UTMACH

FACULTAD DE INGENIERÍA CIVIL

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

Hackeo Ético utilizando mejores prácticas mediante la metodología OSSTMM V3: caso de estudio "Empresa FONET Cia. Ltda."

NAVARRETE MENDEZ BRANDON XAVIER
INGENIERO EN TECNOLOGIAS DE LA INFORMACION

MACHALA
2022

UTMACH

FACULTAD DE INGENIERÍA CIVIL

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

Hackeo Ético utilizando mejores prácticas mediante la metodología OSSTMM V3: caso de estudio "Empresa FONET Cia. Ltda."

NAVARRETE MENDEZ BRANDON XAVIER
INGENIERO EN TECNOLOGIAS DE LA INFORMACION

MACHALA
2022

UTMACH

FACULTAD DE INGENIERÍA CIVIL

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

PROPUESTAS TECNOLÓGICAS

Hackeo Ético utilizando mejores prácticas mediante la metodología OSSTMM V3: caso de estudio "Empresa FONET Cia. Ltda."

NAVARRETE MENDEZ BRANDON XAVIER
INGENIERO EN TECNOLOGIAS DE LA INFORMACION

LOJA MORA NANCY MAGALY

MACHALA
2022

Hackeo Ético en la determinación de riesgos y vulnerabilidades en la infraestructura de la empresa FONET CIA LTDA

por Xavier Navarrete

Fecha de entrega: 13-sep-2022 02:08p.m. (UTC-0500)
Identificador de la entrega: 1899039090
Nombre del archivo: TRABAJO_DE_TITULACION_-_XAVIER_NAVARRETE.pdf (3.69M)
Total de palabras: 17239
Total de caracteres: 92600

Hackeo Ético en la determinación de riesgos y vulnerabilidades en la infraestructura de la empresa FONET CIA LTDA

INFORME DE ORIGINALIDAD

4%	3%	1%	1%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	Submitted to Pontificia Universidad Catolica del Ecuador - PUCE Trabajo del estudiante	<1%
2	slides.com Fuente de Internet	<1%
3	idoc.pub Fuente de Internet	<1%
4	es.slideshare.net Fuente de Internet	<1%
5	www2.cenzic.com Fuente de Internet	<1%
6	Submitted to Champlain College Trabajo del estudiante	<1%
7	Jemison dos Santos, Luiz Eduardo G. Martins, Valdivino A. de Santiago Júnior, Lucas Venezian Povoa et al. "Software requirements testing approaches: a systematic literature review", Requirements Engineering, 2019 Publicación	<1%

8	cvnet.cpd.ua.es Fuente de Internet	<1 %
9	www.dspace.unitru.edu.pe Fuente de Internet	<1 %
10	repositorio.puce.edu.ec Fuente de Internet	<1 %
11	worldwidescience.org Fuente de Internet	<1 %
12	docplayer.com.br Fuente de Internet	<1 %
13	centerforfinancialstability.com Fuente de Internet	<1 %
14	dspace.utb.edu.ec Fuente de Internet	<1 %
15	egyptinnovate.com Fuente de Internet	<1 %
16	repositorio.unsa.edu.pe Fuente de Internet	<1 %
17	Giovanni Hernandez, Alvaro Martinez, Franklin Jimenez, Robinson Jimenez, Alexander Baron. "Learning factory for the Software Engineering area: First didactic transformation", 2021 XLVII Latin American Computing Conference (CLEI), 2021 Publicación	<1 %

18	dspace.unitru.edu.pe Fuente de Internet	<1 %
19	lookformedical.com Fuente de Internet	<1 %
20	plaza.rakuten.co.jp Fuente de Internet	<1 %
21	repositorio.unapiquitos.edu.pe Fuente de Internet	<1 %
22	www.cmdpdh.org Fuente de Internet	<1 %
23	www.myprocessexpo.com Fuente de Internet	<1 %
24	dspace.balikesir.edu.tr Fuente de Internet	<1 %
25	dspace.utpl.edu.ec Fuente de Internet	<1 %
26	fdocuments.ec Fuente de Internet	<1 %
27	fido.mic6090.pp.ru Fuente de Internet	<1 %
28	repositorio.uam.es Fuente de Internet	<1 %
29	www.bannerpublicidad.com Fuente de Internet	<1 %

30	www.powershow.com Fuente de Internet	<1 %
31	(Carlinda Leite and Miguel Zabalza). "Ensino superior: inovação e qualidade na docência", Repositório Aberto da Universidade do Porto, 2012. Publicación	<1 %
32	Eduard Diego Alonso Aroca Sevillano. "Desenvolvimento de metodologia para avaliação do perfil de dissolução de comprimidos de atorvastatina cálcica 20 mg comercializados no Peru, Brasil e Bolívia", Universidade de Sao Paulo, Agencia USP de Gestao da Informacao Academica (AGUIA), 2019 Publicación	<1 %
33	Lian Soto Izquierdo. "Estudio del efecto de diferentes estrategias de formación de la mezcla sobre las emisiones gaseosas y de partículas en nuevos conceptos de combustión de motores de encendido por compresión", Universitat Politecnica de Valencia, 2020 Publicación	<1 %
34	Mónica Chillarón Pérez. "Análisis y desarrollo de algoritmos de altas prestaciones para reconstrucción de imagen médica TAC 3D	<1 %

basados en la reducción de dosis.",
Universitat Politecnica de Valencia, 2021
Publicación

35	cews.africa-union.org Fuente de Internet	<1 %
36	ciencia.lasalle.edu.co Fuente de Internet	<1 %
37	doku.pub Fuente de Internet	<1 %
38	elib.unikom.ac.id Fuente de Internet	<1 %
39	repositorio.unp.edu.pe Fuente de Internet	<1 %
40	transportesynegocios.wordpress.com Fuente de Internet	<1 %
41	www.aurora.com.uy Fuente de Internet	<1 %
42	www.dfcweb.com Fuente de Internet	<1 %
43	www.encolombia.com Fuente de Internet	<1 %
44	www.guiadeprensa.com Fuente de Internet	<1 %
45	www.interactivos.net Fuente de Internet	<1 %

46	www.lisi.usb.ve Fuente de Internet	<1 %
47	www.madridmasd.org Fuente de Internet	<1 %
48	www.racc.es Fuente de Internet	<1 %
49	www.reinformex.org Fuente de Internet	<1 %
50	Andrea Tortorelli, Andrea Fiaschetti, Alessandro Giuseppi, Vincenzo Suraci, Roberto Germanà, Francesco Delli Priscoli. "A security metric for assessing the security level of critical infrastructures", International Journal of Critical Computer-Based Systems, 2020 Publicación	<1 %

Excluir citas	Apagado	Excluir coincidencias	Apagado
Excluir bibliografía	Activo		

CLÁUSULA DE CESIÓN DE DERECHO DE PUBLICACIÓN EN EL REPOSITORIO DIGITAL INSTITUCIONAL

El que suscribe, NAVARRETE MENDEZ BRANDON XAVIER, en calidad de autor del siguiente trabajo escrito titulado Hackeo Ético utilizando mejores prácticas mediante la metodología OSSTMM V3: caso de estudio "Empresa FONET Cia. Ltda.", otorga a la Universidad Técnica de Machala, de forma gratuita y no exclusiva, los derechos de reproducción, distribución y comunicación pública de la obra, que constituye un trabajo de autoría propia, sobre la cual tiene potestad para otorgar los derechos contenidos en esta licencia.

El autor declara que el contenido que se publicará es de carácter académico y se enmarca en las dispociones definidas por la Universidad Técnica de Machala.

Se autoriza a transformar la obra, únicamente cuando sea necesario, y a realizar las adaptaciones pertinentes para permitir su preservación, distribución y publicación en el Repositorio Digital Institucional de la Universidad Técnica de Machala.

El autor como garante de la autoría de la obra y en relación a la misma, declara que la universidad se encuentra libre de todo tipo de responsabilidad sobre el contenido de la obra y que asume la responsabilidad frente a cualquier reclamo o demanda por parte de terceros de manera exclusiva.

Aceptando esta licencia, se cede a la Universidad Técnica de Machala el derecho exclusivo de archivar, reproducir, convertir, comunicar y/o distribuir la obra mundialmente en formato electrónico y digital a través de su Repositorio Digital Institucional, siempre y cuando no se lo haga para obtener beneficio económico.

NAVARRETE MENDEZ BRANDON XAVIER

2350240194

UTMACH

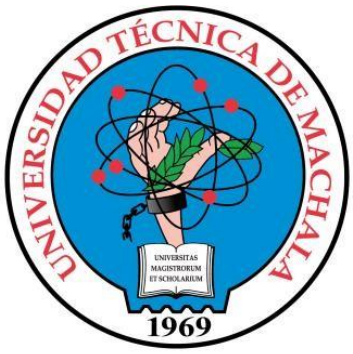
FACULTAD DE INGENIERÍA CIVIL

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

HACKEO ÉTICO UTILIZANDO MEJORES PRÁCTICAS: CASO DE ESTUDIO "EMPRESA FONET CIA LTDA"

NAVARRETE MÉNDEZ BRANDON XAVIER

MACHALA
2022



UTMACH

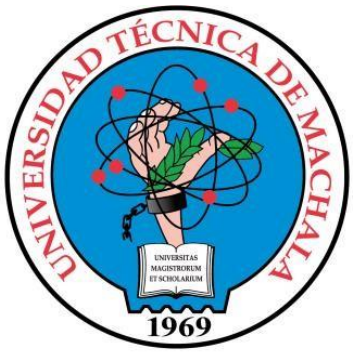
FACULTAD DE INGENIERÍA CIVIL

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

HACKEO ÉTICO UTILIZANDO MEJORES PRÁCTICAS: CASO DE ESTUDIO "EMPRESA FONET CIA LTDA"

NAVARRETE MÉNDEZ BRANDON XAVIER

MACHALA
2022



UTMACH

FACULTAD DE INGENIERÍA CIVIL
CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

TRABAJO DE INTEGRACIÓN CURRICULAR, PROPUESTAS TECNOLÓGICAS

HACKEO ÉTICO UTILIZANDO MEJORES PRÁCTICAS: CASO DE ESTUDIO "EMPRESA FONET CIA LTDA"

NAVARRETE MÉNDEZ BRANDON XAVIER

LOJA MORA NANCY MAGALY

MACHALA, 15 DE JULIO DEL 2022

MACHALA
2022

DEDICATORIA

El presente trabajo de titulación se lo dedico de manera especial a mi familia, que siempre han sido el pilar fundamental a lo largo de mi vida, con sus consejos y apoyo incondicional en cada uno de los proyectos a lo largo de mi vida, ya que su motivación me ha permitido superar cada obstáculo académico.

AGRADECIMIENTO

Agradezco de manera infinita a mis padres quienes siempre me han apoyado y me ayudaron a salir adelante con todos sus esfuerzos y sobre todo en esta etapa de mi vida universitaria.

De igual manera quiero agradecer a las siguientes personas:

A mi tutora la Ing. Nancy Loja y a mi cotutor el Ing. Rodrigo Morocho, los cuales me ayudaron con sus enseñanzas y con sus constantes asesorías hicieron posible que el presente trabajo logre desarrollarse de manera exitosa.

A la Ing. Bertha Mazón y al Ing. Fausto Redrován por compartir sus conocimientos, por su paciencia, por la dedicación y por habernos guiado paso a paso en el proceso de desarrolló de nuestro trabajo curricular.

RESUMEN

En los últimos años se ha podido evidenciar cómo los avances tecnológicos nos han traído grandes mejoras en la vida cotidiana, esto conllevando a que las empresas o instituciones se mantengan en constantes actualizaciones informáticas. Por ello en el presente proyecto se ha tomado como un factor importante la seguridad de la información, generando así una investigación sobre los riesgos y vulnerabilidades que se pueden efectuar dentro de la infraestructura de una empresa, para así evitar ataques informáticos de delincuentes denominados crackers o piratas informáticos.

La empresa INTERNET POR FIBRA ÓPTICA FONET CIA LTDA contaba con la necesidad de realizar un escaneo de sus vulnerabilidades sobre su red interna, para ello se propuso la aplicación de un hackeo ético para detectar dichas vulnerabilidades informáticas y así mismo poder corregirlas para evitar futuros ataques que puedan perjudicar su integridad como institución privada.

La empresa presta servicios de Internet por Fibra Óptica a cientos de abonados, si la empresa sufre ataques informáticos la integridad de sus abonados también puede verse afectada, ya que una empresa de ISP tiene enlaces directos con sus clientes, observando la gravedad que puede tener un efecto como este, es donde la institución abre sus puertas para poner en práctica dicho proyecto y a su vez evitar este tipo de casos y así poder preservar no solo su integridad.

Esta investigación consta de cuatro capítulos, en donde el primer capítulo presenta la fundamentación teórica que describe todos los aspectos sobre seguridad informática y la metodología a usar, también cuenta con otro tipo de fundamentación relacionada a la seguridad informática.

En el segundo capítulo se realiza el desarrollo del prototipo y su definición al igual se indica que metodología de aplicación se hará uso para el desarrollo de la investigación, la metodología selecta es la OSSTMM en su versión 3, esta metodología es una de las más completas para auditorías de seguridad informática, cuenta con un sistema evaluación de riesgos denominado RAVs,

La metodología OSSTMM cuenta con cuatro canales de los cuales se escogieron dos, el canal inalámbrico y el canal de telecomunicaciones, esta metodología indica que se debe verificar, comprobar y contabilizar cada canal según con el objetivo que se ha planteado.

En el capítulo tres se realiza la evaluación del prototipo, en este caso la metodología OSSTMMv3 cuenta con métricas de evaluación, estas métricas se encuentran simplificadas en un archivo CSSV

que se aloja en la página oficial de la metodología. Esto con la finalidad de realizar los cálculos de medición de riesgos correctos para el auditor.

En el capítulo 4 al final del documento se presentan los resultados obtenidos luego de haber efectuado los escaneos correspondientes de vulnerabilidades y así mismo una vez corregidos para saber el estado actual en el que se encuentra la institución.

Haciendo uso de una escala de Likert se demuestra gráficamente el nivel de riesgo con el que cuenta la institución, cabe mencionar que a pesar de que el nivel de riesgo sea de cero por ciento, esto no implica que no sea propensa a un ataque, por ello se indica que las auditorías de seguridad de la información o las aplicaciones de hackeos éticos son fundamentales en los entornos empresariales.

Ya que, en cada actualización de un sistema se pueden encontrar nuevas amenazas y de alguna u otra manera estas deben ser verificadas y tener sus controles.

PALABRAS CLAVE: Seguridad informática, Hackeo Ético, scripts, Kali Linux, OSSTMM

ABSTRACT

In recent years it has been possible to show how technological advances have brought us great improvements in daily life, this leading to companies or institutions being kept in constant informatics updates. For this reason, in this project, information security has been taken as an important factor, thus generating an investigation of the risks and vulnerabilities that can be carried out within the infrastructure of a company, in order to avoid computer attacks by criminals called crackers or computer pirates.

The company INTERNET BY FIBER OPTIC FONET CIA LTDA has the need to perform a scan of its vulnerabilities on its internal network, for this purpose the application of an ethical hack was proposed to detect said computer vulnerabilities and to be able to correct them to avoid future attacks that may prejudice its integrity as a private institution.

The company provides Fiber Optic Internet services to hundreds of subscribers. If the company suffers computer attacks, the integrity of its subscribers may also be affected, since an ISP company has direct links with its clients, noting the seriousness that an attack can have. effect like this, is where the institution opens its doors to put this project into practice and in turn avoid this type of case and thus be able to preserve not only its integrity.

This investigation consists of four chapters, where the first chapter presents the theoretical foundation that describes all aspects of computer security and the methodology to be used, it also has another type of foundation related to computer security.

In the second chapter, the development of the prototype and its definition is carried out, as well as the application methodology that will be used for the development of the research, the selected methodology is the OSSTMM in its version 3, this methodology is one of the most complete for computer security audits, it has a risk assessment system designated RAVs,

The OSSTMM methodology has four channels of which two were chosen, the wireless channel and the telecommunications channel, this methodology indicates that each channel must be verified, purchased and accounted for according to the objective that has been set.

In chapter three, the evaluation of the prototype is carried out, in this case the OSSTMMv3 methodology has evaluation metrics, these metrics are found in a CSSV file that is stored on the official page of the methodology. This in order to perform the calculations of correct risk mix for the auditor.

In chapter 4 at the end of the document, the results obtained after having carried out the corresponding vulnerability scans are presented, as well as once they have been corrected, in order to know the current state of the institution.

Using a Likert scale, the level of risk that the institution has is graphically displayed. It is worth mentioning that although the level of risk is zero percent, this does not imply that it is not prone to an attack, for This indicates that information security audits or ethical hacking applications are essential in business environments.

Since in each update of a system new threats can be found and, in some way, or another they must be verified and have their controls.

KEY WORDS: Computer security, Ethical Hacking, scripts, Kali Linux, OSSTMM

ÍNDICE DE CONTENIDO

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE TABLAS

GLOSARIO

Cracker: es una persona con grandes conocimientos informáticos, el cual accede de manera ilegal o sin consentimiento del propietario a los sistemas informáticos ajenos.

Intranet: es una red informática que comparte información entre sistemas operativos o servicios de computación dentro de una institución.

Kali Linux: es un Sistema Operativo desarrollado en Linux con la finalidad de aplicar auditoría y seguridad informática.

Script: aplicado en informática es una serie de instrucciones escritas dentro de un documento en lenguaje de programación, el cual efectúa al ser ejecutado diversas funciones dentro del programa de una computadora.

INTRODUCCIÓN

En la actualidad la tecnología ha evolucionado trayendo consigo mejoras de manera continua, hoy en día las personas hacen uso de Internet y de diferentes aplicaciones ya sean en teléfonos móviles, tabletas, computadoras, etc. Esto hace que todos se mantengan conectados mediante una red de Internet, en donde los datos viajan a través de un protocolo llamado TCP/IP. Estos dispositivos anteriormente mencionados son esenciales en el día a día, incluso en empresas o instituciones, estos ayudan a agilizar procesos para conseguir eficiencias en la labor. Estos datos al viajar a través de Internet, no son del todo respaldados de manera segura.

Actualmente se ha podido vivir casos donde información de empresas es sustraída por piratas informáticos y luego es vendida a rivales de la misma empresa o a veces suele ser expuesta al público, cuando una empresa pierde información de sus clientes se compromete a grandes demandas por los mismos, las páginas o aplicaciones de escritorio almacenan información en bases de datos que si no llevan un buen protocolo de seguridad está fácilmente puede ceder paso a la extracción de dichos datos.

Teniendo la idea clara de lo peligroso que puede ser no tener un control sobre la información que manejamos a través de Internet, se establece como tema de investigación, implementar las mejores prácticas de hackeo ético para mitigar vulnerabilidades en la Intranet de la empresa de FONET CIA LTDA la cual está ubicada en la ciudad de Pasaje. El hackeo ético es la práctica que consiste en localizar vulnerabilidades para luego solucionarlas, esto mediante ataques controlados.

El hackeo ético utiliza diferentes técnicas para investigar a la organización y así recolectar información relevante para enfocar un ataque. Los ataques son realizados con herramientas de testeo para identificar vulnerabilidades estas pueden ser scripts, también se puede usar el Sistema Operativo (SO) Kali Linux el cual está desarrollado bajo la distribución de Linux con la finalidad de realizar auditorías de seguridad de la información, este sistema operativo contiene múltiples herramientas instaladas por defecto para la penetración en protocolos de red, en el caso de los scripts estos se desarrollan mediante instrucciones escritas en lenguaje Python.

i. Declaración y formulación del problema

La falta de aplicación de Hacking Ético para identificar fallos de seguridad (vulnerabilidades) dentro de los servicios, la Intranet es uno de los problemas principales que tienen las empresas públicas como privadas, como es el caso de FONET CIA LTDA de la ciudad de Pasaje, la cual brinda servicios de Internet, pero carece de seguridad dentro de la institución.

La intención principal del Hackeo Ético se fundamenta en realizar y establecer ataques controlados sobre sus sistemas de información y sus redes, con la finalidad de identificar posibles vulnerabilidades a las que se encuentran expuestos, donde posteriormente se realice definiciones de planes contingentes y de acciones que ayuden a contrarrestar este tipo de amenazas.

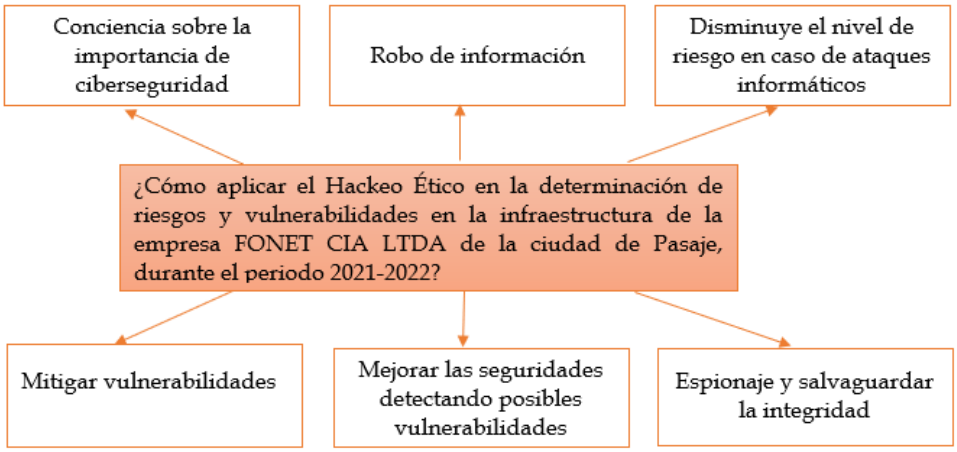


Ilustración 1: *Árbol de Problema*
Fuente: Elaboración propia

}En la **ilustración 1** se ha descrito las causas y los efectos de la problemática que se ha planteado dentro del proyecto de investigación, la cual trata de identificar las vulnerabilidades existentes en la Intranet aplicando mejores prácticas de hackeo ético aplicándolo en una empresa privada de la ciudad de Pasaje, durante el período 2021-2022.

Formulación del problema

- ¿Cómo aplicar el Hackeo Ético en la determinación de riesgos y vulnerabilidades en la infraestructura de la empresa FONET CIA LTDA de la ciudad de Pasaje, durante el período 2021-2022?

i. Objeto de estudio y Campo de acción

Objeto de estudio

- Mitigar vulnerabilidades existentes dentro de la institución
- La comunicación privada y segura dentro de la red interna de la Institución

Campo de acción

- Análisis de los principales Sistemas Operativos
- Conocimientos detallados sobre red
- Seguridad informática: Ingeniería Social, Detección de Intrusos, Creación de Virus.

- Identificar, analizar y evaluar las vulnerabilidades y riesgos de seguridad de las redes, los sistemas informáticos y las aplicaciones.

ii. Objetivos

Objetivo General

- Identificar fallos de seguridad en la Intranet de la empresa FONET CIA LTDA, mediante el uso de herramientas y scripts para la determinación de vulnerabilidades, amenazas y riesgos.

Objetivos específicos

- Encontrar brechas de seguridad en equipos Mikrotik con la finalidad de acceder a redes privadas de un abonado.
- Acceder a un sistema aplicando sentencias SQL para alterar la base de datos o mediante métodos de phishing.
- Elaborar un diccionario de posibles contraseñas mediante la recolección de información relevante con Ingeniería Social para acceder a sistemas aplicando fuerza bruta.
- Verificar posibles vulnerabilidades y errores dentro del ERP ODOO, Sistemas Operativos y de la red interna de la institución.

iii. Hipótesis y variables o Preguntas de investigación

- La aplicación de Hacking Ético, proporciona soporte en la detección de vulnerabilidades, amenazas y riesgos en la Empresa Fonet Cia Ltda.

Variables y dimensionamiento

En la tabla 1 se muestran las variables independientes y dependientes con sus respectivas categorías, indicadores y sus técnicas.

Tabla 1: *Variables y Dimensiones*

Variables	Categorías	Indicadores	Técnicas
Variable Independiente Hacking Ético	• Técnicas • Herramientas • Pruebas de intrusión • Vulnerabilidades • Sistemas Informáticos	• Grado de vulnerabilidad • Políticas de Seguridad • Servicios • Puertos • Metodologías • Software • Información	Recopilación de información para la aplicación de las técnicas de Hackeo.

Variable Dependiente Detectar amenazas, vulnerabilidades y riesgos en los servicios de la Intranet.	• Red • Programas • Recursos Compartidos • Puntos débiles	• Accesos • Contraseñas • Routers • Servidores • Servicios • Filtración de información • Usuarios • Parches • Archivos	Recopilación de información

Fuente: Elaboración propia

iv. Justificación

En la actualidad han existido diferentes fenómenos de ciberseguridad en instituciones privada como públicas en el Ecuador, esto debido a la falta de importancia a las necesidades de seguridad en las infraestructuras de TI, poniendo en peligro la integridad de las instituciones afectadas, por ello es importante aplicar técnicas que ayuden a reforzar la integridad de las instituciones, una de las técnicas más usadas es el Hackeo Ético.

Es por esta razón que se plantea o se propone como proyecto de investigación determinar vulnerabilidades, amenazas y riesgos en la Intranet de la institución este proyecto será desarrollado mediante la metodología OSSTMM la cual involucra la seguridad de la empresa desde Internet hasta la seguridad física.

Probablemente en la Empresa FONET Cia Ltda existan vulnerabilidades en los sistemas internos es por ello que se utilizara Hackeo Ético esto tiene como finalidad el fortalecimiento de vulnerabilidades dentro de una institución privada o pública, con la finalidad de poder parchar servicios con posibles riegos a sufrir ataques dentro de la red interna de dichas instituciones, en el Ecuador una gran cantidad de empresas no cumplen con los controles de seguridad informática basados en una revisión periódica de Hackeo Ético como lo es la empresa FONET CIA LTDA.

Pradeep I y Sakthivel G afirman que “Cada día se desarrollan nuevos tipos de virus, malwares que aumentan la demanda de Hackers Éticos para estar más seguros y protegidos de los ciberdelincuentes y para salvaguardar nuestra información de privacidad” [1].

A lo largo del documento se redactará lo esencial para llevar a cabo esta investigación, por ello está segmentado en capítulos:

Capítulo 1: En este capítulo se detalla toda la fundamentación teórica que forma parte importante para llevar a cabo la investigación.

Capítulo 2: En este capítulo se desarrolló el prototipo a implementar.

Capítulo 3: en este capítulo se establecen los resultados obtenidos, también las conclusiones y recomendaciones basadas en los objetivos que se han propuesto al inicio de la investigación.

1. CAPÍTULO I. MARCO TEÓRICO

1.1. Antecedentes de la investigación

La revisión bibliográfica de los temas investigados en el presente trabajo se realizó mediante la metodología de Revisión Sistemática de la Literatura la cual consiste en revisiones sistemáticas con resúmenes claros y estructurados de estudios anteriores que pueden ser utilizados como aporte a la investigación [2].

a) Preguntas de investigación

En la siguiente **tabla 2** se detallaron las preguntas para la investigación de hackeo ético y su aplicación e importancia dentro de empresas, además de sus herramientas y sus tecnologías existentes.

Español:

Tabla 2: *Preguntas de Investigación*

Pregunta de investigación	Descripción y motivación
RQ1. ¿Cuál es la importancia sobre la implementación de las diferentes metodologías y herramientas informáticas para desarrollar técnicas de Hackeo Ético?	El propósito de esta pregunta es identificar y analizar diferentes enfoques propuestos para la mejor selección de métodos de Hackeo Ético que pueden ser aplicados.
RQ1.1. ¿Cuál es el propósito a analizar sobre la situación actual en la que se desenvuelven los equipos informáticos y servidores de la empresa?	Esta pregunta ayuda a detectar el propósito de las actividades a desarrollar.
RQ1.2. ¿Cuál es la necesidad de emplear una propuesta de modelo de seguridad para una infraestructura tecnológica?	Esta pregunta tiene como objetivo identificar el modelo que se utilizara para el desarrollo de la investigación, para así determinar mediante el mismo las vulnerabilidades existentes dentro de la Intranet de la institución.
RQ1.3. ¿Cuáles son los beneficios de aplicar el Hacking Ético en las instituciones públicas como privadas?	El propósito de esta pregunta es poder analizar los beneficios de los enfoques (seleccionados en RQ1), esto con la finalidad de poder resolver problemas de vulnerabilidades tanto en la red interna de la institución como en los equipos.

Fuente: Elaboración propia

En inglés:

Tabla 3:*Research questions*

Research question	Description and motivation
RQ1. ¿What is the importance of the implementation of the different methodologies and informatics to develop Ethical Hacking techniques?	The purpose of this question is to identify and analyze different approaches proposed for the best selection of Ethical Hacking methods that can be applied.
RQ1.1. ¿What is the purpose to analyze the current situation in which the company's computer equipment and servers operate?	This question helps to detect the purpose of the activities to be developed.
RQ1.2. ¿What is the need to use a security model proposal for a technological infrastructure?	The objective of this question is to identify the model that will be used for the development of the research, in order to determine the existing vulnerabilities within the institution's Intranet.
RQ1.3. ¿What are the benefits of applying Ethical Hacking in public and private institutions?	The purpose of this question is to be able to analyze the benefits of the approaches (selected in RQ1), this in order to be able to solve vulnerability problems both in the internal network of the institution and in the computers.

Fuente: Elaboración propia

b) Palabras claves y Cadena(s) de búsqueda

Para la presente investigación se llevó a cabo una búsqueda automática, en donde se utilizó una cadena específica para los temas de hackeo ético; además se realizó una inclusión manual de artículos reconocidos. Las bases de datos que fueron seleccionadas para la consulta fueron Scopus, IEEEXplore, Science Direct, SpringerLink.

Para la elaboración de la cadena de búsqueda se especificó los términos considerando los temas de investigación (Hackeo ético, seguridad de la información, protocolos de red, piratas informáticos) se excluyeron palabras cuya inclusión no fueron artículos adicionales en la búsqueda automática. Después de diversas iteraciones se definió la cadena de búsqueda, la cual ayudó a encontrar documentación relevante.

Cadena de búsqueda en español:

(“hacking ético”) Y (seguridad O información O cracker O "PROTOCOLO TCP IP")

Cadena de búsqueda en inglés:

(“ethical hacking”) AND (security OR information OR cracker OR “PROTOCOL TCP IP”)

c) Criterios de inclusión y exclusión

En esta **tabla 3** se establecieron los criterios de inclusión y exclusión, mismos que serán utilizados para la búsqueda SRL.

En español:

Tabla 4: *Criterios de inclusión y exclusión*

#	Criterio de inclusión
1	Estudios primarios
2	Estudios que abordan en los objetivos de seguridad informática o hacking ético
3	Estudios publicados a partir del 2016 hasta la actualidad
4	Estudios que relacionan con seguridad de redes
#	**Criterio de exclusión**
1	Estudios secundarios
2	Artículos cortos (≤ 3 páginas)
3	Estudios duplicados (solo se incluyó una copia de cada estudio)
4	Estudios publicados (≤ 2016)
5	Estudios claramente irrelevantes para la investigación, teniendo en cuenta las preguntas de investigación.
6	Estudios donde el enfoque principal no era el hackeo ético.
7	Trabajo redundante de la misma autoría
8	Publicaciones cuyo texto no estaba disponible (a través de buscadores o contactando a los autores)

Fuente: Elaboración propia

En inglés:

Tabla 5: *Inclusion and exclusion criteria*

#	Inclusion Criterion
1	Primary studies
2	Studies that address the objectives of computer security or ethical hacking
3	Studies published from 2016 to the present
4	Studies relating to network security
#	**Exclusion Criterion**
1	Secondary studies
2	Short-papers (≤ 3 pages)
3	Duplicated studies (only one copy of each study was included)
4	Published studies (≤ 2016)
5	Studies clearly irrelevant to the research, taking into account the research questions.
6	Studies where the main focus was not ethical hacking.
7	Redundant work of the same authorship
8	Publications whose text was not available (through search engines or by contacting the authors)

Fuente: Elaboración propia

d) Proceso y resultados de la búsqueda

En este punto se realizó el proceso y resultado de búsqueda, siguiente los 4 pasos como se muestra en la **tabla 4** para la obtención de fuentes bibliográficas relevantes para la investigación y así excluir documentos de poca relevancia.

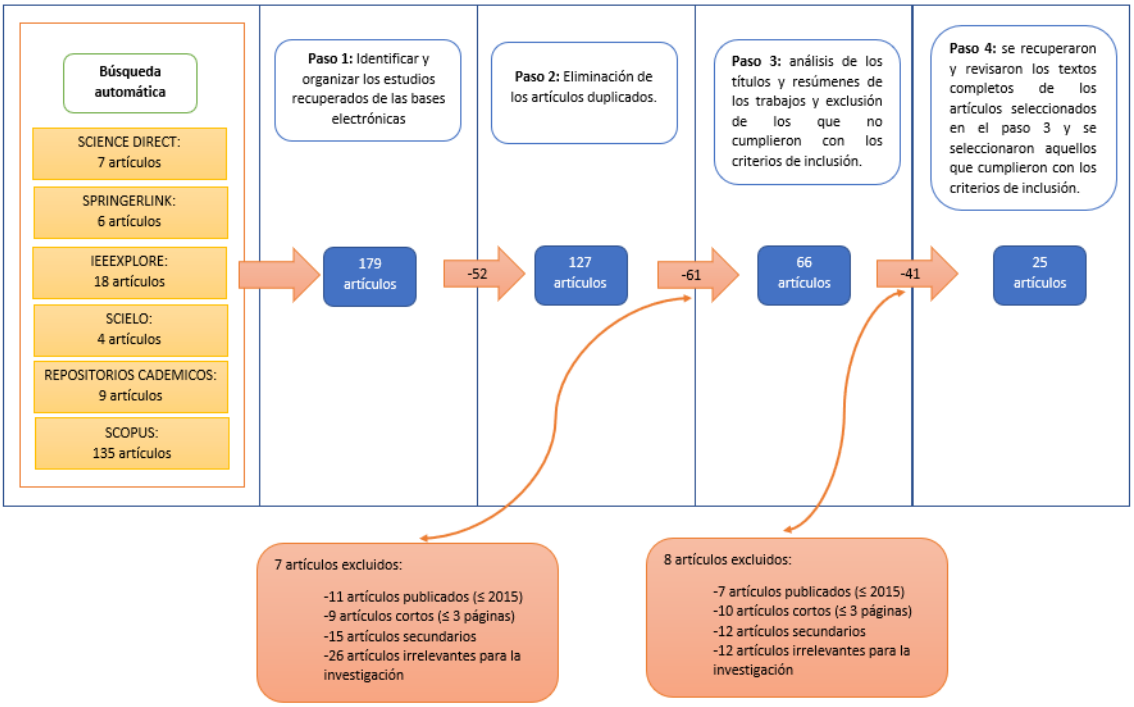


Tabla 6: *Diagrama de Flujo del Proceso de Búsqueda SRL*
Fuente: Elaboración propia

En la **ilustración 2** se indica cuantos artículos han sido usados en la investigación con sus respectivos años, los artículos que se tomaron en cuenta para el grafico son los que han cumplido los requerimientos para la investigación.

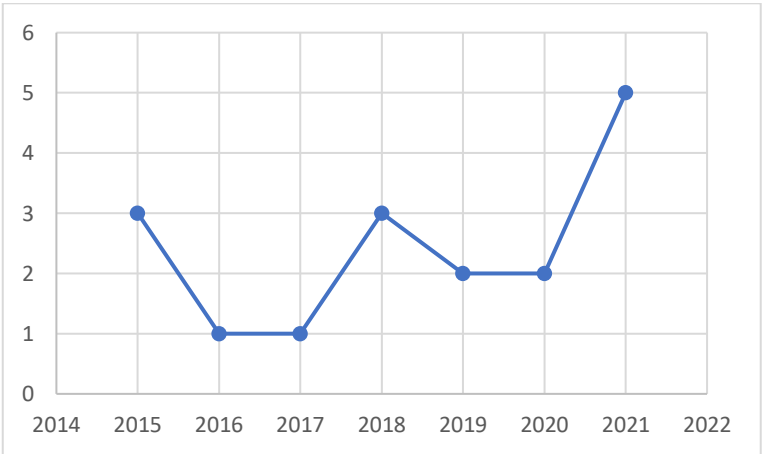


Ilustración 2: *Cantidad de artículos por año*
Fuente: Elaboración propia

En la **ilustración 3** se observa los resultados de la extracción de datos de SCOPUS usando la herramienta VOSviewer donde se tratan los tópicos relacionados al hackeo ético.

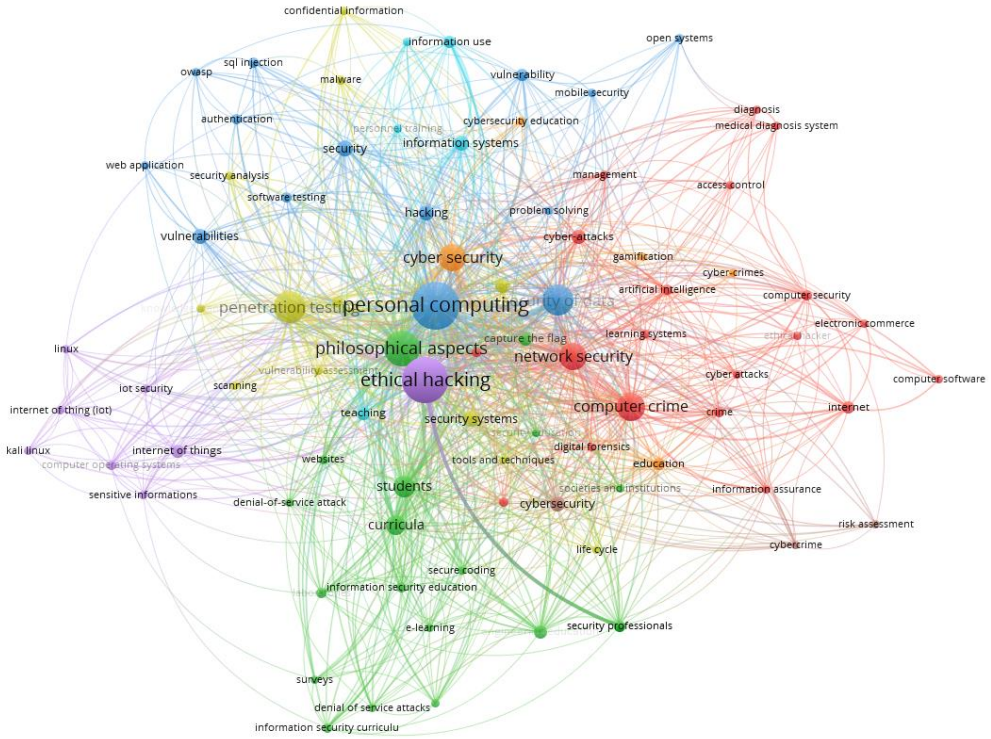


Ilustración 3: *Resultado por Keyword en VOSviewer*
Fuente: Elaboración propia

Se realizó una cadena de búsqueda la cual dio como resultado el gráfico de la **ilustración 4** donde se puede apreciar los documentos por año referentes al hackeo ético, se tomó en cuenta desde el año 2015, la base de datos usada fue SCOPUS

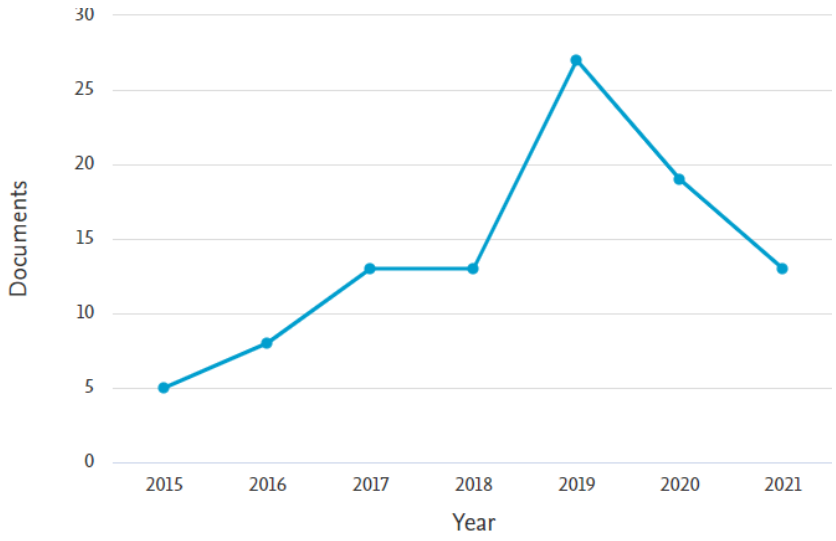


Ilustración 4: *Documentos por año BD SCOPUS*
Fuente: Elaboración propia

1.2. Antecedentes Teóricos

El gráfico a continuación muestra un esquema de los que hará referencia en este punto de la investigación.

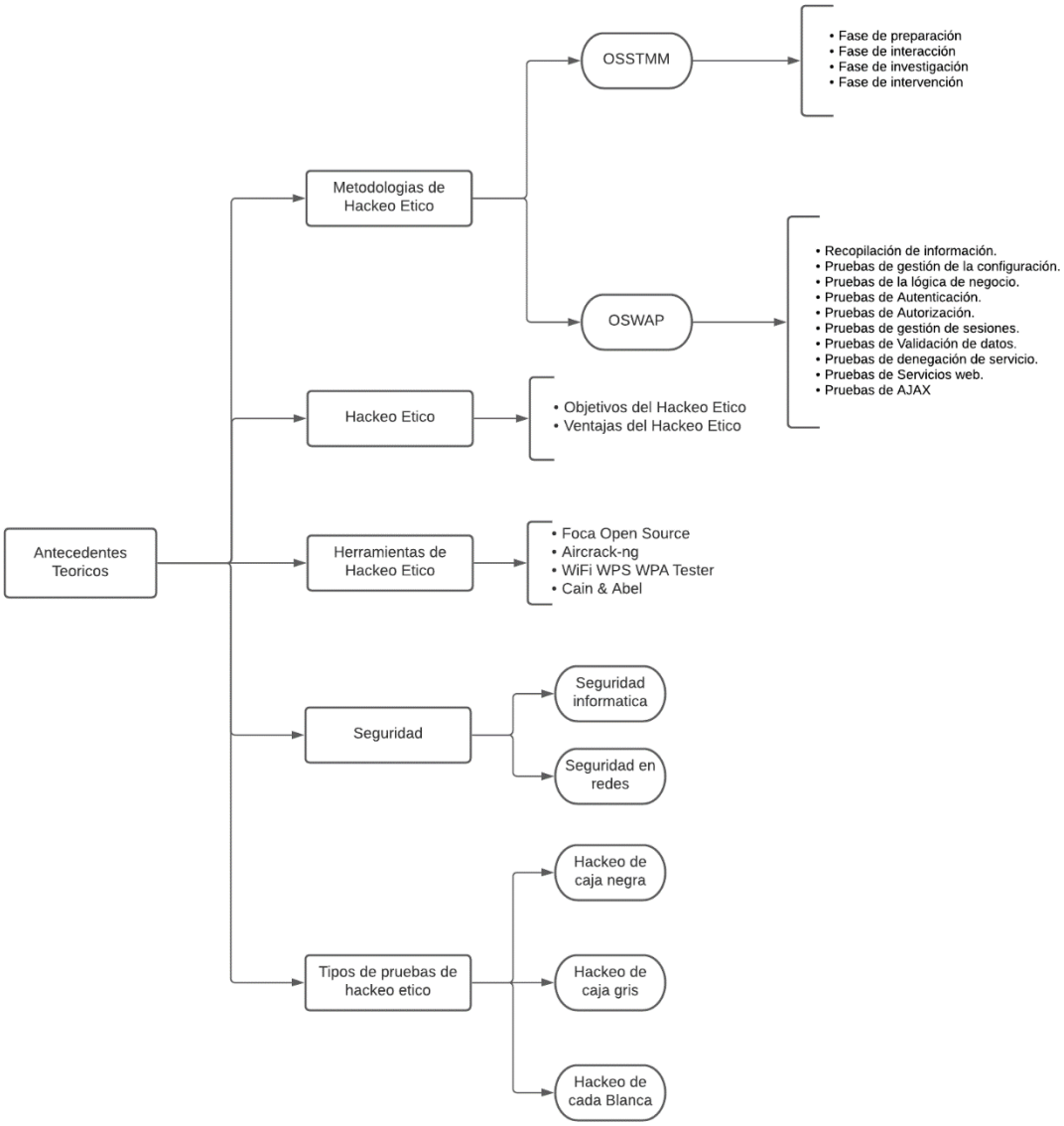


Ilustración 5: *Mapa de antecedentes teóricos*
Fuente: Elaboración propia

1.2.1. Seguridad informática

Según F. Felipe, I. Martínez y M. Sánchez [3] aseguran que sin importar la clase de trabajo que se esté efectuando o que se realice en una computadora es indispensable implementar algún nivel de SI, un usuario doméstico debe tener al menos un antivirus para la protección de datos en caso de virus, de la misma manera en la actualidad los SO (Sistemas Operativos) cuentan con firewall integrado.

Tomando de referencia a los antes mencionado se puede decir que la seguridad informática es un proceso el cual está enfocado en la protección equipos informáticos, software, hardware y datos, estos recursos deben ser únicamente usados por las personas a quienes se les ha autorizado y además deben estar libres de cualquier daño o riego de seguridad.

1.2.2. Seguridad en redes

Según Dabin S. y Bowei Wang [4] aclaran que la evaluación de seguridad en redes hace referencia al control de seguridad en donde se efectúan evaluaciones para determinar si los niveles de seguridad son lo suficientemente estrictos como para evitar violaciones de seguridad.

La seguridad en redes es esencial para prevenir ataques de seguridad, es importante conllevar este tipo de seguridades desde los inicios de las instituciones debido a que con el pasar del tiempo la red se va haciendo más grande y por ende existirán más riesgos de seguridad de datos [5].

Se puede decir que la seguridad en redes es prevenir, impedir y corregir errores mediante niveles de seguridad que ayuden a garantizar la transmisión de datos.

1.2.3. Hackeo Ético

Según Scott Nicholson [6] indica que el hackeo ético se puede clasificar como ético cuando existe un acuerdo entre el hacker ético y la organización, con la aprobación escrita de la organización, de lo contrario al no existir un acuerdo, se declararía como piratería.

James Conrad [7] asegura que una prueba de penetración es una valiosa herramienta que va más allá de un escaneo de vulnerabilidades: es un intento integral de ingresar a un sistema. Se debe comprender que cualquier red puede generar la atención de piratas informáticos, es por esa razón que realizar pruebas éticas ayudan a mantener los sistemas seguros, ataques informáticos pueden resultar en pérdidas de ingresos, puede generar golpes de credibilidad a cualquier organización. Es posible que un probador externo (hacker ético) pueda identificar mejor estos errores [8].

Por lo tanto, el hackeo ético se basa en pruebas técnicas y herramientas que pueden ser aplicadas para la detección de vulnerabilidades de los sistemas informáticos, mencionando que para poder decir que es un hackeo ético se debe tener un acuerdo con la organización, de no ser así se denominaría como piratería informática.

Un hackeo ético cumple la función de solventar fallos de seguridad dentro de las instituciones esto ejerce un trabajo completo muy diferente de un auditor de seguridad, este se encarga de brindar algunas indicaciones de controles a implementar en caso de que existan problemas de seguridad [9].

Objetivos del Hackeo Ético

- Evaluar la preparación de la empresa para saber si esta puede resistir o detectar ataques dirigidos, ya sea de manera externa o interna para así fortalecer los sistemas de la información.
- Acceder a equipos de la organización mediante técnicas de hackeo, con autorización de los encargados de las mismas.
- Brindar mejoras en la protección y en la fiabilidad de los sistemas de información de las empresas.
- Detectar vulnerabilidades y debilidades en la infraestructura de las tecnologías de la información de la empresa.

Ventajas del Hackeo Ético

- Conocer y mitigar las vulnerabilidades de los sistemas informáticos para brindar sugerencias correctivas y necesarias a tiempo.
- Proteger la inversión, tiempo y costos al evitar pérdidas de información, en lugar de costos cuando se responde a un evento de forma reactiva.
- Mantener la integridad corporativa y la confianza de sus contribuyentes.

1.2.4. Metodologías de Hacking Ético

Al hablar de metodologías que pueden aplicarse dentro del área de hackeo ético existen múltiples opciones, entre ellas las más conocidas son OSSTMM y OSWAP [10], estas son las metodologías más usadas para llevar a cabo investigaciones de seguridad informática, para poder comprender el tipo de metodología que puede ser implementada en una investigación se debe identificar el área en el que será aplicada, en la presente investigación se llevará a cabo pruebas dentro de la Intranet, esto implica conocimientos en redes de datos y telecomunicaciones.

1.2.4.1. Metodología OSSTMM

Según M. A. Brignoli y sus colegas [11] indican que la metodología OSSTMM proporciona una metodología para realizar pruebas en profundidad. El control OSSTMM es una medida precisa de seguridad operativa sin suposiciones ni evidencia anecdótica. Es una metodología diseñada para ser consistente y repetible, respaldada por un proyecto de código abierto.

La metodología OSSTMM comúnmente se ha denominado como uno de los estándares profesionales para la evaluación de diferentes tipos de entornos que estén orientados a la seguridad informática. Esta metodología involucra diferentes áreas de seguridad las comunes son las físicas y las de ingeniería social [12].

Esta metodología tiene como límites la evaluación externa, esto quiere decir que se realizan pruebas dentro de un entorno privilegiado a un entorno no privilegiado, para poder acceder a un modo privilegiado se requiere la evasión de componentes de seguridad en la red.

1.2.4.2. Metodología OWASP

Es un proyecto de código abierto dedicado a identificar y combatir las causas que hacen que el software no sea seguro. La fundación OWASP es una organización sin fines de lucro que apoya y administra proyectos e infraestructuras de OWASP. Esta metodología es un método de prueba para aplicaciones web basado en dos fases: pasivo y activo. Su enfoque es la caja negra preferiblemente [13].

Esta metodología está diseñada para la evaluación de seguridad dentro de aplicaciones web. En esta metodología se describen algunas causas que indican cuando un sistema es inseguro, además está compuesta en dos partes: El principio de la evaluación, explicación de las técnicas que esta contiene y el modo de trabajo que maneja OWASP. Su segunda parte es donde se llega a planificar las diferentes técnicas que serán requeridas para poder realizar la evaluación en cada paso del Ciclo de vida del Desarrollo del Software [14].

Como se mencionó anteriormente esta metodología está diseñada para la evaluación de seguridad de aplicaciones web, por ello incluye un apartado donde indica como se deberían realizar pruebas de vulnerabilidades mediante dos fases: Pasivo y Activo.

Modo Pasivo: en este modo la persona encargada de las pruebas debe comprender la lógica de la aplicación para así poder determinar sus puntos de acceso.

Modo Activo: aquí se realizar pruebas, las cuales se dividen en la siguiente subcategoría:

- Recopilación de información.
- Testeo en gestión de configuración.
- Testeo de Autenticación.
- Testeo de Autorización.
- Testeo de Validación de datos.
- Testeo de gestión de sesiones.
- Testeo de denegación de servicio.
- Testeo de Servicios web.

1.2.5. Tipos de Pruebas de Hackeo Ético

1.2.5.1. Hackeo de Caja Negra

El hackeo ético de caja negra es cuando se lleva a cabo una investigación, se recolecta información desde cero lo cual conlleva mucho tiempo, pero esta forma es como lo haría un intruso cualquiera, se experimentan todos los factores que se pueden presentar en el transcurso del hackeo. Como este tipo de hackeo toma demasiado tiempo usualmente se aplica solo en la red perimetral o la red pública del cliente, pero se requiere conocimiento en la infraestructura informática que tiene el cliente. Este tipo de hackeo tiene la finalidad de simular un ataque externo [15].

1.2.5.2. Hackeo de Caja Gris

El hackeo de caja gris se usa cuando se está estudiando la red privada de algún cliente, tiene como finalidad simular ataques por un usuario no autorizado, para que este tipo de hackeo sede hay que tener accesos físicos a la red de la empresa, usualmente estos hackeos se dan por empleados de las empresas o asesores externos [15].

1.2.5.3. Hackeo de Caja Blanca

Entonces esta clase de hacking también se efectúa sobre la red privada del cliente, pero en esta ocasión se nos debe proporcionar un punto de red con direccionamiento IP válido y un listado de las direcciones IP de los equipos a analizar. La idea es simular un ataque perpetrado por un usuario interno autorizado [15].

Se dice que los hackers éticos son probadores de penetración, estos se denominan hacker de sombrero blanco, ya que su propósito es mejorar la seguridad de una empresa y contrarrestar sus vulnerabilidades [16].

1.2.6. Sistemas Operativos

Se le llama sistema operativo al conjunto de programas que tiene incorporado un sistema informático el cual está desarrollado para gestionar recursos de hardware, el sistema operativo se encarga de correr procesos, estos sistemas operativos tienen sus propios fabricantes, en esta investigación se ocuparan dos Kali Linux y Windows server.

1.2.6.1. Kali Linux

Según Eiman Al Neyadi y sus colegas [17] nos dicen que Kali Linux está desarrollado bajo Linux y basado en Debian, con finalidad de realizar pruebas de penetración avanzadas, análisis forense informático, investigación y auditoría de seguridad e ingeniería inversa.

Según ReviTeja G y el Dr. Nandhini [18] afirman que Kali Linux es un sistema operativo de código abierto al estar desarrollado en Linux y este tiene incluidas herramientas para la explotación de vulnerabilidades de un sistema de red.

Kali Linux contiene más de 600 herramientas para auditoría informática, es un árbol Git gratuito, es decir cualquiera puede acceder a sus paquetes según las necesidades específicas que se tengan, se dice que Kali está adherido al estándar de jerarquía de los sistemas de archivos, lo que permite ubicar archivos binarios de manera sencilla, este sistema operativo es un entorno seguro y sobre todo a pesar de ser OpenSource está financiado y mantenido por Offensive Security.

1.2.6.2. Windows Server

Según Swaroop K. y sus colegas [19] indican que Windows server es un sistema operativo pensado para servidores, el cual no es gratuito para su uso se requiere la compra de su licencia de activación. Este servidor puede habilitar de manera selectiva una amplia instrumentación de líneas de comandos de Windows Infraestructura de administración de Windows.

Windows server es comúnmente el más utilizado debido al que ser un sistema operativo de licencia contiene actualizaciones constantes de seguridad, haciéndolo más seguro que un sistema operativo libre, además Windows server trae un entorno más intuitivo para su administración y migración de usuario que se tengan alojados en Active Directory.

1.2.7. Herramientas de Hackeo ético

1.3. Ámbitos de aplicación

En la actualidad se han presentado diversos casos de ataques informáticos en el Ecuador y sobre todo a empresas importantes, algunas de las que se vieron envueltas por esta clase de ataques fueron el banco del pichincha, la agencia nacional de tránsito y el más relevante fue el ataque a la empresa CNT. Este tipo de ataques se dan por la falta de asesoría en seguridad informática, es por ello que se ha propuesto esta investigación, una de las razones principales es incentivar a las demás empresas o instituciones a que hagan este tipo de auditorías para prevenir estos ataques.

La falta de protección de los activos de información puede convertirse en un costo financiero alto y sobre todo público, sin mencionar que esto puede generar interrupciones laborales en las actividades cotidianas de una institución [20].

La investigación tiene como finalidad vulnerar la seguridad de la empresa dentro de su red privada y así poder encontrar posibles falencias que perjudiquen la integridad de la misma. El hackeo ético este hecho para mitigar estas vulnerabilidades, para encontrar vulnerabilidades primero se realiza

una recolección de datos, esto se efectúa mediante herramientas de hackeo, las cuales ayudan a recopilar información mediante el tráfico de red, así mismo se crean scripts con instrucciones que ayuden a realizar alguna tarea específica.

Para esta investigación se usará el Sistema Operativo Kali Linux como base de desarrollo para todo ataque controlado, hacia la Intranet de la empresa que ha brindado su apoyo para la realización de este proyecto, una vez encontradas sus vulnerabilidades se observará el nivel de riesgo y se procederá a fortalecer sus protocolos de seguridad.

1.4. Establecimiento de requerimientos

La aplicación del hackeo ético se divide en las siguientes fases:

Recolección de información, en esta fase se realizó un análisis de la infraestructura de la institución en donde se pudo ver que equipos utilizan y la forma en la que está estructurada su red interna. Para la implementación, se utilizó el sistema operativo Kali Linux para lanzar ataques controlados y así mismo se lo usó para crear scripts en lenguaje Python, para esto se usaron diversas herramientas que vienen integradas en Kali Linux.

La fase de pruebas se realiza una vez terminado de recolectar información de la empresa, con la información se puede identificar que equipos o sistemas de la información pueden ser vulnerados y luego pueden ser rectificados.

2. CAPÍTULO II. DESARROLLO DEL PROTOTIPO

2.1. Definición del prototipo

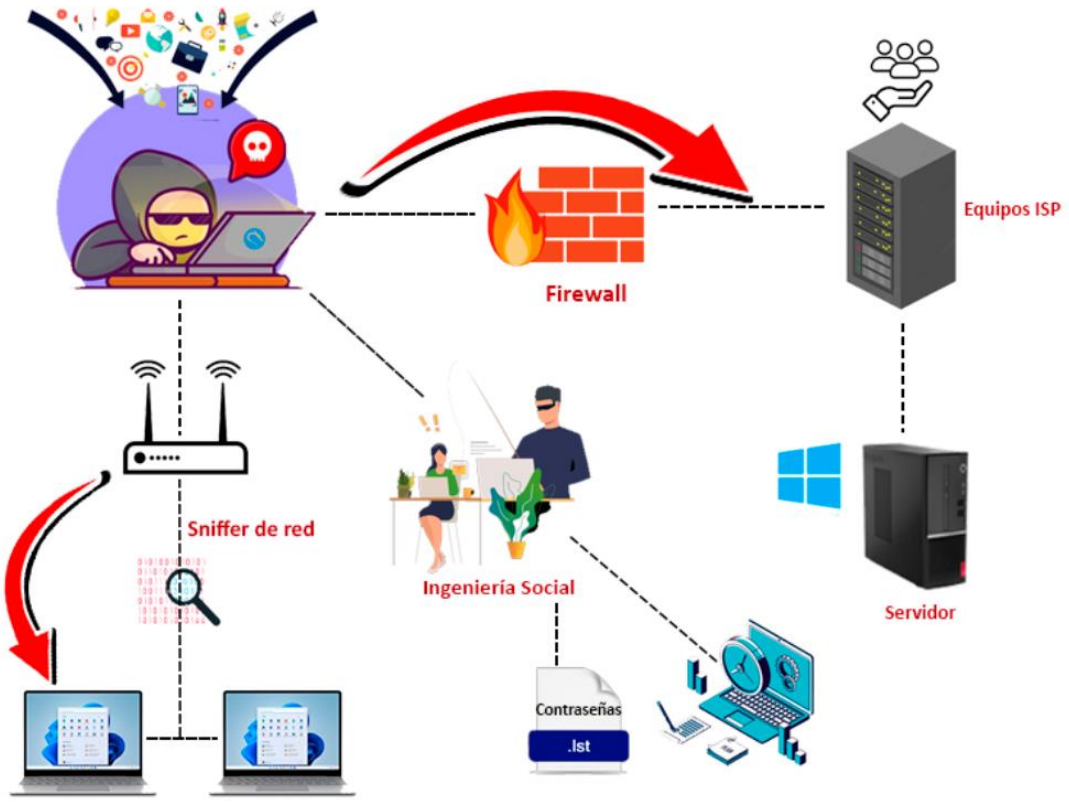


Ilustración 6:*Definición del prototipo*
Fuente: Elaboración propia

En la **ilustración 8** se muestra de manera sencilla el prototipo de la infraestructura interna, donde se aprecia que existe un cortafuegos o firewall para prevenir acceso a intrusos, el objetivo de manera específica es buscar las vulnerabilidades del protocolo de seguridad y acceder a equipos locales que están conectados entre sí para compartir archivos dentro de la red.

El hacker ético haciendo uso de una computadora con Sistema Operativo llamado Kali Linux buscará mediante aplicaciones de auditoría y de desarrollo de scripts con lenguaje Python recolectar información relevante para el ataque controlado, consiguiente así obtener información con el tráfico de red que es enviado a través de paquetes del router.

Una vez dentro de la red del cliente se procede con ataques como phishing para obtener credenciales de acceso, para los router o switch que tienen alojados dentro de sus instalaciones, para así sacar la información de todos sus clientes alojados dentro de estos.

Una vez obtenida la información y las credenciales de acceso se procede a mejorar los protocolos de seguridad para prevenir futuros ataques informáticos, que puedan poner en riesgo la integridad de la empresa.

La capacidad de obtener información con captura de datos financieros a través de sistemas computarizados ha evolucionado en las últimas décadas [21], así es como también existen programas maliciosos que capturan datos en el tráfico de red, gran parte de estos ya lo hacen de manera automatizada facilitando la captura y secuestro de información.

Este prototipo se desarrolló tomando en cuenta la capa de red donde funciona el firewall:

Capa 3 de modelo OSI: en esta capa se controla todo a nivel de routing o IP, es decir es cortafuegos de filtrado de paquetes, para realizar estos filtros se basa en la IP de origen/destino el protocolo que se ha usado y el puerto.

2.2. Metodología de desarrollo del prototipo

2.2.1. Enfoque, alcance y diseño de investigación

Problema de la Investigación: ¿Cómo aplicar el Hackeo Ético en la determinación de riesgos y vulnerabilidades en la infraestructura de la empresa FONET CIA LTDA de la ciudad de Pasaje, durante el período 2021-2022?

El enfoque de investigación

El enfoque que se va utilizar es el presente trabajo será cuantitativo, se llevará a cabo una investigación bibliográfica con la cual se podrá probar la hipótesis planteada. Para esto se realizarán pruebas de hackeo ético controlados para explotar vulnerabilidades, para así poder corregir estos fallos de seguridad.

El alcance de investigación

El estudio se comenzará como exploratorio y luego comenzará la fase descriptiva, en virtud de que se dispone de información sobre estudios que se hayan realizado acerca del hackeo ético dentro de instituciones públicas como privadas, con la finalidad de ayudar a reforzar las vulnerabilidades existentes dentro de las instituciones para prevenir la integridad de las mismas y la de sus empleados.

El diseño de investigación

El diseño de la presente investigación será causi-experimental ya que este será aplicado dentro de una institución privada, en la cual se usarán métodos y herramientas de hackeo ético para mitigar riesgos y de la misma manera fortalecer la seguridad para prevenir pérdidas de información.

2.2.2. Unidades de análisis

Población

La población que se ha considerado para la presente investigación fue la totalidad del personal que ejerce labor dentro del departamento técnico de la empresa FONET CIA LTDA.

Muestra

Como la población a investigar es pequeña la muestra a tomar es el valor de la misma población.

2.2.3. Técnicas de instrumento de recopilación de datos

Para este proyecto es necesario usar técnicas e instrumentos para llevar a cabo el desarrollo de la investigación por ello se establecieron las siguientes.

Tabla 7: *Técnicas de instrumentos de recopilación de datos*

Técnica	**Instrumento**
Observación	Guía de observación, lista de control
Análisis de documentos o datos	Guía de análisis de documentos o de datos
Reunión	Convocatoria con Puntos a tratar en la reunión, presentación electrónica.

Fuente: Elaboración propia

2.2.4. Técnicas de procesamiento de datos para la obtención de resultados

Para la obtención de datos se realizaron 6 procesos incluyendo los procesos para la obtención de información mediante fuentes bibliográficas, a continuación, se detallan los procesos:

- Recolección de datos mediante fuente Bibliográficas
- Proceso de búsqueda SRL
- Mapas conceptuales
- Pruebas de Hipótesis
- Pruebas de hipótesis

2.2.5. Metodología o métodos específicos

Mediante revisiones bibliográficas, se pudo constatar que las metodologías más usadas son la OSSTMM, OWASP y la metodología ISSAF, cada metodología cumple una evaluación de

seguridad diferente, por ello se pretende hacer una comparación entre las 3 metodologías para así poder conocer las diferencias entre sí y poder tener una selección razonable de lo que se va utilizar en la presente investigación.

Comparación de metodologías para hackeo ético

OSSTMM

Está diseñada para ser repetible y ofrecer una estrategia, evaluaciones y medidas de riesgo, un valor intrínseco con respecto a los valores entregados por los test efectuados, esto la hace una metodología novedosa en comparación a las otras metodologías ya que ofrece aquella meticulosidad.

Esta metodología exige que se realicen diversas actividades y se generen varios documentos, aunque es más extensa que la metodología ISSAF para detallar las partes que pertenecen a un proyecto de prueba de penetración profesional.

Con la metodología OSSTMM se tienen más puntos para abarcar al momento de hacer hackeo ético ya que esta no solo se basa en páginas web como la metodología OWASP. Esta metodología cuenta con las siguientes fases:

- Fase de Inducción: en la primera fase se establece un alcance, aquellos requerimientos y las restricciones del hackeo ético.
- Fase de Interacción: se busca descubrir qué relación hay entre el alcance, activos y los objetivos que están involucrados.
- Fase de Requerimientos: en esta fase se verifican los procesos, configuraciones, propiedades intelectuales, datos expuestos y otros.
- Fase de Intervención: se centra en la penetración de sus objetivos y de cómo estos se ven afectados.

OWASP

Esta metodología de código abierto la cual está elaborada para pruebas de penetración en sitios web, aquí pueden ser aplicados todos los tipos de ataques centrados a este tipo de sistemas, la metodología está dividida en varios grupos de pruebas de seguridad de las páginas web:

Recopilación de datos

- Test de seguridad a configuraciones y despliegues
- Test de seguridad a los procesos de autenticación

- Test de seguridad a las gestiones de identidades.
- Test de seguridad al proceso de autorización.
- Test de seguridad a los procesos de gestión de sesiones.
- Test de seguridad para la validación de entradas.
- Test de seguridad a los manejos de errores.
- Test de seguridad a mecanismos de criptografía.
- Test de seguridad en la lógica de negocios.
- Test de seguridad del lado del cliente.

ISSAF

Es una metodología de test de penetración la cual se encarga de evaluar la red de trabajo, sistemas y los controles de aplicaciones, se centra en todo lo que refiere a equipos de cómputo. Esta contiene 3 fases para su función las cuales son:

- Planificación: es el proceso inicial para el intercambio de la información inicial, preparación y planificación para las pruebas de seguridad que serán ejecutadas.
- Evaluación: se procede con un análisis de la infraestructura computacional de la institución y a su vez se detectan las vulnerabilidades.
- Reportes: se genera un reporte o informe con todos los problemas de seguridad que han sido encontrados.

Tabla 8: *Comparación entre metodologías*

	OSSTMM	ISSAF	OWASP
Ámbito Digital	✓	✓	✓
Ámbito Físico	✓		
Ámbito Social	✓	✓	
Guías técnicas			✓
Métricas	✓		
Informes	✓	✓	
Gestión de Proyecto			

Fuente: Elaboración propia

La comparación de la tabla 6 se realiza considerando varios ámbitos sobre donde se aplicará la metodología. Las 3 metodologías abordan el ámbito digital de seguridad, pero solo una abarca el ámbito físico y 2 abarcan el ámbito para la ingeniería social, la cual forma parte importante para esta investigación.

Otro factor relevante es la guía técnica en donde solo OWASP cuentan con este tipo de guías, esto en función a dar a conocer cómo se realizan las pruebas que indica la metodología.

Cuando se efectúa una prueba es importante hacer uso de métricas para establecer notas al estado de seguridad de una infraestructura, para ello la metodología OSSTMM cuenta con métricas.

Cuando una auditoría o pruebas de hackeo ético han finalizado es fundamental entregar un informe, aunque las pruebas estén bien ejecutadas si estas no están documentadas no será posible transmitir de forma idónea la información al cliente, la única que no hace uso de informes es la metodología OWASP.

Metodología seleccionada

La metodología a introducir será la OSSTMM la cual ha sido seleccionada para realizar la guía de aplicación.

¿Por qué fue elegida?

Para esto se toma en consideración la tabla 6 en donde se efectúa una comparación de las metodologías más usadas en auditorías de seguridad, ahí se puede apreciar que OSSTMM es la más completa.

OSSTMM es la única que abarca la mayoría de los ámbitos establecidos, con lo cual se convierte en la única posibilidad de cumplir con los objetivos planteados de seguridad en la institución. Un punto a favor muy importante de esta metodología es que cuenta con métricas y explica cómo se deben hacer los informes.

Esta metodología carece de la gestión de proyectos es donde se incluye la parte de acuerdo previo y la presentación de resultados. Pero esto no es una tarea que le corresponde realizar al analista, por lo cual la falta de esto no es un aspecto negativo para la metodología. Tampoco cuenta con una guía técnica la cual específica sobre cómo llevar a cabo las pruebas que se han propuesto, pero esto es precisamente el objetivo de la investigación con lo cual no se considera un punto negativo.

A partir de las conclusiones mencionadas se considera OSSTMM una metodología adecuada.

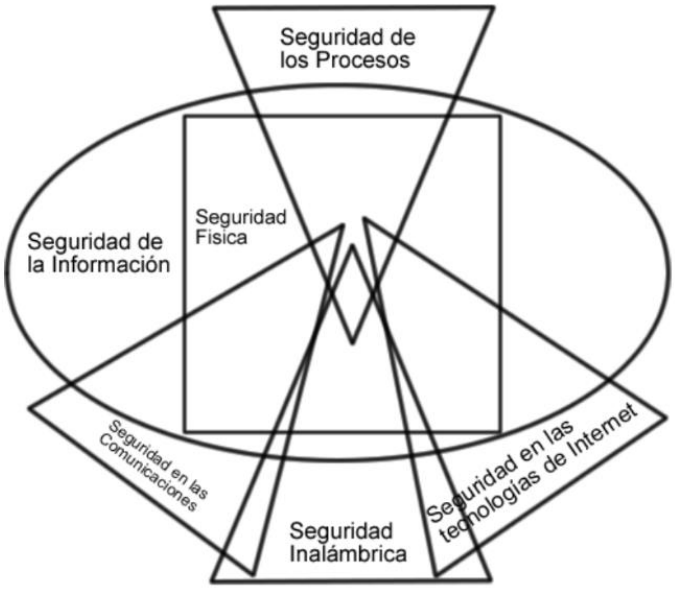


Ilustración 7: *Secciones manual OSSTMM*
Fuente: Obtenido de [18]

Thomas Wilhelm [22] indica que esta metodología ha seguido proporcionando pruebas directas y fácticas para las respuestas fácticas. Incluye información para la planificación del proyecto, la cuantificación de resultados y las reglas de participación para quienes realizan las auditorías de seguridad.

La metodología OSSTMM está compuesta de las siguientes fases:

- Fase de preparación
- Fase de interacción
- Fase de investigación
- Fase de intervención

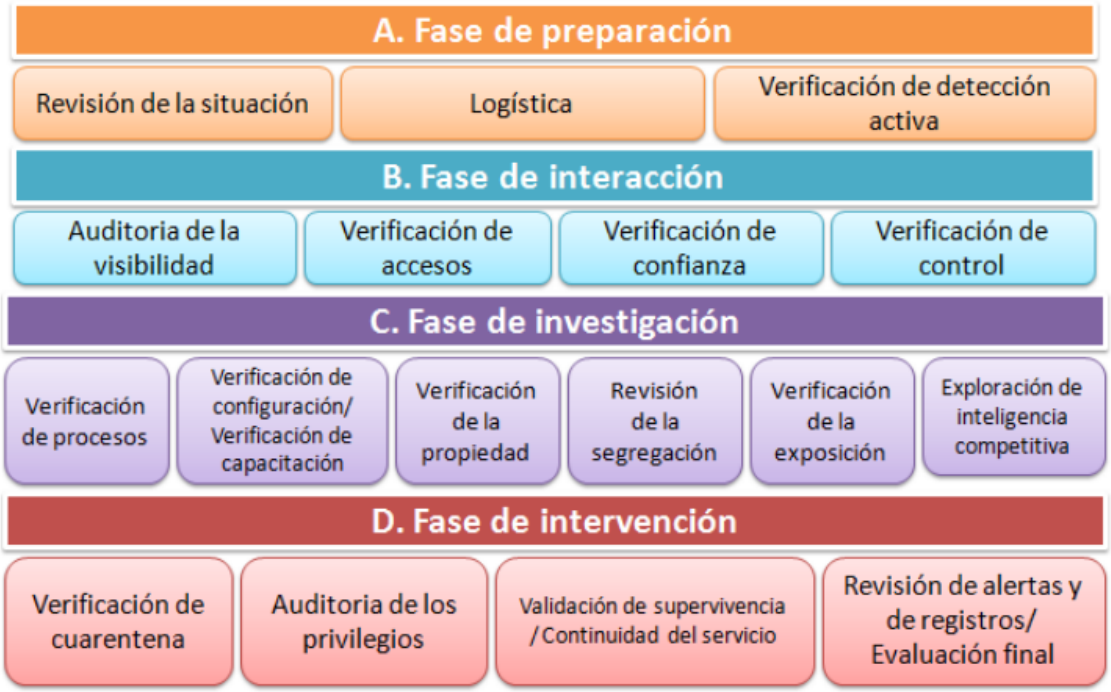


Tabla 9: *Fases de metodología OSSTMM*
Fuente: Obtenido de [23]

2.2.6. Herramientas y/o Materiales

Para la realización del proyecto es imprescindible el recurso material, por ello se ha detallado lo siguiente:

Tabla 10: *Herramientas*

TIPOS DE HERRAMIENTAS	HERRAMIENTAS ESPECÍFICAS
Herramientas de Software	Word Visual Code Python Herramientas para Hackeo Ético: • Foca Open Source • Aircrack-ng • WiFi WPS WPA Tester • Cain & Abel Lucidchart (mapas conceptuales) Sistemas Operativos • Windows Server • Kali Linux • Windows 10
Herramientas de Hardware	Computadora de Escritorio Laptop
Técnicas o métodos de hackeo ético	Ataques controlados Denegación de servicios

Fuente: Elaboración propia

2.3. Desarrollo del prototipo

2.3.1. Fase de preparación

2.3.1.1. Revisión de la situación

Esta fase es el inicio de la investigación para el hackeo ético, se recopila información relevante para poder detectar ataques controlados, al tratarse de una empresa que provee servicios de Internet, debe tener reforzada su seguridad en accesos a sus aplicaciones de control de equipo como router, switch, ect.

INFRAESTRUCTURA INTERNA DE FONET CIA LTDA

Para iniciar la investigación se realizó un diseño de la estructura de red que contiene la empresa internamente, donde se puede observar que cuentan con un Switch Administrable el cual distribuye parte la red interna.

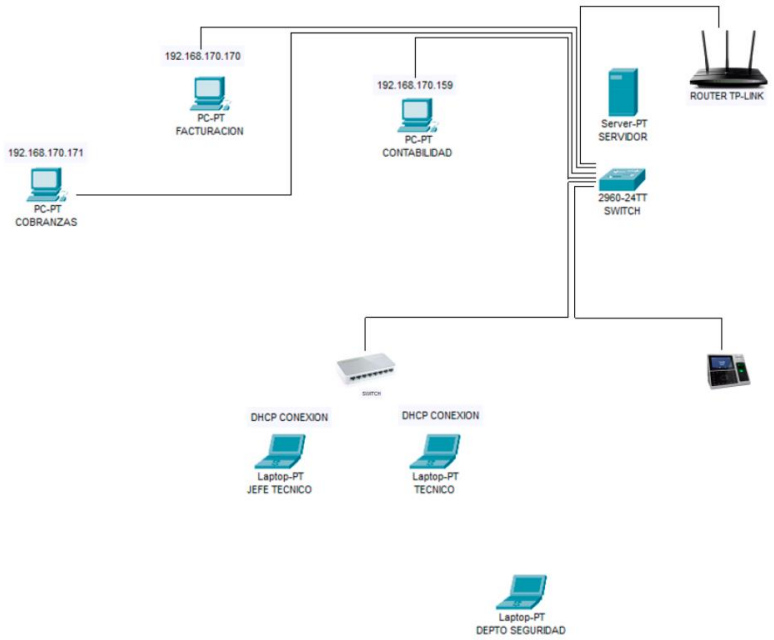


Ilustración 8: *Representación gráfica de infraestructura interna de la Institución*
Fuente: Elaboración propia

Una vez observada la infraestructura de red interna de la institución se pueden obtener ideas para poder validar accesos no autorizados, la mayoría de equipos imparten la red desde el switch administrable de la empresa.

La empresa ofrece a sus clientes una red de Internet, la cual es para que estos puedan bajar facturas o para que hagan pruebas de la calidad del servicio que va a contratar, esto lo usan como una estrategia de venta, pero como se puede apreciar en el gráfico, solo existe un router, haciendo

notorio que dicho router sirve para el uso de los empleados y para las computadoras que están conectadas de manera inalámbrica por DHCP, dando apertura a posibles ataques informáticos.

2.3.1.2. Fase de interacción

La empresa cuenta con equipo Mikrotik el cual proporciona las IP y VLAN, las cuales son asignadas a los clientes, se pudo observar en el departamento técnico que el callcenter al recibir una llamada por algún problema que tenga sus clientes, ingresaba la dirección IP en cualquier navegador y este redireccionaba a la interfaz de login de los equipos de los clientes, accedía e inspeccionaba las configuraciones y cantidad de dispositivos dentro de la red, una de las principales fallas al observar esto, es que las credenciales de login como administrador son las que el fabricante pone por defecto:

Tabla 11: *Claves por defecto del equipamiento de la institución*

CLAVES DE EQUIPOS			
EQUIPOS	ONT HUAWEI	ONT VSOL	ROUTER TP-LINK
Usuario	telecomadmin	admin	admin
Contraseña	admintelecom	stdONUi0i	admin

Fuente: Elaboración propia

Observando esto, se ingresó desde otra computadora a la misma IP para revisar si esto se podía hacer desde cualquier computador conectado a Internet y efectivamente, se podía acceder desde cualquier dispositivo que esté dentro de la red de la empresa, pero no solo de la red interna de la empresa, se puede acceder desde cualquier servicio de Internet de los clientes.

Dando así una vulnerabilidad masiva con gran parte de sus usuarios, se accedió a la red de un cliente y se empezó hacer ping a las IP de diferentes clientes para comprobar si lo indicado era correcto y se pudo corroborar que la red de cierta manera está abierta, ocasionando una vulnerabilidad.

Aplicaciones para gestión de equipos

Tabla 12: *Datos importantes del Sistema U2000*

Nombre del sistema: U2000 SERVER	
Descripción	La aplicación de escritorio ayuda a agilizar el proceso de registro de clientes dentro de la OLT mediante una interfaz gráfica amigable, evitando así la implementación de comandos complejos por consola.
Plataforma	La aplicación se encuentra desarrollada en el Lenguaje de programación Java, con el gestor de base de datos MySQL y se encuentra funcionando en un servidor con el Sistema Operativo Windows Server.

Funciones de nivel 1 y 2	**Nivel1:** El sistema permite llevar el registro de clientes dentro de la OLT de una manera más rápida y sencilla. Permite gestionar configuraciones ISP para cada cliente. El software está elaborado explícitamente para dispositivos Huawei.
Complejidad de aplicaciones	Medio
Divisiones	Administración de RED

Fuente: Elaboración propia

Tabla 13: *Datos importantes del sistema Winbox*

Nombre del sistema: Winbox	
Descripción	Winbox permite la administración de los Mikrotik mediante una interfaz gráfica, esta aplicación permite realizar conexiones vía FTP, TELNET y SSH.
Plataforma	La aplicación se encuentra desarrollada en el Lenguaje de programación Java, se encuentra funcionando en un servidor con el Sistema Operativo Windows Server.
Funciones de nivel 1 y 2	**Nivel1:** Permite gestionar la configuración de Mikrotik como IPs, VLANs, firewalls. Permite analizar el espectro de consumo de Internet de manera general.
Complejidad de aplicaciones	Medio
Divisiones	Administración de RED
Complejidad entre divisiones	Bajo

Fuente: Elaboración propia

2.4. Ejecución del prototipo

La nueva red de internet está expuesta a grandes ciber amenazas que pueden perjudicar diferentes situaciones, ya que estas pueden evolucionar de manera dinámica. Existen diferentes tipos de amenazas como las Persistentes Avanzadas, botnets, zero days entre otras, son ejemplos de algunas amenazas que han avanzado de manera significativas los últimos años [23], con la ejecución del prototipo se observara que tipo de amenazas pueden afectar a la institución que se está llevando la investigación.

2.4.1. Elaboración de VPN o Túnel de datos

Se implementó un VPN con el protocolo PPTP para poder establecer conexión con la red del ISP, este VPN permite poder conectarnos como un cliente más, para esto se efectuó la siguiente configuración.

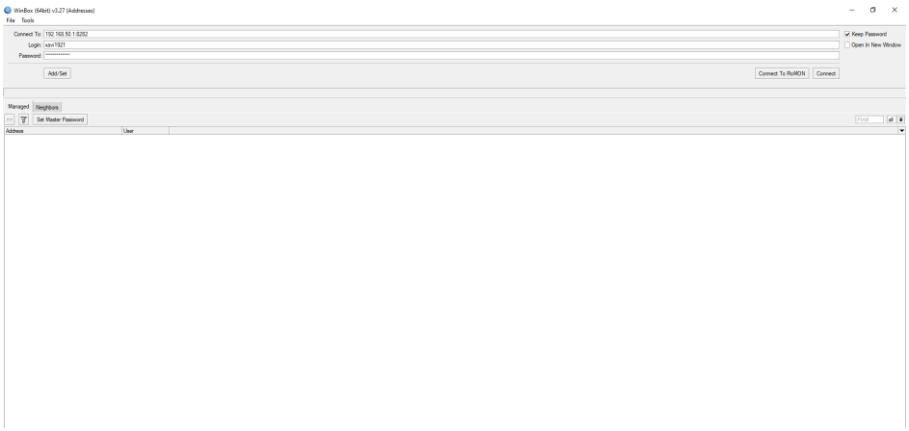


Ilustración 9: *Interfaz de Login en Winbox*
Fuente: Elaboración propia

Primero se deben establecer los DNS, en este caso se están usando los de Google.

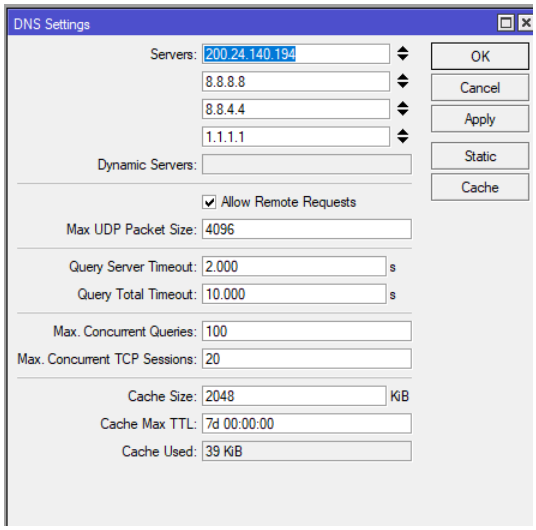


Ilustración 10: *Asignación de los DNS en Winbox*
Fuente: Elaboración propia

Se habilita la conexión PPTP dentro del Mikrotik para establecer conexiones

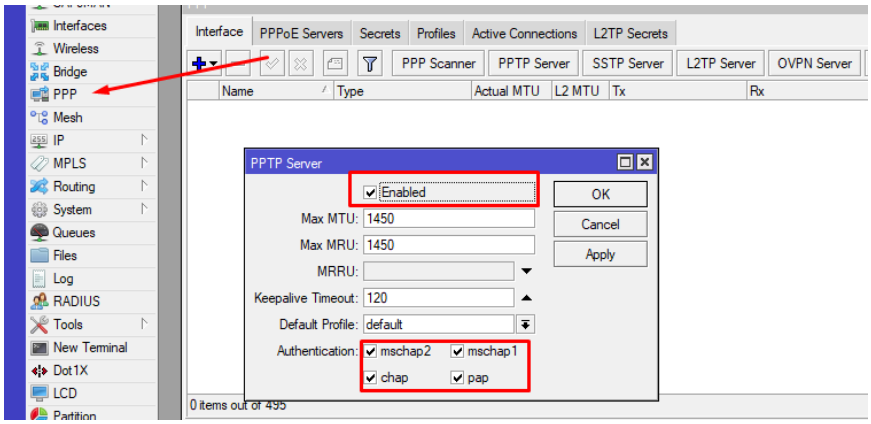


Ilustración 11: *Habilitación de Conexión PPP VPN*
Fuente: Elaboración propia

Se requiere alojar un pool de IPs

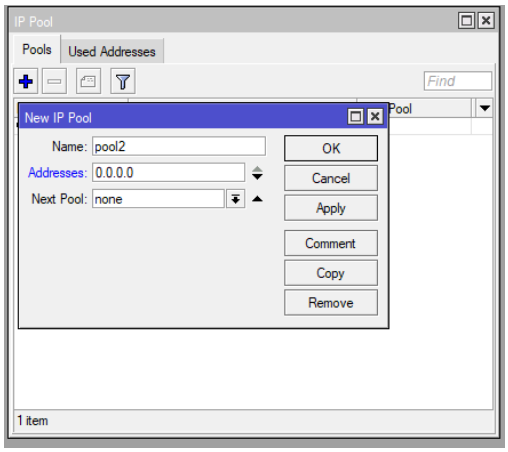


Ilustración 12: *Asignación de rango de IP*
Fuente: Elaboración propia

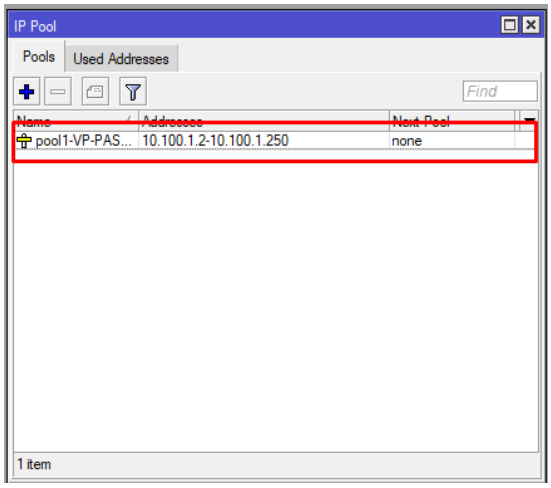


Ilustración 13: *Pool de IP establecida*
Fuente: Elaboración propia

Se debe crear las credenciales de acceso al VPN dentro del Mikrotik

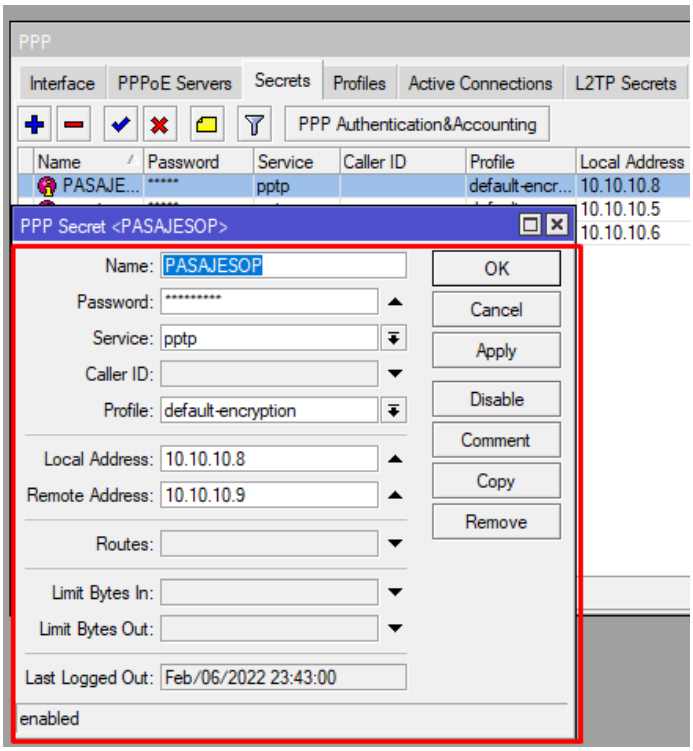


Ilustración 14: *Configuración del VPN con protocolo PPP*
Fuente: Elaboración propia

Ya configurado esto se puede ingresar en un ordenador o en un dispositivo móvil, en este caso se requiere aplicarlo en una computadora para hacer pruebas de conexión. Hay que tomar en cuenta que el tipo de conexión que se escogió es PPTP

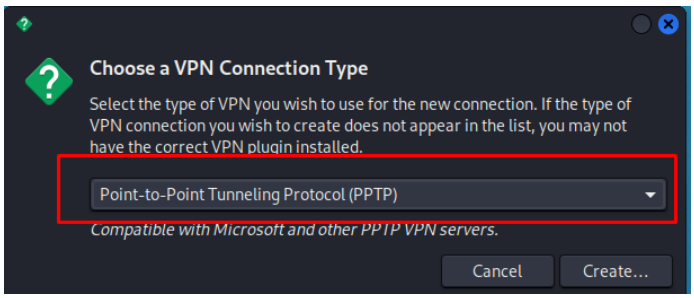


Ilustración 15: *Conexión a VPN desde Kali Linux*
Fuente: Elaboración propia

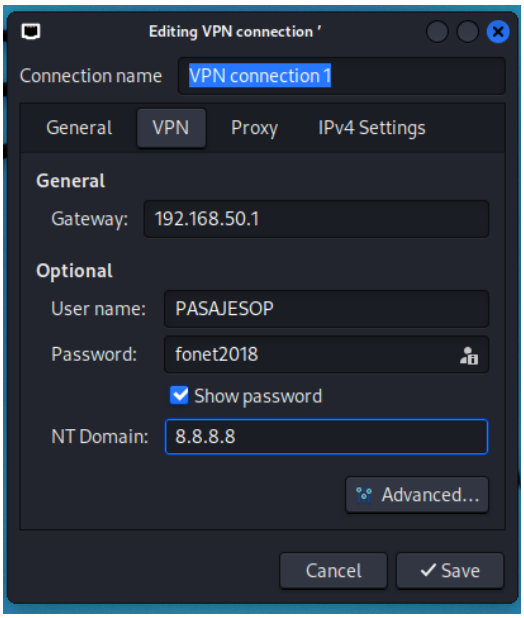


Ilustración 16: *Configuración de protocolo de conexión Kali Linux*
Fuente: Elaboración propia

Ya configurado se establece conexión por el VPN, muestra el apartado de conexión exitosa

Ilustración 17: *Conexión VPN vía PPP*
Fuente: Elaboración propia

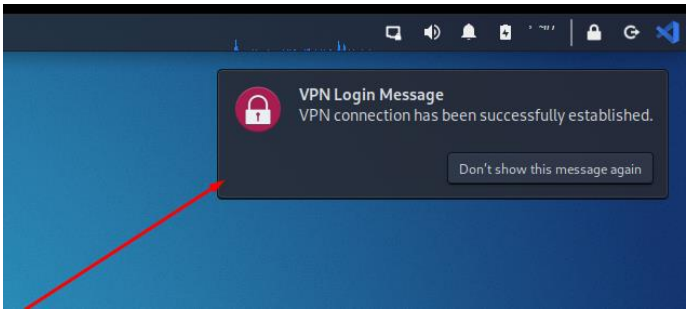


Ilustración 18: *Notificación de conexión exitosa*
Fuente: Elaboración propia

2.4.2. Verificación de protocolos de seguridad y firewall aplicados en equipos Mikrotik

Acceso a clientes por IP

Para efectuar un ataque mediante IPs se necesita tener una IP de cliente activo, para esto mediante la consola de comando se ingresan las IPs con la estructura de 192.168.

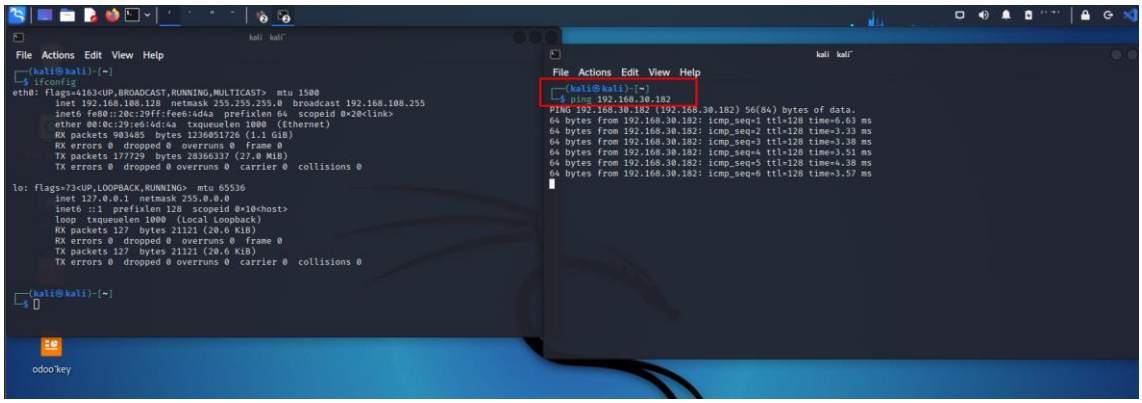


Ilustración 19: *Testeo manual de IPs accesibles remotamente*
Fuente: Elaboración propia

Cuando una IP resulta exitosa mediante su respuesta esta es ingresada al navegador.

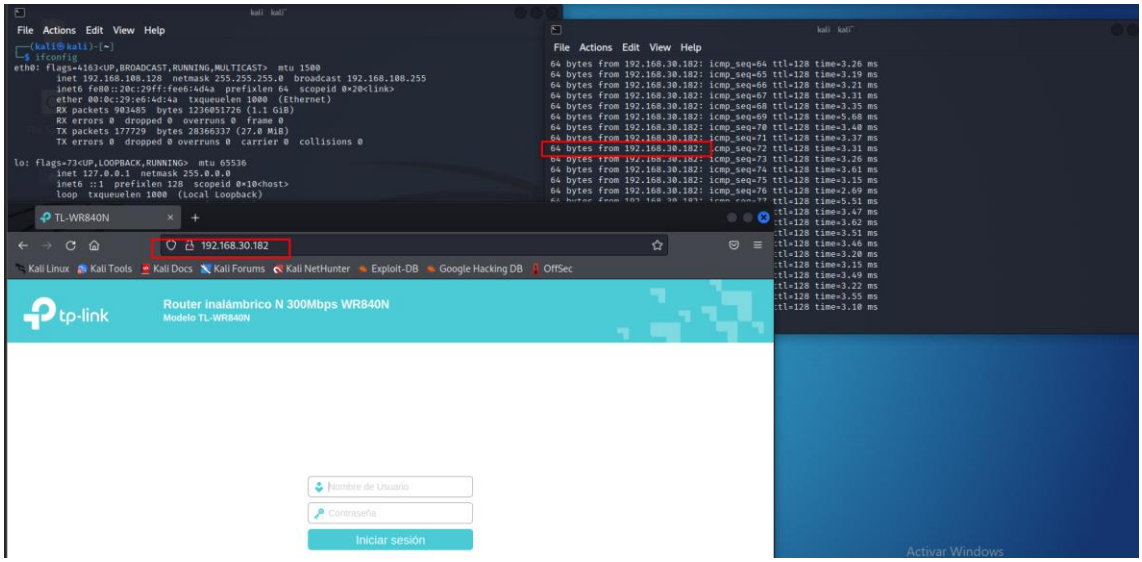


Ilustración 20: *Ingreso a redes privadas de abonados mediante dirección IP*
Fuente: Elaboración propia

Un error común de un ISP es no modificar el usuario y contraseñas de los equipos que aloja en sus clientes, en este caso práctico se ingresan las credenciales de acceso que traen por defecto los equipos. Un ataque sencillo de ejecutar como objeto de prueba es el phishing el cual se puede dar por DNS ocasionando un redireccionamiento a páginas establecidas por el atacante esto puede ser configurado dentro de equipos como router y ONT, para ello se debe buscar los siguientes apartados en las configuraciones.

En este caso se asignan los DNS en DHCP para que afecte únicamente a dispositivos que no tengan configuraciones estáticas.

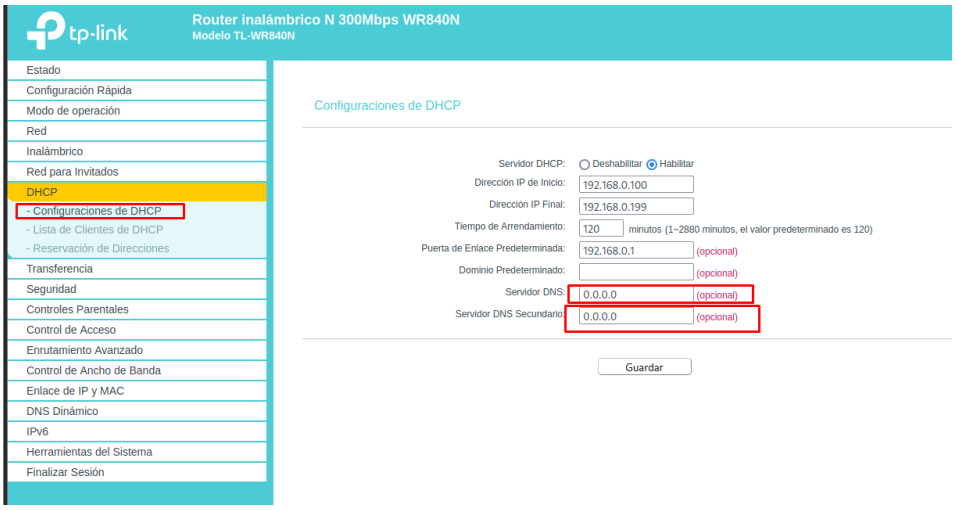


Ilustración 21: *Configuración de DNS malicioso en abonados*
Fuente: Elaboración propia

En la imagen se puede apreciar unos DNS, los cuales contienen redirección de publicidad.

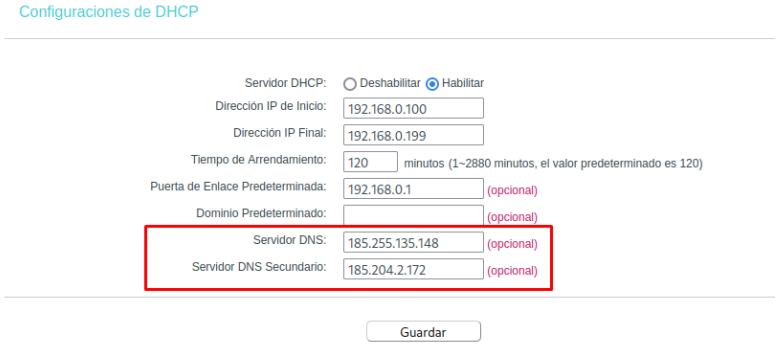


Ilustración 22: *Asignación de DN para Redireccionamiento*
Fuente: Elaboración propia

Al revisar las configuraciones de equipos en DHCP del cliente, se observa cómo tiene por defecto los DNS anteriormente configurados.

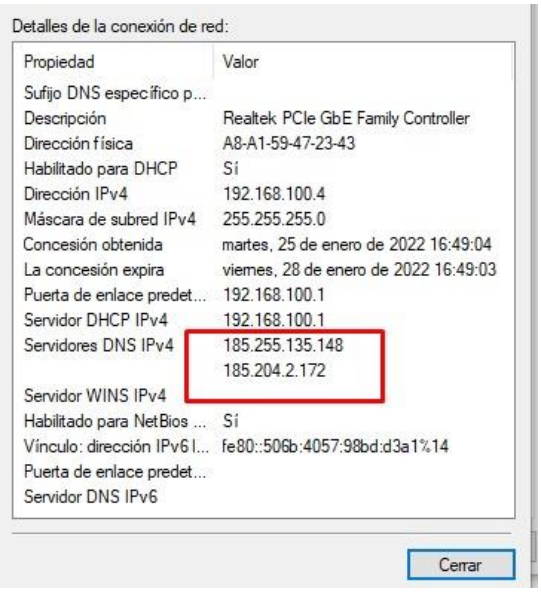


Ilustración 23: *Comprobación de inserción de DNS*
Fuente: Elaboración propia

Como se mencionó anteriormente esto ocasiona una redirección de páginas no seguras, en la mayoría de dispositivos se apreciará una interfaz como se muestra a continuación, en donde el navegador da una advertencia de seguridad.

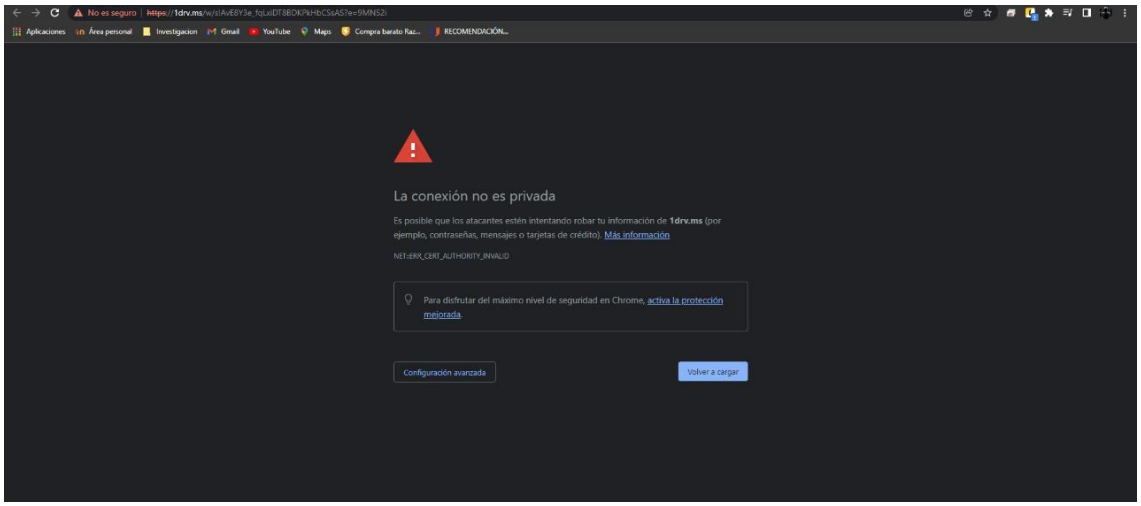


Ilustración 24: *Evidencia en navegador web de escritorio*
Fuente: Elaboración propia

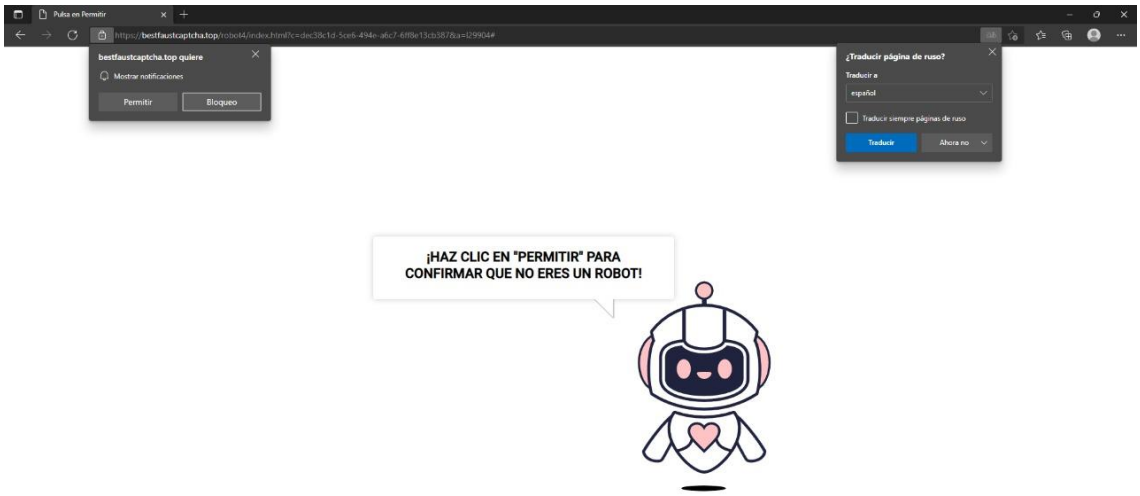


Ilustración 25: *Evidencia de Navegador web*
Fuente: Elaboración propia

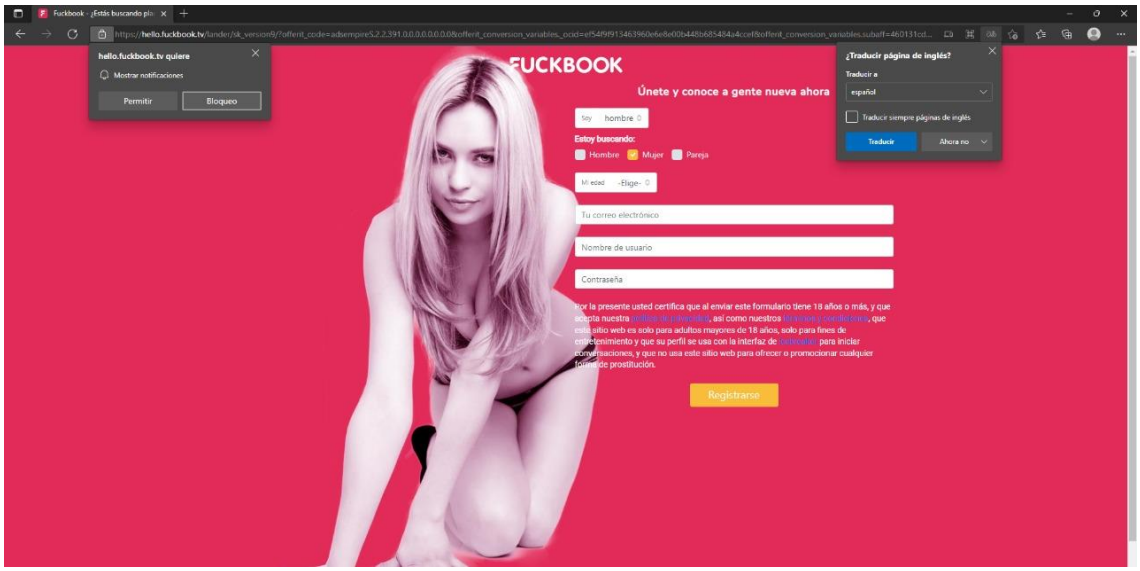


Ilustración 26: *Evidencia en navegador web redireccionamiento de DNS*
Fuente: Elaboración propia

Este tipo de ataques puede afectar la integridad de cualquier dispositivo que se conecte a la red por DHCP.

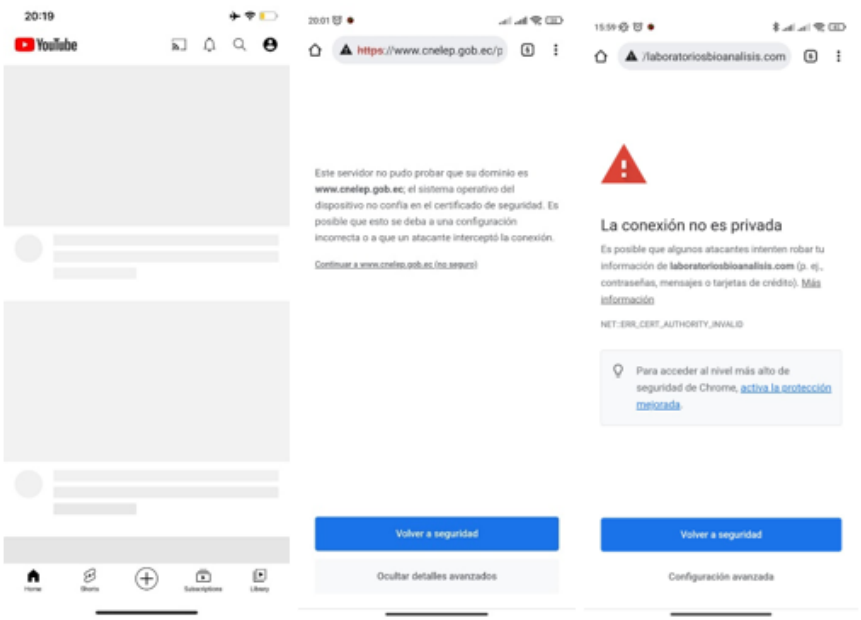


Ilustración 27: *Evidencia de afectación en dispositivos móviles*
Fuente: Elaboración propia

Prevención de acceso a equipos

Se informó al jefe del departamento técnico, que las claves de acceso a los equipos deben ser modificadas, en donde dio a conocer que en algunas ONT Huawei no existe un apartado para modificar la clave de administrador, por tal razón no las cambian, por ello se realizó una modificación al archivo de estos equipos, para ello se ingresó a una ONT Huawei y se sacó un archivo de respaldo.

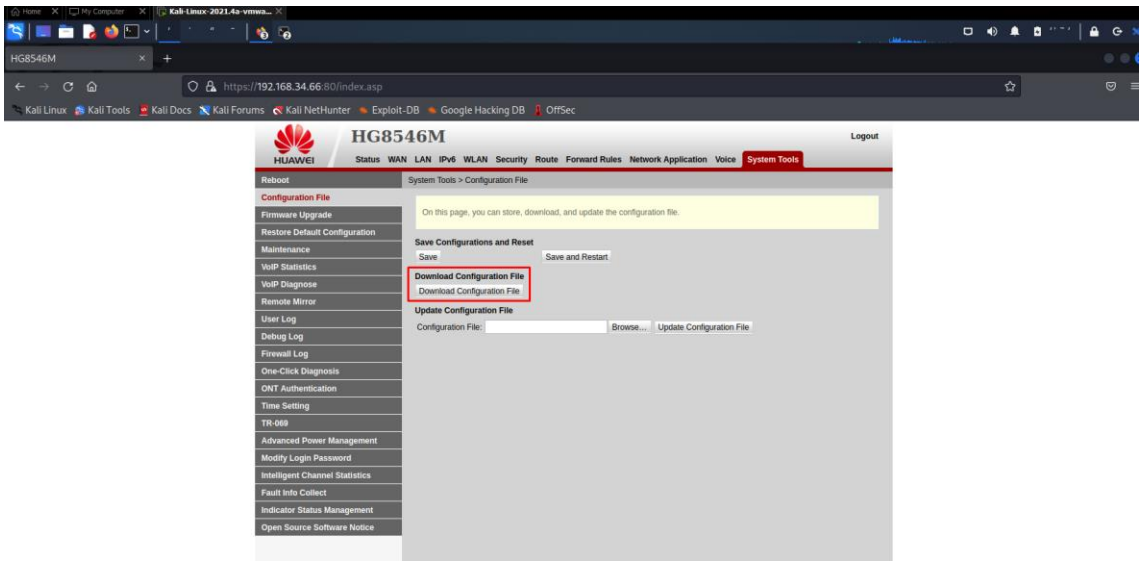


Ilustración 28: *Descarga de archivo de configuración ONT Huawei*
Fuente: Elaboración propia

El archivo de respaldo está escrito en Python, Kali Linux ya tiene incorporado Python, para ellos simplemente solo se abre el archivo en un IDE y se empieza a modificar, en este caso solo se requiere modificar la clave por defecto.

Según el fabricante estos equipos contienen una clave de acceso con doble encriptación primero por md5 y luego en sha-256.

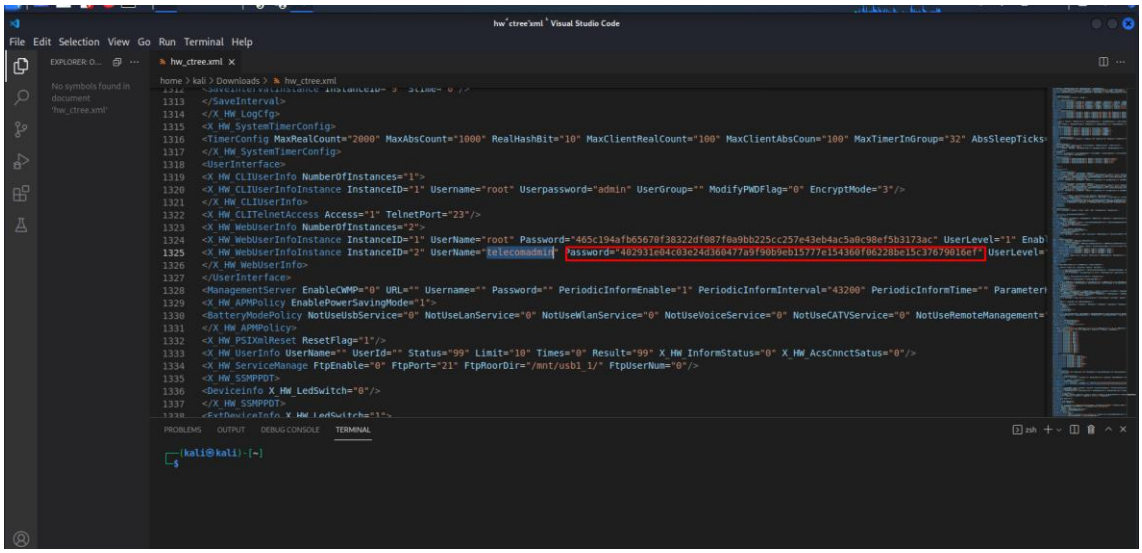


Ilustración 29: *Verificación del tipo de encriptación que utiliza el equipo*
Fuente: Elaboración propia

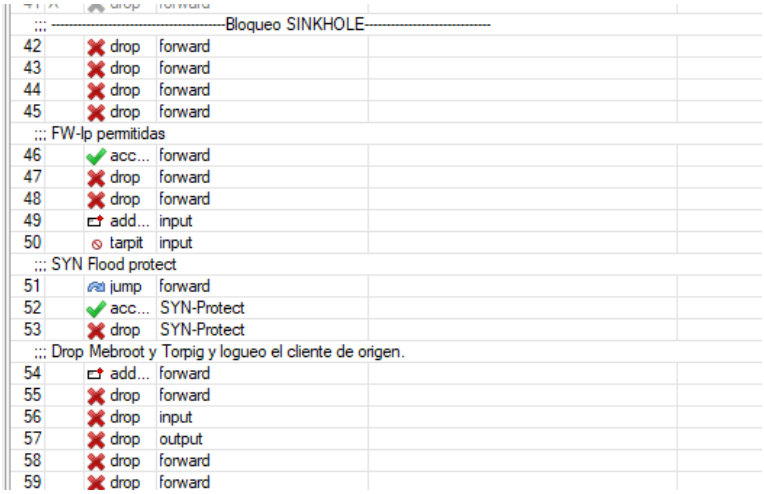
Se modificó el archivo con el mismo tipo de encriptación y se entregó al departamento correspondiente para que cargue en los equipos que se usan con los clientes.

Ilustración 30: *Remplazo de clave por defecto del equipo*
Fuente: Elaboración propia

Solución de red abierta

Para evitar que los clientes tengan acceso a otras IP se requiere aplicar seguridad en el equipo Mikrotik para esto se realizará mediante la herramienta Winbox, la cual se encarga de la gestión

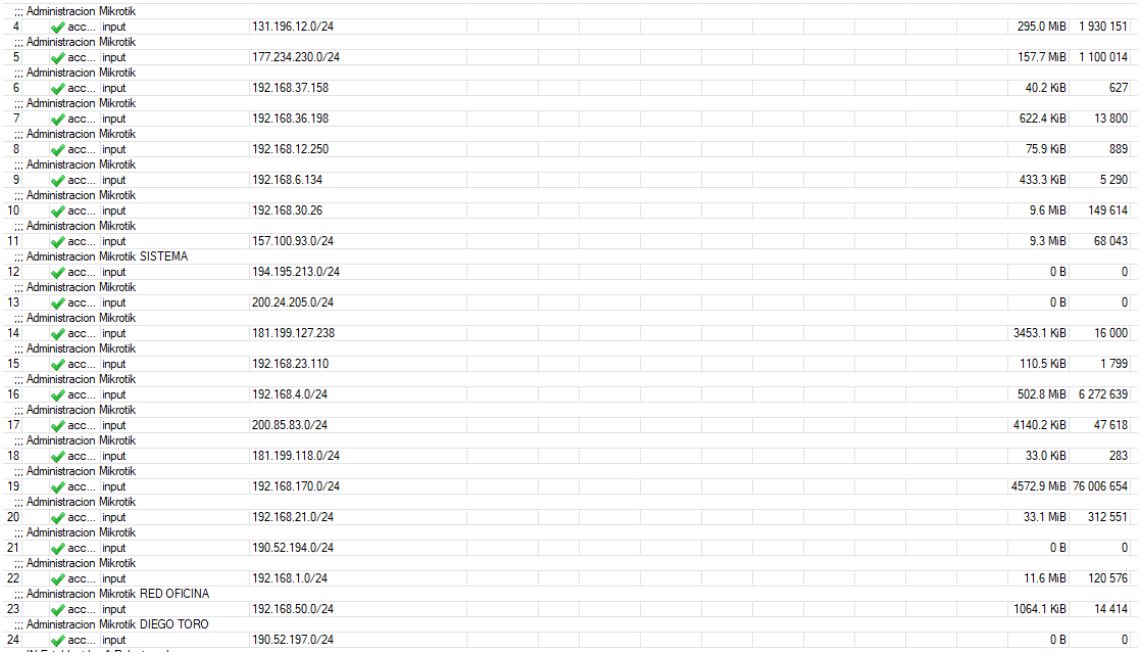
interna del equipo, para comenzar con la configuración fue requerida la ayuda del encargado de los equipos. Se aplicó una regla en el firewall para evitar el acceso no autorizado a los clientes.



	;;;	----------Bloqueo SINKHOLE----------	
42		drop	forward
43		drop	forward
44		drop	forward
45		drop	forward
	;;; FW-Ip permitidas		
46		acc...	forward
47		drop	forward
48		drop	forward
49		add...	input
50		tarpit	input
	;;; SYN Flood protect		
51		jump	forward
52		acc...	SYN-Protect
53		drop	SYN-Protect
	;;; Drop Mebroot y Torpig y logueo el cliente de origen.		
54		add...	forward
55		drop	forward
56		drop	input
57		drop	output
58		drop	forward
59		drop	forward

Ilustración 31: *Configuración de Firewall activos*
Fuente: Elaboración propia

Debido a que la empresa cuenta con personal Técnico que brinda soporte remoto se agregó las IPs de cada uno que conforma el área técnica para que accedan a los clientes y así no interferir en sus labores.



	;;; Administracion Mikrotik				
4	acc...	input	131.196.12.0/24	295.0 MiB	1 930 151
	;;; Administracion Mikrotik				
5	acc...	input	177.234.230.0/24	157.7 MiB	1 100 014
	;;; Administracion Mikrotik				
6	acc...	input	192.168.37.158	40.2 KiB	627
	;;; Administracion Mikrotik				
7	acc...	input	192.168.36.198	622.4 KiB	13 800
	;;; Administracion Mikrotik				
8	acc...	input	192.168.12.250	75.9 KiB	889
	;;; Administracion Mikrotik				
9	acc...	input	192.168.6.134	433.3 KiB	5 290
	;;; Administracion Mikrotik				
10	acc...	input	192.168.30.26	9.6 MiB	149 614
	;;; Administracion Mikrotik				
11	acc...	input	157.100.93.0/24	9.3 MiB	68 043
	;;; Administracion Mikrotik SISTEMA				
12	acc...	input	194.195.213.0/24	0 B	0
	;;; Administracion Mikrotik				
13	acc...	input	200.24.205.0/24	0 B	0
	;;; Administracion Mikrotik				
14	acc...	input	181.199.127.238	3453.1 KiB	16 000
	;;; Administracion Mikrotik				
15	acc...	input	192.168.23.110	110.5 KiB	1 799
	;;; Administracion Mikrotik				
16	acc...	input	192.168.4.0/24	502.8 MiB	6 272 639
	;;; Administracion Mikrotik				
17	acc...	input	200.85.83.0/24	4140.2 KiB	47 618
	;;; Administracion Mikrotik				
18	acc...	input	181.199.118.0/24	33.0 KiB	283
	;;; Administracion Mikrotik				
19	acc...	input	192.168.170.0/24	4572.9 MiB	76 006 654
	;;; Administracion Mikrotik				
20	acc...	input	192.168.21.0/24	33.1 MiB	312 551
	;;; Administracion Mikrotik				
21	acc...	input	190.52.194.0/24	0 B	0
	;;; Administracion Mikrotik				
22	acc...	input	192.168.1.0/24	11.6 MiB	120 576
	;;; Administracion Mikrotik RED OFICINA				
23	acc...	input	192.168.50.0/24	1064.1 KiB	14 414
	;;; Administracion Mikrotik DIEGO TORO				
24	acc...	input	190.52.197.0/24	0 B	0

Ilustración 32: *Control dentro del Firewall para personal Técnico*
Autor: Elaboración propia

Seguridad en nivel de Acceso Winbox

Actualmente existen diferentes tipos de archivos o programas que se encargan de aplicar fuerza bruta para crackear contraseñas, la institución en el acceso del programa Winbox hace uso de una IP, usuario y contraseña.

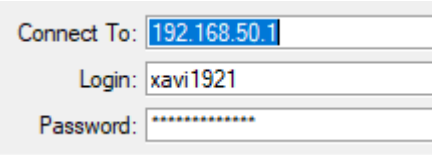


Ilustración 33: *Login de aplicación Winbox*
Autor: Elaboración propia

Para esto, es recomendable usar un puerto adicional el cual evite este tipo de accesos no autorizados, esto le da un mayor nivel de complejidad a tratar de acceder ya que debe encontrar un puerto, IP, usuario y contraseña que coincidan para concretar su acceso.

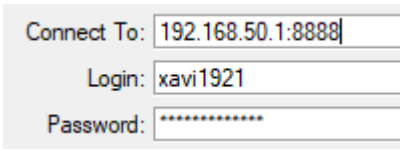


Ilustración 34: *Login de Winbox con protección mediante puerto*
Autor: Elaboración propia

2.4.3. Obtener credenciales de acceso mediante phishing o inyección SQL de un usuario privilegiado

Aplicación de phishing o inyección SQL en el sistema ODOO

Inyección SQL es un ataque que permite explotar vulnerabilidades en aplicaciones que construyen de manera dinámica algunas consultas mediante la entrada de usuarios en bases de datos relacionales [24].

Para poder hacer una revisión del sistema se solicitó un usuario con todos los privilegios, en donde se pudo apreciar que el sistema cuenta con sus validaciones pertinentes para evitar una inyección SQL, con la indagación y revisión de todos los módulos con los que cuenta ODOO se apreció una mala asignación de roles dentro de los empleados. Un ejemplo de esto sería: el personal del área contable tiene acceso al módulo de HTML.

La falta de corrección en la asignación de roles puede traer consecuencias una de estas es la modificación del HTML de la página de login para la captación de datos con los métodos POST y GET. ODOO no da la opción para modificar esa página, pero si se ingresa con la URL directamente esto es posible.

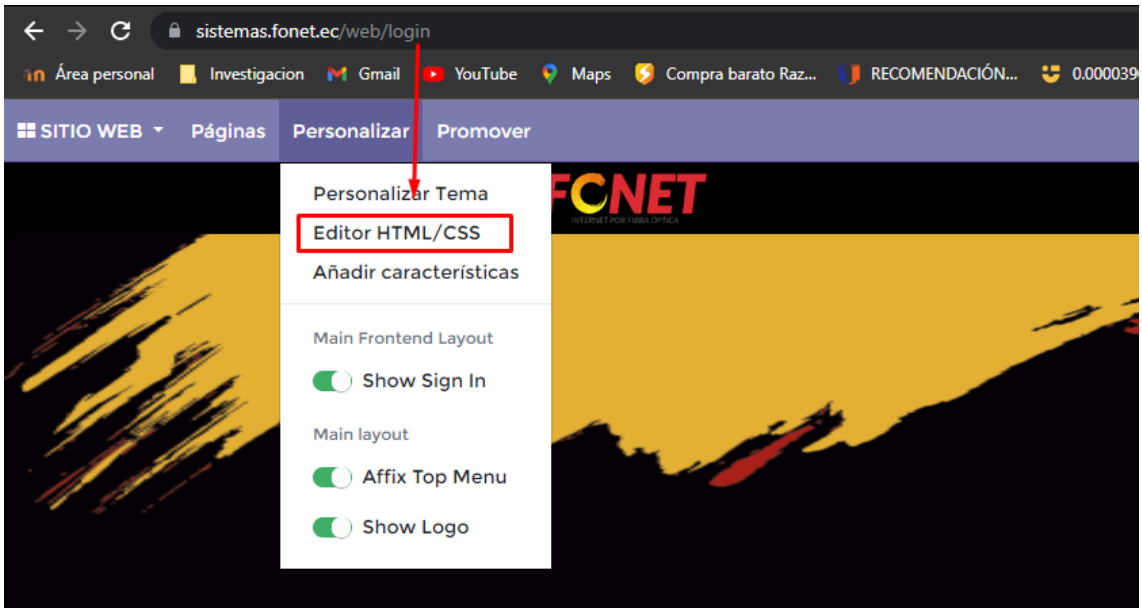


Ilustración 35: *Opción para editar código HTML ODOO*
Autor: Elaboración propia

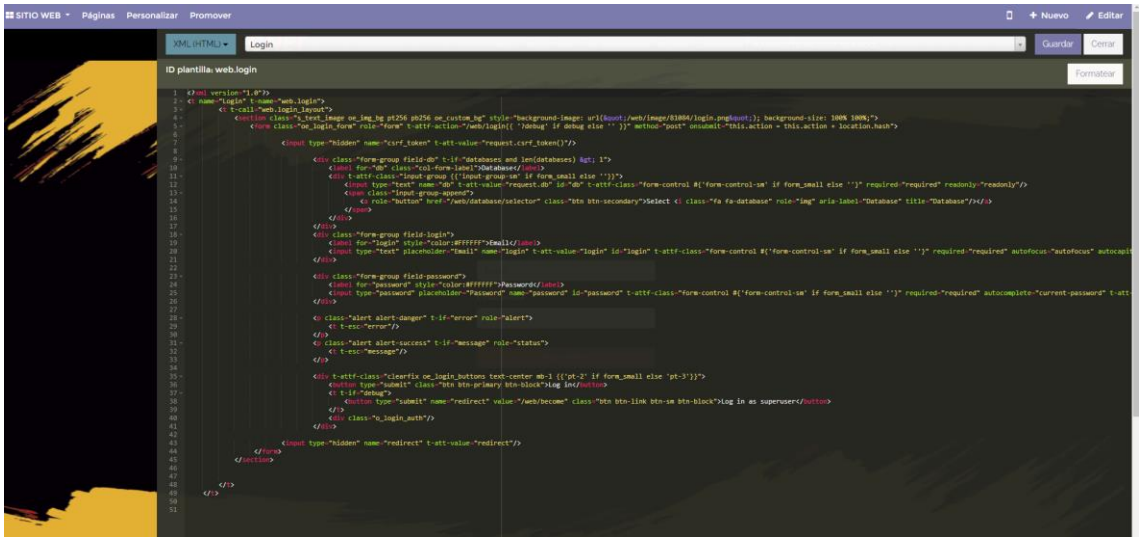


Ilustración 36: *Editor HTML dentro de ODOO*
Autor: Elaboración propia

Para la corroboración de lo anteriormente mencionado se utilizaron las herramientas que trae incorporadas el navegador de Kali Linux

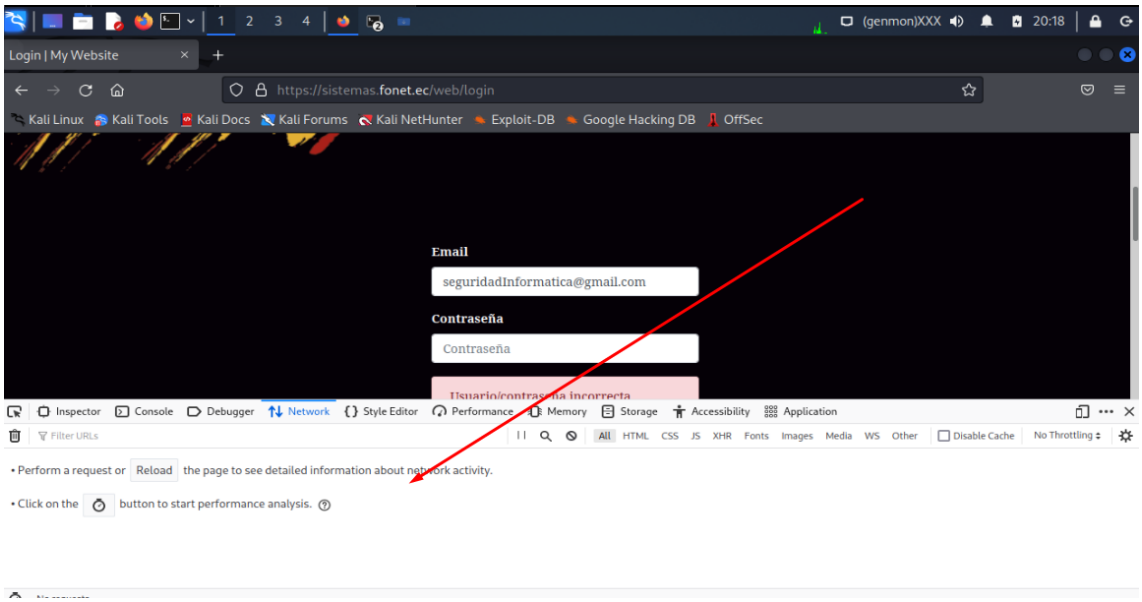


Ilustración 37: *Ventana para desarrollador Navegador Firefox*
Autor: Elaboración propia

Se ingresaron datos erróneos para verificar los métodos GET y POST que se mencionaron anteriormente

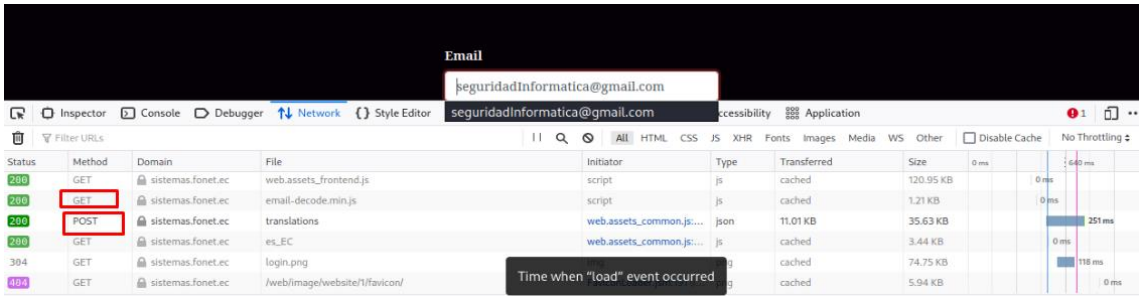


Ilustración 38: *Captura de métodos GET y POST*
Autor: Elaboración propia

Inspeccionado los datos enviados por los métodos se puede encontrar el correo y contraseña, así mismo se aprecian las variables para estos parámetros de autenticación.

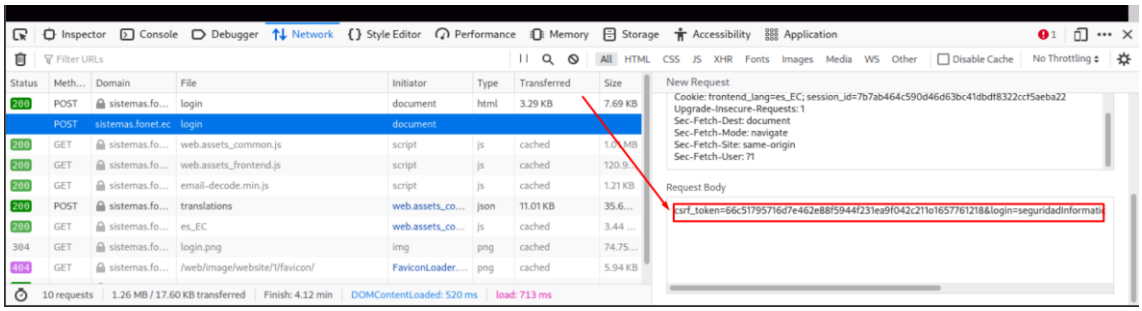


Ilustración 39: *Captura de datos mediante métodos GET y POST*
Autor: Elaboración propia

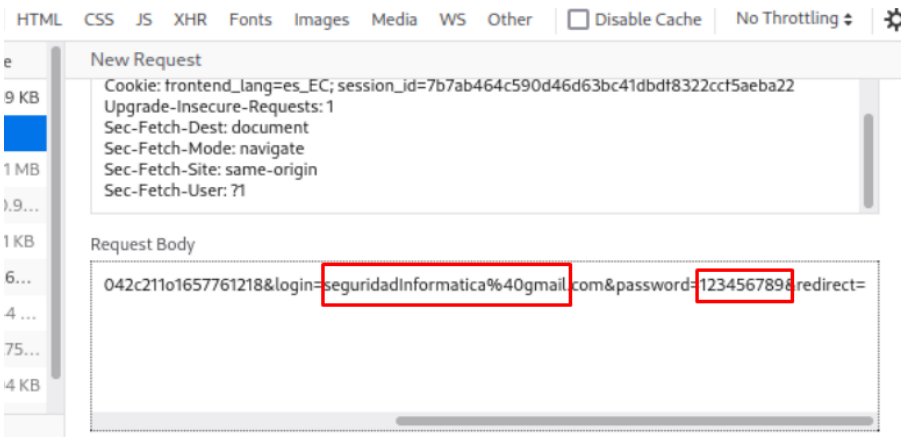


Ilustración 40: *Revelación de datos Login ODOO*
Autor: Elaboración propia

La página de Login es propensa a un ataque de fuerza bruta para evitar cualquier intento de ataque se reportó al personal encargado del sistema que utilicen un método en el cual cada cierta cantidad de intentos evite el acceso o muestre un captcha, de igual manera se recomendó una correcta asignación de roles para cada personal de la institución.

2.4.4. Aplicación de Ingeniería Social para acceder a información relevante dentro de la institución

La ingeniería social es el arte de obtener información a través de la manipulación de usuarios, en este caso se usó toda la información brindada para formar un diccionario de posibles contraseñas, el cual está conformado por nombres del Gerente General, nombre de la institución, fechas de acontecimientos importantes, fecha de inauguración de la institución, entre otros.

Se hizo un archivo. lst con 58 posibles contraseñas con la finalidad de aplicarlas en un ataque preparado con diccionarios. De igual manera esta práctica fue usada para tener información como secciones de IP, información de donde se encuentran alojados algunos archivos importantes como Base de datos, los diferentes Sistemas Operativos que la institución hace uso, entre otros.

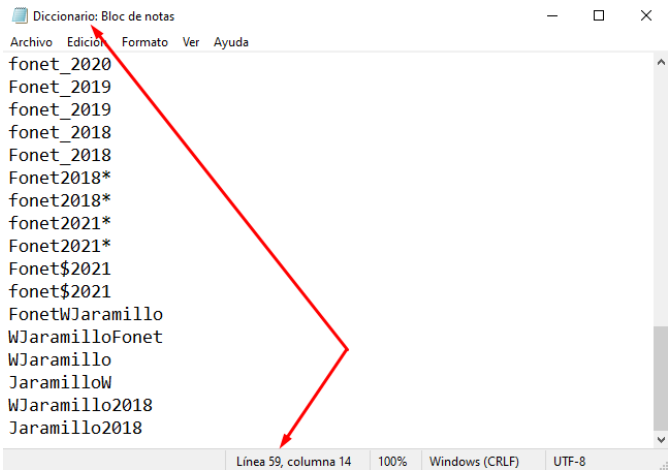


Ilustración 41: *Diccionario de contraseñas*

Autor: Elaboración propia

2.4.5. Crackear contraseñas mediante diccionarios para la obtención de accesos en los diferentes Software y Computadoras

Acceso no controlado RDP (Protocolo de Escritorio Remoto)

Para efectuar este tipo de ataque primero se debió hacer un análisis de cómo está distribuida la red interna, los segmentos de IP que están en uso y que pueden formar parte importante.

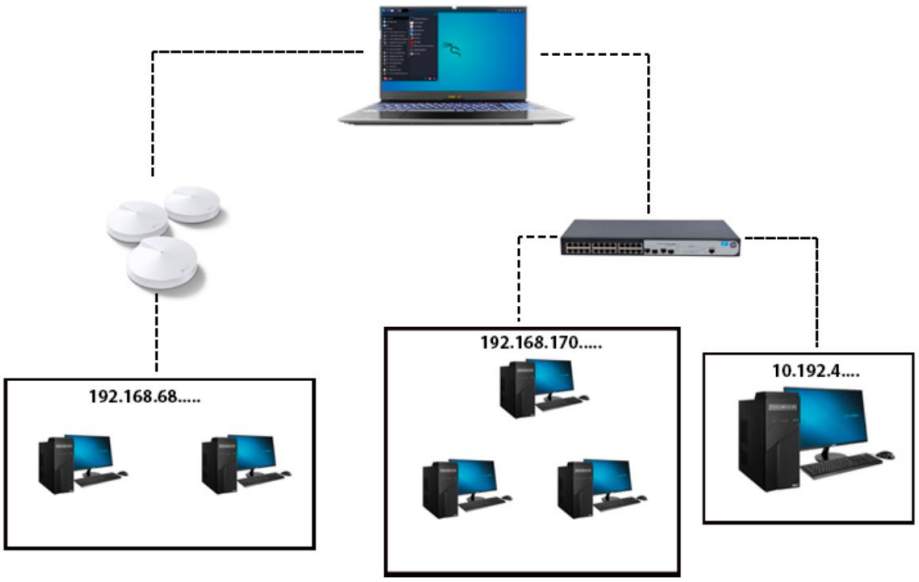


Ilustración 42: *Estructuración de Segmentación de IPs*
Fuente: Elaboración propia

Analizada la estructura de red se obtuvo 3 segmentos de red que podían ser analizadas de las cuales el único segmento con RDP activo fue el segmento del servidor, el cual este cableado a un switch administrable. El análisis de IPs con posibles accesos se realizó con la herramienta msfconsole la cual es un metasploit.

Metasploit es un programa que permite desarrollar e implementar exploits contra los sistemas de destino pueden ejecutar escaneo de redes o también pueden cumplir la función de controlar dispositivos remotamente, infectado el equipo de la víctima [25].

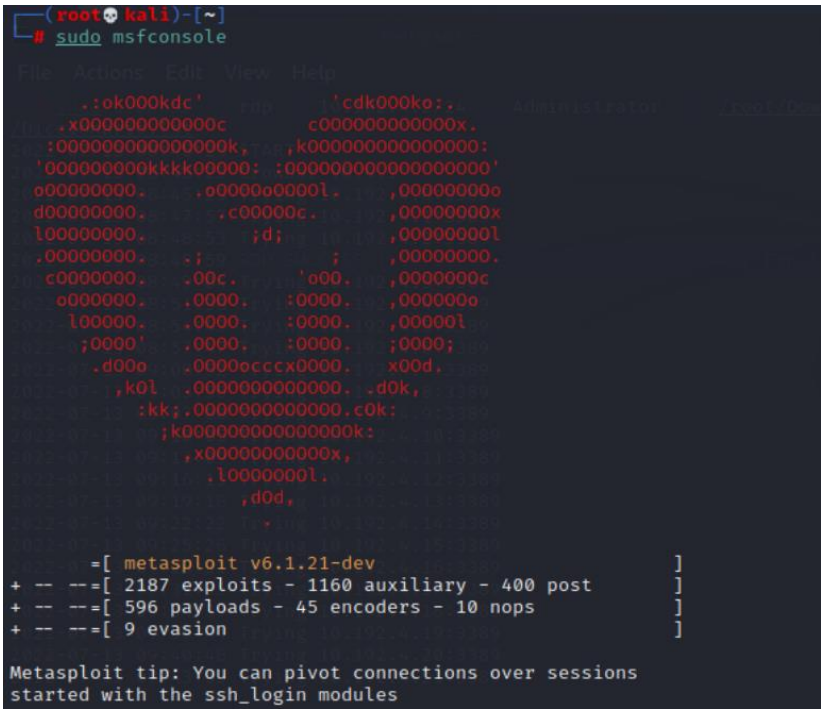


Ilustración 43: *Interfaz mfscosole Kali Linux*
Autor: Elaboración propia

Con el metasploit iniciado se accede a la ruta donde se encuentra rdp_scanner el cual trae las opciones necesarias para iniciar el escaneo.

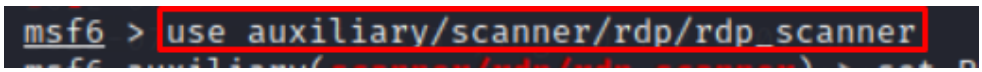


Ilustración 44: *Directorio para rdp_scanner*
Autor: Elaboración propia

Una vez que se accede a la ruta se ingresa el comando para setear el rango de IP, en este caso se asigna /24 para que haga un análisis completo de las 255 IPs en el segmento.

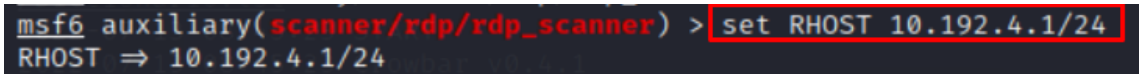


Ilustración 45:*Seteo de rango de IP para escaneo*
Autor: Elaboración propia

Ya aprendido el rango de IP se ingresa el comando exploit para efectuar el análisis y una vez encontrada la IP vulnerable.

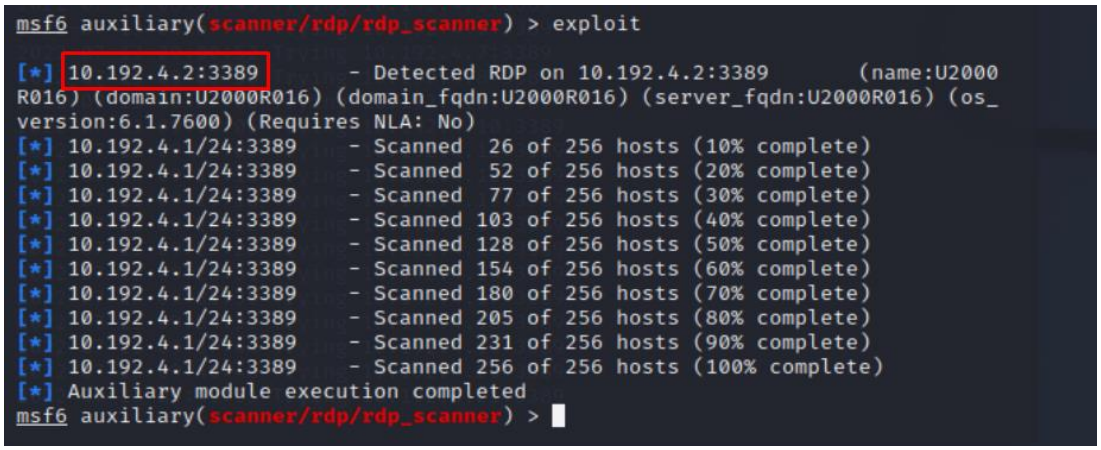


Ilustración 46: *Detección de IP vulnerable para ataques RDP*
Autor: Elaboración propia

Se inicia una consola con crowbar el cual se encarga de aplicar fuerza bruta para el acceso remoto.

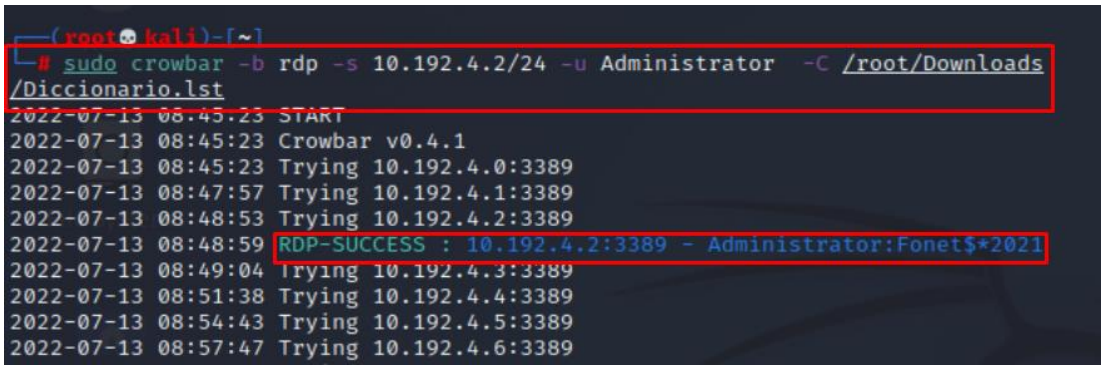


Ilustración 47: *Instrucción de ataque RDP mediante fuerza bruta*
Autor: Elaboración propia

Una vez hecho esto solo se ingresan las credenciales en una aplicación de escritorio remoto de Windows y se obtendrá el acceso no autorizado. Para su corrección y evitar esta clase de ataque debe insertar un número de intentos, para que la computadora rechace la conexión remota esto se puede aplicar en las mismas configuraciones de Windows como se muestra a continuación.

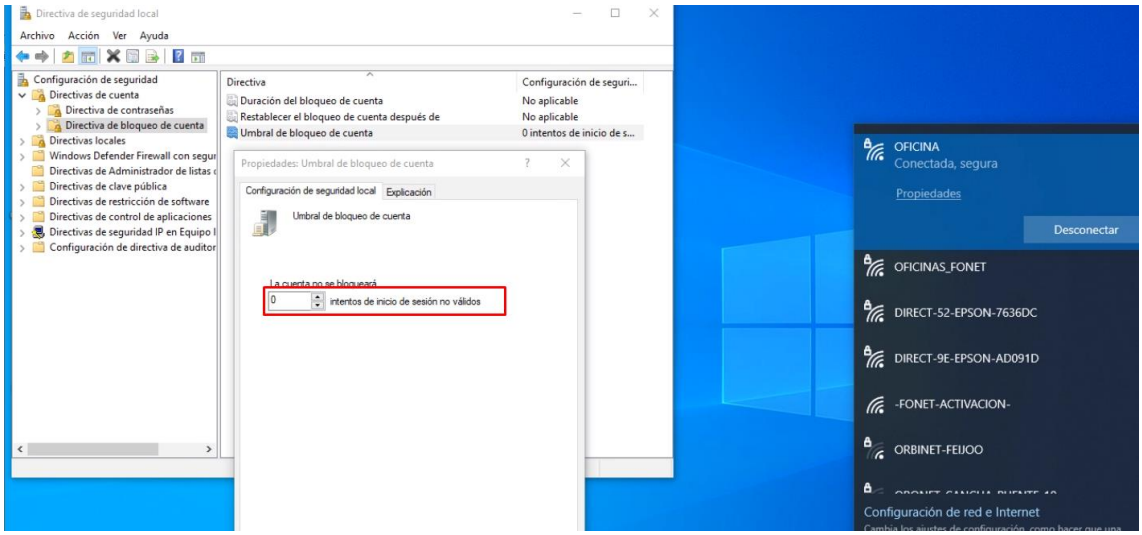


Ilustración 48: *Bloqueo de acceso mediante número de intentos por fuerza bruta*
Autor: Elaboración propia

Acceso no autorizado control de registros de hora

La institución lleva un control de entrada y salida de sus empleados con un biométrico el cual funciona mediante huella digital, este dispositivo es de la marca ZKTime, para su función debe estar conectado a una red para extraer la información el software que se usa es ZKTime.Net, este contiene una base de datos interna alojada en el mismo dispositivo.

Ilustración 49: *Logo ZKTIME*
Autor: Obtenido de [26]

El dispositivo al tener la necesidad de conectarse a una red para poder hacer uso del software que trae, se entiende que debe tener una IP, submascara de red, puerta de enlace y quizás algún puerto para establecer conexión. Para poder corroborar se empezó a manipular el dispositivo el cual no contaba con alguna clave para evitar revisar sus configuraciones, se encontró una parte de configuración de red en donde se obtuvo toda la información anteriormente mencionada.

Ilustración 50: *Configuración de reloj biométrico*
Autor: Elaboración propia

Obtenida la información del biométrico, se procedió a descargar el software desde la página oficial del fabricante, una vez instalado se procedió abrir y este solicitaba un usuario y contraseña. Se aplicó los siguientes datos de manera manual.

Usuario: admin

Contraseña: admin

Con estos datos el acceso resultó exitoso.

Ilustración 51: *Login de sistema de control para biométrico*
Autor: Elaboración propia

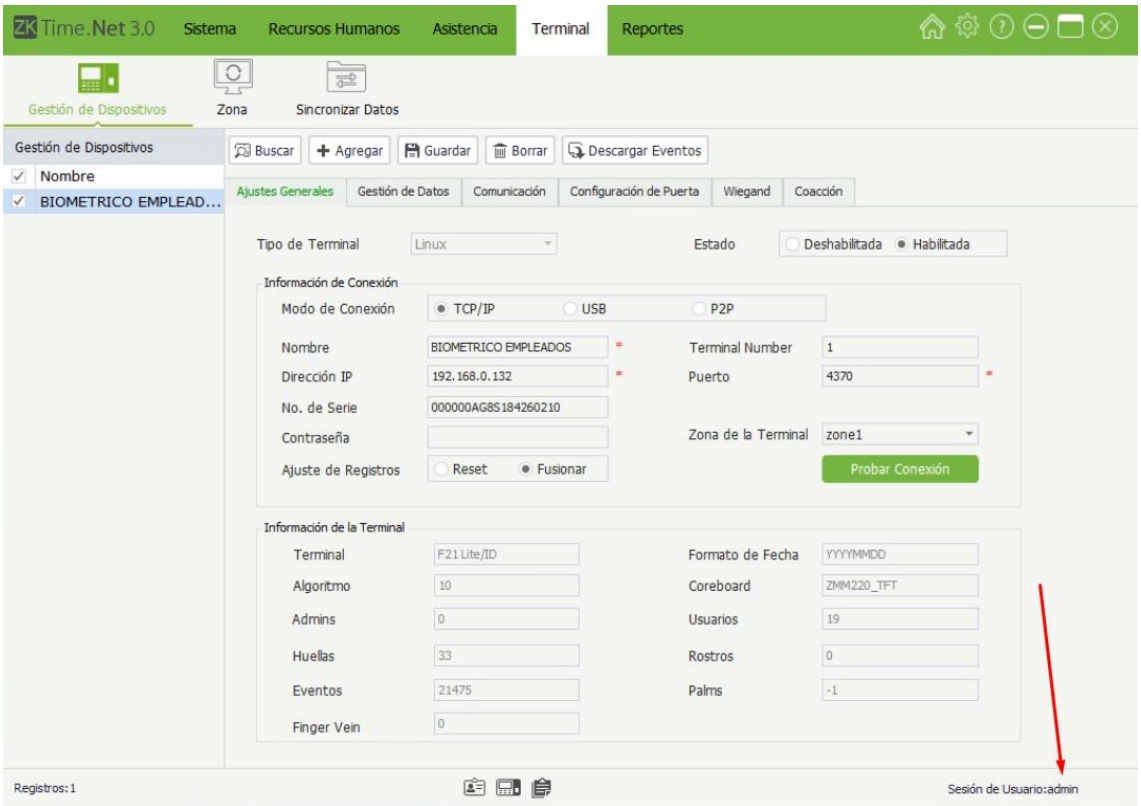


Ilustración 52: *Conexión del sistema con reloj biométrico*
Autor: Elaboración propia

Una vez con el acceso se ingresaron los campos que anteriormente se obtuvieron en sus campos correspondientes y se estableció la conexión con el biométrico, ya se podía modificar el horario de cada empleado, extraer la base de datos alojada en el dispositivo y así mismo se podía alterar su información en cada empleado registrado entre otras funciones que brinda el software.

Para su debida corrección se debe aplicar un puerto que no sea el que trae por defecto y así mismo se debe aplicar una contraseña y usuario diferente con mayor dificultad para descifrar

2.4.6. Aplicación de auditoría de la seguridad en sistema ODOO, arquitectura de red interna.

Auditoría de Sistema ODOO

Para efectuar una auditoría completa del sistema ODOO se modificó un archivo elaborado en Python el cual se encarga de brindar información relevante del sistema como su versión, el tipo de ODOO, nombre de base de datos e información de todos los módulos que tiene instalados. Para la ejecución solo se ingresa la URL a escanear.

Ilustración 53: *Ejecución de script para auditoria del sistema ODOO*
Autor: Elaboración propia

Como se aprecia en la ilustración se da a conocer información que puede ser usada en posibles ataques, el programa brinda las siguientes opciones al ser ejecutado con la URL a escanear.

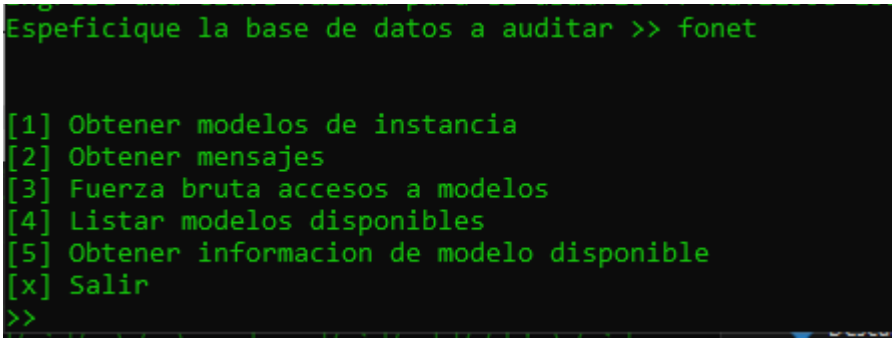


Ilustración 54: *Menú de script para auditoria de ODOO*
Autor: Elaboración propia

De ejemplo se usó la opción 3 donde aplica fuerza bruta para el acceso no autorizado.

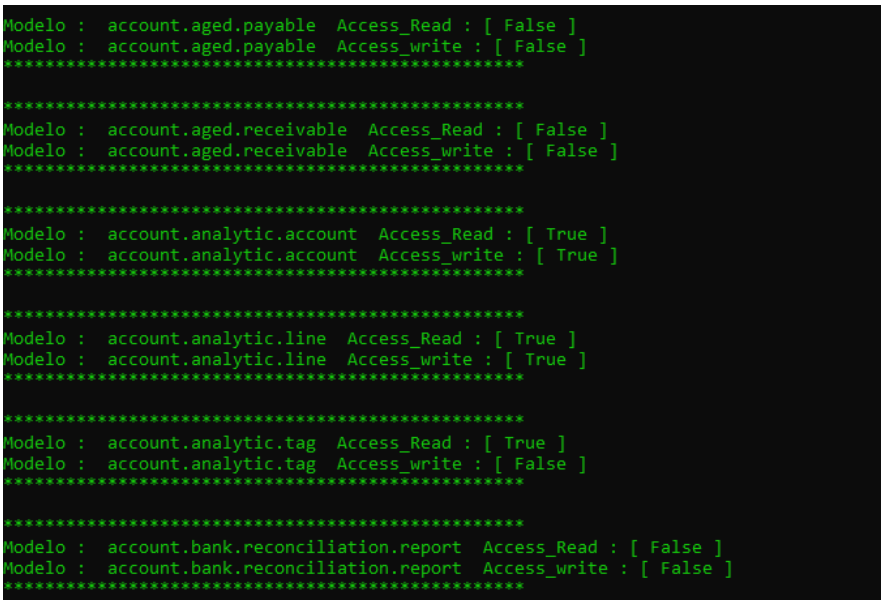


Ilustración 55: *Despliegue de módulos instalados en ODOO*
Autor: Elaboración propia

Base de datos ODOO

En el tiempo que se estuvo efectuando las prácticas en el módulo de sitio web, se cometió un error en la modificación del HTML en la página web, el cual llevó a que se caiga dicho módulo y así mismo arrastro el error con los demás módulos instalados en el sistema.

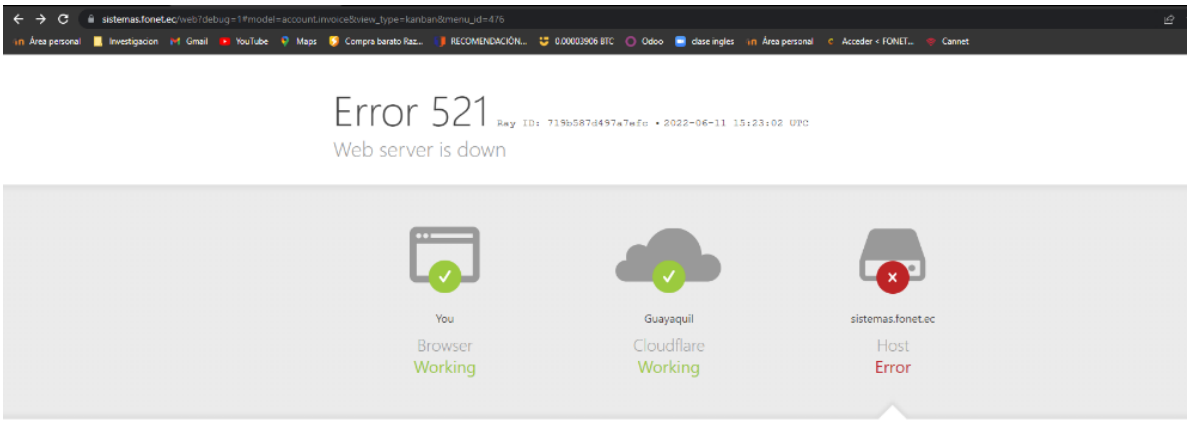


Ilustración 56: *Caída del sistema ODOO*
Autor: Elaboración propia

Debido a que el sistema no es propio de la institución se puso en contacto con el soporte del sistema, los cuales ayudaron a solventar el problema en un lapso de 3 días, perdiendo la información del día en que sucedió dicho error.

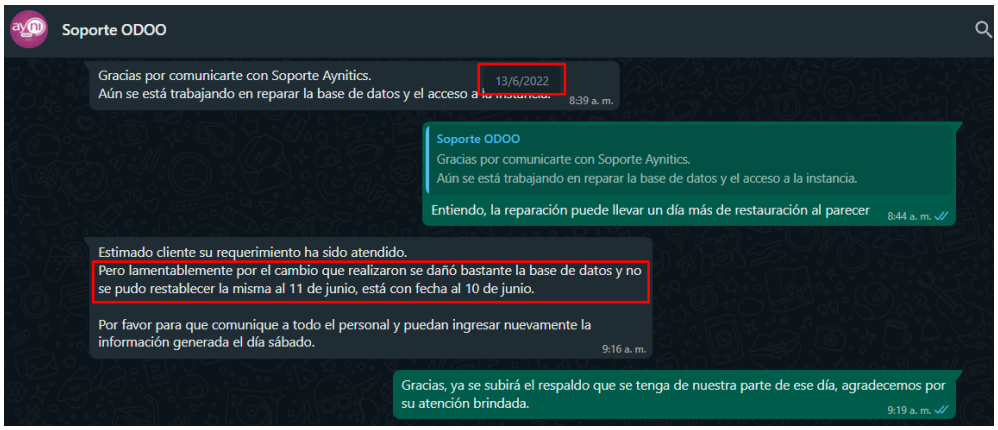


Ilustración 57: *Reporte de caída de sistema ODOO con personal de soporte*
Autor: Elaboración propia

Al no poder recuperar esa información se pudo apreciar que dicho sistema no cuenta con una base de datos centralizada o distribuida, lo cual hubiera ayudado a no perder la información o quizás a no perder gran parte de la información del 11 de junio.

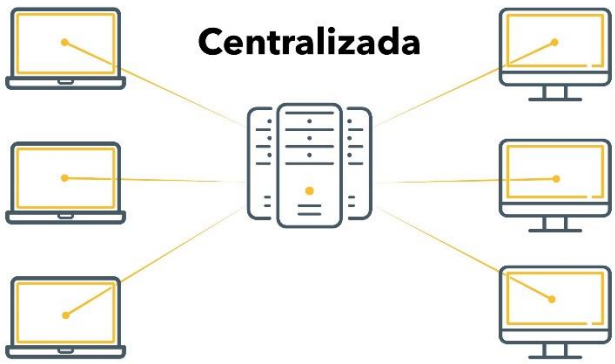


Ilustración 58: *Diseño de una base de datos centralizada*
Autor: Obtenido de [27]

Análisis del tráfico de red interno

La herramienta Wireshar viene previamente instalada dentro del sistema operativo Kali Linux, la herramienta permite hacer un sniffer de red, es decir permite hacer una captación de paquetes que viajan a través del wifi, en estos paquetes se pueden encontrar contraseñas, correos entre otro tipo de información, cabe mencionar que esto es un análisis para determinar si la institución accede a páginas no seguras y ver qué tipo de información están arriesgando a perder.

Ilustración 59: *Logo herramienta Wireshark*
Autor: Obtenido de [28]

Una vez ejecutada la aplicación se observa inmediatamente como empieza a moverse el tráfico de red. En este caso se está conectado a una red wifi de un dispositivo de la marca TP-LINK es un nodo Mesh M5, en la actualidad los dispositivos de alta gama como estos traen consigo configuraciones de seguridad, tales como evitar que un ping de respuesta a la dirección IP que está haciendo uso el equipo, también cuentan con encriptación de información par a evitar este tipo de hackeos inalámbricos.

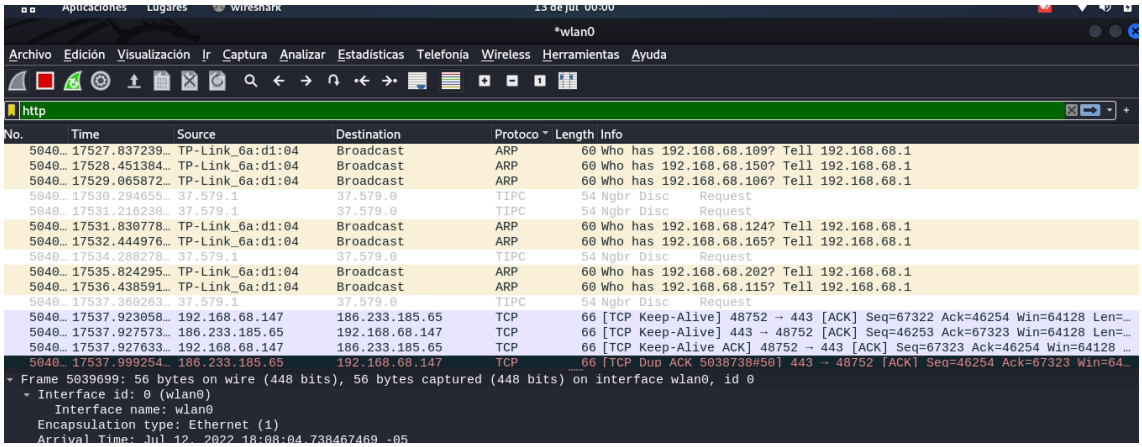


Ilustración 60: *Ejecución de aplicación Wireshark*
Autor: Elaboración propia

Luego de 45 hrs de captación de información no dieron resultados positivos, a menos de un solo paquete que logró ser capturado.

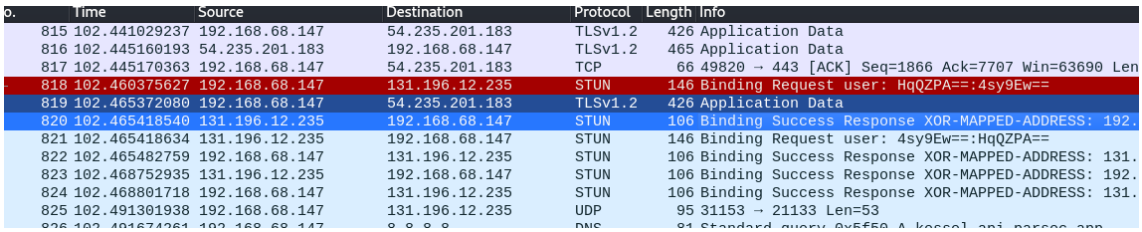


Ilustración 61: *Captura de paquete de datos mediante Wireshark*
Autor: Elaboración propia

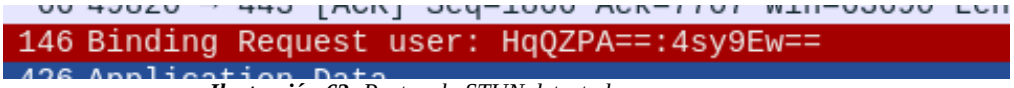


Ilustración 62: *Protocolo STUN detectado como poro seguro*
Autor: Elaboración propia

En este caso se puede apreciar que existe una línea roja más encendida que las demás es una muestra de que existe información importante o de que es un protocolo inseguro, al revisar se observó que mediante el método POST y GET se capturó una contraseña, pero la captación se había efectuado con encriptación de esta, evitando así dar información al atacante.

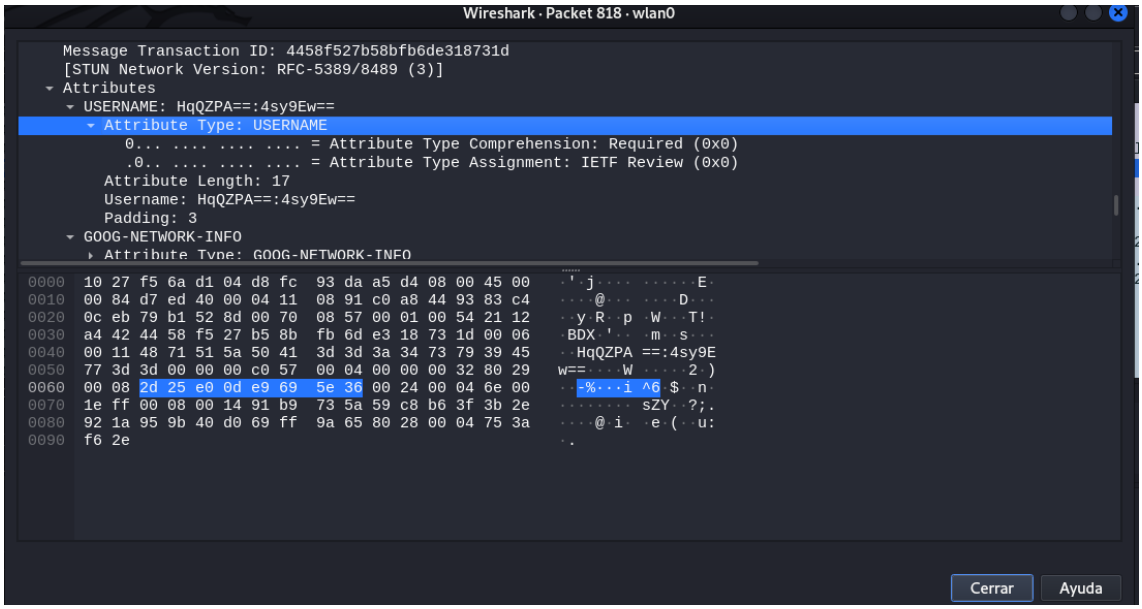


Ilustración 63: *Despliegue de datos capturados protocolo STUN*
Autor: Elaboración propia

Al ingresar a la IP que proporciona el sniffer en la captura se pudo apreciar que era un acceso a un equipo de un cliente, el cual fue proporcionado por el área técnica, ya que estos accedían de manera remota. Todas las peticiones a páginas fueron seguras.

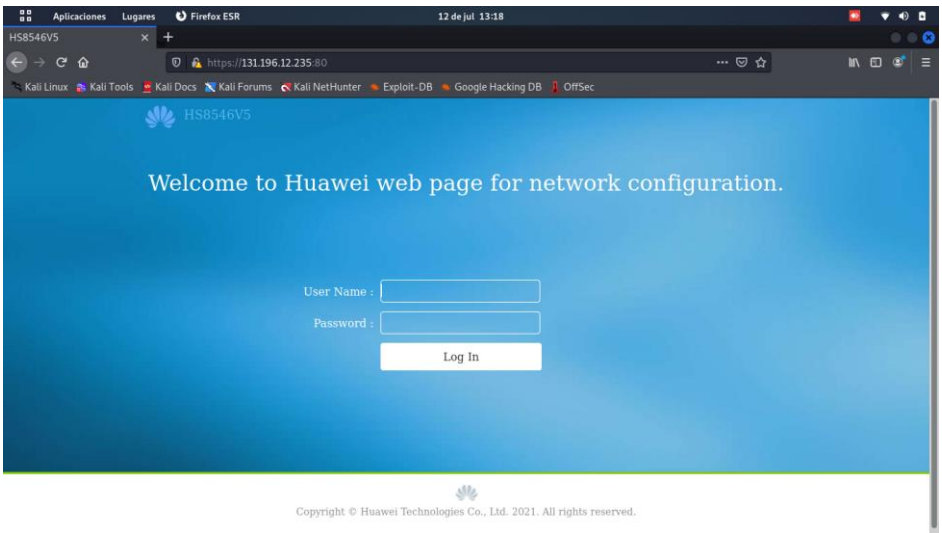


Ilustración 64: *Prueba de datos obtenidos mediante Wireshark*
Autor: Elaboración propia

3. CAPÍTULO III. EVALUACIÓN DEL PROTOTIPO

3.1. Plan de evaluación del prototipo

El plan para evaluar los resultados obtenidos sobre el hackeo ético fue realizado mediante el manual que otorga la metodología OSSTMM la cual consiste en métricas de la seguridad operacional.

La idea principal de la evaluación es evaluar los parámetros después de la ejecución de los procesos de seguridad para así corroborar la efectividad del cumplimiento previsto de reducir las infracciones de seguridad [29].

La evaluación de seguridad y la evaluación de riesgo son dos aspectos separados, la evaluación de seguridad tiene como finalidad reconocer el nivel de seguridad, mientras que la evaluación de riesgo indica cuales son las amenazas y sus eventos asociados, la evaluación de la presente metodología está compuesta para hacer un análisis completo de seguridad y de riesgo [30].

3.1.1. Objetivo del plan de evaluación

Evaluar el hackeó ético para la verificación de su soporte en la detección de vulnerabilidades, amenazas y riesgos dentro de la institución utilizando la metodología OSSTMM.

3.1.2. Cronograma de evaluación

Tabla 14:*Cronograma de Evaluación*

Actividad	Semana 10			Semana 11				
	27 jul	28 jul	29 jul	1 ago	2 ago	3 ago	4 ago	5 ago
Determinar escala de likert								
Cálculo de RAVs								
Elaboración de reporte técnico								

Autor: Elaboración propia

3.1.3. Métricas de evaluación

Para proporcionar un resumen referente a los canales auditados se aplica el RAV, el cual es un balance de porosidad, controles y limitaciones. El cálculo de los valores puede ser calculado de dos maneras, de forma manual o haciendo uso de la herramienta de Excel.

El documento de cálculos se puede obtener mediante la página oficial de la metodología. Para poder obtener el valor numérico de la seguridad actual de cada canal, que es la medida que permite

realizar la evaluación del porcentaje de eficiencia de los controles operacionales que han sido implementados

Porosidad (OPSEC): es la suma de visibilidad (P_V), acceso (P_A) y confianza (P_R).

$$OpSec_{sum} = P_V + P_A + P_R$$

El valor base de la seguridad operacional se determina con la siguiente ecuación.

$$OpSec_{base} = \log 2\,(1 + 100 x OpSec_{sum})$$

Controles: se divide en dos clases

- Clase A: autenticación (LC_{Au}), indemnización (LC_{Id}), resistencia (LR_{Re}), subyugación (LC_{Su}), continuidad (LC_{Ct}).
- Clase B: no-repudio (LC_{NR}), confidencialidad (LC_{Cf}), privacidad (LC_{Pr}), integridad (LC_{It}), alarma (LC_{Al}).

La suma de los controles es la siguiente.

$$LC_{sum} = LC_{Au} + LC_{Id} + LC_{Re} + LC_{Su} + LC_{Ct} + LC_{NR} + LC_{Cf} + LC_{Pr} + LC_{It} + LC_{Al}$$

Obtenido el valor de los controles se requiere determinar la cantidad de Controles faltantes para autenticación MC_{Au}, Autenticación de Control, MC_{sum} para poder evaluar las limitaciones de seguridad.

La ecuación para determinar los controles faltantes para autenticación MC_{Au} es la siguiente:

$$IF\ \ OpSec_{sum} -\ LC_{Au} \leq 0$$

$$\text{THEN } MC_{Au} = 0$$

$$\text{ELSE } MC_{Au} = OpSec_{sum} - LC_{Au}$$

Los totales de controles faltantes de cada uno de los 10 controles debe ser sumado para obtener el valor total del control faltante MC_{sum}.

$$MC_{sum} = MC_{Au} + MC_{Id} + MC_{Re} + MC_{Su} + MC_{Ct} + MC_{NR} + MC_{Cf} + MC_{Pr} + MC_{It} + MC_{Al}$$

Controles verdaderos

Este apartado es todo lo contrario a Controles faltantes, los que significa que debe calcularse cada control individual antes de que los resultados sean calculados en TC_{sum}.

La ecuación para calcular los controles verdades para autenticación TC_{Au} es la siguiente:

$$TC_{Au} = OpSec_{sum} - MC_{Au}$$

Se debe aplicar una suma de los 10 controles para obtener el valor total de TC_{sum}.

$$TC_{sum} = TC_{Au} + TC_{Id} + TC_{Re} + TC_{Su} + TC_{Ct} + TC_{NR} + TC_{Cf} + TC_{Pr} + TC_{It} + TC_{Al}$$

Controles verdaderos es usado para medir la ubicación adecuada de los controles, el valor base ayuda a eliminar la influencia de una colocación desproporcionada de controles sobre la seguridad. La base de los controles verdaderos TC_{base} se da de la siguiente manera.

$$TC_{base} = \log 2\,(1 + 100x(OpSec_{sum} - MC_{sum}x0.1))$$

Basado en la misma idea que controles verdades, verdadera cobertura TC_{vg} se puede utilizar para medir el porcentaje de controles establecidos respecto a la cantidad óptima y su ubicación de los controles.

$$IF\ OpSec_{sum} < 0$$

$$THEN\ TC_{vg} = 0$$

$$ELSE\ TC_{vg} = 1 - \frac{MC_{sum}}{10xOpSec_{sum}}$$

Controles completos

Los controles completos, tienen en cuenta los controles en su lugar. Este valor es fundamental para poder medir el valor de la autenticación en dos factores y otras instancias como visibilidad, acceso o confianza. La base de controles completos FC_{base} se evalúa como:

$$FC_{base} = \log 2\,(1 + 10xLC_{sum})$$

Limitaciones: vulnerabilidad (L_V), debilidad (L_W), preocupación (L_C), exposición (L_E) y anomalía (L_A).

Las limitaciones se ponderan de manera individual. La ponderación de las vulnerabilidades, debilidades y las preocupaciones están basadas en una relación entre la porosidad u $OpSec_{sum}$, los controles de perdida y en el caso de existir anomalías, la existencia de limitaciones también es un papel importante.

La exposición de una anomalía no plantea problemas a menos que presente vulnerabilidades, debilidades o preocupación. La tabla presentada a continuación se utiliza para calcular la variable

$SecLim_{sum}$ como un paso intermedio entre las entradas de limitación de seguridad y la variable $SecLim_{base}$ que es la entrada básica.

$$IF\ OpSec_{sum} \leq 0$$

$$THEN\ MC_{vg} = 0$$

$$ELSE\ MC_{vg} = \frac{MC_{sum}\ X\ 0.1}{OpSec_{sum}}$$

***Tabla 15**: Tabla para calcular le variable SecLimsum [31]*

Entrada	Valor ponderado	Variables
Vulnerabilidad L_V	$\frac{(OpSec_{sum} + MC_{sum})}{OpSec_{sum}}$	MC_{sum}: Suma de controles faltantes.
Debilidad L_W	$\frac{(OpSec_{sum} + MC_A)}{OpSec_{sum}}$	MC_{sum}: Suma de los controles que faltan en la clase de control A.
Inquietud L_C	$\frac{(OpSec_{sum} + MC_B)}{OpSec_{sum}}$	MC_{sum}: Suma de los controles que faltan en la clase de control B.
Exposición L_E	$\frac{((P_V + P_A)x\ MC_{vg} + L_V + L_W + L_C)}{OpSec_{sum}}$	MC_{sum}: Suma de visibilidad MC_{sum}: Suma de Accesos MC_{sum}: Porcentaje de cobertura faltante.
Anomalía L_A	$\frac{(P_T\ x + MC_{vg} + L_V + L_W + L_C)}{OpSec_{sum}}$	MC_{sum}: Suma de visibilidad MC_{sum}: Porcentaje de cobertura faltante.

Autor: Elaboración propia

3.1.4. Herramientas de evaluación de prototipo

Para la obtención de resultados de todas las prácticas de hackeo ético aplicadas, se hará uso del método de evaluación que la misma metodología OSSTMM otorga. La cual ayuda a determinar el nivel de seguridad en cada canal auditado.

Tabla 16: *Tabla para calcular los RAVs con metodología OSSTMM V3*

OPSEC

Visibility	0
Access	0
Trust	0
Total (Porosity)	0

CONTROLS

Class A		Missing
Authentication	0	0
Indemnification	0	0
Resilience	0	0
Subjugation	0	0
Continuity	0	0
Total Class A	0	0

Class B		Missing
Non-Repudiation	0	0
Confidentiality	0	0
Privacy	0	0
Integrity	0	0
Alarm	0	0
Total Class B	0	0

		True Missing
All Controls Total	0	0
Whole Coverage	0,00%	0,00%

LIMITATIONS		Item Value	Total Value
Vulnerabilities	0	0,000000	0,000000
Weaknesses	0	0,000000	0,000000
Concerns	0	0,000000	0,000000
Exposures	0	0,000000	0,000000
Anomalies	0	0,000000	0,000000
Total # Limitations	0		0,0000

OPSEC	0,000000
True Controls	0,000000
Full Controls	0,000000
True Coverage A	0,00%
True Coverage B	0,00%
Total True Coverage	0,00%
Limitations	0,000000
Security Δ	0,00
True Protection	100,00

Actual Security: 100 ravs

Autor: Obtenido de [31]

Al final de tener los resultados obtenidos se debe entregar el reporte de los RAVs que se obtuvieron dando conocer cada canal auditado, el reporte ha sido obtenido de la misma metodología OSSTMM.

Ilustración 65: *Reporte de canales auditados*
Autor: Obtenido de [31]

3.2. Resultados de la evaluación

3.2.1. Escala de Likert

Para la medición del riesgo se emplea la escala de Likert, Bedoya [32] nos indica que para poder hacer uso de esta escala es necesario asignar valores numéricos en cinco diferentes rangos del total

de la medición. Para el presente trabajo se tomará el total con cien puntos, tomando así en consideración que cada escala va contener 20 puntos, los niveles para esta escala son los siguientes:

Tabla 17: *Escala de evaluación para la medición del Riesgo.*

Escala de Likert	
Puntos	Nivel de escala
1-20	Muy Bajo
21-40	Bajo
41-60	Medio
61-80	Alto
81-100	Muy Alto

Autor: Obtenido de [32]

3.2.2. Pruebas de Seguridad Inalámbrica

En este canal se efectúa la interacción del investigador dentro de un rango con los objetivos que se han seleccionado. Los objetivos son barreras físicas y lógicas, los cuales permiten la medición de dichos estándares de seguridad que se han implementado o descrito en los procedimientos efectuados de la compañía.

Las amenazas inalámbricas pueden suceder de múltiples maneras, desde clientes maliciosos que se conectan a un AP (Punto de Acceso) de una organización sin autorización, hasta poder obtener todos los paquetes que viajan a través del aire y así realizar un reconocimiento para sus ataques informáticos [33].

Para realizar la prueba se deben revisar políticas de la institución para el uso de red inalámbrica, en este caso la institución no cuenta con dichas políticas, pero mediante la observación se evidenció dos tipos de redes, una red es proporcionada por un router de la marca Witek el cual genera una red interna cableada y a su vez cuenta con una red inalámbrica la cual no cumple algún objetivo, la segunda red es proporcionada por un Nodo Mesh de la marca TP-LINK el cual tiene como objetivo brindar internet a los empleados de la institución.

Seguridad Operacional (OPSEC)

Visibilidad

En la visibilidad deben verificarse los componentes que conforman el sistema inalámbrico de la institución [34].

Mediante las pruebas se obtuvo la siguiente información Wi-Fi de la institución.

Tabla 18: *Elaboración de la Visibilidad en el canal Inalámbrico*

Técnica implementada	Observación, Entrevista
Visibilidad	1.- Frecuencia 2,4 GHz detectada 2.- Frecuencia 5 GHz detectada 3.- SSID publica 4.- Lector biométrico

Autor: Elaborado a partir de [34]

En la visibilidad se obtuvo la información detallada en la tabla 10 para esto se da un valor de PV=4.

Acceso (PA)

Algunas recomendaciones para la parte de acceso son las siguientes [34]:

- Evaluar los métodos de acceso a la administración de los equipos inalámbricos.
- Verificar los puntos de acceso inalámbricos y comprobar si estos están inactivos en horarios predeterminados durante el día.
- Configurar el/los dispositivos inalámbricos para que puedan captar la mejor potencia de emisión más recomendada, para la mejor operación dentro del límite.
- Comprobar que se hayan modificado los identificadores (SSID) que traen por defecto.
- Evaluar los controles de acceso, verificar la seguridad del área y su capacidad para interactuar o interrumpir con comunicaciones de redes inalámbricas.

Tabla 19:*Elaboración del Acceso en el canal Inalámbrico*

Técnica implementada	Observación, Entrevista
Acceso	1.- Acceso a equipos inalámbricos: Los equipos Wireless no están ubicados en lugares restringidos son accesibles a cualquier empleado. 2.- Los equipos informáticos cuentan con la configuración básica para el acceso a la red inalámbrica. 3.- La institución no cuenta con políticas de uso para equipos solo cableados, hacen uso de redes Wireless. 4.- El equipo se encuentra configurado para que de manera automática escoja el mejor canal de frecuencia. 5.- Los equipos Wireless como modem no tienen configuraciones por defecto. 6.- Los accesos a las diferentes instalaciones no están controladas por ningún medio.

Autor: Elaborado a partir de [34]

Para el acceso a Wireless se dieron algunas recomendaciones a evaluar, dependiendo de ello se asigna el valor numérico para el acceso de **PA=6.**

Confianza (PT)

La confianza hace referencia al acceso a la información tanto física como digital que se tiene sin la necesidad de usar identificaciones o autenticaciones [34].

Tabla 20: *Elaboración de la confianza en el canal inalámbrico*

Técnica implementada	Observación, Entrevista
Confianza	1.- Autenticación Wireless mediante contraseña, no cuenta con usuario y contraseña individual para cada empleado. 2.- Ingreso al Wireless por invitados o autoridades eventuales. • Red abierta sin autenticación 3.- Encriptación de información enviada por paquetes de manera inalámbrica.

Autor: Elaborado a partir de [34]

En confianza se ha obtenido un valor de **PT=3.**

Controles

Autenticación (LC_{Au})

Probar y enumerar los componentes que pueden ser necesarios para las autenticaciones y la autorización a las redes Wireless [34].

Tabla 21: *Elaboración de la autenticación en el canal inalámbrico*

Técnica implementada	Observación, Entrevista
Autenticación	1.- SSID 1 Oculta 2.- SSID 2 Oculta 3.- Confirmación de un administrado para acceder a la red. 4.- Cifrados en red inalámbrica (WPA2)

Autor: Elaborado a partir de [34]

Al contar con acceso a las configuraciones de los equipos Wireless, se obtuvo para las autenticaciones el valor de **LC_{Au}=4**

Indemnización (LCId)

En indemnización se deben observar los activos que se encuentran protegidos contra el abuso en las políticas de los empleados [34].

Tabla 22: *Elaboración de la Indemnización en el canal Inalámbrico*

Técnica implementada	Observación, Entrevista
Indemnización	1.- Existen políticas internas para el buen uso de los recursos institucionales. 2.- Garantías de equipos en caso de averías.

Autor: Elaborado a partir de [34]

En el control de la indemnización se obtuvo un valor de **LCId=4.**

Resiliencia (LC_{Re})

En el control de Resiliencia se debe revisar los encargados de aquellos activos fijos, en caso de desconectar algún activo debido a alguna violación o por algún acuerdo con la política de seguridad interna de la institución [34].

Tabla 23: *Elaboración de la Resiliencia en el canal Inalámbrico*

Técnica implementada	Observación, Entrevista
Resiliencia	1.- Los empleados que desconecten algún equipo, deben notificar con anticipación al encargado de activos fijos o al Gerente General de la institución. 2.- En caso de sospechas de algún equipo inactivo el personal encargado de los activos fijos debe notificar y revisar con las cámaras el acceso al área del suceso.

Autor: Elaborado a partir de [34]

Para la resiliencia se obtuvo un valor de **LC_{RE}=2**

Subyugación (LC_{Su})

El control de Subyugación requiere que se revisen las configuraciones de los equipos inalámbricos y se desactiven las configuraciones que traen por defecto [34].

Tabla 24: *Elaboración de la Subyugación en el canal Inalámbrico*

Técnica implementada	Observación, Entrevista
Subyugación	1.- Ningún equipo cuenta con sus configuraciones por defecto. 2.- Wps activo. 3.- Actualizaciones de Firmware.

Autor: Elaborado a partir de [34]

Para el control de Subyugación se obtuvo un valor de **LC_{Su}=3.**

Continuidad (LC_{Ct})

Para el control de continuidad se debe considerar los equipos que cuentan como backup y pueden funcionar en caso de tener alguna avería del equipo principal [34].

Tabla 25: *Elaboración de la Continuidad en el canal Inalámbrico*

Técnica implementada	Observación, Entrevista
Continuidad	1.- Equipos Wireless no están considerados como un activo de alto riesgo. 2.- En caso de daño del equipo inalámbrico la reparación es en menos de 2 das.

Autor: Elaborado a partir de [34]

Para la continuidad se ha obtenido el valor de **LC_{Ct}=1.**

No Repudio (LC_{Nr})

En el control de no repudio hay que verificar y comprobar los sistemas que generan historiales sobre los eventos de la red inalámbrica con la finalidad de evidenciar acciones efectuadas [34].

Tabla 26: *Elaboración del No Repudio en el canal Inalámbrico*

Técnica implementada	Observación, Entrevista
No Repudio	1.- Se registran los eventos en la aplicación del modem en donde se indica, fecha, hora, dispositivo y la dirección IP. 2.- Para evitar interferencias se registran los canales al momento de autoconfigurarse algún otro canal.

Autor: Elaborado a partir de [34]

El resultado obtenido para el no repudio es de **LC_{Nr}=2.**

Confidencialidad (LC_{Cf})

El control de confidencialidad enumera y examina los equipos que se usan para poder amortiguar las señales electromagnéticas que están fuera de la organización y la encriptación de las transmisiones inalámbricas [34].

Tabla 27: *Elaboración de la Confidencialidad en el canal Inalámbrico*

Técnica implementada	Observación, Entrevista
Confidencialidad	1.- Se efectúan las encriptaciones en las transmisiones de datos en la red inalámbrica.

Autor: Elaborado a partir de [34]

Se obtuvo un valor de **LC_{Cf}=1.**

Privacidad (LC_{Pr})

Se determinan los diferentes niveles de los controles para el acceso físico a los dispositivos que los controlan [34].

Tabla 28: *Elaboración de la Privacidad en el canal Inalámbrico*

Técnica implementada	Observación, Entrevista
Privacidad	1.- Cámaras de seguridad.

Autor: Elaborado a partir de [34]

Para el control de privacidad se obtuvo el siguiente valor **LC_{Pr}=1.**

Integridad (LC_{It})

Determina que la información solo puede ser revisada y modificada por el personal que cuenta con la respectiva autorización y garantiza que el cifrado de la información está aplicado para así garantizar la confidencialidad de las comunicaciones [34].

Tabla 29: *Elaboración de la Integridad en el canal Inalámbrico*

Técnica implementada	Observación, Entrevista
Integridad	1.- Uso de contraseñas. 2.- Cifrado para las redes inalámbricas

Autor: Elaborado a partir de [34]

En integridad se pudo obtener un valor de **LC_{It}=2.**

Alarma (LC_{Ai})

Para el control de alarma se requiere verificar los usos de métodos, registro o mensajes que advierten una situación sospechosa, como intentos de intrusión [34].

Tabla 30: *Elaboración de Alarma en el canal Inalámbrico*

Técnica implementada	Observación, Entrevista
Alarma	1.- Software de antivirus 2.- Sistema de alarma

Autor: Elaborado a partir de [34]

Para el control de alarma se ha obtenido un valor de **LC_{Ai}=2.**

Vulnerabilidad (LV)

La vulnerabilidad puede ser dada por las operaciones de acceso y confianza, cuando un equipo se satura en el canal de radiofrecuencia o cuando existen averías en los equipos impidiendo el correcto funcionamiento de la red inalámbrica [34].

Tabla 31: *Elaboración de Vulnerabilidad en el canal Inalámbrico*

Técnica implementada	Observación, Entrevista
Vulnerabilidades	1.- Se encuentra la vulnerabilidad de WPS. 2.- Contraseñas poco seguras

Autor: Elaborado a partir de [34]

Para la limitación de la vulnerabilidad se obtuvo el valor de **LV=2.**

Debilidad (L_W)

Para las debilidades se debe analizar los controles detallados en la clase A e identificar las diferentes debilidades que puede haber en esos controles [34].

Tabla 32: *Elaboración de la Debilidad en el canal Inalámbrico*

Técnica implementada	Observación, Entrevista
Debilidad	1.- No se puede controlar el acceso inalámbrico, ya que este solo requiere de una contraseña y puede ser compartido por código QR. 2.- Existen protocolos como el UDP el cual permiten obtener credenciales mediante un Sniffer de red,

Autor: Elaborado a partir de [34]

En debilidad se obtuvieron los siguientes valores **L_W=2.**

Preocupación (L_C)

Para obtener el valor de preocupaciones se deben revisar los controles de la clase B para así poder identificar inconvenientes que pueden darse dentro de los controles [34].

Tabla 33: *Elaboración de Preocupación en el canal Inalámbrico*

Técnica implementada	Observación, Entrevista
Preocupación	1.- No se cuentan con amortiguadores para evitar que la señal inalámbrica salga de la institución. 2.- Las claves de las redes inalámbricas presentan problemas debido a que puede haber divulgación de contraseñas.

Autor: Elaborado a partir de [34]

Para la limitación de preocupación se obtuvo el valor de **L_C=2.**

Anomalías (L_A)

Las anomalías son aquellos factores externos que pueden generar fallas en los equipos [34].

En este caso no se cuentan con anomalías por ello el valor es de **L_A=0.**

Resultados obtenidos del canal inalámbrico

Tabla 34: *Calculo de RAVS, pruebas de Seguridad Inalámbrica*

Attack Surface Security Metrics

OSSTMM version 3.0

Fill in the white number fields for OPSEC, Controls, and Limitations with the results of the security test. Refer to OSSTMM 3 (www.osstmm.org) for more information.

OPSEC				
Visibility	4			
Access	6			
Trust	3			
Total (Porosity)	13			
CONTROLS				
Class A		Missing		
Authentication	4	9		
Indemnification	2	11		
Resilience	2	11		
Subjugation	3	10		
Continuity	2	11		
Total Class A	13	52		
Class B		Missing		
Non-Repudiation	2	11		
Confidentiality	1	12		
Privacy	1	12		
Integrity	2	11		
Alarm	2	11		
Total Class B	8	57		
		True Missing		
All Controls Total	21	109		
Whole Coverage	16,15%	83,85%		
LIMITATIONS		Item Value	Total Value	
Vulnerabilities	2	9,384615	18,769231	
Weaknesses	2	5,000000	10,000000	
Concerns	2	5,384615	10,769231	
Exposures	0	1,106509	0,000000	
Anomalies	0	0,655030	0,000000	
Total # Limitations	6		39,5385	

OPSEC	9,698723
True Controls	5,402289
Full Controls	5,402289
True Coverage A	20,00%
True Coverage B	12,31%
Total True Coverage	16,15%
Limitations	12,939341
Security Δ	-17,24
True Protection	82,76

Actual Security: 82,7962 ravs

Fuente: Elaborado a partir de [28]

3.2.2.1. Seguridad de Telecomunicaciones

El canal de Seguridad de Telecomunicaciones resguarda la interacción entre el investigador y los objetivos analizados. El verdadero objetivo es evidenciar brechas de seguridad que se determinan

en el estándar de seguridad, políticas de la institución, industrias de regulaciones o legislaciones regionales [34].

Los siguientes objetivos de ataque son planteados por el investigador:

- Prueba de puertos abiertos
- Pruebas de acceso no vigilado por IP
- Pruebas de Firewall equipos ISP
- Pruebas de protocolos RDP
- Testeo de protocolos de seguridad en sitios web de la institución
- Prueba de red conmutada por paquetería

Visibilidad

La enumeración del objetivo al alcance mediante la interacción directa e indirecta entre los sistemas activos [34].

- Identificar los diferentes segmentos de red distribuida en la institución.
- Consultar nombres de servidores con protocolos activos o con zonas de transferencias de datos.
- Efectuar rastreo de red para localizar los controles por los cuales se envían respuestas o solicitudes.

Para poder identificar los segmentos de red se obtuvo los diferentes segmentos mediante la observación y pruebas manuales de conexión a diferentes redes, al igual aplicaron revisiones de segmentos en los diferentes dispositivos conectados a una red.

Tabla 35: *Elaboración de la Visibilidad en el canal de Seguridad de Telecomunicaciones*

Técnica implementada	Observación, Entrevista, Kali Linux
Visibilidad	1.- Base de Datos Principal 2.- Salida de Internet 3.- Equipos Activos 4.- Servidor para consultas externas

Autor: Elaborado a partir de [34]

En la visibilidad se obtuvo la información detallada en la tabla 28 para esto se da un valor de **PV=4.**

Acceso (PA)

Algunas recomendaciones para la parte de acceso son las siguientes [34]:

- Verificar servicios comunes que hacen uso de UDP para conexiones de diferentes conexiones.
- Solicitudes comunes de servicios VPN.
- Verificar los servicios de red y el enrutamiento para acceder a restricciones anteriores.
- Identificar el tiempo de actividad que se da en los sistemas operativos con ultimas las vulnerabilidades y las versiones de los parches.

Tabla 36: *Elaboración de Acceso en el canal de Seguridad de Telecomunicaciones*

Técnica implementada	Observación, Entrevista
Acceso	Puertos frecuentes = 30 Puertos para servicios = 2 Puertos VPN = 1

Autor: Elaborado a partir de [34]

Para el acceso a Wireless se dieron algunas recomendaciones a evaluar, dependiendo de ello se asigna el valor numérico para el acceso de **PA=33.**

Confianza (PT)

La confianza hace referencia al acceso a la información tanto física como digital que se tiene sin la necesidad de usar identificaciones o autenticaciones [34].

Se efectuaron pruebas de phishing mediante email, el personal de la institución al encontrar archivos de correos desconocidos informó a departamentos con mayores conocimientos en áreas de seguridad y no descargaron los archivos enviados y tampoco ingresaron a la URL.

Se hicieron pruebas para el acceso a equipos desde la red inalámbrica, en donde se pudo obtener acceso a redes privadas de clientes de la institución, mediante un firewall se evitó el tipo de acceso no autorizado.

En confianza se ha obtenido un valor de **PT=0,** con las correcciones pertinentes en la seguridad.

Controles

Autenticación (LC_{Au})

Probar y enumerar los componentes que pueden ser necesarios para las autenticaciones.

- Especificar los tipos de acceso que deben hacer uso de autenticación.
- Especificar como obtener una credencial segura para las autenticaciones.
- Especificar los procedimientos lógicos para la autenticación.
- Especificar la solidez que se debe tener en la autenticación

Tabla 37: *Elaboración de Autenticación en el canal de Seguridad de Telecomunicaciones*

Técnica implementada	Observación, Entrevista
Autenticación	1.- Políticas para las contraseñas 2.- Accesos a la red mediante MAC

Autor: Elaborado a partir de [34]

Al contar con acceso a las configuraciones de los equipos Wireless, se obtuvo para las autenticaciones el valor de $\mathbf{LC_{Au}=2}$

Indemnización (LCId)

- En indemnización se deben observar los activos que se encuentran protegidos contra el abuso en las políticas de los empleados.
- Examinar el contrato de la póliza de seguros para obtener las limitaciones en caso que existan daños que pueden cubrir la póliza.

En este caso la institución no cuenta con documentación de póliza, solo se tiene una cláusula en el contrato de empleados donde se da a conocer que la información de la institución no puede ser divulgada ni usada de manera personal.

En el control de la indemnización se obtuvo un valor de **LCId=0.**

Resiliencia (LC_{Re})

Examinar puntos de falla dentro de la infraestructura de red donde los cambios o las fallas pueden generar la indisponibilidad del o los servicios [34].

Tabla 38: *Elaboración de Resiliencia en el canal de Seguridad de Telecomunicaciones*

Técnica implementada	Observación, Entrevista
Resiliencia	1.- Obsolescencia de Hardware equipos ISP 2.- Incompatibilidad de aplicaciones 3.- Descontinuidad de actualizaciones en Hardware

Autor: Elaborado a partir de [34]

Para la resiliencia se obtuvo un valor de $\mathbf{LC_{RE}=3}$

Subyugación LC_{Su}

En las pruebas de redes si un Log-in puede estar en HTPP como también en HTTPS, pero se necesita que el usuario logre hacer una distinción, entonces se puede producir una subyugación, sin embargo, si la aplicación por defecto solicita el modo seguro, cumple con el control de subyugación para su alcance.

Tabla 39: *Elaboración de Subyugación en el canal de Seguridad de Telecomunicaciones*

Técnica implementada	Observación, Entrevista
Subyugación	1.- Quipux 2.- Cuenta Google 3.- Entidades Bancarias = 3

Autor: Elaborado a partir de [34]

Para el control de Subyugación se obtuvo un valor de **LC_{Su}=5.**

Continuidad (LC_{Ct})

- Para el control de continuidad se debe considerar los equipos que cuentan como backup y pueden funcionar en caso de tener alguna avería del equipo principal.
- Validar los diferentes sistemas con bloque que tiene la institución a intento de ingresos errores contra intrusos.

La institución no cuenta con equipos de Backup en caso de problemas por los altos costos que estos representan, a falta de disposición económica se dio la recomendación de obtener cada mes por lo mínimo un archivo de respaldo.

Tabla 40: *Elaboración de Continuidad en el canal de Seguridad de Telecomunicaciones*

Técnica implementada	Observación, Entrevista
Continuidad	1.- Desastres Naturales 2.- Archivos de Backup

Autor: Elaborado a partir de [34]

Para la continuidad se ha obtenido el valor de **LC_{Ct}=2.**

No Repudio (LC_{Nr})

En el control de no repudio hay que verificar y comprobar los sistemas que generan historiales sobre los eventos efectuados dentro de la institución [34].

- Enumerar los sistemas que son utilizados para identificar o registrar el acceso a la propiedad, que ayude como evidencia para el repudio.
- Verificar la profundidad de las interacciones que se han registrado y los procesos para identificación.
- Verificar que los procesos de interacción se encuentren registrados con identificaciones.

Tabla 41: *Elaboración de No Repudio en el canal de Seguridad de Telecomunicaciones*

Técnica implementada	Observación, Entrevista
No Repudio	1.- Identificación de logs 2.- Sistema de CCTV 3.- Rastreo de direcciones IP 4.- Control de Huellas digitales

Autor: Elaborado a partir de [34]

El resultado obtenido para el no repudio es de **LC_{Nr}=4.**

Confidencialidad (LC_{Cf})

Para el control de confidencialidad se recomienda lo siguiente [34]:

- Enumerar interacciones con servicios dentro de los objetivos o activos transportados por un canal seguro, cifrado.
- Enumerar todos los métodos admisibles que permitan mantener la confidencialidad.
- Enumerar los límites en las comunicaciones, que protegen mediante los métodos que se aplican en la confidencialidad.

Tabla 42: *Elaboración de Confidencialidad en el canal de Seguridad de Telecomunicaciones*

Técnica implementada	Observación, Entrevista
Confidencialidad	1.- La manipulación de información está de acuerdo a las funciones del personal. 2.- En aplicaciones web se cuentan con los protocolos de seguridad necesaria en confidencialidad. 3.- Se hace uso de encriptación de datos.

Autor: Elaborado a partir de [34]

Se obtuvo un valor de **LC_{Cf}=3.**

Privacidad (LC_{Pr})

Se determinan los diferentes niveles de los controles para el acceso físico a los dispositivos que los controlan.

Tabla 43: *Elaboración de Privacidad en el canal de Seguridad de Telecomunicaciones*

Técnica implementada	Observación, Entrevista
Privacidad	1.- Cámaras de seguridad.

Autor: Elaborado a partir de [34]

Para el control de privacidad se obtuvo el siguiente valor **LC_{Pr}=1.**

Integridad (LC_{It})

Determina que la información sólo puede ser revisada y modificada por el personal que cuenta con la respectiva autorización y garantiza que el cifrado de la información esta aplicado para así garantizar la confidencialidad de las comunicaciones [34].

Tabla 44: *Elaboración de la Integridad en el canal de Seguridad de Telecomunicaciones*

Técnica implementada	Observación, Entrevista
Integridad	1.- Políticas para respaldos 2.- Control de cambios para información

Autor: Elaborado a partir de [34]

En integridad se pudo obtener un valor de **LC_{It}=2.**

Alarma (LC_{Ai})

Para el control de alarma se requiere verificar los usos de métodos, registro o mensajes que advierten una situación sospechosa, como intentos de intrusión.

Tabla 45: *Elaboración de Alarma en el canal de Seguridad de Telecomunicaciones*

Técnica implementada	Observación, Entrevista
Alarma	1.- Notificación de antivirus 2.- Notificación de firewall 3.- Notificación de respaldos

Autor: Elaborado a partir de [34]

Para el control de alarma se ha obtenido un valor de **LC_{Ai}=3.**

Vulnerabilidad (LV)

La vulnerabilidad puede ser dada por las operaciones de acceso y confianza.

Tabla 46: *Elaboración de Vulnerabilidad en el canal de Seguridad de Telecomunicaciones*

Técnica implementada	Observación, Entrevista
Vulnerabilidades	1.- Discontinuidad de Software U2000

Autor: Elaborado a partir de [34]

Para la limitación de la vulnerabilidad se obtuvo el valor de **LV=1.**

Debilidad (L_W)

Para las debilidades se debe analizar los controles detallados en la clase A e identificar las diferentes debilidades que puede haber en esos controles [34].

Tabla 47: *Elaboración del a Debilidad en el canal de Seguridad de Telecomunicaciones*

Técnica implementada	Observación, Entrevista
Debilidad	1.- Obsolencia en nivel de Hardware 2.- Descontinuidad en Software.

Autor: Elaborado a partir de [34]

En debilidad se obtuvieron los siguientes valores $\mathbf{L_W=2.}$

Preocupación (L_C)

Para obtener el valor de preocupaciones se deben revisar los controles de la clase B para así poder identificar inconvenientes que pueden darse dentro de los controles [34].

Tabla 48: *Elaboración de Preocupación en el canal de Seguridad de Telecomunicaciones*

Técnica implementada	Observación, Entrevista
Preocupación	1.- No todos los sistemas de software hace uso de encriptación de datos. 2.- Existen aplicaciones que omiten el control de antivirus.

Autor: Elaborado a partir de [34]

Para la limitación de preocupación se obtuvo el valor de $\mathbf{L_C=2.}$

Anomalías (L_A)

Las anomalías son aquellos factores externos que pueden generar fallas en los equipos.

En este caso no se cuentan con anomalías por ello el valor es de $\mathbf{L_A=0.}$

Tabla 49:*Calculo de RAVS, pruebas de Seguridad de Telecomunicaciones*

Attack Surface Security Metrics

OSSTMM version 3.0

Fill in the white number fields for OPSEC, Controls, and Limitations with the results of the security test. Refer to OSSTMM 3 (www.osstmm.org) for more information.

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

OPSEC				
Visibility	4			
Access	33			
Trust	0			
Total (Porosity)	37			

OPSEC
12,732901

CONTROLS			
Class A		Missing	
Authentication	2	35	
Indemnification	0	37	
Resilience	3	34	
Subjugation	5	32	
Continuity	2	35	
Total Class A	12	173	
Class B		Missing	
Non-Repudiation	4	33	
Confidentiality	3	34	
Privacy	2	35	
Integrity	2	35	
Alarm	3	34	
Total Class B	14	171	
		True Missing	
All Controls Total	26	344	
Whole Coverage	7,03%	92,97%	

True Controls
5,840151

Full Controls
5,840151

True Coverage A
6,49%

True Coverage B
7,57%

Total True Coverage
7,03%

Open Source Security Testing Methodology Manual
OSSTMM
www.osstmm.org

LIMITATIONS		Item Value	Total Value
Vulnerabilities	1	10,297297	10,297297
Weaknesses	2	5,675676	11,351351
Concerns	2	5,621622	11,243243
Exposures	0	1,064865	0,000000
Anomalies	0	0,135135	0,000000
Total # Limitations	5		32,8919

Limitations
12,370843

Security Δ
-19,26

True Protection
80,74

Actual Security: 80,8455 ravs

Fuente: Elaborado a partir de [31]

3.3. Interpretación de los resultados

Los valores Obtenidos con la aplicación de la metodología OSSTMM sobre la intranet de la institución INTERNET POR FIBRA ÓPTICA FONET CIA LTDA.

Tabla 50: *Valores obtenidos de la evaluación de riesgo en los canales aplicados*

Canal	**Valores de Evaluación de Riesgo (RAV)**	
	Situación Actual	**Riesgo**
Canal Inalámbrico	82,7962	-17,24
Canal de Telecomunicaciones	80,8455	-19,26

Autor: Elaboración propia

Los valores de la **tabla 46** fueron obtenidos aplicando la metodología OSSTMM v3, la columna de situación actual hace referencia al nivel de seguridad que se encontró, mientras que la columna de riesgo indica la insuficiencia o la carencia de la aplicación de controles por cada canal.

Con los valores representados en la tabla 13 sobre la escala de Likert y la tabla 46 sobre los valores obtenidos por la metodología OSSTMMv3 se realiza la medición del riesgo actual:

Tabla 51: *Escala de Likert, Medición del Riesgo en los canales aplicados*

Canal	**Niveles de Riesgo**				
	Muy Alto	**Alto**	**Medio**	**Bajo**	**Muy Bajo**
Canal Inalámbrico					- 17,24
Canal de Telecomunicaciones					- 19,26

Autor: Elaboración propia

Si bien los dos canales auditados cuentan con un nivel de riesgo Muy Bajo, se debe considerar las acciones necesarias para corregir, debido a que todos los canales contienen información de importancia, se debe recordar sobre todo que ningún sistema es seguro, para esto es recomendable realizar auditorías de seguridad cada cierto periodo, el porcentaje de riesgo es debido a que algunas acciones de seguridad no fueron parchadas debido a que no se contó con la autorización o con el acceso, como es el caso del sitio web, el cual es de una empresa de servicios de Software se solicitaron las correcciones pertinentes, pero esto depende netamente de la empresa desarrolladora.

4. CONCLUSIONES

- Se logró identificar los fallos de seguridad en la empresa INTERNET POR FIBRA ÓPTICA FONET CIA. LTDA. mediante el uso de herramientas como Metasploit, Wireshark, RDP del sistema operativo Kali Linux y técnicas como la observación y la entrevista; además de scripts necesarios que hicieron posible identificar varios fallos de seguridad en la intranet de la empresa.
- Se determinó que, si existen brechas de seguridad en los equipos Mikrotik debido a una falta de seguridad en los firewalls, lo que permitió el acceso no autorizado a redes privadas de abonados de la institución; además, las credenciales de acceso para estos equipos carecían de seguridad, por ello fue necesario agregar un puerto en la dirección IP a fin de evitar el acceso no autorizado mediante ataques de fuerza bruta.
- Se efectuaron pruebas de inyección SQL en el sistema ODOO en donde no se pudo evidenciar vulnerabilidad alguna haciendo que no sea posible alterar la base de datos de la empresa, pero sí se encontraron fallos en la asignación de roles de los empleados y la falta de una base de datos centralizada para evitar pérdidas de información ante cualquier suceso sobre esta.
- Se aplicaron técnicas de Ingeniería Social para recolectar información importante de la institución, logrando formar un archivo con posibles contraseñas, el cual sirvió para encontrar fallos de seguridad en el puerto por defecto del RDP en el sistema operativo del servidor tras haber aplicado fuerza bruta con el diccionario previamente estructurado.
- Se verificaron vulnerabilidades y errores del sistema ODOO haciendo uso de un script para la extracción de información, también se efectuó un sniffer de red en donde se evidenció que es posible capturar paquetes de datos de la red wifi de la empresa.

5. RECOMENDACIONES

- Seleccionar herramientas de software libre con el fin de facilitar el uso y posibles modificaciones de códigos fuente destinados a la identificación de fallos de seguridad de una institución.
- Investigar sobre los dispositivos en los que se efectuarán las pruebas de seguridad para conocer las vulnerabilidades que estos pueden contener, antes de efectuar cualquier prueba o revisión de firewall con la finalidad de que los ataques de seguridad sean totalmente controlados por el investigador.
- Tener conocimiento sobre los diferentes tipos de inyección SQL que pueden ser aplicados en sistemas web o de escritorio que hagan uso de bases de datos SQL pertenecientes a la institución en la cual se efectuará la investigación.
- Para aplicar correctamente la Ingeniería Social es necesario generar confianza en el personal que labora en la institución que se está investigando y así poder extraer información relevante y necesaria como contraseñas, acontecimientos importantes, datos privados, etc.
- Indagar sobre los sistemas que se utilizan dentro de la institución además de las versiones de estos, la base de datos que utiliza, su dirección de dominio, los protocolos de recolección de información como los métodos GET y POST, entre otros, con la finalidad de desarrollar un script que pueda ser útil para verificación de posibles vulnerabilidades y errores que estos puedan contener.

6. REFERENCIAS BIBLIOGRÁFICAS

[1] P. I y S. G, «Ethical hacking and penetration testing for securing us form Hackers,» de *Ethical hacking and penetration testing for securing us form Hackers*, Vancouver, 2020.

[2] B. Moreno, M. Muñoz, J. Cuella, S. Domanic y J. Villanueva, «Revisiones Sistemáticas: definición y nociones básicas,» *Clin. Periodoncia Implantol. Rehabil. Oral*, pp. 184,185, 2018.

[3] F. D, M. S y S. M, «Improving Informatics Security Using Quality Control Circles,» *IEEE*, p. 1, 2015.

[4] D. Sun y B. Wang, «Analysis of On-site Evaluation Methods of Network Security in the Evaluation of Information Security Level Protection,» *IEEE*, p. 260, 2021.

[5] Y. Tian, G. Li y Y. Han, «Analysis on solid protection system of industrial control network security in intelligent factory,» *IEEE*, p. 52, 2021.

[6] S. Nicholson, «How ethical hacking can protect organisations from a greater threat Scott Nicholson,» *ScienceDirect*, nº 5, p. 15, 2019.

[7] J. Conrad, «Seeking help: the important role of ethical hackers,» *ELSIEVER*, vol. 2021, nº 8, p. 5, 2021.

[8] P. I y S. G, «Ethical hacking and penetration testing for securing us form Hackers,» *SCOPUS*, p. 5, 2015.

[9] U. Mukhtar y S. Islam, «A unified framework for cloud security transparency and audit,» vol. 54, nº 2, p. 2, 2020.

[10] H. R. Gonzalez Brito y R. Montesino Perurena, «Capacidades de las metodologías de pruebas de penetración para detectar vulnerabilidades frecuentes en aplicaciones web,» *RCCI*, vol. 12, nº 4, pp. 59,60, 2018.

[11] B. M. A., C. A. P., C. F, D. M, L. M y M. W, «A distributed security tomography framework to assess the exposure of ICT infrastructures to network threats,» *ScienceDirect*, vol. 59, p. 3, 2021.

[12] A. Giuseppi, A. Tortorelli, R. Germanà, F. Liberati y A. Fiaschetti, «Securing Cyber-Physical Systems: an Optimization Framework based on OSSTMM and Genetic Algorithms,» *SCOPUS*, p. 51, 2019.

[13] R. E. López de Jimenez, «Pentesting on Web Applications using Ethical Hacking,» *IEEE*, p. 5, 2016.

[14] B. Akashdeep, H. S. Syed Bilal, S. Achyut, A. Mamoun y K. Manoj, «Penetration testing framework for smart contract Blockchain,» *SCOPUS*, 2021.

[15] «Hacking etico para detectar vulnerabilidades en los servicios de la Intranet del Gobierno Autónomo descentralizado municipal del Cantón Cevallos,» *Universidad de Ambato*, p. 17, 2015.

[16] J. M. Hatfield, «Virtuous human hacking: The ethics of social engineering in penetration-testing,» *ELSEVIER*, vol. 83, p. 358, 2019.

[17] A. N. Eiman, A. S. Shaima, A. S. Ameera, . A. H. Noora, Q. Mohammad y A. Saed, «Discovering Public Wi-Fi Vulnerabilities Using Raspberry pi and Kali Linux,» de *Discovering Public Wi-Fi Vulnerabilities Using Raspberry pi and Kali Linux*, Sozopol, Bulgaria, 2020.

[18] R. Galddam y N. M, «An Analysis of Various Snort Based Techniques to Detect and Prevent Intrusions in Networks,» *IEEEXPLORE*, p. 12, 2017.

[19] K. Swaroop, W. Bruce, Z. Qi y S. Vishal, «Characterization of Storage Workload Traces from Production Windows Servers,» *IEEEXPLORE*, p. 121, 2018.

[20] J. A. y M. Leary, «Chapter 9 - Security Compliance Management and Auditing,» de *Building a Practical Information Security Program*, Syngress, 2015, p. 158.

[21] H. Hermantha y H. Tejaswini, «IT security auditing: A performance evaluation decision model,» *Elsevier*, vol. 57, p. 2, 2014.

[22] T. Wilhelm, «Methodologies,» de *Professional Penetration Testing*, ScienceDirect, 2010, pp. 171-172.

[23] R. Leszczyna, «Standards on cyber security assessment of smart grid,» vol. 22, p. 2, 2018.

[24] J. Thomé, K. S. Lwin, D. Bianculli y L. Briand, «Julian Thome, Lwin Khin Shar, Domenico Bianculli, Lionel Briand,» vol. 137, p. 4, 24.

[25] S. R. Ellis, «Chapter 30: Ehical Hacking,» de *Computer and Information Security Handbook* , Morgan Kaufmann, 2017, p. 476.

[26] «The Security Mill,» [En línea]. Available: https://securitymill.co.za/product/zktime-net-3-0-enterprise/. [Último acceso: 15 07 2022].

[27] Anonimo, «Tecnologias Información,» [En línea]. Available: https://www.tecnologias-informacion.com/distribuidas.html. [Último acceso: 20 07 2022].

[28] R. Velasco, «Redes Zone,» 06 03 2017. [En línea]. Available: https://www.redeszone.net/2017/03/06/wireshark-2-2-5-disponible-la-nueva-version-del-analizador-paquetes/. [Último acceso: 21 07 2022].

[29] H. Hemantha y H. Tejaswini, «Post-audits for managing cyber security investments: Bayesian post-audit using Markov Chain Monte Carlo (MCMC) simulation,» *Elsevier*, vol. 37, nº 6, p. 5, 2018.

[30] R. Leszczyna, «Review of cybersecurity assessment methods: Applicability perspective,» *ELSEVIER*, vol. 108, p. 3, 2021.

[31] ISECOM, «OSSTMM The Open Source Security Testing Methdology Manual,» ISECOM, 2010.

[32] C. A. Bedoya Laguna, «Diseño de un instrumento tipo escala Likert para la descripción de las actitudes hacia la tecnología por parte de los profesores de un colegio público de Bogotá,» Universidad Distrital Francisco José de Caldas, Bogota, 2017.

[33] A. Devi, A. Kumar Mohan y M. Sethumandhavan, «Wireless Security Auditing: Attack Vectors and Mitigation Strategies,» vol. 115, p. 675, 2017.

[34] H. D. Calero Suntasig, «Analisis de vulnerabilidades para la infraestructura de red de la bolsa de valores de Quito, aplicando una metodología de ethical hacking,» *Universidad Internacional SEK*, pp. 57-66, 2020.

[35] A. Fuertes Mestro, «Elaboración de una metodología de test de instrusión dentro de la auditoria de seguridad,» *UNIR*, p. 15, 2015.

[36] H. Pete, «OSSTMM 2.1 Manual de la Metodología Abierta de Testeo de Seguridad,» ISECOM, 2003.

[37] D. Forte, «Security audits in mixed environments,» *ELSEVIER.*

ANEXOS

Anexos A: Evaluaciones de canales auditados antes de la aplicación de controles.

Attack Surface Security Metrics

OSSTMM version 3.0

Fill in the white number fields for OPSEC, Controls, and Limitations with the results of the security test. Refer to OSSTMM 3 (www.osstmm.org) for more information.

OPSEC			
Visibility	4		
Access	6		
Trust	3		
Total (Porosity)	13		

CONTROLS			
Class A		Missing	
Authentication		13	
Indemnification	0	13	
Resilience	0	13	
Subjugation	0	13	
Continuity	0	13	
Total Class A	0	65	
Class B		Missing	
Non-Repudiation	0	13	
Confidentiality	0	13	
Privacy	0	13	
Integrity	0	13	
Alarm	0	13	
Total Class B	0	65	
		True Missing	
All Controls Total	0	130	
Whole Coverage	0,00%	100,00%	

LIMITATIONS		Item Value	Total Value
Vulnerabilities	4	11,000000	44,000000
Weaknesses	5	6,000000	30,000000
Concerns	7	6,000000	42,000000
Exposures	0	2,000000	0,000000
Anomalies	0	1,461538	0,000000
Total # Limitations	16		116,0000

OPSEC
9,698723
True Controls
0,000000
Full Controls
0,000000
True Coverage A
0,00%
True Coverage B
0,00%
Total True Coverage
0,00%
Limitations
16,520123
Security Δ
-26,22
True Protection
73,78

Actual Security: 75,3834 ravs

Ilustración 66: *Resultados de evaluación Inalámbrica antes de aplicar controles*
Autor: Elaborado a partir de [31]

Attack Surface Security Metrics

OSSTMM version 3.0

Fill in the white number fields for OPSEC, Controls, and Limitations with the results of the security test. Refer to OSSTMM 3 (www.osstmm.org) for more information.

OPSEC				
Visibility	4			
Access	33			
Trust	0			
Total (Porosity)	37			

CONTROLS			
Class A		Missing	
Authentication		37	
Indemnification	0	37	
Resilience	0	37	
Subjugation	0	37	
Continuity	0	37	
Total Class A	0	185	
Class B		Missing	
Non-Repudiation	0	37	
Confidentiality	0	37	
Privacy	0	37	
Integrity	0	37	
Alarm	0	37	
Total Class B	0	185	
		True Missing	
All Controls Total	0	370	
Whole Coverage	0,00%	100,00%	

LIMITATIONS		Item Value	Total Value
Vulnerabilities	5	11,000000	55,000000
Weaknesses	3	6,000000	18,000000
Concerns	1	6,000000	6,000000
Exposures	0	1,243243	0,000000
Anomalies	0	0,243243	0,000000
Total # Limitations	9		79,0000

OPSEC
12,732901
True Controls
0,000000
Full Controls
0,000000
True Coverage A
0,00%
True Coverage B
0,00%
Total True Coverage
0,00%
Limitations
15,191925
Security Δ
-27,92
True Protection
72,08

Actual Security: 74,0095 ravs

Ilustración 67: Resultados de evaluación de red cantes de aplicar controles
Autor: Elaborado a partir de [31]

Anexo B: Reporte de evaluación por la metodología OSSTMM

Security Test Audit Report
OSSTMM 3.0 Security Verification Certification
OSSTMM.ORG - ISECOM.ORG

Reporte ID	R1	**Fecha**	1/9/2022
Auditor	Brandon Navarrete	**Duración de prueba**	1 mes
Canales	Inalámbrico	**Tipo de Test**	
Soy responsable de la información contenida en este informe y he verificado personalmente que toda la información contenida en este documento es objetiva y verdadera.			

Firma		**Sello de la Empresa**	

OPERATIONAL SECURITY VALUES		**VALORES DE LOS CONTROLES**	
Visibilidad	4	**Autenticación**	4
Acceso	6	**Indemnización**	2
Confianza	3	**Resilencia**	2
		Subyugación	3
		Continuidad	2
		No-Repudio	2
Valor de Limitaciones		**Confidencialidad**	1
		Privacidad	1
Vulnerabilidad	2	**Integridad**	2
Debilidad	2	**Alarma**	2
Preocupación	2		
Exposición	0		
Anomalías	0		

Protección verdadera	82,76	**Seguridad Actual**	82,7962 ravs

Ilustración 68: *Reporte de canal inalámbrico*
Autor: Elaborado a partir de [31]

Observaciones del canal Inalámbrico

En el presente canal de ejecución del proyecto, se dejó un residual de riesgo el cual debido a las limitaciones para poder resolver no pudo ser mitigado, es por ello que se indica lo siguiente:

1. Aplicar seguridad mediante credenciales de acceso a redes inalámbricas.
2. Proporcionar una red individual para abonados.
3. Aplicar medidas de seguridad en el control de accesos a equipos de red inalámbrica.
4. Efectuar auditorias para evitar futuros ataques informáticos.

Security Test Audit Report

OSSTMM 3.0 Security Verification Certification

OSSTMM.ORG - ISECOM.ORG

Reporte ID	R2	**Fecha**	1/8/2022
Auditor	Brandon Navarrete	**Duración de prueba**	1 mes
Canales	Telecomunicaciones	**Tipo de Test**	
Soy responsable de la información contenida en este informe y he verificado personalmente que toda la información contenida en este documento es objetiva y verdadera.			

Firma		**Sello de la Empresa**	

OPERATIONAL SECURITY VALUES		**VALORES DE LOS CONTROLES**	
Visibilidad	4	**Autenticación**	2
Acceso	33	**Indemnización**	0
Confianza	0	**Resilencía**	3
		Subyugación	5
		Continuidad	2
		No-Repudio	4
Valor de Limitaciones		**Confidencialidad**	3
		Privacidad	2
Vulnerabilidad	1	**Integridad**	2
Debilidad	2	**Alarma**	3
Preocupación	2		
Exposición	0		
Anomalías	0		

Protección verdadera	80,74	**Seguridad Actual**	80,8455 ravs

Ilustración 69: *Reporte de canal de Telecomunicaciones*
Autor: Elaborado a partir de [31]

Observaciones del canal de telecomunicaciones

En el presente canal de ejecución del proyecto, se dejó un residual de riesgo el cual debido a las limitaciones para poder resolver no pudo ser mitigado, es por ello que se indica lo siguiente:

1. Se requiere adquisición de equipos para backup en caso de caída de algún servidor.
2. Se debe efectuar una mejor revisión de los firewalls activos dentro de los equipos como Mikrotik.
3. Archivas los respaldos del Mikrotik con encriptación.
4. Aplicar medidas de seguridad en el control de accesos a equipos ISP.
5. Efectuar auditorias de seguridad para proporcionar seguridad constante a los abonados.
6. Aplicar mayor protección en los puertos, ya que estos son la puerta de acceso para un pirata informático.