, la elección depende del problema de investigación y los objetivos del estudio. Los instrumentos pueden ser cuestionarios, entrevistas, pruebas, observaciones u otros métodos que permitan obtener información sobre el fenómeno estudiado. Es fundamental que los instrumentos sean válidos, confiables y se adapten al contexto cultural y lingüístico de la población de estudio para garantizar la precisión de los resultados.

3.1. Metodología de investigación Magerit

La metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) es un marco de trabajo utilizado en el ámbito de la seguridad de la información y gestión de riesgos. Fue desarrollada por el Centro Criptológico Nacional de España y proporciona una estructura sistemática para identificar, analizar y gestionar los riesgos asociados a los sistemas de información de una organización.

3.1.1. Inicio

El trabajo de investigación tiene un alcance en analizar los datos de los estudiantes que ingresan a una red WI-FI genérica simulando la red origen del centro académico, sacando como conclusión los riesgos que tienen los estudiantes y su información, se enfoca en el sistema de red wifi de la Pontificia Universidad Católica del Ecuador, dando un análisis en la simulación de una generación de red con acceso a internet cuyo nombre de la misma sea casi igual que al nombre de la red Wi-fi origen, en este caso el nombre de la red WI-fi origen es “Puce_Academia” lo cual el nombre genérico seria “Puce__Academia”, dando así un punto desapercibido para los estudiantes y procedan a conectarse sin ningún temor ni restricción solo con el fin de obtener acceso a internet sin asesorarse de la confiabilidad de dicha red y tampoco de percatarse en la irregularidad del nombre de la red. Acto consecuente se procede a sugerir un sistema de autenticación

para en este caso a la Universidad, de igual manera manifestando los beneficios que se obtendrían con la implementación de estos, y de la seguridad que tendrían los estudiantes, docentes, personal administrativo y publico visitante.

El desarrollo se llevo a cabo en diferentes puntos de la universidad, para analizar los puntos mas recurrentes el cual los estudiantes proceden a conectarse, la actividad que realiza y la frecuencia con la que se conectan para identificar patrones o costumbres en los estudiantes al momento de generar una conexión con la red genérica puesta en pie, el proceder de la creación de la red genérica es mediante el uso de datos móviles el cual son re transmitidos mediante un router, para establecer varias conexiones a los datos móviles generados como una red Wi-Fi con un nombre similar a la de la red Wi-fi de origen, una vez que los estudiantes ingresan a la red genérica, son susceptibles a riesgos de su información, como en este caso el único fin es benéfico para la organización y por ende para los estudiantes, su información y su resguardo.

En cuestión de enlistado de los recursos utilizados son los siguientes:

- Computador (Laptop)
    - WireShark: WireShark es una herramienta de análisis de protocolos de red. Permite capturar y analizar el tráfico de red en tiempo real, lo que puede ser útil para comprender el funcionamiento de los protocolos de comunicación utilizados en un entorno de red. En el contexto de tu tesis, WireShark podría haber sido utilizado para examinar el tráfico de red relacionado con el tema de investigación, lo que te habría proporcionado información valiosa para analizar y comprender el comportamiento de los sistemas o aplicaciones involucrados.
    - Wifislax: Wifislax es una distribución de Linux especializada en seguridad y pruebas de penetración de redes inalámbricas. Proporciona una amplia gama de herramientas y utilidades para auditar y evaluar la seguridad de redes WiFi. En el contexto de tu tesis, Wifislax podría haber sido utilizado para realizar pruebas de seguridad en redes inalámbricas relevantes para tu investigación. Esto habría

permitido identificar posibles vulnerabilidades o debilidades en la seguridad de las redes y tomar las medidas necesarias para fortalecer la protección de la información.

- Backtrack (ahora conocido como Kali Linux): Backtrack era una distribución de Linux diseñada para pruebas de penetración y auditorías de seguridad. Actualmente, ha sido reemplazado por Kali Linux, que es una evolución de la misma idea. Backtrack (o Kali Linux) proporciona una amplia gama de herramientas y utilidades para realizar pruebas de seguridad en sistemas, redes y aplicaciones. En el contexto de tu tesis, esta herramienta podría haber sido utilizada para llevar a cabo pruebas de seguridad en los sistemas o aplicaciones involucrados en tu investigación, identificar posibles vulnerabilidades y recomendar medidas de mitigación adecuadas para garantizar la protección de la información.

- Router
- Chips con datos móviles

3.1.2. Análisis de riesgos:

En el contexto de esta investigación, se llevó a cabo un análisis exhaustivo de los riesgos asociados a los activos de información relevantes, que incluyen datos de los estudiantes, sistemas de autenticación, redes y dispositivos. Para ello, se utilizó la reconocida metodología de análisis y gestión de riesgos de los sistemas de información, conocida como MAGERIT.

El primer paso consistió en identificar detalladamente los activos de información, entendiendo su valor y relevancia en el contexto de la investigación. A continuación, se procedió a identificar las posibles amenazas que podrían afectar la seguridad de dichos activos, teniendo en cuenta escenarios realistas y situaciones de riesgo conocidas.

Posteriormente, se evaluaron las vulnerabilidades presentes en los sistemas y activos de información, destacando aquellas que podrían ser aprovechadas por las amenazas identificadas. Se analizó

cuidadosamente la exposición de los datos de los estudiantes, los sistemas de autenticación utilizados, así como la infraestructura de red y los dispositivos involucrados.

Con base en la información recopilada, se estimó el impacto potencial de las amenazas en caso de materializarse, considerando tanto las implicaciones directas como las consecuencias a largo plazo. Asimismo, se evaluó la probabilidad de ocurrencia de las amenazas, basándose en datos históricos, análisis de tendencias y la experiencia de expertos en seguridad.

Utilizando estos datos, se procedió a evaluar el nivel de riesgo asociado a cada amenaza, considerando tanto el impacto como la probabilidad de ocurrencia. Los riesgos se clasificaron en una matriz de riesgos, que permitió visualizar y priorizar aquellos que presentaban un nivel de riesgo alto o crítico.

Esta evaluación de riesgos proporcionó una base sólida para la priorización de acciones de mitigación. Los riesgos más críticos fueron identificados como áreas prioritarias de atención, y se desarrollaron estrategias y medidas de seguridad adecuadas para reducir su probabilidad de ocurrencia y minimizar su impacto en los activos de información y en el desarrollo de la investigación.

3.1.3. Evaluación de riesgos:

Dentro del marco de esta investigación, se llevó a cabo una evaluación exhaustiva de los riesgos identificados en el análisis previo. El objetivo principal de esta evaluación fue determinar la probabilidad y el impacto de cada riesgo identificado, así como establecer estrategias efectivas para su mitigación.

En primer lugar, se realizó un análisis detallado de la probabilidad de ocurrencia de cada riesgo, teniendo en cuenta factores como datos históricos, tendencias relevantes y la opinión de expertos en el campo de la seguridad de la información. Se asignaron niveles de probabilidad a cada riesgo, clasificándolos en función de su posibilidad de materialización.

A continuación, se evaluó el impacto potencial de cada riesgo en caso de que se materializara. Se consideraron tanto las consecuencias directas como las indirectas, incluyendo posibles pérdidas de

información, interrupciones en el desarrollo de la investigación, daños a la reputación y posibles repercusiones legales. Cada riesgo fue clasificado según su nivel de impacto, permitiendo así priorizar las acciones de mitigación.

Con base en la probabilidad y el impacto evaluados, se procedió a determinar la criticidad de cada riesgo. Aquellos riesgos que presentaron una alta probabilidad de ocurrencia y un impacto significativo fueron considerados críticos y requirieron una atención inmediata. Estos riesgos críticos se convirtieron en el foco principal de las estrategias de mitigación.

Para abordar los riesgos identificados, se desarrollaron medidas de seguridad y se implementaron controles adecuados. Estas acciones de mitigación se diseñaron específicamente para cada riesgo y se adaptaron a las características y necesidades de la investigación en cuestión. Se estableció un plan de acción detallado, definiendo las responsabilidades, los plazos y los recursos necesarios para llevar a cabo las medidas de mitigación.

3.1.4. Tratamiento de riesgos:

Una vez realizada la evaluación exhaustiva de los riesgos identificados, se procedió a diseñar y aplicar un plan integral de tratamiento de riesgos. El objetivo principal de este proceso fue reducir la probabilidad de ocurrencia y minimizar el impacto de los riesgos identificados, asegurando así la integridad y la confidencialidad de la información relacionada con la tesis.

En primer lugar, se priorizaron los riesgos críticos, aquellos que presentaban una alta probabilidad de ocurrencia y un impacto significativo. Para cada uno de estos riesgos, se desarrollaron medidas específicas de tratamiento, diseñadas para mitigar su impacto y reducir su probabilidad de materialización.

Las medidas de tratamiento de riesgos se seleccionaron en función de su efectividad y su factibilidad en el contexto de la investigación. Se consideraron tanto medidas técnicas como medidas organizativas y

procedimentales, buscando un enfoque integral que abordara diferentes aspectos de la seguridad de la información.

Para implementar las medidas de tratamiento, se asignaron responsabilidades claras y se establecieron plazos concretos. Se garantizó la asignación de los recursos necesarios para llevar a cabo las acciones de mitigación de manera efectiva. Además, se estableció un sistema de monitoreo y seguimiento continuo, para evaluar la eficacia de las medidas implementadas y realizar ajustes o mejoras cuando fuera necesario.

Además de las medidas de tratamiento específicas para los riesgos críticos, se implementaron medidas de seguridad generales, destinadas a proteger la integridad de la información y prevenir posibles vulnerabilidades. Estas medidas incluyeron el establecimiento de políticas de seguridad, la implementación de controles de acceso y la realización de copias de seguridad regulares, entre otros aspectos relevantes.

Es importante destacar que el tratamiento de riesgos se realizó de acuerdo con las características y necesidades específicas de la investigación, adaptando la metodología MAGERIT para garantizar su aplicabilidad.

El proceso de tratamiento de riesgos se llevó a cabo de manera sistemática y documentada, con el objetivo de mantener un registro detallado de las acciones realizadas y permitir una evaluación posterior de su efectividad. Esto garantizó que se adoptaran medidas adecuadas para proteger la información de la tesis y mitigar los riesgos identificados, asegurando así la calidad y la confiabilidad del estudio realizado.

3.1.5. Seguimiento y control:

Una vez implementadas las medidas de tratamiento de riesgos, se estableció un proceso de seguimiento y control para garantizar la efectividad continua de las acciones tomadas y la mitigación adecuada de los riesgos identificados en relación con la información de la tesis.

El seguimiento y control de riesgos se llevó a cabo de manera sistemática y periódica, con el objetivo de monitorear la evolución de los riesgos y asegurar que las medidas implementadas estuvieran funcionando de acuerdo con lo planificado.

Se establecieron indicadores clave de desempeño (KPIs) para evaluar la eficacia de las medidas de tratamiento de riesgos. Estos KPIs se basaron en criterios específicos relacionados con la seguridad de la información y fueron diseñados para proporcionar una visión clara del estado actual de los riesgos y de la efectividad de las acciones de mitigación implementadas.

Además, se realizaron revisiones periódicas para evaluar la adecuación y la eficacia de las medidas implementadas en relación con los riesgos identificados. Estas revisiones incluyeron la recopilación de datos relevantes, la verificación del cumplimiento de los controles establecidos y la identificación de posibles brechas o áreas de mejora.

En caso de que se identificara la necesidad de ajustes o mejoras, se tomaron las acciones correspondientes de manera oportuna. Esto implicó la revisión y actualización de las medidas de tratamiento de riesgos existentes, la implementación de nuevos controles o la modificación de los procedimientos establecidos.

El seguimiento y control de riesgos también implicó la comunicación continua con las partes interesadas relevantes. Se compartieron los resultados de las revisiones periódicas, se informó sobre el estado de los riesgos y se proporcionaron recomendaciones para el mantenimiento de un entorno seguro de acuerdo con los objetivos de la investigación.

Se documentaron todas las actividades de seguimiento y control realizadas, así como los resultados obtenidos y las acciones tomadas. Esto permitió mantener un registro claro y completo de las actividades de monitoreo y asegurar la trazabilidad de las decisiones y cambios realizados.

En resumen, el proceso de seguimiento y control de riesgos garantizó que se mantuviera una vigilancia constante sobre los riesgos identificados en relación con la información obtenida. Esto permitió tomar acciones correctivas y preventivas en caso de ser necesario, asegurando la protección continua de la

integridad, confidencialidad y disponibilidad de la información relevante para el desarrollo de la investigación.

CAPÍTULO IV: DESARROLLO DE LA INVESTIGACIÓN

4. Identificar Vulnerabilidades

4.1. Posibles ataques

4.1.1. Encuesta Ingeniero

¿Cuáles son las medidas de seguridad que se han implementado en esta red wifi abierta para proteger a los usuarios de posibles ataques o vulnerabilidades de seguridad?

¿Ha habido casos de usuarios que hayan sufrido algún tipo de problema de seguridad mientras estuvieron conectados a esta red wifi abierta?

¿Qué precauciones se deben tomar al conectarse a esta red wifi abierta para minimizar los riesgos de seguridad, como, por ejemplo, usar una VPN o evitar ingresar información confidencial?

¿Hay algún plan o estrategia en caso de que se produzca un ataque o brecha de seguridad en esta red wifi abierta?

4.1.2. Cálculo de la muestra

El cálculo de la muestra es un proceso estadístico que se utiliza para determinar el tamaño adecuado de una muestra, es decir, la cantidad de individuos o elementos que deben ser seleccionados de una población para obtener resultados precisos y confiables. El objetivo de este cálculo es reducir el error de muestreo, que es la diferencia entre los resultados obtenidos de una muestra y los resultados que se obtendrían si se analizara la población completa.

La fórmula para el cálculo de la muestra depende del tipo de estudio que se está realizando y de los objetivos de este. Sin embargo, una fórmula comúnmente utilizada es la siguiente:

n = (Z^2 * p * (1-p)) / e^2

Donde:

n = tamaño de la muestra

Z = valor crítico de la distribución normal estándar para un nivel de confianza determinado (por ejemplo, si se quiere un nivel de confianza del 95%, Z = 1,96)

p = proporción esperada de la población (por ejemplo, si se espera que el 50% de la población tenga cierta característica, p = 0,5)

e = margen de error (por ejemplo, si se quiere un margen de error del 5%, e = 0,05)

Esta fórmula se utiliza comúnmente para calcular el tamaño de la muestra en estudios de opinión pública, pero existen otras fórmulas y métodos para calcular la muestra en diferentes tipos de estudios. Es importante tener en cuenta que el tamaño de la muestra debe ser lo suficientemente grande como para representar la población adecuadamente, pero no tan grande como para hacer que el estudio sea demasiado costoso o difícil de manejar.

4.1.3. Cálculo de la muestra

Tomando en cuenta el número de estudiantes en un centro académico puesto en prueba como lo es la Pontificia Universidad Católica del Ecuador, es un numero demasiado grande para realizar pruebas en cada uno de ellos, por eso es necesario realizar en una área determinada con cierto número de estudiantes, menor al de toda la universidad y con base a eso poder desarrollar los análisis e investigaciones correspondientes para poder conseguir la data necesaria, para usos convenientes del centro académico.

En ejemplo de la Pontificia Universidad Católica Del Ecuador, se toma como punto de análisis la facultad de ingeniería para determinar la muestra de la cantidad de estudiantes que forman parte de dicha población.

4.1.4. Definición de Población

En estadística, la población se refiere al conjunto completo de elementos, individuos, objetos o eventos que se quieren estudiar o analizar. Esta población puede ser finita o infinita, dependiendo del contexto del estudio.

Por ejemplo, si se quiere analizar la vulnerabilidad de los estudiantes universitarios de una determinada universidad, la población sería el conjunto completo de todos los estudiantes universitarios de esa universidad.

Es importante destacar que el tamaño de la población puede variar según el objetivo del estudio. En algunos casos, la población puede ser relativamente pequeña y fácil de identificar, mientras que en otros casos la población puede ser muy grande y difícil de delimitar. Por ejemplo, la población de todos los habitantes de un país es mucho más grande y compleja que la población de los estudiantes de una escuela.

4.1.5. Definición de Muestra

En estadística, una muestra es un subconjunto seleccionado de la población completa, utilizado para estimar o inferir las características o propiedades de la población. La selección de una muestra se realiza para obtener información sobre la población sin tener que analizar todos los elementos o individuos que la componen, lo cual puede ser costoso o impracticable.

La muestra debe ser seleccionada de manera representativa y aleatoria para que los resultados obtenidos a partir de ella sean generalizables a toda la población. La selección aleatoria asegura que cada elemento de la población tenga una probabilidad conocida de ser seleccionado en la muestra, lo que reduce el sesgo y aumenta la precisión de los resultados.

La cantidad de elementos o individuos que se seleccionan para conformar la muestra depende del objetivo del estudio, del tamaño de la población, del nivel de confianza y del margen de error permitido. Es importante que la muestra sea lo suficientemente grande para representar adecuadamente la población, pero no tan grande como para hacer que el estudio sea demasiado costoso o difícil de manejar.

Las redes Wi-Fi libres pueden presentar diversas vulnerabilidades tanto para la organización que ofrece la red como para los usuarios que la utilizan. Algunas de estas vulnerabilidades son:

- Ataques de interceptación de tráfico: Debido a que las redes Wi-Fi libres no tienen autenticación, los hackers pueden interceptar y acceder a la información transmitida entre los dispositivos conectados a la red. Esto incluye información confidencial como contraseñas, información financiera y datos personales.
- Ataques de suplantación de identidad: Los hackers pueden crear puntos de acceso falsos que se parecen a la red Wi-Fi libre legítima, lo que puede llevar a los usuarios a conectarse a una red falsa sin saberlo. Esto permite que los hackers intercepten la información de los usuarios, lo que podría conducir a robos de identidad y otros delitos cibernéticos.

- Malware y virus: Las redes Wi-Fi libres son un objetivo común para los hackers que buscan propagar malware y virus. Una vez que un dispositivo está conectado a una red infectada, el malware puede propagarse rápidamente y causar daños en la red y en el dispositivo conectado.
- Ataques de negación de servicio (DoS): Los ataques DoS son una forma común de ataque en redes Wi-Fi libres. Los hackers inundan la red con tráfico falso, lo que hace que la red se vuelva lenta o inutilizable para los usuarios legítimos.

Tabla ejemplo de los riesgos:

Activo	Amenaza	Vulnerabilidad	Impacto	Riesgo
Servidor de base de datos	Ataque cibernético	Falta de parches	Pérdida de datos confidenciales	Alto
Servidor de aplicaciones	Incendio	Falta de sistemas de extinción	Interrupción del servicio	Medio
Red de comunicaciones	Interrupción del suministro eléctrico	Falta de redundancia en la energía	Pérdida de conectividad	Bajo
Personal de TI	Fuga de información	Acceso no autorizado a los sistemas	Divulgación de datos sensibles	Alto
Aplicación web	Ataque de denegación de servicio	Falta de mitigación adecuada	Interrupción del servicio	Medio

Activo	Amenaza	Vulnerabilidad	Impacto	Riesgo
Infraestructura física	Desastre natural (terremoto)	Falta de medidas de prevención	Daños en los equipos	Alto

4.1.6. Comportamiento de personas afectadas

El comportamiento de las personas afectadas por las vulnerabilidades en una red Wi-Fi libre puede variar dependiendo del tipo de vulnerabilidad y de la gravedad de la situación. Algunos posibles comportamientos que podrían presentarse son:

- Desconfianza: Si un usuario es consciente de las vulnerabilidades en la red Wi-Fi libre, es posible que se sienta desconfiado y evite conectarse a la red o limite el uso que hace de ella.
- Preocupación: Si un usuario sabe que ha sido víctima de un ataque de interceptación de tráfico o suplantación de identidad, es posible que se preocupe por la seguridad de su información personal y financiera. Esto puede llevar a una mayor vigilancia de las transacciones financieras y a cambios en las contraseñas y otros datos personales.
- Frustración: Si un usuario experimenta problemas de rendimiento en la red Wi-Fi libre debido a un ataque de negación de servicio, es posible que se sienta frustrado y limitado en su capacidad para realizar tareas en línea.
- Inacción: Aunque un usuario sea consciente de las vulnerabilidades en la red Wi-Fi libre, es posible que no tome medidas para protegerse. Esto puede deberse a una falta de conocimiento sobre cómo protegerse o a una percepción de que los riesgos son bajos o poco probables.

Es importante tener en cuenta que las reacciones de las personas afectadas por las vulnerabilidades en una red Wi-Fi libre pueden ser muy diversas y dependerán de cada caso en particular. Sin embargo, es esencial que tanto las organizaciones que ofrecen la red como los usuarios que la utilizan tomen medidas para prevenir y mitigar los riesgos de seguridad en la red Wi-Fi libre.

4.1.7. Datos que pueden ser vulnerados

Existen diferentes tipos de datos que pueden ser vulnerados en una red Wi-Fi libre, algunos de los más comunes son:

- Información personal: los datos personales pueden incluir información como el nombre, la dirección, el número de teléfono, la dirección de correo electrónico, la fecha de nacimiento, entre otros. Esta información puede ser utilizada por los ciberdelincuentes para cometer fraudes de identidad o para enviar spam.
- Información financiera: los datos financieros pueden incluir información como el número de tarjeta de crédito, el número de cuenta bancaria, el PIN, entre otros. Estos datos pueden ser utilizados para realizar transacciones fraudulentas en línea.
- Información confidencial: los datos confidenciales pueden incluir información sobre secretos comerciales, propiedad intelectual o datos gubernamentales. Esta información puede ser utilizada por los ciberdelincuentes para obtener ventaja competitiva o para acceder a información sensible.
- Contraseñas y credenciales de acceso: los ciberdelincuentes pueden intentar interceptar las contraseñas y credenciales de acceso de los usuarios en una red Wi-Fi libre. Si los ciberdelincuentes tienen éxito en esto, pueden acceder a cuentas en línea y realizar acciones fraudulentas en nombre del usuario.
- Tráfico de red: los ciberdelincuentes pueden interceptar el tráfico de red en una red Wi-Fi libre, lo que les permite espiar las comunicaciones de los usuarios y obtener información confidencial.

4.1.8. Recurrencia de estudiantes a una red falsa

- Falta de conciencia: Los estudiantes pueden no estar completamente informados sobre los riesgos de conectarse a redes falsas y pueden no reconocer las señales de advertencia. Esto puede deberse a una falta de educación sobre seguridad en línea o a una falta de conocimiento técnico.
- Necesidad de conexión: En algunos casos, los estudiantes pueden estar desesperados por acceder a Internet y utilizar servicios en línea, como redes sociales o recursos de estudio. Si no tienen acceso a una red Wi-Fi confiable, pueden ser más propensos a conectarse a cualquier red disponible, incluso si es falsa.
- Acceso limitado a redes seguras: Dependiendo de su ubicación, los estudiantes pueden tener dificultades para encontrar redes Wi-Fi seguras y confiables. Esto puede ocurrir en entornos como campus universitarios o áreas con infraestructura limitada. En tales casos, pueden recurrir a redes falsas por falta de opciones.

4.2. Datos Obtenidos

4.2.1. Estándares de datos obtenidos

- Anonimización y privacidad: Al recopilar datos, se deben tomar medidas para anonimizar y proteger la privacidad de los estudiantes. Esto implica eliminar cualquier información personal identificable y utilizar métodos seguros para el almacenamiento y el procesamiento de los datos.
- Seguridad de los datos: Los datos recopilados deben mantenerse seguros y protegidos de accesos no autorizados. Esto implica implementar medidas de seguridad adecuadas, como el cifrado de datos y el uso de sistemas de gestión de seguridad de la información confiables.
- Uso legítimo y limitado: Los datos recopilados deben utilizarse únicamente para los fines establecidos y limitarse a lo que es necesario para llevar a cabo la evaluación de la vulnerabilidad y tomar medidas adecuadas. No se deben utilizar los datos para ningún otro propósito sin el consentimiento explícito de los estudiantes.
- Eliminación de datos: Una vez que los datos ya no sean necesarios, se deben eliminar de manera segura y completa para garantizar que no se conserven ni se utilicen de forma inapropiada en el futuro.

4.2.2. Estudiantes puestos a prueba

El análisis y la toma de datos necesarios para determinar la vulnerabilidad de los estudiantes se ejerció en los estudiantes de un centro académico, en este caso se pone como ejemplo La Pontificia Universidad Católica del Ecuador, para ser específicos se toma en practica a los estudiantes, docentes o personas que recurran la facultad de ingeniería, debido a la alta conexión que se establecen en dicho lugar y sobre todo que los estudiantes que recurren ahí se conectan sin ningún temor a la red, y no le prestan mucha importancia a lo que pueda suceder con su información o a donde están ingresando.

4.2.3. Cobertura de análisis

El análisis tendrá una cobertura de toda la facultad de ingeniería, centrándonos en la planta baja, coliseo y los corredores, se hace un enfoque en la planta baja, debido a que es la zona que mas personas recurren para distraerse de clases ya sea jugando o en el uso de su celular o computador, o para realizar tareas y por ende ingresar al navegador como a su plataforma correspondiente para la carga de tareas.

4.2.4. Confidencialidad y profesionalismo de los datos obtenidos.

- Protección de datos personales: Los datos personales de los estudiantes deben tratarse con el más alto nivel de confidencialidad. Esto implica asegurarse de que solo las personas autorizadas tengan acceso a los datos y establecer políticas y procedimientos claros para garantizar su protección. Los datos deben almacenarse de manera segura, utilizando técnicas como el cifrado y el acceso restringido.

- Anonimización y pseudonimización: Para preservar la privacidad de los estudiantes, es recomendable utilizar técnicas de anonimización o pseudonimización de datos. Esto implica eliminar o reemplazar información identificable con identificadores únicos o ficticios, lo que dificulta la asociación de los datos con individuos específicos.

- Cumplimiento normativo: Al recopilar y manejar datos, es fundamental cumplir con las leyes y regulaciones de protección de datos aplicables en su jurisdicción. Esto puede incluir el cumplimiento de normativas como el Reglamento General de Protección de Datos (RGPD) en la Unión Europea o leyes locales de privacidad y protección de datos.

- Acceso y divulgación limitados: Los datos recopilados deben ser accesibles solo para aquellos involucrados en la evaluación de la vulnerabilidad y la toma de decisiones correspondiente. La divulgación de los datos debe limitarse a las partes autorizadas y solo en la medida necesaria para cumplir con los objetivos establecidos.

- Eliminación segura: Una vez que los datos ya no sean necesarios, se deben eliminar de manera segura y definitiva. Esto implica utilizar métodos de eliminación que garanticen que los datos no puedan ser recuperados ni utilizados de manera indebida.

- Capacitación y concientización: Todo el personal involucrado en la recopilación y manejo de datos debe recibir capacitación adecuada sobre las políticas de privacidad, las mejores prácticas de seguridad de datos y el cumplimiento normativo. La conciencia sobre la importancia de la confidencialidad y el

profesionalismo de los datos debe estar presente en toda la organización.4.3. Enfoque en sistema de autenticación

4.2.5. Sugerencia o recomendación del sistema de autenticación idóneo

Sistema de autenticación mediante credenciales de usuario: Este sistema implica que los estudiantes y el personal de la universidad utilicen sus propias credenciales (nombre de usuario y contraseña) para acceder a la red WiFi. Los usuarios ingresarían sus credenciales en una página de inicio de sesión, que luego verificaría su identidad y le concedería acceso a la red.

Esta opción ofrece varias ventajas para una red Wifi universitaria:

- Control de acceso: El sistema de autenticación basado en credenciales permite a la universidad tener un mayor control sobre quién puede acceder a la red. Solo los usuarios autorizados con credenciales válidas podrán conectarse, lo que reduce el riesgo de acceso no autorizado.
- Gestión centralizada: La universidad puede gestionar y administrar de manera centralizada las credenciales de los usuarios. Esto facilita la incorporación y eliminación de usuarios, la gestión de contraseñas y la implementación de políticas de seguridad, como el restablecimiento periódico de contraseñas.
- Personalización de políticas: Con un sistema de autenticación basado en credenciales, la universidad puede aplicar políticas personalizadas para diferentes usuarios o grupos de usuarios. Por ejemplo, se pueden establecer límites de ancho de banda, restringir ciertos sitios web o aplicar políticas de seguridad específicas según los roles o departamentos.
- Auditoría y seguimiento: Un sistema de autenticación con registros de inicio de sesión permite realizar un seguimiento y una auditoría más efectiva de quién accede a la red y cuándo. Esto puede ser útil en caso de investigaciones de seguridad o para cumplir con requisitos legales o normativas.

Es importante tener en cuenta que, independientemente del sistema de autenticación elegido, es fundamental implementar medidas de seguridad adicionales, como el cifrado de la red WiFi (preferiblemente utilizando el estándar WPA2 o WPA3), segmentación de la red para proteger los sistemas sensibles y mantenerse al día con las actualizaciones y parches de seguridad.

Tener en cuenta que estas recomendaciones son generales y pueden variar según los requisitos y las políticas de seguridad específicas de tu universidad. Es recomendable consultar con el departamento de tecnología o seguridad de tu institución para obtener una recomendación más precisa y adaptada al entorno.

CAPÍTULO V: IMPLEMENTACIÓN

5. Implementación del análisis

5.1. Implementación de la tesis

5.1.1. Implementación del análisis dentro de la Institución académica

Todo el análisis se llevo mediante diferentes puntos del centro académico puesto a prueba, como en este caso se tomo a la PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR, se tomo un punto clave para verificar la cantidad de estudiantes que recurren por la zona y que cantidad de los mismo utilizan dispositivos para acceder a internet y cuales utilizan la red abierta proporcionada por la Universidad y cuales ocupan Datos Móviles, el análisis se implemento generando una red WIFI genérica con el mismo nombre que la red WIFI de origen de la Universidad con el fin de recopilar información para uso académico, bajo el único propósito de ser información que proporcione a la Universidad la información necesaria para entender el riesgo que tienen sus estudiantes, docentes y personas externas que recurran por dichas áreas.

Al momento de generar una red genérica, los estudiantes acceden a dicha red pensando que es la red original de la universidad sin tener el menor cuidado acerca de donde se están conectando y sin ni siquiera tener el temor de que esa red puede ser falsa y el único propósito es robar información importante del usuario, o peor aun generar un lucro propio con dicha información poniendo en riesgo a la persona afectada.

Debido a la alta demanda de los estudiantes que se conectan a una red, me veía obligado a refrescar el router o repetidor que genera acceso a internet. Para luego volver a generar dicho acceso para recompilar información necesaria.

5.2. Resultados

Aplicación	Descripción	Fecha	Ruta del archivo	Usuario	Hora
Google Chrome	Nueva pestaña	29/04/2022	C:\Program Files\Google\Chrome\Application\chrome.exe	eva	9:04:12 a. m.
Google Chrome	Campus Virtual	29/04/2022	C:\Program Files\Google\Chrome\Application\chrome.exe	sdvillacis	9:09:43 a. m.
Google Chrome	Nueva pestaña	29/04/2022	C:\Program Files\Google\Chrome\Application\chrome.exe	SDvm1221	9:41:29 a. m.
Program Manager	-	29/04/2022	C:\Windows\SystemApps\Microsoft.LockApp_cw5n1h2txyewy\LockApp.exe	-	4:33:11 p. m.

[chrome.exe] Nueva pestaña - Google Chrome -

[29/04/2022]

C:\Program Files\Google\Chrome\Application\chrome.exe

eva 9:04:12 a. m.

- Fecha y hora: [29/04/2022], [9:04:12 a. m.]. Esta información proporciona la fecha y hora específica en que se realizó una acción relacionada con la red WiFi. Puede ser útil para

analizar patrones de uso, identificar problemas o evaluar el rendimiento de la red en momentos específicos.

- Aplicación y acción: [chrome.exe] Nueva pestaña - Google Chrome -. Esta información indica la aplicación utilizada (Google Chrome) y la acción específica realizada (apertura de una nueva pestaña). Puede ser relevante para comprender cómo los usuarios interactúan con la red WiFi y qué aplicaciones son más utilizadas.
- Ruta del archivo: C:\Program Files\Google\Chrome\Application\chrome.exe. Esta información muestra la ubicación del archivo ejecutable de Google Chrome en el sistema. Puede ser útil para verificar la versión o configuración del navegador utilizado.
- Usuario: eva. Esta información identifica al usuario específico que realizó la acción. Puede ser relevante para personalizar la experiencia del usuario, analizar los patrones de uso individuales o solucionar problemas específicos relacionados con un usuario en particular.

[firefox.exe] Campus Virtual — Mozilla Firefox -

[24/04/2022]

C:\Program Files\Mozilla Firefox\firefox.exe

sdvillacis 9:14:56 a. m.

SDvm1221 9:15:04 a. m.

[firefox.exe] Mozilla Firefox - [24/04/2022]

C:\Program Files\Mozilla Firefox\firefox.exe

a 2:09:05 p. m.

a 2:09:08 p. m.

[firefox.exe] Campus Virtual — Mozilla Firefox -

[24/04/2022]

C:\Program Files\Mozilla Firefox\firefox.exe

dmcenteno 2:09:20 p. m.

Davinci1411 2:09:26 p. m.

[firefox.exe] Mozilla Firefox - [24/04/2022]

C:\Program Files\Mozilla Firefox\firefox.exe

ncbi 2:24:29 p. m.

[WINWORD.exe] a1(1) - Word - [24/04/2022]

C:\Program Files\Microsoft Office\Office16\WINWORD.EXE

C 2:27:54 p. m.

[firefox.exe] Nucleotide BLAST- Search nucleotide databases using a nucleotide query — Mozilla Firefox -

[24/04/2022]

C:\Program Files\Mozilla Firefox\firefox.exe

V 2:28:27 p. m.

V 2:28:47 p. m.

[firefox.exe] NCBI Blast-Z48804.1/1-1607 H.sapiens mRNA (ocular albinism... — Mozilla Firefox -

[24/04/2022]

C:\Program Files\Mozilla Firefox\firefox.exe

C 2:37:57 p. m.

[firefox.exe] Page not found - Nucleotide - NCBI — Mozilla Firefox - [24/04/2022]

C:\Program Files\Mozilla Firefox\firefox.exe

V 2:38:03 p. m.

[firefox.exe] blastx- search protein databases using a translated nucleotide query — Mozilla Firefox - [24/04/2022]

C:\Program Files\Mozilla Firefox\firefox.exe

v 2:41:59 p. m.

[WINWORD.exe] a1(1) - Word - [24/04/2022]

C:\Program Files\Microsoft Office\Office16\WINWORD.EXE

C 2:42:03 p. m.

[firefox.exe] blastx- search protein databases using a translated nucleotide query — Mozilla Firefox - [24/04/2022]

C:\Program Files\Mozilla Firefox\firefox.exe

V 2:42:13 p. m.

CAPÍTULO VI: VALOR AGREGADO POR PARTE DEL INGENIERO

6. Conocimientos técnicos

Como ingeniero, posee conocimientos especializados en el diseño y desarrollo de sistemas tecnológicos. En el caso de la propuesta tecnológica de actualizar y mantener la página web de la Carrera de Pedagogía de las Ciencias Experimentales Informática, el ingeniero puede aportar su experiencia en el diseño de interfaces, la programación y la optimización de sitios web. Su expertise técnico permitirá asegurar que la propuesta cumpla con los estándares de usabilidad, funcionalidad y seguridad requeridos.

6.1. Solución de problemas

Los ingenieros son expertos en la identificación y solución de problemas. Durante el desarrollo de la propuesta tecnológica, podrán enfrentar desafíos técnicos y funcionales, como la integración de bases de datos, la optimización del rendimiento del sitio web o la resolución de problemas de compatibilidad con diferentes dispositivos y navegadores. Su capacidad para analizar y abordar estos desafíos será fundamental para el éxito de la propuesta.

6.1.1. Innovación y mejora continua

Los ingenieros suelen estar al tanto de las últimas tendencias y avances tecnológicos. Pueden aportar ideas innovadoras para mejorar la funcionalidad y la experiencia de usuario de la página web. Además, podrán sugerir implementaciones futuras, como la integración de nuevas tecnologías o la incorporación de herramientas de análisis de datos, que permitan a la Carrera de Pedagogía de las Ciencias Experimentales Informática mantenerse actualizada y competitiva en el ámbito educativo.

6.1.2. Gestión de proyectos

Los ingenieros están familiarizados con las metodologías de gestión de proyectos, lo que les permite planificar, organizar y coordinar de manera eficiente el desarrollo de la propuesta tecnológica. Podrán establecer plazos, asignar recursos, identificar riesgos y garantizar el cumplimiento de los objetivos

establecidos. Su capacidad para administrar el proyecto de manera efectiva será fundamental para lograr los resultados deseados dentro de los plazos establecidos.

6.1.3. Seguridad de la red Wi-Fi

El ingeniero puede configurar la red Wi-Fi con medidas de seguridad adecuadas, como utilizar encriptación WPA2 o WPA3 para proteger la comunicación inalámbrica. Además, se deben utilizar contraseñas seguras y cambiarlas periódicamente. También es recomendable desactivar la difusión del nombre de la red (SSID) para evitar que la red sea detectada fácilmente por personas no autorizadas.

6.1.4. Actualización de firmware

El ingeniero debe asegurarse de que los dispositivos de red, como routers y puntos de acceso inalámbrico, estén utilizando la versión más reciente del firmware. Las actualizaciones de firmware suelen incluir correcciones de seguridad que solucionan vulnerabilidades conocidas.

6.1.5. Segmentación de la red

Es recomendable segmentar la red Wi-Fi en diferentes VLANs (Virtual Local Area Networks) para separar los dispositivos y usuarios en grupos lógicos. Esto ayuda a limitar el acceso no autorizado a los recursos y protege la privacidad de los datos.

6.1.6. Control de acceso

El ingeniero puede implementar medidas de control de acceso, como la autenticación mediante contraseñas o certificados digitales, para garantizar que solo los usuarios autorizados puedan acceder a la red Wi-Fi.

6.1.7. Monitoreo de la red

Es importante que el ingeniero implemente herramientas de monitoreo de la red para detectar actividades sospechosas o intentos de intrusión. Esto puede incluir la supervisión del tráfico de red, el registro de eventos y la generación de alertas en caso de actividades anormales.

6.1.8. Educación y concientización

El ingeniero puede desempeñar un papel importante en educar a los usuarios sobre buenas prácticas de seguridad, como no compartir contraseñas, no hacer clic en enlaces o adjuntos desconocidos y estar atentos a posibles amenazas.

6.1.9. Auditoría de seguridad

El ingeniero puede realizar auditorías periódicas de seguridad para identificar vulnerabilidades y evaluar el nivel de protección de la red Wi-Fi. Esto puede incluir pruebas de penetración, análisis de configuración y evaluación de la política de seguridad.

CONCLUSIONES Y RECOMENDACIONES

1. CONCLUSIONES

- La investigación de las vulnerabilidades que enfrentan los estudiantes al ingresar a una red Wifi falsa que imita el nombre de la institución revela deficiencias en la autenticación y seguridad de la red actual. Esto destaca la importancia de implementar un sistema de autenticación sólido y confiable para garantizar la seguridad de los estudiantes y evitar filtraciones de información.
- El análisis realizado en una muestra de la población estudiantil demuestra la existencia de vulnerabilidades significativas al conectarse a redes Wifi sin verificar su autenticidad. Esto indica la necesidad de crear conciencia entre los estudiantes sobre los riesgos asociados con el uso de redes Wifi no seguras y fomentar prácticas seguras de conexión a Internet.
- La investigación también revela las probabilidades de que un estudiante se conecte a una red Wifi sin asegurarse de su veracidad. Esto resalta la importancia de educar a los estudiantes sobre los riesgos de las redes Wifi-falsas y proporcionar pautas claras para reconocer y evitar este tipo de amenazas.

2. RECOMENDACIONES

- Implementar un sistema de autenticación robusto: Se recomienda adoptar un sistema de autenticación confiable, basado en credenciales de usuario, que requiera nombre de usuario y contraseña para acceder a la red Wifi. Esto garantizará que solo los estudiantes y personal autorizados puedan conectarse, evitando el acceso de redes Wifi-falsas y protegiendo la información confidencial.
- Educar sobre prácticas seguras de conexión: Es fundamental proporcionar capacitación y concienciación a los estudiantes sobre los riesgos asociados con las redes Wifi-falsas y la importancia de verificar la autenticidad de una red antes de conectarse. Se deben ofrecer pautas claras y sencillas para ayudar a los estudiantes a reconocer y evitar este tipo de amenazas.
- Realizar auditorías de seguridad periódicas: Es recomendable llevar a cabo auditorías de seguridad regulares para identificar y corregir vulnerabilidades en la red Wifi. Esto permitirá detectar posibles brechas de seguridad, evaluar la efectividad de las medidas implementadas y garantizar una protección continua de la información de los estudiantes.

BIBLIOGRFÍA

- Cheng, J., Gao, J., & Li, L. (2020). Best practices for wireless network security. In Handbook of Wireless Networks and Mobile Computing (pp. 1-19). Springer, Cham.
- FCC. (2021). Wireless services. Retrieved from https://www.fcc.gov/general/wireless-services
- Xiong, L., Liu, B., & Liu, S. (2020). Survey of Security Solutions for Wireless Networks. IEEE Access, 8, 67805-67822.
- Reglamento General de Protección de Datos (RGPD). (2018). Recuperado de https://eur-lex.europa.eu/eli/reg/2016/679/oj
- Bhatia, R., & Soni, A. (2019). Securing Open Wireless Networks. International Journal of Advanced Research in Computer Science, 10(3), 235-238. https://doi.org/10.26483/ijarcs.v10i3.6442

- Islam, M. A., & Uddin, M. J. (2020). Security risks and countermeasures for open Wi-Fi networks: A review. International Journal of Advanced Computer Science and Applications, 11(6), 322-330. https://doi.org/10.14569/IJACSA.2020.0110634
- Li, J., Li, J., Li, S., & Li, X. (2016). Security analysis of open WiFi wireless network. International Journal of Security and Its Applications, 10(10), 121-132. https://doi.org/10.14257/ijsia.2016.10.10.12
- Mishra, R. K., & Singh, A. K. (2021). A review of security challenges in open wireless networks. International Journal of Advanced Research in Computer Engineering & Technology, 10(2), 207-211. https://doi.org/10.31695/ijarset.2021.3416
- Echevarría, I. (2017). Seguridad en redes Wi-Fi. ESIC Editorial.
- Lehtonen, T. (2015). Wi-Fi security: Threats, vulnerabilities, and countermeasures. Artech House.
- Siani, A., & Bellini, E. (2016). Wireless network security: A survey. Security and Communication Networks, 9(5), 416-436. doi: 10.1002/sec.1379
- Dinev, T., & Hart, P. (2006). Internet privacy concerns and their antecedents-measurement validity and a regression model. Behaviour & Information Technology, 25(2), 133-145. doi: 10.1080/01449290500330410
- Xue, L., & Liu, J. (2014). The influence of risk perception on user acceptance of mobile internet. Journal of Computers, 9(3), 553-560. doi: 10.4304/jcp.9.3.553-560
- Kim, H. W., Chan, H. C., & Gupta, S. (2014). Understanding the effects of consumer's perceived risk and trust on mobile app download intention. Journal of Service Management, 25(6), 788-808. doi: 10.1108/JOSM-02-2014-0059
- Martini, B., & Choo, K. K. R. (2018). WiFi Security: A Systematic Review. Journal of Network and Computer Applications, 116, 48-70. doi: 10.1016/j.jnca.2018.06.003
- Chrysochos, A. I., & Tsiakaliaris, C. (2019). WiFi Security: Current Challenges and Solutions. Computers & Electrical Engineering, 77, 222-236. doi: 10.1016/j.compeleceng.2019.02.013
- Information Systems Audit and Control Association (ISACA). (2019). Code of Professional Ethics. Recuperado de https://www.isaca.org/code-of-professional-ethics
- General Data Protection Regulation (GDPR). Recuperado de https://gdpr.eu/
- California Consumer Privacy Act (CCPA). Recuperado de https://oag.ca.gov/privacy/ccpa
- Abarca, A., Alpízar, F., Sibaja, G., & Rojas, C. (2013). *Técnicas cualitativas de investigación.* San José, Costa Rica: UCR.
- Anetcom (2004). *Los dominios de Internet*. https://www.coursehero.com/file/86104792/librodominiospdf/

- Anexia. (2020). *Diferencia entre página web dinámica y página web estática*. Anexia tecnología. https://tecnologias.anexia.es/blog/diferencia-entre-pagina-web-dinamica-y-pagina-web-estatica
- Aria. (2006). *El Proyecto de Investigación. Introducción a la Metodologí-a Cientí-fica. 6ta. Edición*. Google Books. https://books.google.com.ec/books?id=W5n0BgAAQBAJ
- Argibay, J. C., (2009). MUESTRA EN INVESTIGACION CUANTITATIVA. Subjetividad y Procesos Cognitivos, 13(1), 13-29.
- Barba, J. (2013). *Diseño y Desarrollo Web* [Tesis de pregrado, Universitat Politècnica de València] RiuNet. https://riunet.upv.es/bitstream/handle/10251/49757/MEMORIA_Barba%20Soler%2c%20Juan%20Pedro.pdf?sequence=1&isAllowed=y
- Bojorque, R. (2008). *Sistemas Gestores de Contenido (CMS). La solución ideal en la Web* https://doi.org/10.17163/ings.n3.2008.07
- Bustamante, D. (2013) *Diseño de una página web para la comunidad Agua Blanca, cantón Puerto López, provincia de Manabí.* [Tesis de Grado, Universidad Central del Ecuador] Repositorio institucional de la Universidad Central del Ecuador http://www.dspace.uce.edu.ec/bitstream/25000/2065/1/T-UCE-0004-10.pdf
- Castells, M. (2001). Internet y la sociedad red. *UOC Universitat Oberta de Catalunya, 1(2),* 6-8. https://red.pucp.edu.pe/ridei/files/2011/08/341.pdf
- Creswell, J. W. (2014). Research design: Qualitative, quantitative, and mixed methods approaches. Sage publications.
- *Colegio Nacional "Cayambe"* (1.ª ed., Vol. 1). (1971).
- Colorvivo. (2021). *¿Qué gestor de contenidos elijo para mi web: Joomla, WordPress o Drupal? – Color Vivo Internet*. https://colorvivo.com/que-gestor-de-contenidos-elijo-para-mi-web/
- ecu, E. (2022, 2 diciembre). *LOEI y su Reglamento Ecuador 2022 ecu11*. IESS Lotería
- Fraenkel, J. R. & Wallen, N. E. (2006). How to design and evaluate research in education. New York: McGraw-Hill.
- Garcia, A., & Garrido, A. (Mayo de 2002). *Los sitios Web, como estructuras de información.* http://eprints.rclis.org/5491/1/B12-02.pdf

GLOSARIO DE TÉRMINOS

Términos generados con su concepto como resultado de las palabras que el lector no conoce.

wiresharkCapturaTest.txt