UNIVERSIDAD TÉCNICA DE COTOPAXI
EXTENSIÓN LA MANÁ

FACULTAD DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

CARRERA DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES

PROYECTO DE INVESTIGACIÓN

SEGURIDAD INFORMÁTICA MEDIANTE HACKING ÉTICO EN LA APLICACIÓN DE PENTESTING PARA EL ANÁLISIS DE VULNERABILIDADES EN LAS REDES DE DATOS DE LA COOPERATIVA SIERRA CENTRO SUCURSAL LA MANÁ, PROVINCIA DE COTOPAXI.

Proyecto de Investigación presentado previo a la obtención del Título de Ingeniería en Informática y Sistemas Computacionales.

AUTORAS:
Garcia Vega Ana Rebeca

Morales Baren Dayana Jamileth

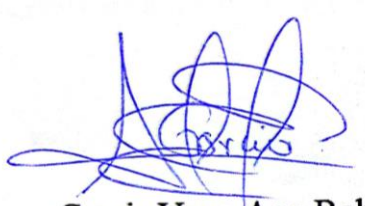
TUTOR:
Ing. MSc. Najarro Quintero Rodolfo

LA MANÁ-ECUADOR
MARZO-2022

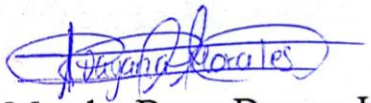
DECLARACIÓN DE AUDITORÍA

Nosotras Garcia Vega Ana Rebeca y Morales Baren Dayana Jamileth, declaramos ser autoras del presente proyecto de investigación: SEGURIDAD INFORMÁTICA MEDIANTE HACKING ÉTICO EN LA APLICACIÓN DE PENTESTING PARA EL ANÁLISIS DE VULNERABILIDADES EN LAS REDES DE DATOS DE LA COOPERATIVA SIERRA CENTRO SUCURSAL LA MANÁ, PROVINCIA DE COTOPAXI, siendo el Ing. MSc. Najarro Quintero Rodolfo, tutor del presente trabajo; y eximo expresamente a la Universidad Técnica de Cotopaxi y a sus representantes legales de posibles reclamos o acciones legales.

Además, certifico que las ideas, conceptos, procedimientos y resultados vertidos en el presente trabajo investigativo, son de nuestra exclusiva responsabilidad.



Garcia Vega Ana Rebeca
C.I: 1205283383



Morales Baren Dayana Jamileth
C.I: 1208262095

AVAL DEL TUTOR DE PROYECTO DE INVESTIGACIÓN

En calidad de tutor del trabajo de Investigación sobre el título:

"SEGURIDAD INFORMÁTICA MEDIANTE HACKING ÉTICO EN LA APLICACIÓN DE PENTESTING PARA EL ANÁLISIS DE VULNERABILIDADES EN LAS REDES DE DATOS DE LA COOPERATIVA SIERRA CENTRO SUCURSAL LA MANÁ, PROVINCIA DE COTOPAXI", de Garcia Vega Ana Rebeca y Morales Baren Dayana Jamileth de la carrera Ingeniería en Informática y Sistemas Computacionales, considero que dicho Informe Investigativo cumple con los requerimientos metodológicos y aportes científico-técnicos suficientes para ser sometidos a la evaluación del Tribunal de Validación de Proyecto que el Honorable Consejo Académico de la Facultad Académica de Ciencias de la Ingeniería y Aplicadas (CIYA) de la Universidad Técnica de Cotopaxi designe, para su correspondiente estudio y calificación.

La Maná, 2 de febrero del 2022

Ing. MSc. Najarro Quintero Rodolfo

TUTOR

APROBACIÓN DEL TRIBUNAL DE TITULACIÓN

En calidad de Tribunal de Lectores, del presente trabajo investigativo, de acuerdo a las disposiciones reglamentarias emitidas por la Universidad Técnica de Cotopaxi Extensión La Maná; por cuanto, el o los postulantes: GARCIA VEGA ANA REBECA y MORALES BAREN DAYANA JAMILETH con el título de Proyecto de Investigación "SEGURIDAD INFORMÁTICA MEDIANTE HACKING ÉTICO EN LA APLICACIÓN DE PENTESTING PARA EL ANÁLISIS DE VULNERABILIDADES EN LAS REDES DE DATOS DE LA COOPERATIVA SIERRA CENTRO SUCURSAL LA MANÁ, PROVINCIA DE COTOPAXI", han considerado las recomendaciones emitidas oportunamente y reúne los méritos suficientes para ser sometido al acto de Sustentación de Proyecto.

Por lo antes expuesto, se autoriza realizar los empastados correspondientes, según la normativa institucional.

La Maná, 25 de marzo del 2022

Para constancia firman:

Ing. MSc. Geovanny Silva Peñafiel
C.I: 060289176-4
LECTOR 1 (PRESIDENTE)

Ing. MSc. Daisy Nata Castro
C.I:120512408-2
LECTOR 2 (DELEGADO)

Ing. MSc. Víctor Cusco Vinueza
C.I: 180464775-6
LECTOR 3 (SECRETARIO)

AGRADECIMIENTO

Agradezco a Dios por siempre protegerme y por estar conmigo en cada paso que doy, y por haber puesto en mi camino personas que han sido mi soporte durante todo mi trayecto de vida tanto personal como académico. A mis padres Roberto García y María Vega; gracias por su apoyo incondicional en los buenos y malos momentos, a mis hermanos Luis, David, Abel, Javier y Juana García; muchas gracias por haberme cuidado en todo momento desde mi formación académica y vida profesional.

Garcia Ana.

Mi agradecimiento a Dios, en especial a mi familia Morales Barén, quienes son fundamentales en mi vida, gracias por el apoyo en esta experiencia como estudiante universitaria. A mis padres Héctor Antonio Morales y Bella Narcisa Baren Morales por su esfuerzo realizado en mi formación académica, a mis hermanos Nixon, William, Alexander y Jandry por su apoyo incondicional, a mis hermanas Jenny y Jasú por su amor e inteligencia, a mis sobrinos Josue, Juneidy, Leider, Deylan, William, Ariana, Samanta, Ahitana y Aldair, y por todos ellos; Gracias familia.

Morales Dayana.

DEDICATORIA

El proyecto de investigación se los dedico a las personas incondicionales que son mis padres Roberto Garcia y María Vega que siempre me apoyaron en el proceso académico en base a la moral y la motivación para poder ser un profesional al servicio de mi país, a mis hermanos Luis, David, Abel, Javier y Juana Garcia gracias por el apoyo. A la Universidad Técnica de Cotopaxi donde forje mi camino profesional en conjunto con toda su planta de docentes profesionales, por guiarnos hacia una educación de calidad y excelencia.

Garcia Ana.

A Dios por ser la guía y cuidado, a mi padre Héctor Antonio Morales por su sacrificio día a día, confianza, y esmero convirtiéndose en el pilar fundamental en mi formación académica, a mi madre Bella Narcisa Baren Morales por su amor y motivación en cada actividad académica que realice , y a mis hermanos Nixon, William, Alexander y Jandry por su cariño y confianza, A mis hermanas Jenny y Jasú por su apoyo y paciencia; A mis grandes amigas Jeniffer, Suanny y Josselyn por el apoyo incondicional durante toda la carrera convirtiéndose así uno de mis motivos para culminar mi meta. A la UTC en especial a mi docente tutor Ing. Rodolfo Najarro Quintero por siempre llenarnos de conocimientos y sabiduría ¡Por su esfuerzo y sacrificio este proyecto es para ustedes!

Morales Dayana.

UNIVERSIDAD TÉCNICA DE COTOPAXI

FACULTAD DE CIENCIAS DE LA INGENIERÍA Y APLICADA CIYA

TÍTULO: "SEGURIDAD INFORMÁTICA MEDIANTE HACKING ÉTICO EN LA APLICACIÓN DE PENTESTING PARA EL ANÁLISIS DE VULNERABILIDADES EN LAS REDES DE DATOS DE LA COOPERATIVA SIERRA CENTRO SUCURSAL LA MANÁ, PROVINCIA DE COTOPAXI".

Autoras:
Garcia Vega Ana Rebeca
Morales Baren Dayana Jamileth

RESUMEN

La Cooperativa de Ahorro y Crédito Sierra Centro es una entidad financiera de la provincia del Cotopaxi la cual presta servicios de financiamiento y captación de recursos, operaciones y servicios financieros brindando confianza y seguridad para propiciar el desarrollo local social y económico de sus clientes. Teniendo en cuenta y dada la importancia a la información que manipula los departamentos financieros de entidad privada es necesario implementar mecanismos que den soporte a nivel de seguridad informática que protejan datos e información tanto de los recursos compartidos como la interacción de una red de datos, permitiendo así aplacar los recursos que pueden estar expuestos a que se violen sus brechas de seguridad mediante el acceso a una determinada información. La presente investigación se basa en la aplicación de pentesting mediante hacking ético en las redes de datos bajo la normativa ISO 27001 *(Organización Internacional De Normalización)* aplicada en la Cooperativa de Ahorro y Crédito Sierra Centro, sucursal La Maná, lo que permitirá que la información sea segura y libre de ataques informáticos mediate la aplicación de análisis técnico en la detección de brechas vulnerables; implementando reglas de seguridad mediante el uso de Kali Linux como sistema operativo de seguridad ofensiva que permita una administración segura y correcta, mediante el monitoreo de las redes de datos de la entidad privada.

Palabras claves: SEGURIDAD INFORMÁTICA, HACKING ÉTICO, PENTESTING, VULNERABILIDADES, ISO, MALWARE, REDES DE DATOS, FIREWALL.

TECHNICAL UNIVERSITY OF COTOPAXI

FACULTY OF ENGINEERING AND APPLIED SCIENCES

TITLE: "SEGURIDAD INFORMÁTICA MEDIANTE HACKING ÉTICO EN LA APLICACIÓN DE PENTESTING PARA EL ANÁLISIS DE VULNERABILIDADES EN LAS REDES DE DATOS DE LA COOPERATIVA SIERRA CENTRO SUCURSAL LA MANÁ, PROVINCIA DE COTOPAXI".

Authors:
Garcia Vega Ana Rebeca
Morales Baren Dayana Jamileth

ABSTRACT

The Sierra Centro Savings and Credit Cooperative is a financial institution in the province of Cotopaxi which provides financing services and fundraising, operations and financial services providing confidence and security to promote the local social and economic development of its customers. Taking into account and given the importance of the information manipulated by the financial departments of private entities, it is necessary to implement mechanisms that support computer security that protect data and information both from shared resources and the interaction of a data network, thus allowing to placate the resources that may be exposed to their security breaches being violated through access to certain information. This research is based on the application of pentesting through ethical hacking in data networks under the ISO 27001 (International Organization for Standardization) standard applied in the Sierra Centro Savings and Credit Cooperative, La Maná branch, which will allow the information to be secure and free of computer attacks through the application of technical analysis in the detection of vulnerable gaps; implementing security rules by using Kali Linux as an offensive security operating system that allows a secure and correct administration, by monitoring the data networks of the private entity.

Keywords: COMPUTER SECURITY, ETHICAL HACKING, PENTESTING, VULNERABILITIES, ISO, MALWARE, DATA NETWORKS, FIREWALL.

AVAL DE TRADUCCIÓN

En calidad de Docente del Idioma Inglés de la Universidad Técnica de Cotopaxi; en forma legal **CERTIFICO** que:

La traducción del resumen al idioma inglés del proyecto de investigación cuyo título es: **"SEGURIDAD INFORMÁTICA MEDIANTE HACKING ÉTICO EN LA APLICACIÓN DE PENTESTING PARA EL ANÁLISIS DE VULNERABILIDADES EN LAS REDES DE DATOS DE LA COOPERATIVA SIERRA CENTRO SUCURSAL LA MANÁ, PROVINCIA DE COTOPAXI".** Presentado por: **Garcia Vega Ana Rebeca** y **Morales Baren Dayana Jamileth,** egresadas de la Carrera de: **Ingeniería en Informática y Sistemas Computacionales,** perteneciente a la **Facultad de Ciencias de la Ingeniería y Aplicadas,** lo realizaron bajo mi supervisión y cumple con una correcta estructura gramatical del Idioma.

Es todo cuanto puedo certificar en honor a la verdad y autorizo al peticionario hacer uso del presente aval para los fines académicos legales.

La Maná, 07 abril del 2022

Atentamente,

Firmado electrónicamente por:
OLGA SAMANDA
ABEDRABBO
RAMOS

Lic. Olga Samanda Abedrabbo Mg.
DIRECTOR DEL CENTRO DE IDIOMAS-UTC
C.I: 050351007-5

ÍNDICE GENERAL

ÍNDICE DE TABLA

ÍNDICE DE GRÁFICOS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

1. INFORMACIÓN GENERAL

Título del Proyecto:

"Seguridad Informática Mediante Hacking Ético En La Aplicación De Pentesting Para El Análisis De Vulnerabilidades En Las Redes De Datos De La Cooperativa Sierra Centro Sucursal La Maná, Provincia De Cotopaxi."

Fecha de inicio:	Octubre 2021
Fecha de finalización:	Marzo 2022
Lugar de ejecución:	Cantón La Maná, Provincia de Cotopaxi
Unidad académica que auspicia:	Facultad de Ciencias de la Ingeniería y Aplicadas
Carrera que auspicia:	Ingeniería en Informática y Sistemas Computacionales
Proyecto de investigación vinculado:	Universidad Técnica de Cotopaxi Extensión La Maná

Equipo de trabajo:

Estudiante: Garcia Vega Ana Rebeca
Correo: ana.garcia3383@utc.edu.ec
Teléfono: 098 825 9160
Estudiante: Morales Baren Dayana Jamileth
Correo: dayana.morales2095@utc.edu.ec
Teléfono: 098 852 4891
Tutor: MSc. Najarro Quintero Rodolfo
Correo: rodolfo.najarro@utc.edu.ec
Teléfono: 098 730 9973

Línea de Investigación:	Tecnologías de la Información y Comunicación (Tics).

Sub líneas de investigación de la carrera: Diseño, implementación y configuración de redes y Seguridad Computacional, aplicando normas y estándares internacionales.

2. DESCRIPCIÓN DEL PROYECTO

El presente proyecto investigativo tiene como objetivo realizar la aplicación de un análisis técnico mediante pentesting para la evaluación, análisis y detección de vulnerabilidades en las redes de datos, de la Cooperativa Sierra Centro sucursal La Maná, Provincia de Cotopaxi, lo cual se verificará el estado de las redes de comunicación para la confiabilidad de la información dentro de las normas y estándares internacionales ISO.

La aplicación tanto de análisis técnico como la configuración de barreras de seguridad informática permitirá que la información de la entidad financiera no sea manipulada por terceros que violen las barreras de acceso mediante técnicas de ataques informáticos, lo que puede generar pérdidas y extracción de información. Con la evaluación de las redes de datos y la implementación de mecanismos de seguridad permitirá que la información sea segura y libre de intrusos para la correcta utilización de los servicios en red de la organización.

3. JUSTIFICACIÓN DEL PROYECTO

La ejecución orientada al análisis del estado de una infraestructura empresarial en el marco de las normativas ISO, permitirá establecer aspectos como la prevención y la detección a los ataques a nivel de seguridad informática; el propósito es segmentar la confidencialidad de la información y la protección de servicios tecnológicos que puedan verse comprometidos ante los ataques de infraestructura de comunicaciones. Para ello en la aplicación de los procesos de gestión de la seguridad informática orientados a la evaluación de las redes de datos, se permite contemplar la ejecución del análisis técnico en las redes de datos basado en las normativas ISO 27001 como una actividad de control obligatoria, dando como resultado llevar la gestión adecuada ante posibles ataques de información confidencial de la entidad privada.

Para la aplicación en la evaluación de las redes de datos se considera especificar las etapas de hacking ético lo cual hacen referencia al reconocimiento pasivo y activo considerando la recopilación de la información de la institución financiera; complementada por la fase de escaneo que consistirá en tomar determinada información para examinar la red mediante herramientas de exploración y por ultimo obtener el acceso; que mediante el reconocimiento pasivo, activo y escaneo se podrá acceder a destino de una red mediante red de área local o de estado inalámbrico.

El presente proyecto de investigación busca responder a las necesidades de la red de datos, permitiendo así diseñar e implementar mecanismos de seguridad en base a la aplicación de pentesting, para la detección de amenazas y vulnerabilidades dentro de la red de datos de la cooperativa, estableciendo así la integración y disponibilidad de la información mediante las conexiones de exploración en el servicio de la red para así poder prevenir ataques de infraestructura de servicios en el futuro. Esto permitirá mediante la aplicación de un estudio realizar un análisis de seguridad a nivel de infraestructura de recursos compartidos para tener consigo una perspectiva más detallada ante las vulnerabilidades y ataques informáticos que puedan estar expuestos tanto los sistemas de gestión de la información como en las redes de datos.

4. BENEFICIARIOS DEL PROYECTO

El presente proyecto beneficiará a la cooperativa de ahorro y crédito Sierra Centro Sucursal La Maná, mediante la aplicación de protección y detección de vulnerabilidades en sus redes de datos de comunicaciones.

Tabla 1: Beneficiarios Directos

Beneficiario	Beneficiario Directos	Total
Socios de la Cooperativa De Ahorro Y Crédito Sierra Centro	19	**19**

Fuente: Cooperativa de ahorro y crédito Sierra Centro
Realizado por: Las investigadoras

Tabla 2: Beneficiarios Indirectos

Beneficiarios	Beneficiarios Indirectos		Total
	Hombres	Mujeres	
Atención al Cliente	15	12	**27**
Asesores de Créditos	13	12	**25**
Departamento de sistemas	5	2	**7**
Asesores de Inversiones	10	8	**18**
Gerentes de sucursales	6	2	**8**
Secretaria	3	8	**11**
Consejo de Administración	6	3	**9**
TOTAL	58	47	**105**

Fuente: Cooperativa de ahorro y crédito Sierra Centro
Realizado por: Las investigadoras

5. PROBLEMA DE INVESTIGACIÓN

En la actualidad, la extracción de datos a nivel mundial se perfila bajo el condicionamiento de información personal y datos a nivel empresarial, lo que hace que cualquier ataque cibernético en dispositivos de comunicación o redes de datos sean vulnerables contra cualquier tipo de amenaza, menguando así los riesgos tanto lógicos como físicos. (Baca, 2016)

Constantemente las amenazas informáticas pueden afectar a la integridad de la información de una organización. Pero es preciso indicar que problema incide dado al incremento de situaciones que redirigen al uso prioritario de la información en la falta de políticas de privacidad en la aplicación de las normas ISO y de los eventos causados por personas externas al querer acceder de manera forzada a un determinado contexto de información, aplicando mecanismos de ataque o violaciones dirigidos al acceso de los recursos tecnológicos o servicios de recursos compartidos en redes.

En base al proceso y desarrollo investigativo en la Cooperativa de Ahorro y Crédito Sierra Centro, las redes de datos se encuentra en procesos de adaptación, pero tienen falencias dentro de la administración de sus servicios y de sus brechas de seguridad a nivel comunicacional, manteniendo así la posibilidad de que exista amenazas y vulnerabilidades mediante ataques informáticos externos dentro de los dominios de las infraestructuras de redes datos de tipo LAN (Red De Área Local), siendo así deficiente el control de los recursos compartidos y de los sistemas de comunicación.

6. OBJETIVOS

6.1. Objetivo general

Implementación de seguridad informática mediante hacking ético en la aplicación de pentesting para el análisis de vulnerabilidades en las redes de datos de la cooperativa "Sierra Centro" sucursal La Maná.

6.2. Objetivos específicos

- Identificar los mecanismos, medidas y aplicación de pentesting bajo la normativa ISO 27001 en la seguridad informática para el desarrollo de la propuesta de investigación.
- Realizar análisis de la red ante vulnerabilidades existentes dentro de la infraestructura tecnológica mediante entornos controlados de virtualización y conmutadores NMAP *(Network Mapper)*.
- Aplicar seguridad informática mediante pentesting para la penetración y análisis de vulnerabilidades y mejoramiento de las redes de datos mediante IDS (*Intrusion Detection System)*.

7. ACTIVIDADES Y SISTEMA DE TAREAS EN RELACIÓN A LOS OBJETIVOS PLANTEADOS

Tabla 3: Actividades y sistema de tareas en relación a los objetivos planteados

Objetivo	Actividad	Resultado de la actividad	Medios de verificación
Objetivo Específico 1: Identificar los mecanismos, medidas y aplicación de pentesting bajo la normativa ISO 27001 en la seguridad informática para el desarrollo de la propuesta de investigación mediante citas bibliográficas y de campo.	• Investigar artículos bibliográficos que son analizados en el proceso de investigación.	• Revisión Bibliográfica.	• Marco teórico del proyecto de investigación.
Objetivo Específico 2: Realizar análisis de la red ante vulnerabilidades existentes dentro de la infraestructura tecnológica mediante entornos controlados de virtualización y conmutadores NMAP *(Network Mapper)*.	• Establecer mecanismos y contramedidas de seguridad informática. • Estudio y evaluación de la infraestructura de red de la cooperativa sierra centro.	• Resultados del escaneo aplicado a la infraestructura de red mediante exploraciones TCP Connect y explotación FTP.	• Desarrollo de la propuesta técnica del proyecto de investigación.
Objetivo Específico 3: Aplicar seguridad informática mediante pentesting para la penetración y análisis de vulnerabilidades y mejoramiento de las redes de datos mediante IDS (*Intrusion Detection System)*.	• Control de la red de datos bajo la normativa ISO 27001. • Virtualización y Configuración de los mecanismos de control en la red LAN.	• Pentesting en el análisis de vulnerabilidades • Configurar reglas de seguridad mediante SNORT en la red de datos de la entidad financiera.	• Elaboración de técnico de auditoría sobre los resultados de la aplicación de pentesting en el análisis de amenazas y vulnerabilidades de la red de datos.

Fuente: Elaborado por las Investigadoras

8. FUNDAMENTACIÓN CIENTÍFICO TÉCNICA

8.1. Antecedentes de la investigación

La investigación realizada evalúa las brechas de seguridad en las redes LAN situando así la aplicación y creación de entornos virtuales orientadas a la seguridad informática mediante el uso de firewalls lógicos ante ataque externos. Manifestando que el proceso el proceso de configuración tanto del servidor y DNS de clientes permitirán aplicar técnicas de test en penetración a las redes de datos basándose en la normativa ISO 27001 (Mancheno & Robles, 2013).

Su investigación es aplicada a la seguridad informática para la red de datos, basándose la configuración de barreras firewall de tipo software a través de la configuración de una red compartida en los diferentes departamentos de dicha entidad para así prevenir ataques informáticos externos en la extracción de información financiera de entidad privada (Garces, 2015).

Su investigación se aplicó en base al análisis de seguridad informática en la aplicación de la norma ISO/IEC 27001 en los sistemas de gestión de la información y la evaluación de datos de una empresa de servicios financieros en base a la seguridad de procesos críticos de los controles y brechas en seguridad de redes TCP, permitiendo así la ejecución de análisis de riesgos en la que se da a conocer el nivel de impacto de amenazas informáticas identificadas en cada activo mediante datos relevantes propias del negocio (Bermúdez & Bailón, 2015).

Aplica un estudio dirigido hacia el análisis y diseño de un sistema de seguridad de red perimetral en la Empresa Aseguradora del Sur, permitiendo así aplicar un control basado en la utilización del firewall lógico dentro de una red de datos, en base al análisis y filtración desde redes externas, evitando así que la compañía se encuentre expuesta ante posibles operaciones de ataque mediante penetración de datos (Bonilla, 2016).

El trabajo investigativo fue orientado en la implementación de ambientes de simulación para la detección de vulnerabilidades en las redes de datos mediante la aplicación de distintas técnicas de modelos autorregresivos integrales, permitiendo así la detección y bloqueo de ataques de denegación de servicios de red mediante servidores web externos (Chávez, 2016).

Aplicó en su proceso de investigación un plan de seguridad informática basada en la norma ISO 27001 para el control de accesos externos a la red de datos, lo que permite aplicar de manera adecuada los estándares de normalización ISO; permitiendo así implementar estrategias en la optimización y mejora de control de los accesos a una red privada ante posibles ataques informáticos en el futuro (Zatán, 2017).

El propósito de su investigación fue analizar vulnerabilidades mediante la aplicación y el uso de Phishing en las redes de datos, para poder así mejorar las brechas de seguridad de las redes de datos que tenían falencias en los equipos de cómputo siendo víctima de ataques externos. Esto permitió cumplir el objetivo de pruebas mediante conceptos de valoración de riesgo y cambio de perspectiva del atacante (Alvarado, 2017).

Mediante su trabajo investigativo basado en la aplicación del hacking ético para evaluar la infraestructura de redes, se aplicó una análisis técnico informática bajo el proceso de penetración a la información para poder así realizar el análisis de penetración bajo la premisa de detectar si existe una brecha previamente aperturada en los equipos de la red de datos; sin embargo se obtuvo como resultado el análisis y evaluación de las redes de comunicación en la prevención ante ataques de cibercriminales (Rojas,2018).

El estudio se basa en la detección de vulnerabilidades en las redes de datos y vulnerabilidades de la información de las máquinas y recursos compartidos por red, ya el proceso investigativo realiza un análisis mediante software libre en referencia de Kali Linux; identificando así los activos de información y componentes sobre las medidas de seguridad informática que se pueden implementar en la institución en base a una auditoría interna de la infraestructura comunicacional y recursos compartidos (Lino, 2019).

Se aplica los mecanismos de seguridad en caso de ataques a las redes LAN mediante evaluaciones de comunicación entre paquetes de datos dentro de las operaciones financieras que garanticen las actividades de contingencia ante ataques y técnicas de extracción de información externas, manteniendo así las políticas de seguridad y estándares en su aplicación de normas internacionales ISO/EC, ISO/IEC/ 27001 (Borbor, 2020).

8.2. ISO

La Organización Internacional de Normalización (ISO) es una federación mundial de organismos nacionales de normalización que son miembros de ISO. El mundo de la normalización encuentra así su referencia a nivel internacional en la ISO (Sánchez & Piattini, 2012).

8.2.1. Qué son las normas ISO

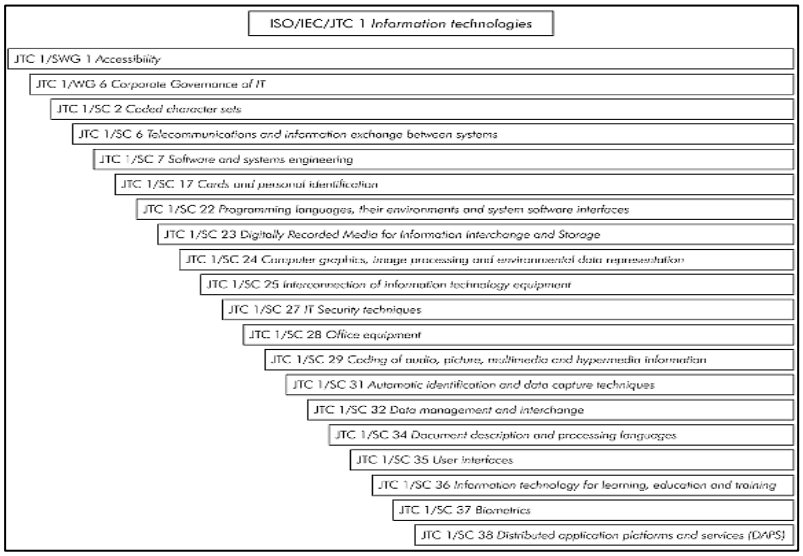
La norma ISO, aplicada y extendida hoy en día a todas las actividades técnicas, industriales y comerciales, se define como una especificación técnica otro documento accesible al público establecido con la cooperación y el consenso o la aprobación general de todas las partes interesadas, basada sobre resultados conjugados de la ciencia, la tecnología y la experiencia, que comtenpla ventajas para el conjunto de la comunidad y aprobada por un organismo cualificado a nivel nacional, regional o internacional (Sánchez & Piattini, 2012).

8.2.2. Normas y estándares para el gobierno y la gestión de las TICs

A nivel mundial, el sistema de normalización lo constituyen ISO (Organización Internacional de Normalización), IEC (Comisión Electrotécnica Internacional) y UIT (Unión Internacional de Telecomunicaciones). Para el ámbito de las tecnologías de la información, se creó un comité conjunto entre ISO e IEC, el denominado JTC 1 Information Technologies, que es en la actualidad la fuente de referencia para abordar las iniciativas de normalización en este ámbito, y origen de las series de normas que veremos más adelante y que configuran el marco de gestión de las TIC.

La estructura del comité JTC 1 está formada por más de veinte subcomités, y cada año se incorporan nuevos órganos de trabajo que permiten dar respuesta a través de la normalización internacional a nuevas demandas y necesidades del mercado de la sociedad de la información. Las relaciones y colaboraciones del JTC 1 con el resto de comités de normalización, tanto internacionales como europeos como extra continentales, se fortalecen constantemente debido a la colateralidad de las TIC con la mayoría de los procesos industriales y de negocio, así como con el día a día de los ciudadanos, lo que permite aumentar la interoperabilidad y usabilidad de los sistemas de información (Sánchez & Piattini, 2012).

Gráfico 1: Estándares ISO/TEC



Fuente: Balderras. estándar asignado ISO (2019)

8.2.3. Norma ISO/IEC 27001 en la gestión de la seguridad de la información

Esta norma proporciona una visión general de las normas que componen la serie 27001, indicando para cada una de ellas su alcance de actuación y el propósito de su publicación. Recoge todas las definiciones para la serie de normas 27001 y aporta las bases de por qué es importante la implantación de un SGSI, una introducción a los Sistemas de Gestión de Seguridad de la Información, una breve descripción de los pasos para el establecimiento, monitorización, mantenimiento y mejora de un SGSI. Actualmente se cita como referencia normativa la norma ISO / IEC 27001: 2018 tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Descripción general y vocabulario (Costas, 2014).

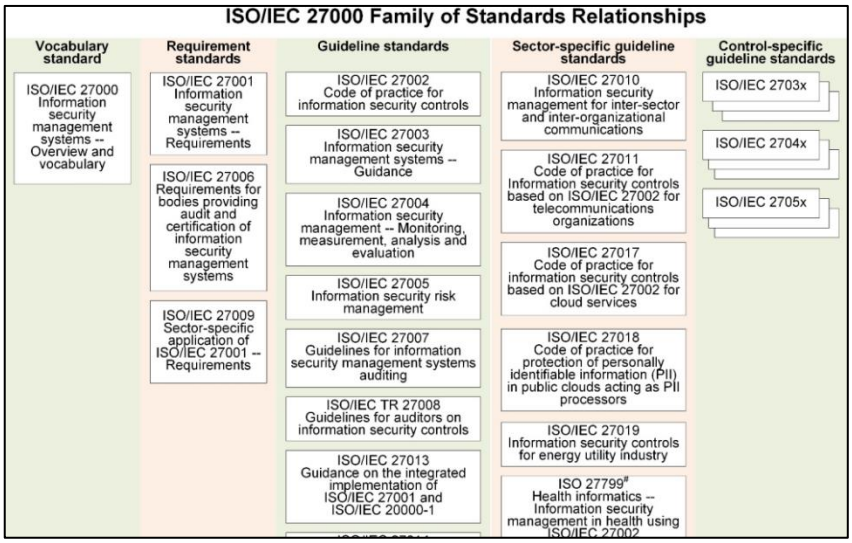
Gráfico 2: Recopilación de datos aplicando análisis técnico

Fuente: Balderras. estándar asignado ISO (2019)

8.2.4. ISO 27001 aplicado a los sistemas SGSI

Un sistema de Gestión para la seguridad de la información consta de una serie de políticas, procedimientos e instrucciones o directrices específicas para cada actividad o sistema de información que persiguen como objetivo la protección de los activos de información en una organización (Sánchez & Piattini, 2012).

Gráfico 3: Normas ISO aplicadas a sistemas SGSI



Fuente: ISO 27001. familia ISO (2019)

8.2.5. SGI en base a los procesos sistemáticos

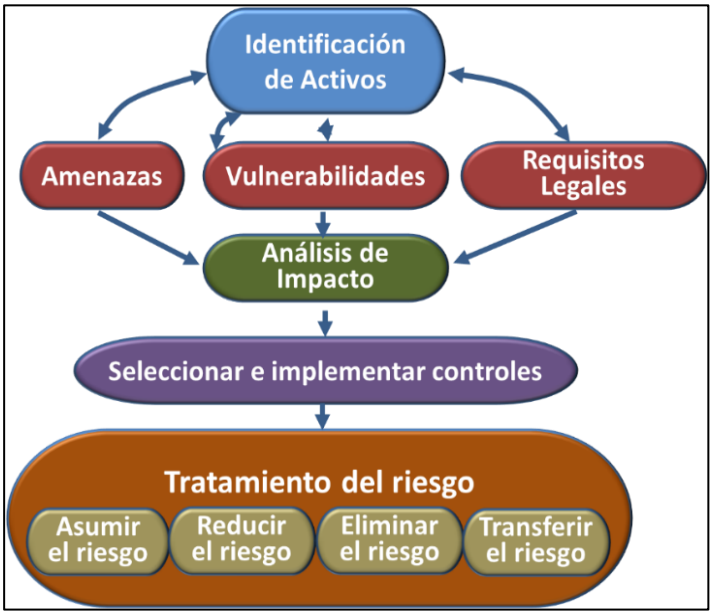
- Establece o planifica la Seguridad de la información estableciendo los procesos y objetivos a conseguir.
- Se implementa la Seguridad de la información dentro de los procesos de la organización.
- Se opera y mantienen los procesos establecidos para la seguridad de la información.
- Se miden los resultados (Monitoreo) e indicadores de los distintos procesos de la seguridad de la información.
- Se evalúa (Revisión) la efectividad de los procesos de la seguridad en base a los objetivos establecidos.
- Se analizan los resultados y se establecen nuevos objetivos.

8.2.6. Características de la norma ISO/IEC 27001

Esta norma contiene varias características que pueden aplicarse a cualquier tipo de empresa, ya sea grande o pequeña, de cualquier sector y ubicada en cualquier localidad

del mundo. Pero es altamente útil para aquellas empresas que tienen actividades financieras, sanitarias, aseguradoras, sector público y tecnologías de la información (Sánchez & Piattini, 2012).

Gráfico 4: Características de la norma ISO/IEC 27001



Fuente: Revista Aenor, elementos de norma ISO/IEC 27001 (2015)

- **Confidencialidad:** La propiedad que esta información esté disponible no sea divulgada a personas, entidades o procesos no autorizados.
- **Seguridad de información:** Preservación de la confidencialidad, integridad, disponibilidad de la información; además, también pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, no-repudio, y confiabilidad
- **Sistema de gestión de la seguridad de la información:** Es parte del sistema gerencial general, basado en un enfoque de riesgo comercial; para establecer, implementar, monitorear, revisar, mantener y mejorar la seguridad de la información.
- **Análisis de riesgo:** La norma exige que la empresa haga un análisis de riesgos de seguridad periódicamente y siempre que se propongan o se establezcan cambios significativos. Para que este análisis se haga de la manera correcta, es necesario establecer criterios de aceptación de riesgo, así como la definición de cómo esos riesgos serán medidos. También se deben evaluar las posibles consecuencias de los riesgos identificados, la probabilidad de que ocurran y sus niveles.

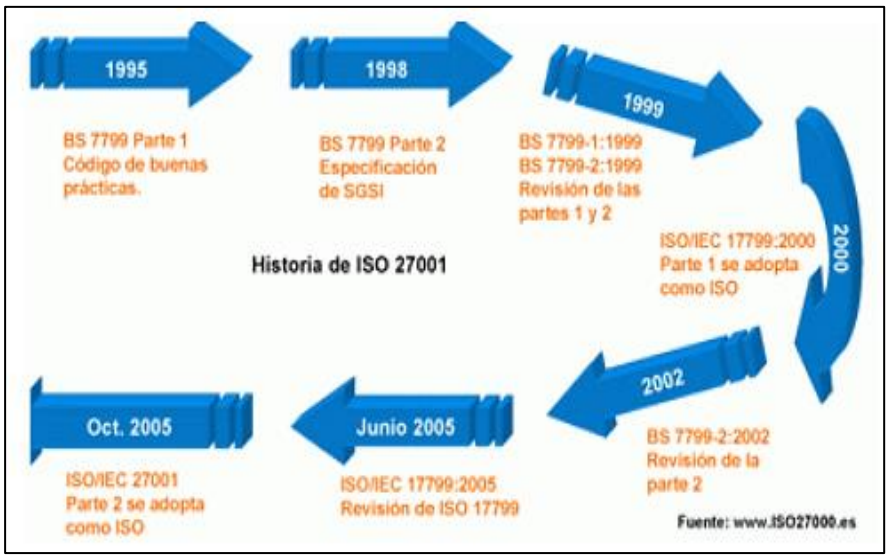
- **Compromiso de alta dirección:** La norma también exige que la alta dirección demuestra compromiso con el SGSI, además de ser esa parte de la empresa ella misma la responsable por la seguridad de la información. Los líderes son también responsables de asegurar que todos los recursos para la implantación del sistema estén disponibles y asignados correctamente, y además tienen la obligación de orientar a los colaboradores para que el sistema sea verdaderamente eficiente.
- **Definición de objetivos y estrategias:** Durante la planificación, la empresa necesita tener muy claro cuáles son sus objetivos de seguridad y cuáles serán las estrategias establecidas para alcanzar esos objetivos. Los objetivos, sin embargo, no pueden ser genéricos, deben ser mensurables y tener en cuenta los requisitos de seguridad.
- **Recursos y competencias:** La organización también debe garantizar que todos los recursos necesarios no sólo para la implementación, sino que también para el mantenimiento del sistema estén disponibles. Además, es necesario establecer cuáles son las competencias necesarias y garantizar que las personas responsables sean suficientemente calificadas, incluso con documentación comprobatoria.
- **Documentación de la información:** La norma exige que toda la información sea apropiadamente documentada, con identificación, definición y formato. La información debe actualizarse siempre que haya cambios en las definiciones iniciales del proyecto, siendo necesario que se aprueben los cambios antes de que sean formalizados y consolidados.
- **Seguimiento de rendimiento:** En ese momento, los objetivos definidos en pasos anteriores deben ser medidos y acompañados, a través de la aplicación de indicadores que posibiliten análisis de la eficiencia del sistema.
- **Mejora continua:** Una vez que se alcancen los objetivos en cuanto al sistema, es necesario que la empresa implemente y mantenga un sistema de mejora continua a fin de corregir no conformidades. Esta mejora se puede llevar a cabo, por ejemplo, usando análisis críticos por la dirección y también con auditorías internas.

8.3. Regulaciones

Las normas internacionales que pertenecen a la familia 27001 permitirán establecer como base regulatoria la creación y operación de los sistemas de gestión de información

mediante la gestión de la seguridad de la información y ambientar términos técnicos utilizados mediante la aplicación de una estandarización (Sánchez & Piattini, 2012).

Gráfico 5: Ciclo de regulaciones ISO



Fuente: Vicalza, familia de ISO 27001 (2009)

La serie 27001 de la normativa ISO proporciona mediante el marco de gestión, la seguridad de la información como garantía utilizable para cualquier tipo de información de una empresa tanto pública como privada (Sánchez & Piattini, 2012).

8.3.1. Regulaciones internacionales

Normalmente las agencias gubernamentales incluidas las regulaciones europeas (RGPD) regulan también mediante procedimientos como deberemos compartir información acerca de la seguridad de la información. A nivel nacional se realiza una revisión de la privacidad de la información recibida. También están regulado los fines para los que se puede utilizar la información sobre la seguridad de la información, algo que afecta no solo a entidades externas con las que se puede compartir información a través de una organización, tomando en cuento que las regulaciones tanto para compartir como para proteger información de gran relevancia es bajo la responsabilidad de dicha organización (Sánchez & Piattini, 2012).

8.3.2. Regulaciones Ecuatorianas

De acuerdo con el Anexo SL de las Directivas ISO/IEC de la Organización Internacional para la Normalización estas regulaciones rigen a nivel mundial, dentro del Ecuador, las normativas de ISO 27001 son iguales que en ISO 22301:2012, la norma ISO 9001:2015 (COIP,2014)

- **Introducción**: Se basa en el objetivo de ISO 27001 y su adaptabilidad con otras normas de gestión.
- **Alcance:** Se aplica esta norma a cualquier tipo de organización sea privada o pública.
- **Referencias normativas**: La norma ISO/IEC 27001 cómo estandarización en el que se proporcionan términos y condiciones.
- **Términos y definiciones:** Hace referencia a la norma ISO/IEC 27001.
- **Contexto de la organización**: Es parte de la fase de Planificación del ciclo PDCA y define los requisitos para comprender cuestiones externas e internas, también define las partes interesadas, sus requisitos y el alcance del SGSI.
- **Liderazgo:** Parte de la fase de Planificación del ciclo PDCA y define las responsabilidades de la dirección, el establecimiento de roles y responsabilidades y el contenido de la política de alto nivel sobre seguridad de la información.
- **Planificación:** Es parte de la fase de Planificación del ciclo PDCA y define los requisitos para la evaluación de riesgos y el tratamiento de riesgos en base a los objetivos de seguridad de la información.
- **Apoyo**: Es parte de la fase de Planificación del ciclo PDCA y define los requisitos sobre disponibilidad de recursos, competencias, concienciación, comunicación y control de documentos y registros.
- **Funcionamiento:** Es parte de la fase de Planificación del ciclo PDCA y define la implantación de la evaluación y el tratamiento de riesgos, como también los controles de procesos en base a la manipulación de la información.
- **Evaluación del desempeño**: Forma parte de la fase de Revisión del ciclo PDCA y define los requisitos para monitoreo, medición, análisis, evaluación, auditoría interna y revisión por parte de la dirección.
- **Mejora:** Forma parte de la fase de Mejora del ciclo PDCA y define los requisitos para el tratamiento de no conformidades, correcciones, medidas correctivas y mejora continua.

8.3.3. Regulaciones Ecuatorianas en base a la norma ISO 27001

8.3.3.1. Ley de protección de datos personales

Establecido en base a la ley constitucional en su Art. 66, menciona que la constitución del Ecuador dispone que se “Reconozca y que brinde las garantías a la ley de protección

de datos de carácter personal" lo cual a su vez incluye el acceso a determinada información de carácter importante (COIP,2014).

8.3.3.2. Ley de comercio electrónico, firmas electrónicas y mensaje de datos

Lo establecido en el Art. 5 menciona que es pertinente disponer la confiabilidad y reserva de la información, manteniendo así los principios de confidencialidad para diferentes servicios, como el proceso de compra en el comercio electrónico y la mensajería de datos roaming. Manifestando que toda violación a estos principios basado en el Art. 5 se representan como una forma ilegal ante el acceso a la información y por ende será sancionado conforme dispuesto a ley vigente (COIP,2014).

8.3.3.3. Ley de propiedad intelectual

Según la Ley de Propiedad Intelectual, En su Art. 183 manifiesta que pertinente dispone que la información proporcionada no sea divulgada o relacionada con fin hacia terceros, manteniendo así que dicha información sea secreta en el entendido conjunto o configuración y composición de la protección en base al conocimiento tecnológico mediante procedimientos de fabricación y producción (COIP,2014).

8.3.4. Especificaciones de la norma ISO 27001

- Cumplimiento.
- Seguridad Física y del entorno.
- Seguridad de las comunicaciones.
- Adquisición, desarrollo y mantenimiento de sistemas.
- Control de acceso.
- Criptografía.
- Seguridad de las operaciones.
- Gestión de incidentes de la seguridad de la información.
- Aspectos de la seguridad de la información y gestión del negocio.
- Gestión de activos.
- Políticas de seguridad de la información.
- Seguridad de recursos humanos.
- Relación con los proveedores.

8.3.5. Normativas secundarias dentro de la ISO 27001

Las normas internacionales que pertenecen a la familia de ISO 27001, permitirán en base a la creación de sistemas de gestión y evaluación de redes de datos como parte de un modelo resultando un consenso entre especialistas, se debe tener en cuenta la estandarización para el segmento de la seguridad de una información o compartición de dato (Sánchez & Piattini, 2012).

Gráfico 6: Familia de las normativas ISO 27001

Fuente: Vicalza, familia de ISO 27001 (2009)

8.4. Políticas de seguridad

La política de privacidad hace referencia a una regla que se debe cumplir dentro de una entidad privada como pública, la cual esta debe asegurar la integridad, disponibilidad y privacidad de los datos que se manipulan en dicha empresa, a su vez también aplica al conjunto de infraestructuras informáticas, lo cual definen mantener un correcto nivel de protección y seguridad (Costas, 2014).

8.4.1. Políticas de gestión de información y contratación de servicios tecnológicos

- **Manipulación De Datos:** Responsabilidad del manejo de usuarios, recursos de información y brechas de seguridad.
- **Adquisición De Antivirus:** Se componen de un motor dentro de un servidor, permitiendo así que el sistema operativo este de una manera estable, permitiendo que la información sea protegida ante ataques de fuerza bruta para la extracción de una data.

- **Cortafuegos:** Filtra una información de paquetes y bloquea el tráfico no autorizado de una web.
- **Protocolos de autenticación remotos:** Son conexiones basadas en accesos telefónicos mediante modem.
- **Servidores para autenticar información:** Centraliza la red mediante de un proveedor de internet, lo cual permite mediante una clave criptográfica autenticar distintos usuarios y servidores de una entidad.

8.4.2. Base legal en Ecuador como medida de seguridad informática

La gestión de información de la República del Ecuador, garantiza implementación de medidas de seguridad mediante bases legales que reposan en nuestra constitución y el COIP (Código Orgánico Penal), tanto así que nos garantiza confidencialidad, integridad y disponibilidad de nuestra información lo cual se muestra a continuación las leyes, regulaciones y normativas que permiten establecer medidas de seguridad (COIP,2014)

- Constitución de la República del Ecuador (Decreto Legislativo 0 / Registro Oficial 449 de 20-oct-2008 / Última modificación: 13-jul-2011).
- Ley Orgánica de Servicio Público, LOSEP (Ley 0 / Registro Oficial Suplemento 294 de 06-oct-2010).
- Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (Ley No. 2002-67).
- Ley Orgánica de Transparencia y Acceso a la Información Pública No. 24, publicado en el Registro Oficial Suplemento 337 del 18 de mayo del 2004.
- Reglamento General a la Ley Orgánica del Servicio Público (Decreto Ejecutivo 710 / Registro Oficial Suplemento 418 de 01-abr-2011 / Última modificación: 10-oct-2011).
- Acuerdo No. 166, Esquema Gubernamental de Seguridad de la Información EGSI (19 de septiembre de 2013).
- Norma Técnica Ecuatoriana NTE INEN-ISO/IEC 27002:2009 Código de Práctica para la Gestión de la Seguridad de la Información.

8.5. Ataques informáticos

8.5.1. Virus informático

El virus informático es un pequeño programa basado en un script que se instala de manera automática en un ordenador sin el consentimiento de una persona. Por lo general ataca a los archivos o al sector de arranque de un disco duro (López, 2009).

8.5.2. Características principales de los virus informáticos

- **Reorientación:** El virus reorienta la lectura del disco duro para evitar la detección de un programa de protección.
- **Desinformación:** Los datos sobre el tamaño del directorio infectado son modificados, para evitar que se descubran los bits que aportan al virus.
- **Encripta-miento:** El virus se encripta en símbolos sin sentidos para no ser detectado, pero para destruir o replicarse debe desencriptar siendo entonces detectable.
- **Polimorfismo:** Muta cambiando segmentos del código para parecer distinto en cada nueva generación, lo que resulta difícil de ser detectado y ser desinfectado.
- **Gatillables:** Se relaciona con un evento que es el encargado de la ejecución del virus que puede alterar datos como las fechas, o alterar combinaciones de tecla. Generalmente son asociados con el tipo de virus troyano.

8.5.3. Capacidad de propagación de los virus informáticos

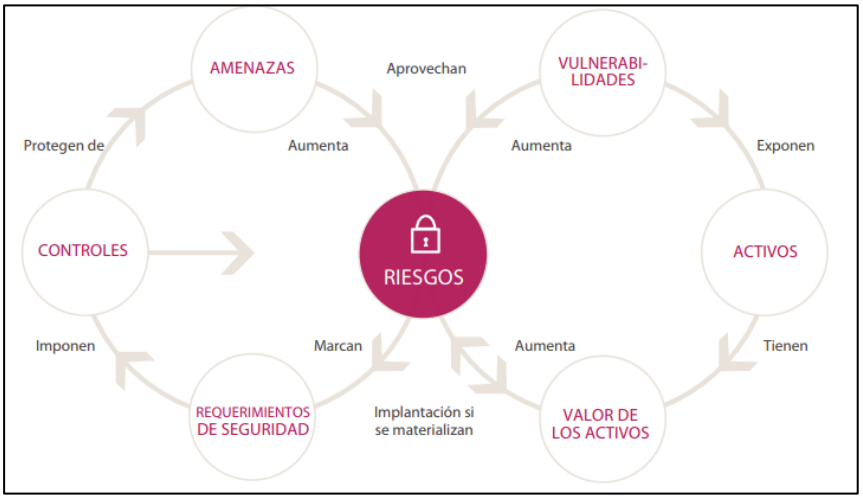
- **Adware**: Muestra publicidad, generalmente está relacionado con los espías, los que suelen conectar algún servidor remoto para enviar peticiones de información recopilada y recibir publicidad.
- **Bloqueador**: Incide la ejecución de determinados programas o aplicaciones, también puede bloquear el acceso a internet.
- **Bomba lógica**: Programa o parte de un programa que se instala en un ordenador y no se ejecuta hasta que cumpla una condición determinada.
- **Bulo**: Mensaje electrónico enviado por un conocido que intenta hacer creer al destinatario algo que es falso, como alertar de virus inexistentes, noticias con contenido engañoso.
- **Espía**: Roba información del equipo para enviarla a un servidor remoto. El tipo de información obtenida varía según el tipo de espía.

- **Exploit:** Tipo de software que se aprovecha de un agujero o de una vulnerabilidad en el sistema de un usuario para tener el acceso desautorizado al sistema.

8.6. Hacking Ético

La aplicación de hacking ético o procesos de test de penetración, es considerado un procedimiento de ciberseguridad orientada a una puesta en práctica de ataques reales para poder filtrar información de gran relevancia tanto bajo un sistema informático propietario o en una red de datos vulnerada, siempre y cuando basándose al consentimiento de los involucrados. La aplicación de hacking ético en la actualidad es de gran importancia permitiendo detectar vulnerabilidades tanto en hardware como en software en una determinada compañía entenderá la necesidad en seguridad que afronta y así le permitirá mejorar sus sistemas según lo que requieran (Costas, 2014).

Gráfico 7: Etapas del Hacking Ético



Fuente: Pedraza, fases del hacking ético **(**2014**)**

8.6.1. Hackers

Hacker no define a una persona o grupo de personas que usa su alcance basado en conocimientos sólidos para implementarlos del lado del bien o del mal, por ello el término se encuentra segmentado en tres tipos:

- **Sombrero blanco:** derivados también por parte del hacking ético, son considerados profesionales con amplio conocimiento técnico de seguridad informática lo cual realizan test de penetración tanto en hardware como en software para buscar brechas de seguridad vulnerables y así aplicar metodologías de seguridad bajo el consentimiento de una entidad.

- **Sombrero negro:** profesional opuesto al hacker de sombrero blanco, su denominación es de crackers y no laboran en base a una entidad, buscan causar daño en la extracción y robo de la información para fines personales o entrega a un tercero.
- **Sombrero gris:** terminología ambigua en la actualidad, pero se consideran un hibrido entre hackers de sombrero blanco y sombrero negro.

8.6.2. Etapas del hacking

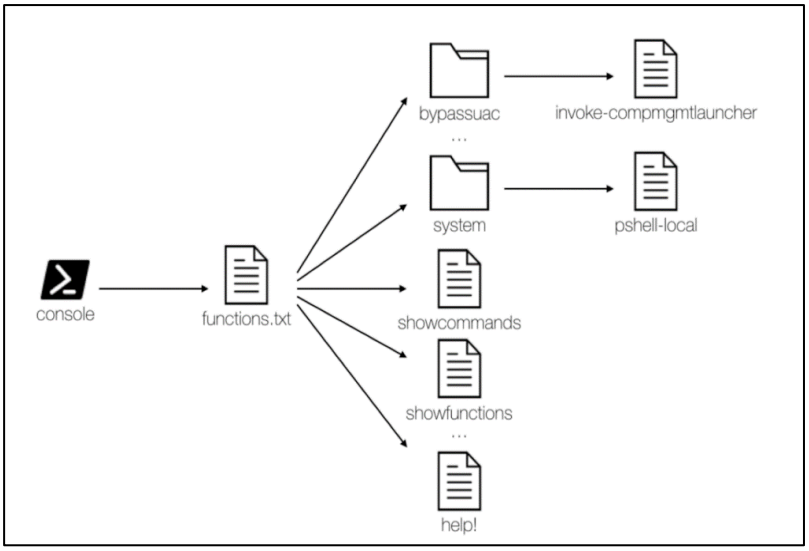
El hacking ético deriva de varias etapas para su aplicación, estas se definen en una serie de pasos dependiendo de las metodologías que se apliquen en una investigación direccionada al análisis y vulneración de información (Costas, 2014).

- **Recopilación de la información:** Se refiere a la fase de preparación en la que se busca detectar toda la información esencial y precisa del objetivo, esto dependerá de la metodología y estrategia aplicada.
- **Enumeración de información;** Mediante esta etapa se compila la indagación obtenida en la fase anterior de la "recopilación de la información" lo que permite la detección de equipos de manera activa, rangos de IP, sistemas operativos y software de gestión de información.
- **Análisis de información:** Se basa en la aplicación del modelo en arquitectura de servicios y aplicaciones mediante la identificación de fallas detectadas.
- **Explotación:** Centralizado en la detección de exploits, aplicando herramientas de ataque y penetración de vulnerabilidades y fallas encontradas, esta fase pretende demostrar la materialización de una amenaza.
- **Documentación:** Generar informe técnico al ejecutivo donde se aplicó seguridad informática.

8.7. Pentesting

Pentest o más conocido como pentesting hace referencia a los ataques simulados y autorizados hacia un objetivo informático, esto permitirá la aplicación de evaluaciones tanto de un sistema de información o redes de datos. Durante la aplicación de pentesting se identifica las vulnerabilidades de la exploración de información con fines maliciosos, permitiendo así que el pentester realice la aplicación orientada a la evaluación de riesgos en una dicha actividad y así poder sugerir medidas correctivas orientadas a la seguridad informática (Guillen, 2017).

Gráfico 8: Arquitectura del Pentesting



Fuente: Pedraza, fases del hacking ético **(**2014**)**

8.7.1. Tipos de Pentesting

Dentro de los procedimientos de pentesting para los procesos de detección de vulneraciones tanto en software conocidos como los sistemas de gestión de información o evaluar las redes de datos existen pentest más utilizados:

- **Pentest caja negra:** Se basa en recopilar en menor información recaudada, no se establece conocimientos de arquitectura a cuál atacar, sin embargo, esta tiene que recopilar previa información sobre el objetivo.
- **Pentest caja blanca:** Al contrario, mencionado anteriormente, este tipo de pentest se basará en la proporcionalidad mayor de información posible recolectada sobre el objetivo atacar, pueden ser en entornos de aplicativos móviles, sistemas operativos, redes de datos, infraestructura de comunicaciones.
- **Pentest caja gris:** Este tipo de pentest tiene una pequeña fracción o limitada información proporcionada ante el ataque de un objetivo mediante detalles internos.

8.7.2. ISSAF (Information Systems Security Framework)

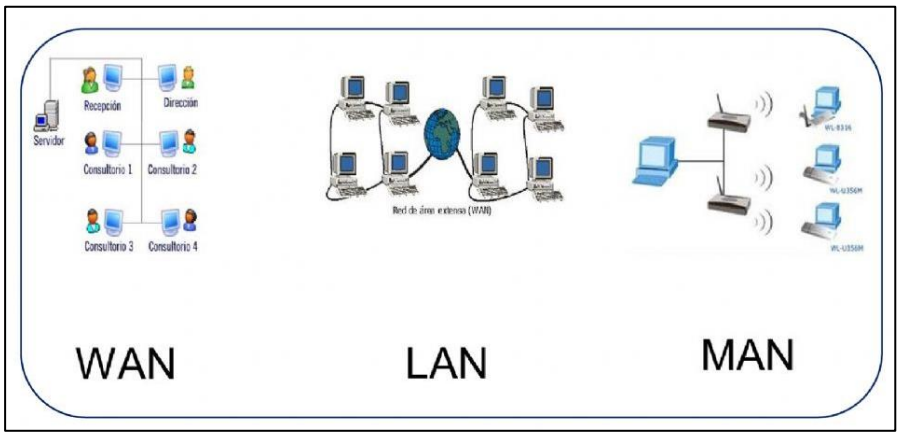
El objetivo de esta metodología es proporcionar elementos de manera minuciosa para el análisis de comprobación en base a la información de los sistemas de gestión en una situación. Las redes de datos cumplen el rol de conectar computadoras entre puntos de conexión, lo cual requiere de requerimientos a cumplir de manera óptima, estos son

sistemas formados por múltiples equipos que se enlazan por medio de comunicaciones, estas pueden ser conexiones de cable LAN, señal de radio y fibra óptica (Ayala, 2016).

8.7.3. Tipos de redes de datos

- Red de área local (LAN)
- Red de área extendida (MAN)
- Red de área amplia (WAN)
- Red de área Personal (PAN)

Gráfico 9: Tipo de redes de datos



Fuente: Pedraza, fases del hacking ético **(**2014**)**

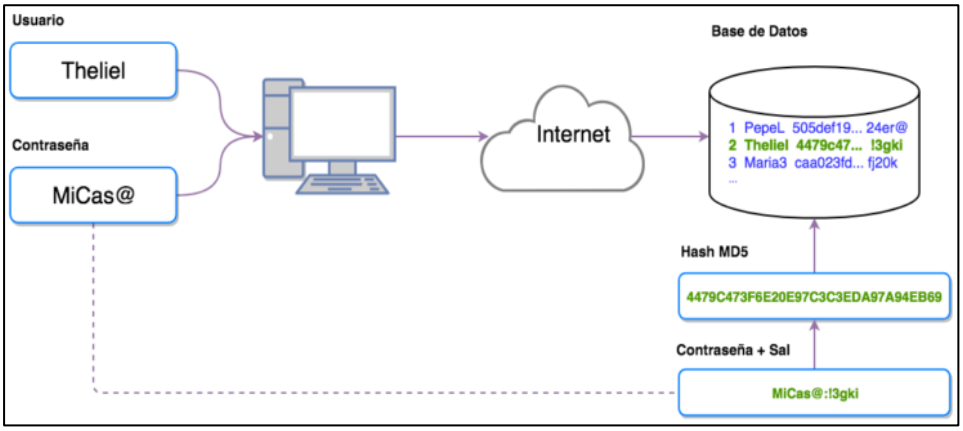
8.7.4. Seguridad lógica

La seguridad lógica hace referencia a la aplicación de barreras y procedimientos que realice resguardo de información confidencial en el acceso a los mismos, solo está permitido al acceso a personal autorizado para su manipulación y estos están distribuidos mediante controles en base a roles de la seguridad lógica (Guillen, 2017).

- **Roles:** Se lo realiza controlando a través de una función específica asignada a un usuario a dicho acceso mediante una regla de validación.
- **Control de acceso:** Se refiere a la implementación de dicho control unitario en base a una red para mantener la integridad de una información almacenada en una infraestructura de redes y estos resguardan los datos confidenciales no autorizados hacia terceros.
- **Autenticación:** Identifica el acceso mediante las reglas de validación permitiendo o denegando el acceso a un sistema de información o ejecuciones de configuración mediante identificación de usuario.

- **Limitación en servicios:** Los controles se refieren a las reglas basadas en una restricción de parámetros propios en la aplicación o pre configurados por parte del administrador.

Gráfico 10: Arquitectura de la seguridad lógica en redes



Fuente: SmartCity, sistema de seguridad y administración de eventos (2019)

8.7.5. Seguridad física

La seguridad física no es imprescindible al momento de diseñar un esquema en la aplicación de las redes de datos, pero sin embargo es un punto importante a destacar, permitiendo la implementación de barreras en los procedimientos de control como las medidas preventivas y contramedidas ante los ataques y obtención de manera ilegal de información confidencial en base a componentes o controles de acceso físico tangibles de una organización (Guillen, 2017).

8.7.6. Amenazas direccionadas a la seguridad física

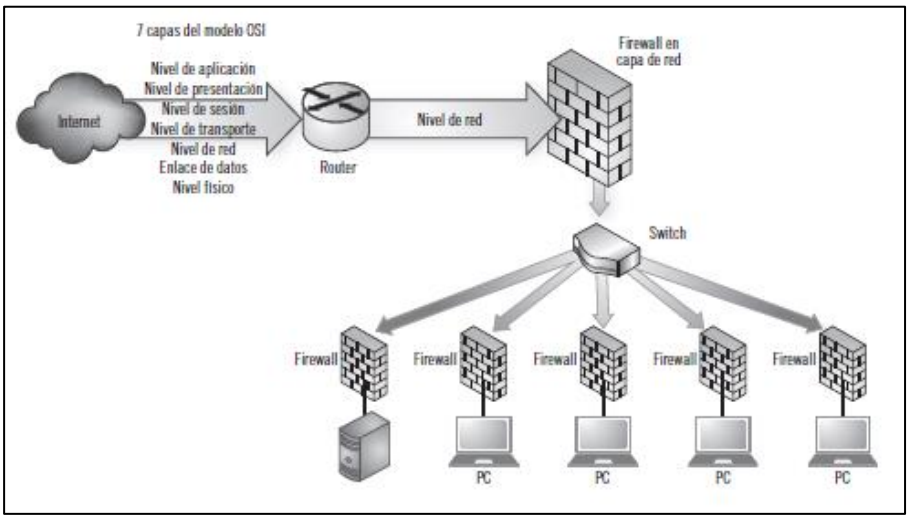
- **Momentos fortuitos:** Terremotos, inundaciones, tormentas eléctricas.
- **Manipulación por el hombre:** Robos de documentos, demoliciones, accesos a departamentos sin previa autorización, incendios.

8.8. Firewall como herramienta de seguridad

El servicio de firewall hace mención a la analogía de “Pared”, o dispositivo que evita la propagación del fuego. El objetivo del firewall es proteger ante ataques a computadoras tanto personales como corporativas conectadas a una red, estos ataques se dan mediante software malicioso debido a la falta de control en la manipulación en las instalaciones de programas de terceros y exceso de tráfico en la red. El firewall se puede configurar para aplicar un bloqueo proveniente de ataques de diferentes sitios, realizando así una barrera

protectora ante la sustracción de información importante de una organización (Guillen, 2017).

Gráfico 11: Arquitectura de Firewall en las capas de red



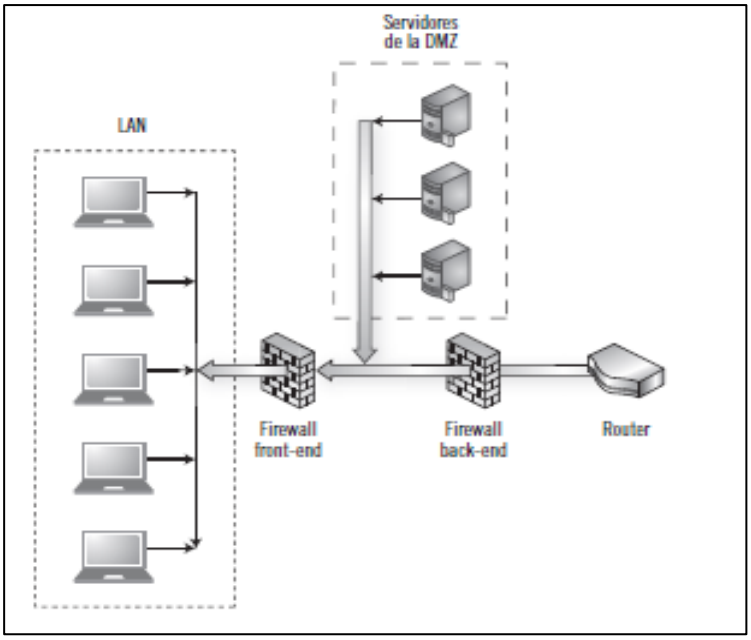
Fuente: SmartCity, sistema de seguridad y administración de eventos (2019)

Considerar que una empresa al momento que aplica seguridad informática a su red de datos, tiene que considerar la regla operacional del firewall para que así permita las debidas conexiones correspondientes, sea para aprobación o rechazo de solicitud.

8.8.1. Tipos de firewall

- **Nivel de aplicación en pasarela:** El nivel de aplicación en pasarela proporciona mecanismos de seguridad basadas en telecomunicaciones, son protocolos de tipo TELNET que permiten la funcionalidad de una administración remota, lo que es posible realizar determinada acción a ejecutar, como el chequeo de todas las computadoras conectadas a una misma red de datos para el análisis e identificación de intrusión o de cualquier tipo, al aplicar el nivel de tipo pasarela se debe contar como requisito software especial para gestionar las conexiones.
- **Circuito a nivel de pasarela:** Este tipo de firewall solo realiza el bloque y la protección de una sola máquina mediante una red interna, se puede detectar de manera más eficiente los intrusos provenientes de otras redes; lo que se aplica un filtrado de paquetes de datos que son enviados por internet en base al apoyo de un hardware de red dedicada.
- **Zona desmilitarizada:** Constituye en una brecha de seguridad orientada a una red interna, permitiendo así el enlace de dos redes mediante el paquete de datos donde se podrá aplicar barreras de prevención en los servidores de correo electrónico y conexión a internet mediante DNS (Domain Name System).

Gráfico 12: Tipos de Firewall



Fuente: SmartCity, sistema de seguridad y administración de eventos (2019)

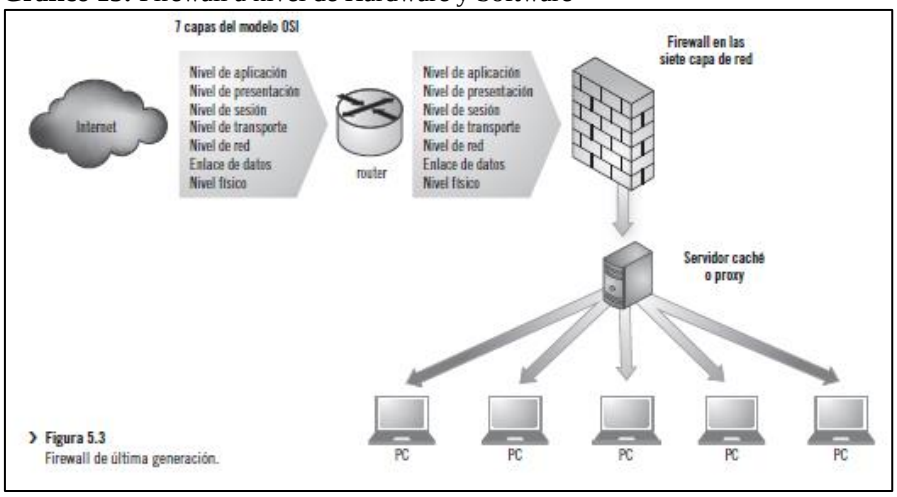
8.8.2. Firewall de software y hardware

Las amenazas que se encuentran en la actualidad provienen del internet, especialmente la técnica de ataques hacia el objetivo por parte de los hackers, estos ataques mencionados pueden disminuir mediante la aplicación de un firewall lo que resultará útil para mediana y grandes empresas, aunque si esté implementado firewall mediante hardware.

Los firewalls orientados al hardware son conocidos como routers de banda ancha para la navegación de internet, lo cual cuenta con mínimo de 4 puertos que no requieren de una configuración inicial para la conexión a otros puertos. La función del firewall mediante hardware permitirá filtrar los paquetes de datos, mediante un examen exhaustivo de números establecidos en una IP del paquete, con el propósito de observar su origen y destino, lo que nos permitirá compartir información con grupos definidos mediante reglas acceso lo cual el paquete será aprobado o rechazado, recalcar que los firewalls basados en hardware poseen de más elementos para la protección de computadoras conectadas a una red de datos.

Sin embargo, si realiza la implementación de un firewall mediante software, se encuentra en la probabilidad que fuerce al usuario que ya tiene definido las reglas de acceso para tomar las decisiones para el permiso de paquetes, cuando en la realidad debería negarlo o validar cuando se muestra una señal de alarma en pantalla (Guillen, 2017).

Gráfico 13: Firewall a nivel de Hardware y Software



Fuente: SmartCity, sistema de seguridad y administración de eventos (2019)

9. HERRAMIENTAS DE DESARROLLO

9.1. Virtual Box

Virtual Box es un software propietario de la empresa ORACLE lo que permite emular varias máquinas de tecnologías de virtualización mediante sistemas operativos, esto quiere decir que si un usuario necesita montar un sistema operativo dentro de una máquina anfitrión o física lo que puede ejecutar siempre y cuando cumpla con los requerimientos de virtualización (Fernández, 2020).

9.2. Kali Linux

Kali Linux es un sistema operativo mediante la distribución libre GNU/Linux, orientada a la seguridad informática permitiendo realizar mediante sus herramientas técnicas de penetración en la detección y evaluación de vulnerabilidades tanto en sistemas de información como en redes de datos (Rubén, 2016).

9.3. Nmap

Network Mapper, de la abreviatura Nmap es una herramienta de código libre basada en la distribución de Kali Linux lo cual sirve para para exploración de vulnerabilidades y detección de redes de datos, lo que permite a los administrados identificar qué dispositivos se ejecutan dentro de una línea de comunicación mediante la disponibilidad de los hosts activos y servicios que ofrecen los mismos cual permitirá observar y encontrar puertos abiertos y detectar los riesgos de seguridad. Nmap puede ser ejecutado y orientado para monitorear no solo puertos de gran alcance sino más bien se aplica para

el monitoreo de host individuales que acceden a miles de dispositivos y multitudes de subredes.

9.3.1. Uso de Nmap

Mediante la herramienta de código libre podemos utilizar como parte de la monitorización de redes, exploits y escáner de vulnerabilidades de código, permitiendo que destaque dentro de los departamentos de IT y de redes que necesitan conocer su accesibilidad y potencia (De la Fuente, 2018).

- **Mapeo de red:** Identifica los dispositivos anclados a una misma red mediante un host, incluyendo servidores, enrutador y conmutadores conectados de manera física.
- **Identificación y detección de S.O:** Puede detectar sistemas operativos que se ejecutan en segundo plano mediante un dispositivo de red, proporcionando así el nombre de un proveedor en base a la actividad y estimación de tiempo de un dispositivo.
- **Detección de servicios:** Identifica la actividad de un servidor de correo electrónico, aplicaciones o DNS (Domain Name System).
- **Análisis orientado a la seguridad informática:** La herramienta NMAP permite indagar sobre los versionamientos de los sistemas operativos que se ejecutan mediante la entrada de un host, permitiendo así que los administradores de red reciban alertas de vulnerabilidades en canales con fallas específicas.

9.4. Traceroute

Tracert o Traceroute es una herramienta conocida orientada a la manipulación mediante consola lo cual recibe el soporte de GNU/Linux. La finalidad de Traceroute es trazar la ruta de un paquete de datos a una red entrante, lo cual viene navegando directamente desde un host o punto de red hasta un ordenador, a su vez esta herramienta nos permite realizar diagnósticos de red cuando se envía paquetes mediante estadísticas RTT o latencia de red mediante la dirección IP hasta llegar a destino (Fernández, 2020).

9.5. Whois

Whois basado en Linux es un directorio de servicio gratuito de acceso que contiene información técnica de datos y registros del titular de dominio previamente registrado. Esto permite que whois recopile la información necesaria lo que se encargará de recopilar

y tenerlas actualizadas a disposición de quien solicite dicha información (Espinoza, 2019).

Tener en cuenta que la herramienta Whois como servicio consiste en que el cliente, tanto como servidores, repositorios de datos se utilizan términos y condiciones lo cual se mencionan a continuación:

- **Recaudación de información:** Al momento de registrar un nombre de dominio o dirección IP estos datos son recopilados mediante el servicio de Whois con consentimiento del involucrado.
- **Protocolo:** Se refiere al documento RFC 3912 que define la estandarización de protocolos de red mediante Whois.
- **Protocolo al acceso de datos:** Se definen como el registro de dominio DNRD-AP mediante los elementos de comunicación e intercambio de acceso a un determinado registro.
- **Servicio de directorio de datos:** El directorio de datos hace referencia a los ISP que usan el servicio de Whois responsables del funcionamiento de una red o dominio de internet.

9.6. Dig

Domain Information Groper es una herramienta basada en Linux de código libre, lo cual se hace uso mediante terminal y comandos permitiendo así la búsqueda de registros de DNS (Domain Name System) a través de nombre de servidores previamente configurados, de esta forma se envía la consulta DNS a los nombres de servidores mediante un listado de archivo a resolver específicamente (Deyimar, 2020).

10. HIPÓTESIS

La instalación de recursos orientados a la seguridad informática en la aplicación evaluativa para las redes de datos brinda como resultado de la detección de manera preventiva ante ataques de sustracción de la información, lo cual es importante establecer barreras de protección de manera adecuada mediante la monitorización de eventos de una red de comunicación.

11. METODOLOGÍAS Y DISEÑO EXPERIMENTAL

11.1. Métodos De Investigación

11.1.1. Método Documental

La metodología documental nos permite aplicar en el proceso de la investigación la obtener de recursos de información mediante citas bibliográficas, artículos y revistas sobre el tema "Seguridad informática mediante hacking ético en la aplicación de pentesting para el análisis de vulnerabilidades en las redes de datos de la cooperativa sierra centro sucursal La Maná, provincia de Cotopaxi.", el uso de esta metodología de investigación permitirá fundamentar de manera técnica la definición de herramientas a utilizar, partiendo desde el análisis y presentación de los objetivos planteados.

11.1.2. Método analítico sintético

El método analítico sintético permite a las investigadoras mantener la veracidad de los hechos, en base a las partes y elementos para observar el origen de la investigación, como la aplicación de pentesting basada en las normas estandarizadas ISO, la evaluación de las redes de datos, aplicación de seguridad informática para la prevención de ataques de información confidencial tanto en hardware como en software. El estudio dirigido a la seguridad informática y la aplicación de hacking ético permitirá obtener conocimientos en la aplicación del desarrollo del proyecto de investigación.

11.1.3. Método deductivo

La aplicación del método investigativo deductivo específica la propuesta basada en los elementos sobre el tema "Seguridad informática mediante hacking ético en la aplicación de pentesting para el análisis de vulnerabilidades en las redes de datos de la cooperativa sierra centro sucursal La Maná, provincia de Cotopaxi.", permite en base a la problemática de la investigación recolectar las conclusiones y recomendaciones, basándose en los resultados de la entrevista de manera concisa y útil para el desarrollo del proyecto.

11.2. Tipos de Investigación

11.2.1. Investigación Bibliográfica

La aplicación de la investigación bibliográfica es de suma importancia, permitirá tener de manera concisa las bases teóricas por las autoras de la investigación en referencia a la

propuesta planteada, lo que permite la obtención de los elementos sobre el tema "Seguridad informática mediante hacking ético en la aplicación de pentesting para el análisis de vulnerabilidades en las redes de datos de la cooperativa sierra centro sucursal La Maná, provincia de Cotopaxi.", esta investigación es amparada en base a las citas bibliográficas de revistas, artículos y sitios web, lo que permitirá establecer la fundamentación teórica del caso de estudio a desarrollar.

11.2.2. Investigación Aplicada

El desarrollo de la propuesta sobre el tema "Seguridad informática mediante hacking ético en la aplicación de pentesting para el análisis de vulnerabilidades en las redes de datos de la cooperativa sierra centro sucursal La Maná, provincia de Cotopaxi.", mediante especificaciones técnicas de herramientas como entornos de desarrollo, Frameworks, API , y software libre, como resultado obtendremos un test de penetración correcto e informe técnico detallando posibles problemas dentro de las redes de datos de la Cooperativa de ahorro y crédito Sierra Centro del Cantón La Maná, Provincia de Cotopaxi.

11.3. Técnica de Investigación

11.3.1. Entrevista

Mediante esta técnica se recopila información de relevancia en el desarrollo de un cuestionario elaborado por los investigadores para el progreso de la conversación al entrevistado y conocer su apreciación en base a la aplicación y evaluación de las redes de datos mediante la aplicación de pentesting en la cooperativa Sierra Centro. La entrevista consistió en conocer la opinión del Ing. Wilmer Alcaciega Guanín, gerente de la sucursal que se encuentra ubicada en el cantón La Maná, esto es necesario para recopilar información de relevancia sobre el control de información de la entidad.

11.3.2. Encuesta

La aplicación de la encuesta como técnica de investigación permite obtener la información de varias personas a encuestar, mediante un anexo de preguntas que se entregan a la persona y lo cual debe de responder. Esta técnica recopiló información del personal laboral de la cooperativa Sierra Centro, sucursal La Maná, sobre la influencia de la seguridad informática y cómo prevenir futuros ataques a la información. La redacción de las preguntas tiene que ser correctamente estructuradas con el fin de obtener información necesaria para el desarrollo de la investigación.

11.4. Población y muestra

11.4.1. Población

Se procesaron los cálculos de la muestra a las personas que pertenecen a la cooperativa de ahorro y crédito Sierra Centro. Para el procesamiento y análisis de los datos proporcionados por la entidad privada, se consideró la información y necesidades que se requiere ante la evaluación en las redes de datos orientada en la seguridad informática.

Tabla 4: Población

Indicador	Población
Atención al Cliente	27
Asesores de Créditos	25
Departamento de Sistemas	7
Asesores de Inversiones	18
Gerente de Sucursales	8
Secretaria	11
Consejo de Administración	9
TOTAL	**105**

Fuente: Elaborado por las Investigadoras

11.4.2. Muestra

Para definir el tamaño de la muestra aplicamos muestreo aleatorio que reside en dividir la población en estratos, es necesario realizar la aplicación de la fórmula para la obtención de resultados.

Cálculo de la muestra de la Cooperativa de ahorro y crédito SIERRA CENTRO ubicada en el Cantón la Maná, Provincia del Cotopaxi.

Fórmula N°1. Muestra

$$n = \frac{N}{(E)^2 (N-1) + 1}$$

Datos

n = Tamaño de la muestra =?

N = Población a investigarse = 105

E = Índice de error máximo admisible = 0,05

Desarrollo

$$n = \frac{105}{(0,05)^2 (105-1) + 1}$$

$$n = \frac{105}{(0,0025)\ (118) + 1}$$

$$n = \frac{105}{1.29}$$

$$n = 81$$

Realizado los cálculos, se obtendrá una muestra de 81 personas, lo cual son empleados que pertenecen a la cooperativa de ahorro y crédito SIERRA CENTRO, tomando una población de 105 personas al azar que ejercen varias labores financieras y ejecutivas dentro de la entidad privada.

11.4.3. Distribución de la muestra

En la distribución de la muestra se aplicará la fórmula del coeficiente de proporcionalidad, lo cual nos permitirá conocer con más detalle cada uno de los elementos y estratos de clasificación o grupos.

Fórmula N°2. Índice de proporcionalidad de la Cooperativa SIERRA CENTRO.

$$\mathbf{f = \frac{n}{N}} \qquad \mathbf{f = \frac{81}{105}} \qquad f = 0,77142857$$

Tabla 5: Segmentación de la encuesta

SEGMENTACIÓN	CANTIDAD	índice	CANTIDAD
Atención al Cliente	27	0,7714	14
Asesores de Créditos	25	0,7714	23
Departamento de Sistemas	7	0,7714	6
Asesores de Inversiones	18	0,7714	12
Gerente de Sucursales	8	0,7714	8
Secretaria	11	0,7714	9
Consejo de Administración	9	0,7714	8
TOTAL	**105**	0,7714	**81**

Fuente: Elaborado por las Investigadoras

11.4.4. Antecedente de la cooperativa de Ahorro y Crédito Sierra Centro

La Cooperativa de Ahorro y Crédito Sierra Centro Ltda., es una entidad dedicada a la intermediación financiera que nace hace 12 años, mediante Acuerdo Ministerial N° 022-09; un 04 de diciembre del 2009, calificada por la Superintendencia de Economía Popular y Solidaria Resolución N° ROEPS-000718; con la iniciativa de un grupo de jóvenes socios fundadores indígenas y mestizos de la sierra centro del país de las provincias de Tungurahua y Cotopaxi.

La cooperativa nace con la iniciativa de 19 jóvenes socios fundadores tanto de la provincia de Tungurahua y Cotopaxi, conformado entre indígenas y mestizos. Como respuesta a la necesidad de conceder créditos a personas de escasos recursos económicos que no tienen acceso al crédito de la banca privada.

La finalidad del ente financiero es la prestación de servicios en la captación de recursos financieros crediticios destinados a micro empresas, dando confianza y seguridad para el aporte al desarrollo social y económico de sus socios y clientes, convirtiéndose así en un modelo de crecimiento moderado en el sector financiero.

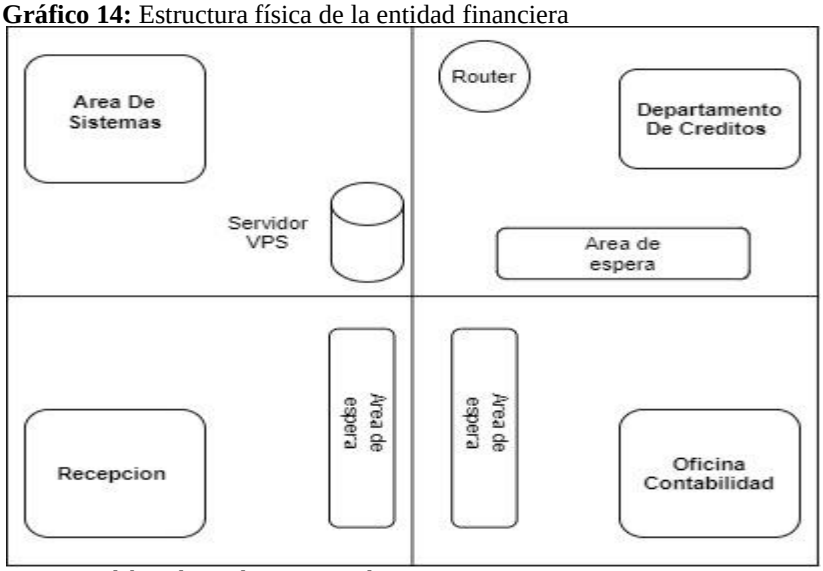
11.4.5. Infraestructura Física de la Cooperativa

La cooperativa sierra centro sucursal la maná, cuenta con una planta baja y en su edificación se comunican por secciones divididas en oficinas.

- La ubicación de la infraestructura física de la cooperativa es planta baja junto con sus oficinas.
- Existen departamentos desde la oficina de gerencia hasta atención al cliente.
- Se encuentran a disposición las oficinas de caja para la recepción del dinero.
- Existe una oficina del área de Tics e informática.

Los servidores implementados son de tipo VPS, lo cual hace referencia que este tipo de comunicación se basa en entornos virtuales mediante la compartición de un servidor en nube, lo cual hace una simulación para que todo funcione como un servidor físico.

Gráfico 14: Estructura física de la entidad financiera

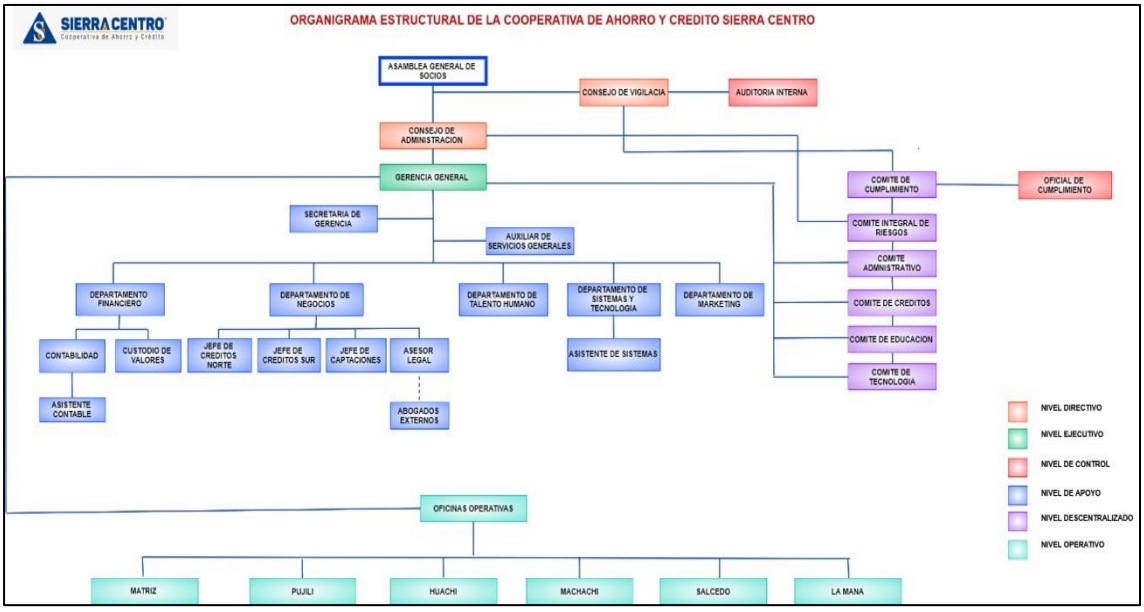


Fuente: Elaborado por las Investigadoras

11.4.6. Organigrama Estructural de la cooperativa

Una vez establecida la revisión y funcionamiento de la infraestructura física de la cooperativa de ahorro y crédito Sierra Centro, hay que recordar que esta se basa en un organigrama de las actividades que se realizan, por lo tanto, se ha sintetizado la estructura organizacional de la entidad.

Gráfico 15: Organigrama institucional



Fuente: Cooperativa de ahorro y crédito Sierra Centro

Identificado el organigrama institucional de la cooperativa con sus respectivas funciones que se asigna a cada departamento, se procede aplicar las gestiones de seguridad en base al análisis que se realice a las redes de datos en la protección la información, lo cual está enfocado a la red de datos de la Cooperativa de ahorro y crédito Sierra Centro. Esto

conlleva a instaurar políticas para mejorar las prácticas en la utilización de la red y de todos los recursos compartidos que interactúan entre sí.

11.4.7. Análisis de la red de datos de la cooperativa de ahorro y crédito Sierra Centro

Dentro de los análisis de red en una entidad, se debe considerar en cómo se detalla la infraestructura de red y sus componentes LAN como recursos activos, con la información que se obtuvo en colaboración con los encargados de los departamentos técnicos nos detallaron los recursos de red que se utilizan en la actualidad en la cooperativa SIERRA CENTRO SUCURSAL LA MANÁ, PROVINCIA DE COTOPAXI, con lo detallado se podrá hacer una análisis de la estructura LAN de la entidad financiera sobre la situación actual que presenta las redes de datos en base al margen de la seguridad informática; para poder así determinar las causantes que se detecten en dicha red de comunicación y de qué manera se procederá a implementar la seguridad informática.

11.4.8. Estructura LAN de la Cooperativa

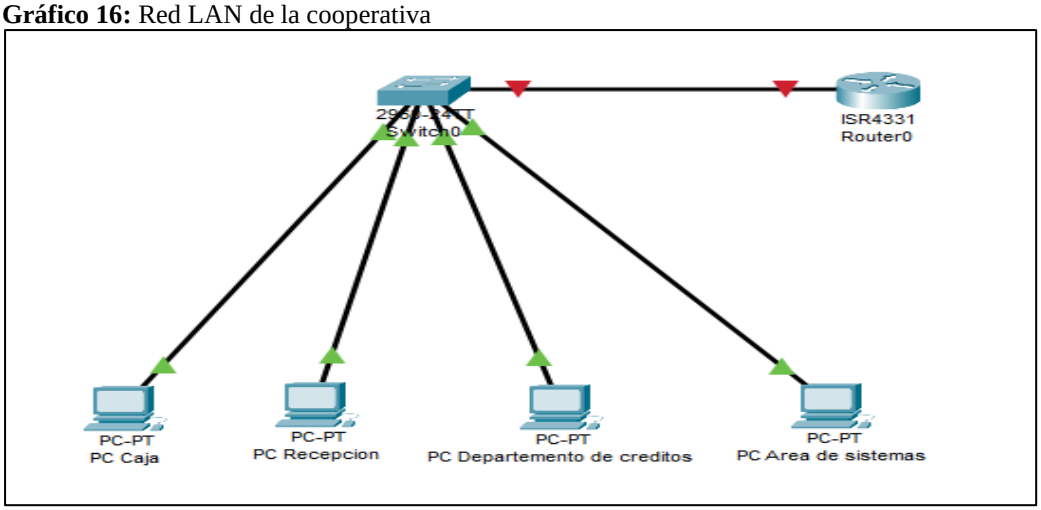
La infraestructura de la cooperativa SIERRA CENTRO SUCURSAL LA MANÁ, PROVINCIA DE COTOPAXI está conformada por los siguientes activos tecnológicos que se muestran a continuación:

Tabla 6: Recursos y activos tecnológicos

Activos de recursos tecnológicos	Tipo de activos tecnológicos	Número de elementos
Servidor virtual (VPS)	Servicios Cloud	1
Máquina Virtual	Servicio	2
Dominios	Servicio	2
Nodos en la red	Servicio	8
Equipos Windows 10	Servicio	12
Equipo portátil	Servicio	4
Router	Comunicación	8
Firewall Lógico	Comunicación	0
IDS	Comunicación	0
Página web	Comunicación	2
Servidor DBA	Comunicación	1
Conexiones a internet	Comunicación	1
VPN interna	Comunicación	1
Cámara de vigilancia	Vigilancia	8
Antispam para correos	Comunicación	0

Fuente: Elaborado por Sierra Centro

Gráfico 16: Red LAN de la cooperativa



Fuente: Elaborado por las Investigadoras

11.4.9. Detalle de servidor para las comunicaciones de la entidad financiera

La entidad para su proceso comunicacional cuenta con servidores de tipo VPS, lo cual es una infraestructura en nube privada para la automatización de información y acceso para el área de sistemas, detallando sus características a continuación:

- Servidor Cloud VPS Hostinger
- Memoria RAM 8GB DDR 5
- VCPU de 8 núcleos
- Sistema operativo Linux
- Almacenamiento de 1TB SSD
- Hosting de tipo compartido

11.4.10. Estaciones de trabajo

Las estaciones de trabajo de la cooperativa de ahorro y crédito Sierra Centro cuentan con varios elementos de diferentes características han sido obtenidas en la actualidad. La red LAN no cuenta con mecanismos de seguridad para evitar futuros ataques en la extracción de información, para así llevar el monitoreo y seguridad de la red de datos.

11.4.11. Estructura WAN de la cooperativa

La cooperativa de ahorro y crédito SIERRA CENTRO SUCURSAL LA MANÁ, PROVINCIA DE COTOPAXI, cuenta con dos puertas de enlace, la primera establece la conexión que emite el proveedor de internet; la segunda emite la conexión de la matriz con la sucursal en base a la trasmisión de datos, tanto del sistema virtual de clientes como sus enlaces a páginas web que utilizan.

Tabla 7: Puertas de enlace en Red

Entidad Financiera	Ancho de banda	Tipo	WAN	LAN
SIERRA CENTRO SUCURSAL LA MANÁ, PROVINCIA DE COTOPAXI	4028 kbps	Fibra Óptica	186.2.60.38	186.3.44.97/28
SIERRA CENTRO SUCURSAL PUJILÍ, PROVINCIA DE COTOPAXI	4028 kbps	Antena de radio enlace	101.23.150.146	192.169.0.198/29
SIERRA CENTRO SUCURSAL LATACUNGA, PROVINCIA DE COTOPAXI	1024 kbps	Antena de radio enlace	10.25.150.147	186.168.2.199/24
SIERRA CENTRO SUCURSAL SALCEDO, PROVINCIA DE COTOPAXI	4028 kbps	Fibra Óptica	10.23.155.148	192.169.2.199/24

Fuente: Elaborado por las Investigadoras

12. ANÁLISIS Y DISCUSIÓN DE LOS RESULTADOS

Tabla 8: Personas que intervienen el proceso de investigación

Agente	Funciones	Técnicas, espacios y distribución	Población	Muestra
Tutor	Guía	Técnica experimental	1	1
Estudiantes	Investigadores	Ejecutores del proyecto	2	2
Gerente de la entidad financiera	Finanzas	Entrevista	1	1
Empleados	Suministra información	Encuesta	105	81

Fuente: Elaborado por las Investigadoras

12.1. Resultados de la entrevista Aplicada

Mediante la entrevista realizada se obtuvo los siguientes datos:

La entrevista se realizó al Ing. Wilmer Alcaciega Guanín, gerente de la cooperativa de ahorro y crédito Sierra Centro quien brindó la información necesaria y fundamental para

el desarrollo de la propuesta del proyecto de investigación con el título "SEGURIDAD INFORMÁTICA MEDIANTE HACKING ÉTICO EN LA APLICACIÓN DE PENTESTING PARA EL ANÁLISIS DE VULNERABILIDADES EN LAS REDES DE DATOS DE LA COOPERATIVA SIERRA CENTRO SUCURSAL LA MANÁ, PROVINCIA DE COTOPAXI".

La entrevista permitió preparar previamente las preguntas que se establecieron para conocer así los antecedentes y problemas que afectan a las redes de datos hoy en día sin la prevención de seguridad a nivel informático.

12.2. Resultados de la encuesta Aplicada

Proceso de tabulación de la información en base a la encuesta dirigida a los directivos y personal de la entidad financiera SIERRA CENTRO SUCURSAL LA MANÁ, PROVINCIA DE COTOPAXI.

Tabla 9: Resultados de la encuesta aplicada

Pregunta	Resultado	Análisis	Interpretación
1.- ¿Es necesario implementar mecanismos de seguridad informática para evitar futuros ataques en la extracción de información financiera?	Si 65% No 35%	65% está de acuerdo en la implementación de mecanismos de seguridad informática, caso contrario del 35% que no está de acuerdo en su implementación.	Del 100% de la población encuestada el 65% cree necesario aplicar mecanismos de seguridad informática, el 35% no está de acuerdo en aplicar procedimientos de seguridad en las empresas financieras. Tras conocer los resultados esto refleja que la mayoría de la población encuestada está de acuerdo que se implemente soluciones que hagan referencia a la seguridad informática para evitar la extracción de información.
2.- ¿Ha escuchado mencionar sobre los ataques informáticos que se dan hoy en día a las entidades bancarias mediante técnicas de extracción de información por terceros?	Si 85% No 15%	85% ha escuchado mencionar sobre los ataques suscitados ante las entidades financieras en la actualidad, el 15% desconoce el tema sobre ataques informáticos.	Del 100% de la población encuestada el 60% tiene conocimientos sobre los ataques informáticos en las entidades financieras privadas, mientras que el 32% manifiesta que no ha escuchado mencionar sobre aquello. Tras

			conocer los resultados esto refleja que la mayoría de la población encuestada tiene previo conocimiento o está al tanto de la gestión de la seguridad informática en las entidades financieras y cual importante es su implementación.
3.- ¿Cómo trabajador ha tenido experiencia en detectar fallas o avisos sobre ataques informáticos en la entidad?	Buena 20% Regular 23% Mala 49%	El 29% determina que su experiencia es buena haciendo referencia a la detección de fallas informáticas, el 23% manifiesta que regularmente pueden detectar aquella anomalía y el 49% desconoce sobre temas de seguridad informática, por lo tanto, su experiencia es mala.	Del 100% de la población encuestada el 20% menciona que su experiencia al detectar fallas informáticas fue buena; el 23% en la detección de vulnerabilidades de seguridad fue regular; mientras que el 49% manifiesta que su experiencia fue mala en la detección de ataques informáticos. Tras conocer los resultados esto refleja que existe un gran desconocimiento sobre la gestión de seguridad informática y protección tanto de información financiera como activos tecnológicos.
4.- ¿Conoce usted sobre la importancia de las redes de datos a nivel comunicacional en una entidad privada basadas en las normativas ISO 27001?	Si 20% No 80%	El 20% conoce sobre la importancia de una red datos en una entidad financiera, mientras tanto el 80% desconoce de su implementación.	Del 100% de la población encuestada el 20% menciona que, conoce la importancia de la aplicación de la normativa ISO como estándar mundial, el 80% no ha escuchado mencionar sobre las normas de estandarización. Tras conocer los resultados esto refleja que la mayoría de la población encuestada

			no tiene conocimiento en su totalidad sobre la implementación de las normativas ISO 27001 orientadas a las redes de datos.
5.- ¿Considera usted que se implemente seguridad informática a la red de datos de la cooperativa de ahorro y crédito sierra centro?	Si 80% No 20 %	El 80% considera que es importante la implementación de seguridad informática a la red de datos para las comunicaciones, mientras el 20% considera que no es importante la implementación de seguridad lógica.	Del 100% de la población encuestada el 80% menciona que es importante la implementación de seguridad informática en las redes de datos basándose en la aplicación de la normativa internación ISO 27001, mientras que el 20% manifiesta que no es necesario la aplicación de seguridad informática en las redes de datos de la cooperativa. Tras conocer los resultados esto refleja que la mayoría de la población encuestada entiende que es necesario implementar seguridad en las redes de datos para el análisis y evaluación de la misma.

Fuente: Elaborado por las Investigadoras

La tabulación de los resultados se encuentra detallados en el anexo 7.

13. DISEÑO DE LA PROPUESTA TÉCNICA

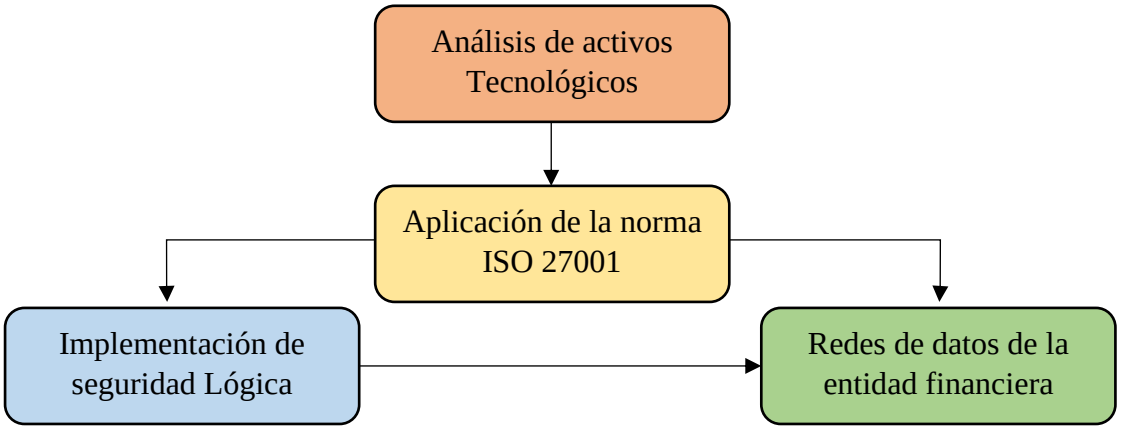
13.1. Mecanismos y contramedidas en seguridad informática

La seguridad informática debe contar con el respaldo de confianza a que los equipos donde se va a realizar la evaluación de las redes de datos tanto para envío y recepción de información deben estar correctamente asegurados, considerando así que la implementación de la seguridad de la información sea necesario que se base en normas internacionales y marcos legales internos como una guía correcta en la implementación de la seguridad lógica.

Tener en cuenta que toda institución financiera debe cumplir ciertas normas y estándares por lo cual estas regulan su funcionamiento. Dentro de los procesos tecnológicos deben

acatar normas basadas en ISO, permitiendo un conjunto de metodologías establecidas para el manejo de varios procesos dentro de una institución. Mediante los lineamientos de los mecanismos y contramedidas en seguridad informática basadas en normas ISO 27001 se realizará los procedimientos del diseño e implementación de la seguridad informática en la red de datos de la cooperativa SIERRA CENTRO SUCURSAL LA MANÁ, PROVINCIA DE COTOPAXI.

Figura 1: Medidas de seguridad informática



Fuente: Elaborado por las Investigadoras

13.1.1. Aplicación de norma ISO 27001 en la entidad financiera

La aplicación de la norma ISO 27001 como regulador, es proporcionar determinados modelos en la implementación tanto de operación, monitorización y mantenimiento; en este caso el uso de las redes de datos de la cooperativa SIERRA CENTRO SUCURSAL LA MANÁ, PROVINCIA DE COTOPAXI.

Haciendo referencia sobre la importancia de su implementación:

- Comprender los requerimientos que se deben tener al momento de aplicar seguridad informática en una institución.
- Operar controles y manejos de riesgos de la seguridad, tanto en áreas referidas que pueden ser físicas, ambientales y de recursos humanos.
- Monitorear y evaluar el desempeño de las redes de datos.

El propósito de la evaluación de una red de datos en base a normas ISO en la gestión de la seguridad de la información es, garantizar que los riesgos de la seguridad de información sean conocidos y asumidos por la entidad financiera de forma documentada en base a los resultados obtenidos por el examen de penetración (Pentesting).

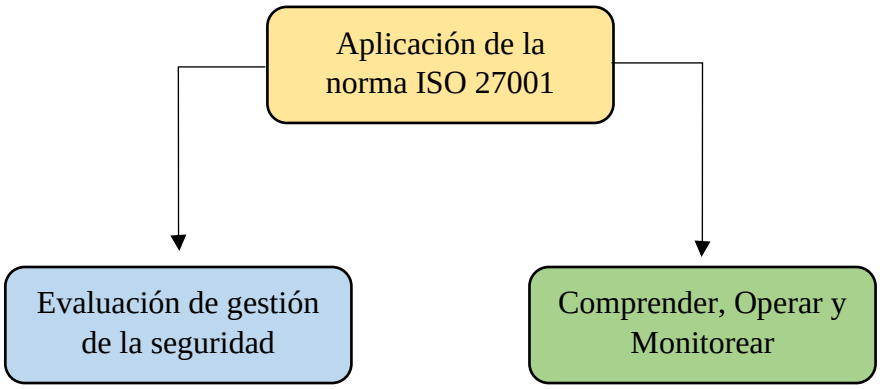
Para garantizar que la seguridad de la información de la organización es gestionada correctamente, se debe identificar los aspectos y ciclos de vida adoptados en base a las normativas ISO como son:

- **Confidencialidad:** La información no es expuesta a disposición de terceros, no es de conocimiento público ni revelada en procedimientos no autorizados.
- **Integridad:** Exactitud de la información y sus métodos de procesamiento de la misma.
- **Disponibilidad:** Acceso a la información y comunicación en la trasmisión de datos, que pueden estar disponibles en procesos autorizados cuando la entidad financiera lo requiera.

Para establecer y gestionar la red de datos en base a la información y normativa ISO 27001, se utiliza en ciclo de vida PDCA tradicional, implementado en los sistemas de gestión de la calidad.

- Plan: planificación para establecer la evaluación en las redes de información.
- DO: referencia a la implementación del ciclo PDCA.
- Check: monitorización y revisión de la red de datos.
- Act: Mantenimiento.

Figura 2: Norma ISO 27001 en la entidad financiera



Fuente: Elaborado por las Investigadoras

13.1.2. Planificación para la evaluación de las redes de datos

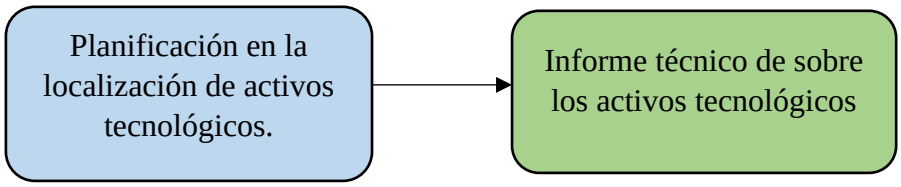
Para definir los alcances de la organización tanto en localización como activos tecnológicos, es necesario que se definan límites en la evaluación de las redes de datos, se recomienda empezar por información y accesos de alcance limitado; importante en la disponibilidad de procesos del negocio. Esto permitirá determinar la influencia sobre la

seguridad de la información y su alcance en las redes de las ubicaciones físicas y disposición de requisitos legales relacionados con la seguridad de la información.

Las políticas en la implementación de seguridad informática tienen que hacer referencia a la declaración de intenciones que la gerencia de la entidad debe tener en cuenta, lo cual se detallan a continuación:

- Considerar los requisitos y requerimientos legales basadas en una normativa de regulación ISO relativo a la seguridad de la información.
- Lineamientos con el contexto en base a una estrategia de gestión de riesgos de la información que mantendrá las redes de datos.
- Establecer criterios en base a lo que se va a evaluar en la entidad financiera.
- Informe técnico de la seguridad informática (Pentesting).

Figura 3: Evaluación de las redes de datos



Fuente: Elaborado por las Investigadoras

Definiendo las políticas de implementación de seguridad informática, hay que tener en cuenta la evaluación de los riesgos al momento del examen. Es necesario definir una estrategia adecuada en el pentesting para así especificar los niveles de riesgos aceptables, lo cual existen estándares para la evaluación de una red de datos; sin embargo, la organización o ente financiero puede optar o hacer uso de una normativa ISO de su preferencia, teniendo en cuenta que es bajo responsabilidad al combinar varias.

A continuación, se detalla las estrategias adecuadas para el examen de generación (Pentesting) en las redes de datos de la cooperativa SIERRA CENTRO SUCURSAL LA MANÁ, PROVINCIA DE COTOPAXI.

13.1.2.1. Identificación de los riesgos

- Identificar de manera adecuada los activos como: La identificación de información de la organización que está en su límite y alcance para la evaluación de la red de datos.
- Identificar amenazas que se encuentran alojadas en la red de datos.

- Medir el impacto que se podría tener en base a una pérdida de información confidencial de la entidad financiera.

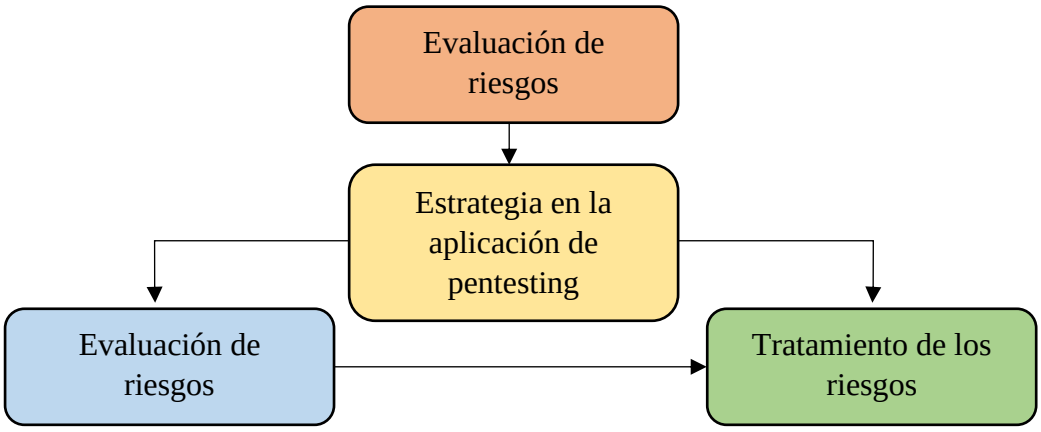
13.1.2.2. Evaluación de riesgos

- Medir el impacto en la entidad financiera en base a un fallo de seguridad en la red de datos, teniendo en cuenta la integridad y disponibilidad de la información.
- Evaluar la probabilidad de un fallo en relación a las brechas de seguridad de la entidad financiera en base a los ataques externos mediante la implementación de técnicas de vulneración en activos y recursos tecnológicos.
- Evaluar los niveles de riesgo que existe en una red de datos con activos tecnológicos compartidos.

13.1.2.3. Evaluación para el tratamiento de riesgos

- Monitorización de los controles adecuados para la mitigación de ataques externos.
- Aceptar los niveles de riesgos, siempre y cuando se cumpla con las reglas y políticas internas mediante los criterios establecidos en la aceptación de riesgos en el examen de penetración.
- Minimizar los riesgos en la evaluación de las redes de datos.

Figura 4: Políticas de implementación en seguridad informática



Fuente: Elaborado por las Investigadoras

13.1.3. Monitorización y revisión de la entidad financiera

Para la monitorización de activos tanto tecnológicos como manejo de información, la entidad financiera debe tener en cuenta lo siguiente:

- Detectar los resultados de la información del examen de penetración.
- Identificar brechas de seguridad con falencias.

- Identificar el alojamiento de malware en las redes de datos.
- Detectar y prevenir eventos e incidentes mediante el uso de indicadores de seguridad informática.
- Resolver brechas de seguridad con falencias.

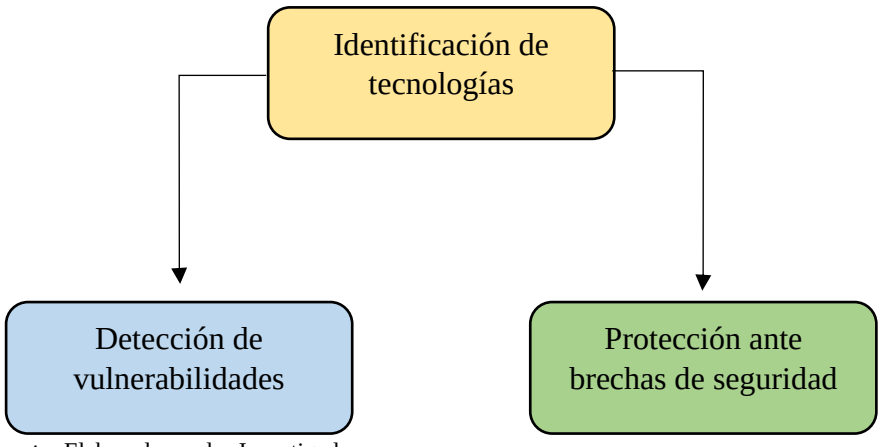
Para la monitorización y revisión de la entidad financiera se debe tener en cuenta que; los intervalos planificados son en base a las evaluaciones de riesgos con niveles aceptables, siendo que existan cambios dentro de la organización, tanto a nivel tecnológico y procesos de negocios. La monitorización permite identificar amenazas de tipo malware y ataques externos mediante técnicas de extracción de datos, identificación de estos como efectivos a la hora de llevar el control interior y exterior de los activos de información.

Periódicamente en base al proceso de monitorización de la entidad, es necesario aplicar auditorías internas basadas en las normas ISO 27001, lo cual permitirá llevar los controles, procesos y aspectos técnicos bajo el entorno legal en base a los requisitos y objetivos de la seguridad informática de la organización financiera, implementando así elementos de eficacia y rendimiento en base a la respuesta esperada.

13.1.4. NIST SP800.53

El objetivo de NIST (publicación especial 800-53 del NIST) permite elaborar patrones de medida y normas en tecnologías, permitiendo así la productividad y rendimiento en los ciclos de vida tecnológicos. NIST establecerá las directrices en base a una documentación sobre seguridad de la información, adoptando así un enfoque de varios niveles de gestión para su aplicación.

Figura 5: Flujo NIST SP800.53



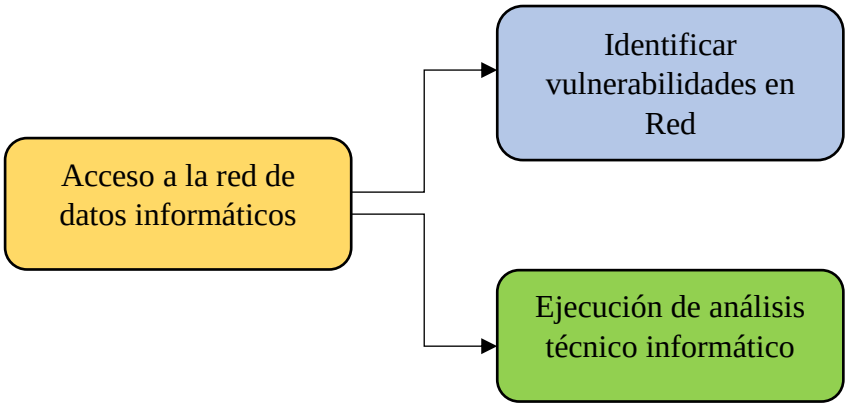
Fuente: Elaborado por las Investigadoras

13.1.5. Aplicación de NIST serie 800

Mediante la aplicación de NIST debemos tener en cuenta los controles de seguridad adoptados y recomendados para el uso de sistemas de información privada en la cooperativa SIERRA CENTRO SUCURSAL LA MANÁ, PROVINCIA DE COTOPAXI, lo cual se especificará el control necesario por la cual se realizará el examen de análisis técnico para la protección de la información lo cual debemos tener en cuenta los siguientes elementos:

- Control de acceso a las redes de datos como activo tecnológico.
- Responsabilidad al momento de ejecutar el proceso de análisis en los recursos tecnológicos de la entidad financiera.
- Administrar la seguridad en las redes de datos.
- Identificar vulnerabilidades de manera constante.
- Respuesta y soluciones ante ataques informáticos externos en la extracción de la información.

Figura 6: Aplicación de NIST serie 800



Fuente: Elaborado por las Investigadoras

13.2. Infraestructura de red de la cooperativa Sierra Centro

Para la recopilación de información necesaria para poder aplicar el procedimiento investigativo en base a la evaluación de redes de datos mediante hacking ético y pentesting, se basa en el uso de la norma de estándares internacionales ISO 27001, esto permitirá que los procesos que se lleven a cabo en el examen sea sistemático y su ejecución de forma correcta, dado que la entidad financiera en la actualidad está en constante crecimiento en el país; lo cual es necesario que se cumplan los parámetros establecidos en las normas estandarizadas.

13.2.1. Gestión de seguridad en la cooperativa Sierra Centro

Los diseños de sistemas de gestión para implementar seguridad informática en base a la normativa ISO 27001, nos indica que se debe realizar y ejecutar de manera correcta los aspectos técnicos para llegar al correcto diseño de implementación de brechas de seguridad, lo cual se procederá a definir los aspectos que se encuentran en la norma internacional aplicados en la cooperativa SIERRA CENTRO SUCURSAL LA MANÁ, PROVINCIA DE COTOPAXI.

13.3. Seguridad Lógica y utilización de los servicios en red

13.3.1. Seguridad en comunicaciones

Para obtener conocimiento acerca de una infraestructura de la red de datos es importante realizar un análisis para establecer los niveles de seguridad con la que cuenta la entidad financiera con el objetivo de proteger sus recursos y activos tecnológicos.

13.3.1.1. Software Antivirus

La entidad financiera adquirió en el año 2018 una licencia ilimitada del software antivirus Malware Bits profesional, lo cual se encuentra instalado en todas las máquinas de las oficinas matriz como las sucursales, este tipo de herramienta hace consumo de paquetes de datos mediante una red de internet; se necesita estar constantemente actualizado tanto el software para su funcionamiento como su base de datos para la detección de malware y nuevas técnicas de ataque a los recursos tecnológicos.

En la ejecución del software antivirus se han presentado inconvenientes al momento de localizar infecciones en las estaciones de trabajos, recursos compartidos y VPS de la cooperativa, siendo así que dentro de la lectura se han localizado objetos con alto nivel de infección ocasionados por el ingreso de dispositivos extraíbles como son las unidades de almacenamiento USB y descargas de páginas externas.

13.3.1.2. Ataques en la red de datos

Dentro de los estudios que se realizaron a la entidad financiera se ha constatado que las redes de datos no tienen herramientas lógicas para prevenir ataques externos en la extracción de la información y afectación de los recursos, sin embargo, no se ha presentado amenazas detectadas.

13.3.2. Seguridad lógica en las aplicaciones

13.3.2.1. Seguridad lógica de la Base de Datos

En el análisis de la seguridad lógica de la cooperativa, se encontró que esta entidad utiliza el gestor de base de datos DBA SQL 2014 express, la cual es de licencia gratuita, sin embargo, cabe recalcar que en base análisis de software; este motor de tipo licencia express es limitado para una entidad financiera, sus procedimientos de almacenado y administración son limitados por su licencia. Pero dentro de la implementación ellos procesan peticiones de información diaria en tiempo real sin ningún problema al ser institución financiera pero el tipo de licencia no es el adecuado.

El acceso a este software de gestión de datos acceden por un usuario root y una contraseña con 5 caracteres representando así un nivel de seguridad débil, lo cual genera una brecha de inseguridad grave al momento de gestionar información de socios y clientes de la entidad financiera, aun así, no existe privilegios adicionales establecidos para la gestión de la base de datos como roles de usuario para la administración, recalcar que la base de datos no cuenta con un archivo de respaldo automatizado en caso de aplicar una recuperación de imagen o información que se encuentre no disponible.

13.3.2.2. Control de Software de Terceros

En los departamentos de la cooperativa se encuentran instalado software de terceros tanto gratuitos o de pago, pero estos son gestionados por el administrador del área de sistemas para su instalación y su ejecución en cada máquina operativa, el trabajador de oficina no tiene la asignación de privilegios necesarios para modificar, instalar o eliminar un programa. No existe un manual de usuario para emitir ese procedimiento de configuración de instalación.

13.3.3. Cuadro comparativo de sistemas operativos

Para definir el sistema operativo a utilizar en el desarrollo de la investigación, se realizará un cuadro comparativo a nivel del tipo de proyecto, ventajas y desventajas y el consumo de recursos a nivel de hardware y software.

Tabla 10: Cuadro comparativo de sistemas operativos

OS	Tipo de proyecto	Ventajas	Desventajas	Recursos a nivel de hardware
Kali Linux	Proyecto GNU/LINUX	• Aplicación en el uso de informática forense y auditorias basadas en hacking ético. • Sistema operativo gratuito. • Entorno de desarrollo seguro para amateurs. • Suite de herramientas completas para el proceso de análisis de elementos y explotación de información.	• No es fácil de aprender, su sintaxis es compleja. • Reduce espacio en disco en cada configuración. .	• Bajo consumo de recursos a nivel de hardware.
Parrot Security	Proyecto GNU/LINUX	• Suite completa para la generación de ataque y defensa en seguridad informática. • Entorno de desarrollo amigable. • Fácil de aprender.	• Versiones de sistema operativo por separado. • Pago adicional por el uso de herramientas en la aplicación de pentesting. • Fallas e Inestabilidad en la conexión de la red.	• Alto consumo de recursos a nivel de hardware.
Blackarch	Proyecto GNU/LINUX	• Suite completa y gratuita en base a los repositorios de GitHub. • Actualizaciones constantes para dar soporte al sistema operativo. • Herramientas completas para la aplicación de seguridad informática.	• Interfaz gráfica no amigable. • Falta de compactibilidad con versiones de 64 bits. • No contiene actualizaciones del sistema. • El soporte de Blackarch está bajo la comunidad Linux.	• Bajo consumo de recursos a nivel de hardware.

Archstrike	Proyecto GNU/LINUX	• Distribución para la aplicación de hacking ético. • Aplicaciones de seguridad informática estables. • Herramientas especiales para la ejecución de pentesting y hacking. • Apto para profesionales de la rama en seguridad, análisis y pentesting.	• No es un sistema operativo para el uso diario. • No apto para principiantes por la complejidad de sus comandos. • Paquetes de herramientas no son actualizadas constantemente.	• Bajo consumo de recursos a nivel de hardware.

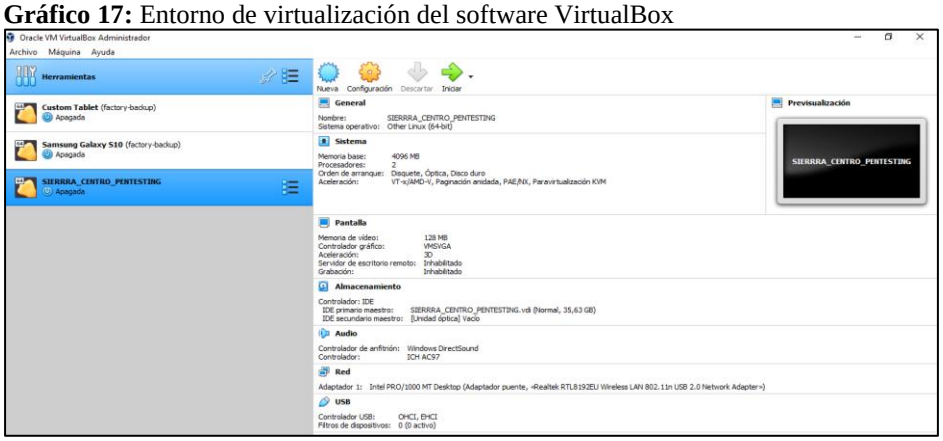
Fuente: Elaborado por las Investigadoras

En base a la comparativa diseñada de las distribuciones y opciones por la cual se puede optar, se consideró que en el desarrollo de la investigación el sistema o distribución que va de acorde a los resultados que se desea obtener; la selección del sistema operativo Kali Linux permitirá y facilitará las tareas de hacking ético y pentesting de manera concreta, considerando que esta distribución se basa en Debian y por ende asegura su mantenimiento y seguridad.

13.4. Instalación de VirtualBox

Se procede a configurar en el entorno de virtualización; en este caso se optó por el entorno Virtual Box, lo que permitirá ejecutar la virtualización de un sistema operativo en una máquina física anfitriona con pocos recursos de hardware para su ejecución.

Gráfico 17: Entorno de virtualización del software VirtualBox



Fuente: Elaborado por las Investigadoras

13.4.1. Configuración de sistema operativo Kali Linux

Una vez configurado el entorno de ejecución de la virtualización, se procede a instalar el sistema operativo donde se va a realizar en análisis de las redes de datos y aplicación de pentesting llamado Kali Linux, permitiéndonos así interactuar mediante una interfaz gráfica.

Gráfico 18: Configuración e instalación de Kali Linux

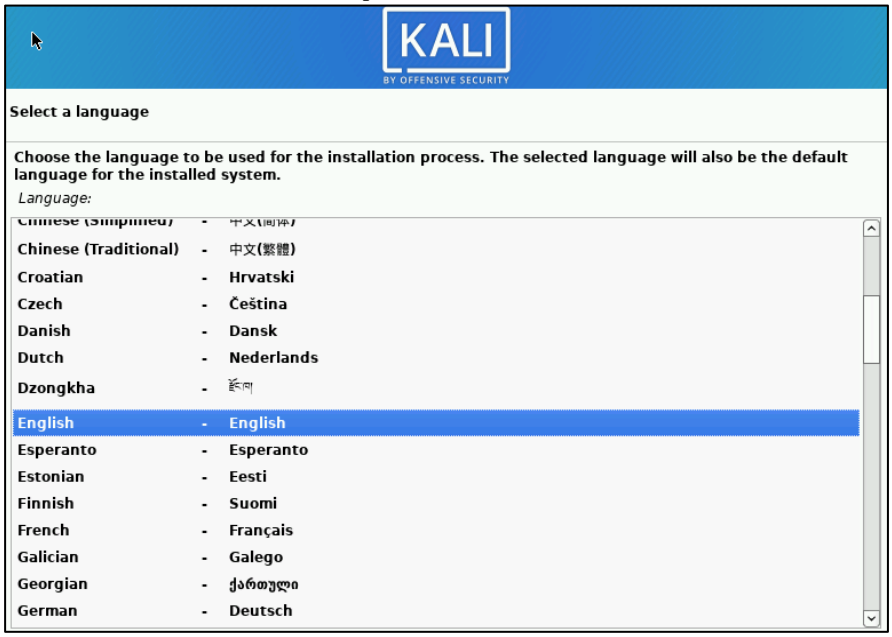
Fuente: Elaborado por las Investigadoras

Cabe recalcar que el sistema operativo Kali Linux existen varias alternativas de instalación que son mencionadas a continuación:

- Instalación mediante interfaz gráfica para el usuario común.
- Instalación de tipo avanzada, su configuración es en base a una ventana de comandos para una configuración inicial.
- El modo de instalación Dark Contrast hace referencia a una combinación de interfaz gráfica con un cambio de contraste en sus colores y ciertas configuraciones mediante ventana de comandos.

Realizada la selección del asistente de instalación, en este caso se optó por el asistente de instalación gráfico, se procede a configurar el idioma y región para la accesibilidad del sistema operativo. Existe una variedad de idiomas, lo cual se procedió a seleccionar el idioma español latino con su región latinoamericana; al seleccionar un tipo de idioma y una región hará que el sistema donde se va ejecutar el test de penetración se encuentre totalmente actualizado con nuevas funcionalidades y herramientas para uso futuro.

Gráfico 19: Selección de idioma para la accesibilidad del sistema

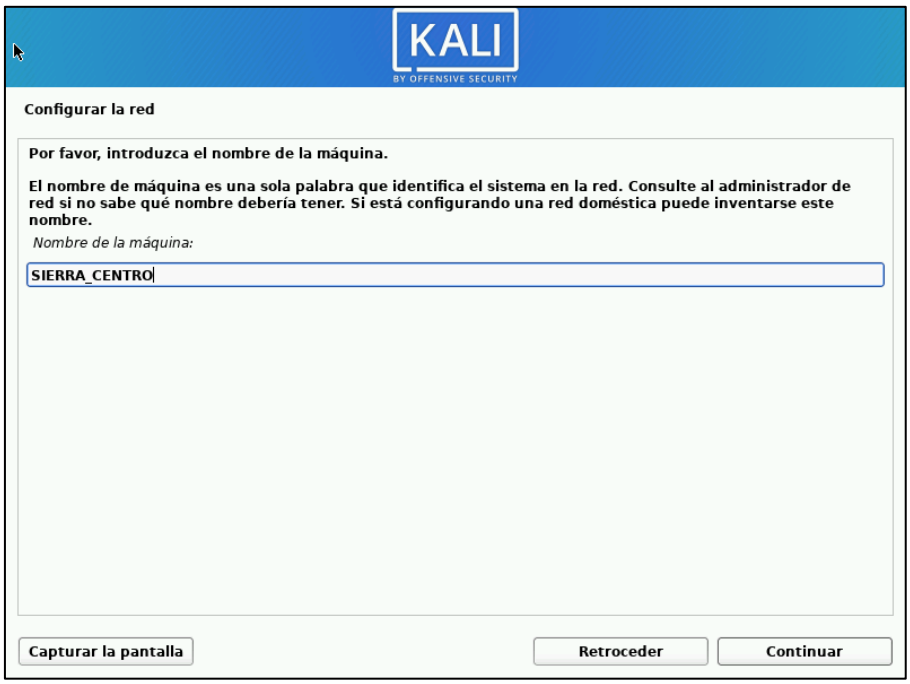


Fuente: Elaborado por las Investigadoras

Seleccionado la región y el idioma para su accesibilidad y obtener constantes actualizaciones en el sistema operativo, se procede a configurar la red comenzando por el nombre de usuario en el cual va acceder, en este caso el nombre de usuario tiene que ser para una sola máquina anfitrión para que esta sea identificada en la red que va estar anclada para el examen de penetración, sin embargo, siempre se define nombres de red mediante el administrador de la red doméstica, pública o privada. Para establecer el nombre de usuario que va a estar anclado a la red que se va a evaluar hay que tener en cuenta lo siguiente:

- Nombre en caracteres, pueden ser intercalados entre mayúsculas y minúsculas.
- Tener en cuenta a la red que se va asociar la máquina virtual para el análisis.
- Nombre fácil donde se pueda identificar de manera fácil la máquina configurada.
- Es recomendable anclar a redes de tipo doméstica o estrictamente que sean privadas, en este caso la cooperativa cuenta con una configuración de tipo privada.

Gráfico 20: Configuración del nombre de máquina anclada a la red de datos



Fuente: Elaborado por las Investigadoras

Configurada la red donde se va anclar el sistema operativo, se procede a gestionar el acceso y contraseñas de la máquina donde se va a realizar la evaluación en las redes de datos de la entidad financiera.

Gráfico 21: Configuración de usuarios y contraseñas

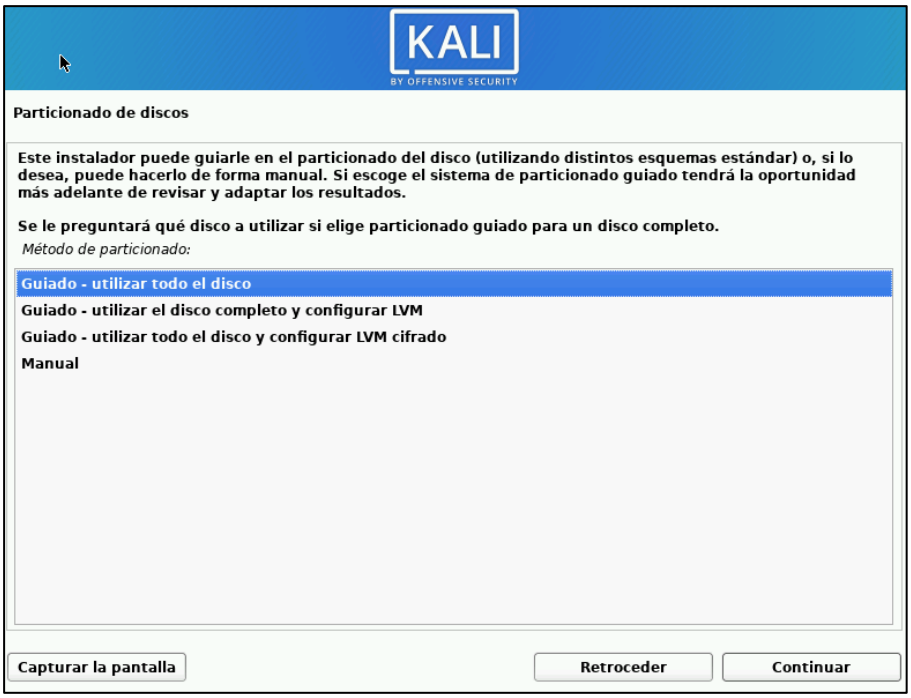
Fuente: Elaborado por las Investigadoras

Definido el nombre de la máquina a virtualizar, procedemos al particionamiento de discos para alojar la información del sistema operativo y sus herramientas de análisis para

seguridad informática, permitiendo que estos esquemas de particionamiento se realicen de forma correcta teniendo en cuenta lo siguiente:

- La partición de disco guiada permite de manera automática gestionar la cantidad establecida en el disco duro virtual y la reserva del mismo.
- La forma guiada de disco completo hace referencia en tomar los valores absolutos para una configuración en la administración de los volúmenes lógicos.
- El guiado de tipo LVM cifrado permitirá en la instalación dividir en varios volúmenes lógicos al disco duro permitiendo que no abarque más de una unidad física.
- Para configuración de particionamiento tanto LVM como partición estándar, se recomienda que hacer uso de la configuración para novatos, ya que esta permite una secuencia automática del proceso de instalación y configuración de particionamiento tanto de almacenamiento físico como lógico reservado del sistema.

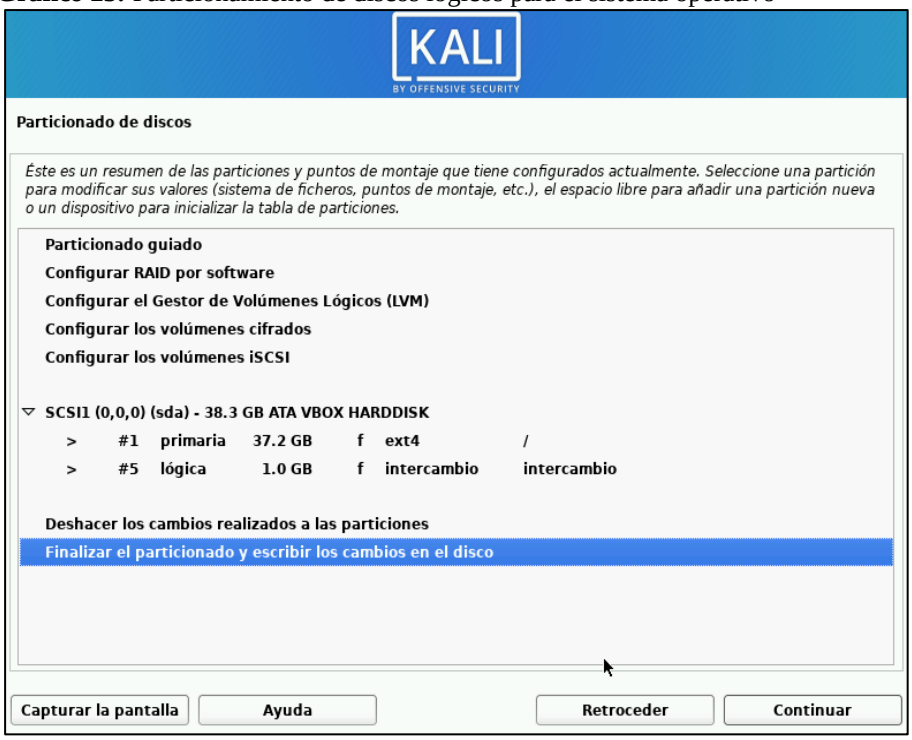
Gráfico 22: Particionamiento de disco duro virtual



Fuente: Elaborado por las Investigadoras

Seleccionado el tipo de participación para el almacenamiento del sistema operativo Kali Linux, se procede a marcar la gestión de puntos en el montaje de una partición guiada tanto primaria como volumen de almacenamiento lógico.

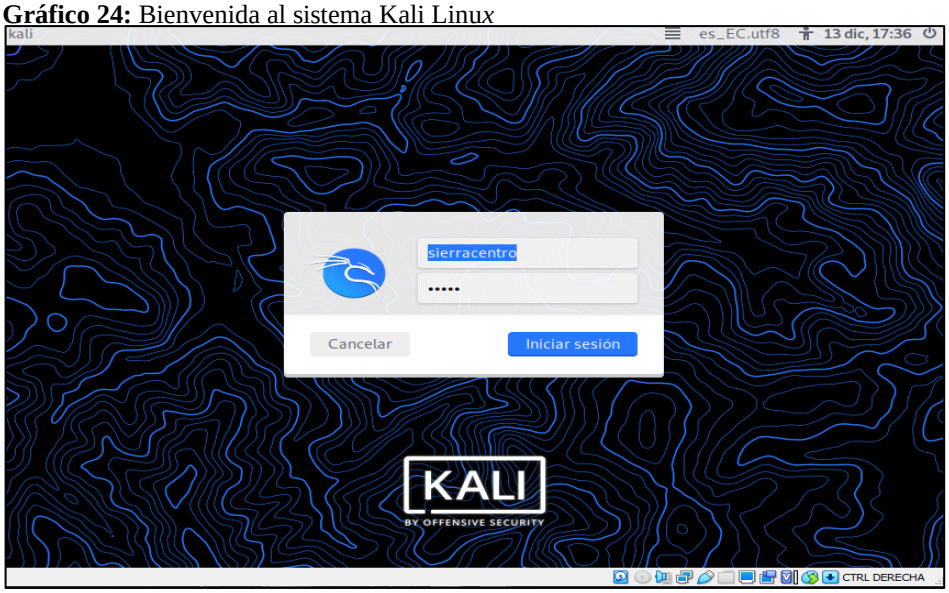
Gráfico 23: Particionamiento de discos lógicos para el sistema operativo



Fuente: Elaborado por las Investigadoras

Particionado tanto los discos de almacenamiento primario como la parte lógica donde se gestionará todos los archivos del sistema, instalado el mismo se visualiza la pantalla de bienvenida al sistema, tomando en cuenta que el usuario donde se va a realizar el examen de penetración (Pentesting) lleva como nombre “sierracentro” siendo el lugar de ejecución.

Gráfico 24: Bienvenida al sistema Kali Linux

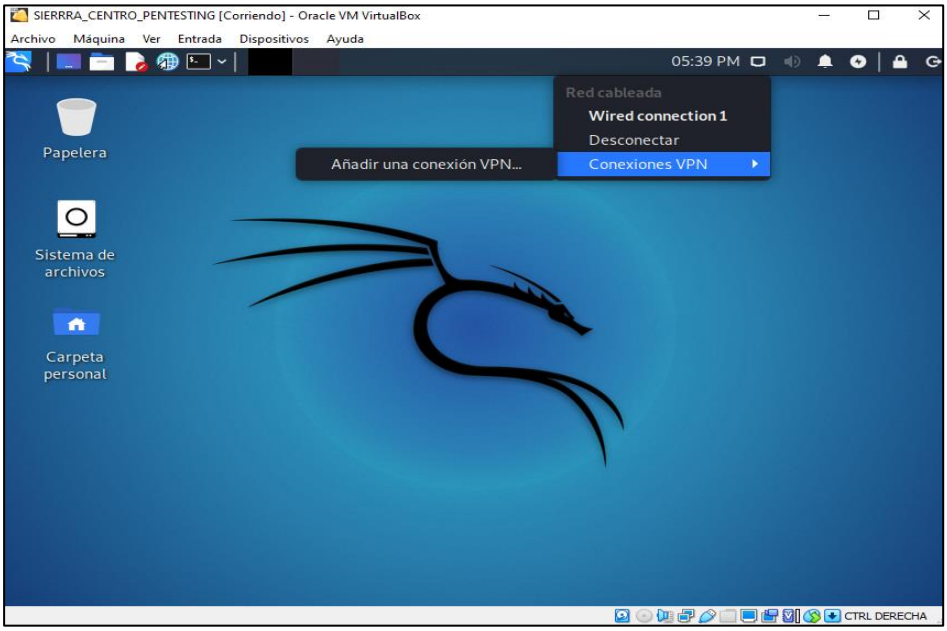


Fuente: Elaborado por las Investigadoras

Una vez registrado el acceso al sistema Kali Linux conectada con la red de datos de la entidad financiera SIERRA CENTRO SUCURSAL LA MANÁ, PROVINCIA DE

COTOPAXI se procede a ejecutar la penetración y exploración en las redes para su análisis en la detección de brechas de seguridad y tomar las medidas adecuadas para su blindaje lógico.

Gráfico 25: Acceso al escritorio del sistema Kali Linux



Fuente: Elaborado por las Investigadoras

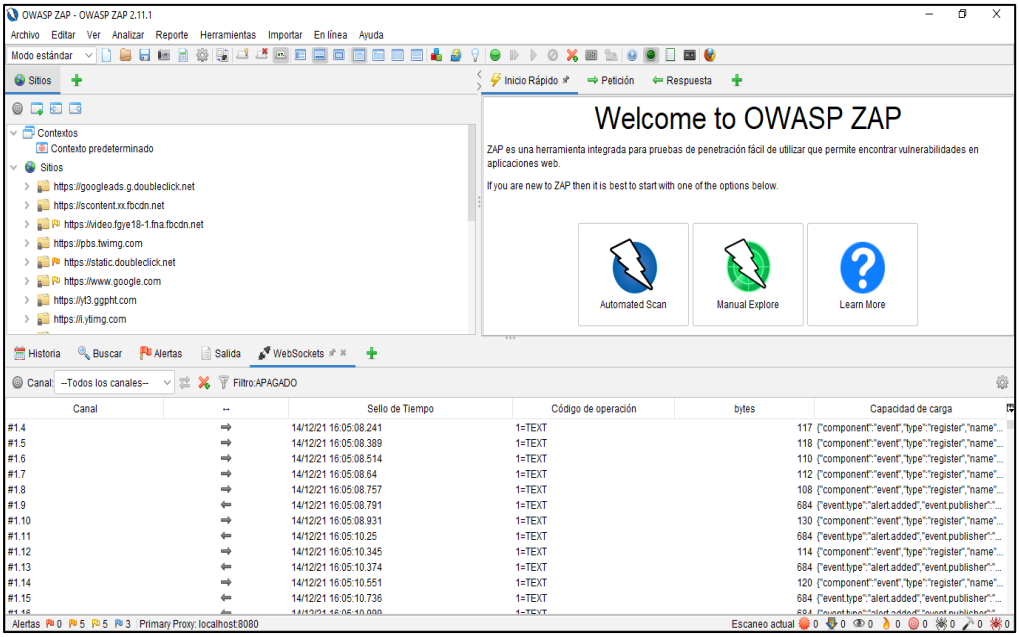
13.5. Análisis del sistema financiero mediante ZAP

Una vez configurado el sistema operativo que nos va a permitir realizar el análisis técnico en base a la aplicación del examen de penetración del sistema financiero SIERRA CENTRO SUCURSAL LA MANÁ, PROVINCIA DE COTOPAXI

Vamos a dedicar y a escanear, detectar y enumerar las vulnerabilidades que existen en la aplicación como objetivo de análisis y estudio, permitiendo así que el CVE (Ente regulador de vulnerabilidades) sea intermediario entre la máquina y el ente regulatorio donde se va a registrar la vulnerabilidad que existen.

Dentro de su suite de Kali Linux procederemos a ejecutar la herramienta OWASP ZAP, esta herramienta está centrada en el análisis y explotación de vulnerabilidades tanto de CMS como redes de datos en comunicación, en este caso se aplicará a las conexiones de LAN del ente financiero.

Gráfico 26:Escaneo y enumeración del análisis del sistema financiero



Fuente: Elaborado por las Investigadoras

Mediante el escaneo que se realizó al sistema financiero de la cooperativa SIERRA CENTRO SUCURSAL LA MANÁ, PROVINCIA DE COTOPAXI, se procede a detallar en la siguiente tabla los resultados de la penetración en base al sumario de alertas en base al nivel de riesgo y números de alertas procesados mediante el software OWASP ZAP.

Tabla 11: Enumeración de análisis

Nombre de alerta	Nivel de riesgo	Numero de instancia
CSP: Wildcard Directive	Medio	3
CSP: script-src unsafe-inline	Medio	3
CSP: script-src unsafe-inline	Medio	3
Desconfiguración de Dominio cruzado	Medio	12
Desconfiguración de Dominio cruzado	Medio	6
Cookie with SameSite Attribute None	Bajo	4
Cross-Domain JavaScript Source File Inclusion	Bajo	3
Incomplete or No Cache-control Header Set	Bajo	9
X-Content-Type-Options Header Missing	Informativo	12

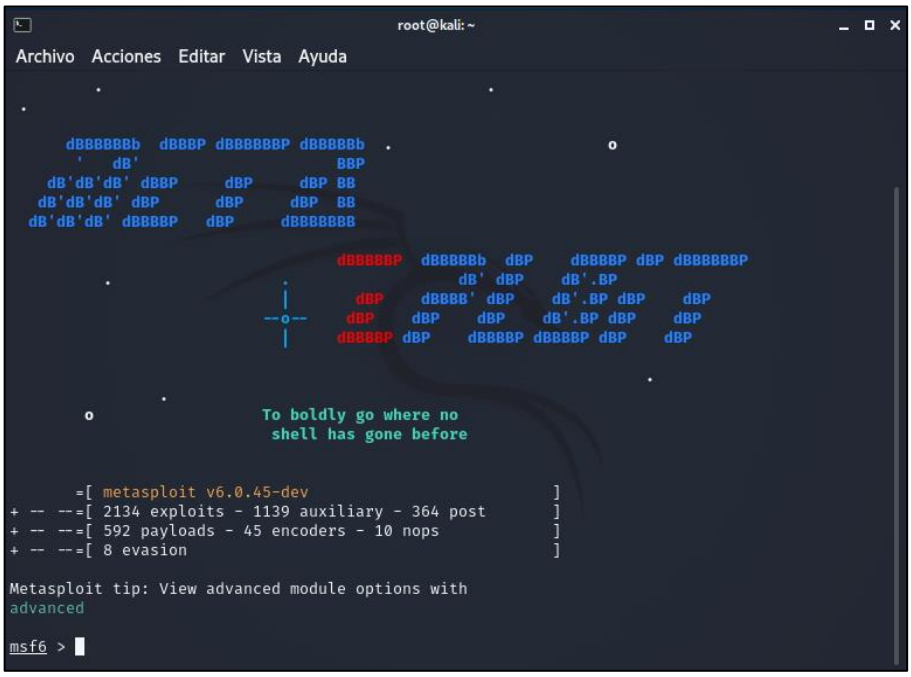
Divulgación de la marca de hora - Unix	Informativo	41
Amplia gama de Cookies	Informativo	3
Amplia gama de Cookies	Informativo	121

Fuente: Elaborado por las Investigadoras

13.5.1. Metasploit a las redes de datos

Mediante la consola y usuario root@kali, procederemos a ejecutar en la ventana de comandos el servicio de PosgreSQL como complemento e instalador de Metasploit mediante la sentencia #sudo service PostgreSQL star; permitiendo así que se instale el framework donde se ejecutará el ataque a la red de datos de la cooperativa SIERRA CENTRO SUCURSAL LA MANÁ, PROVINCIA DE COTOPAXI para la detección de vulnerabilidades. Una vez ejecutado el servicio de Metasploit para la detección de comunicación entre la red de datos y el sistema financiero de la cooperativa, se procede aplicar la evaluación y diagnóstico del estado de comunicación entre los dos elementos mencionados, teniendo como conclusión lo siguiente:

Gráfico 27: Ejecución del servicio Metasploit

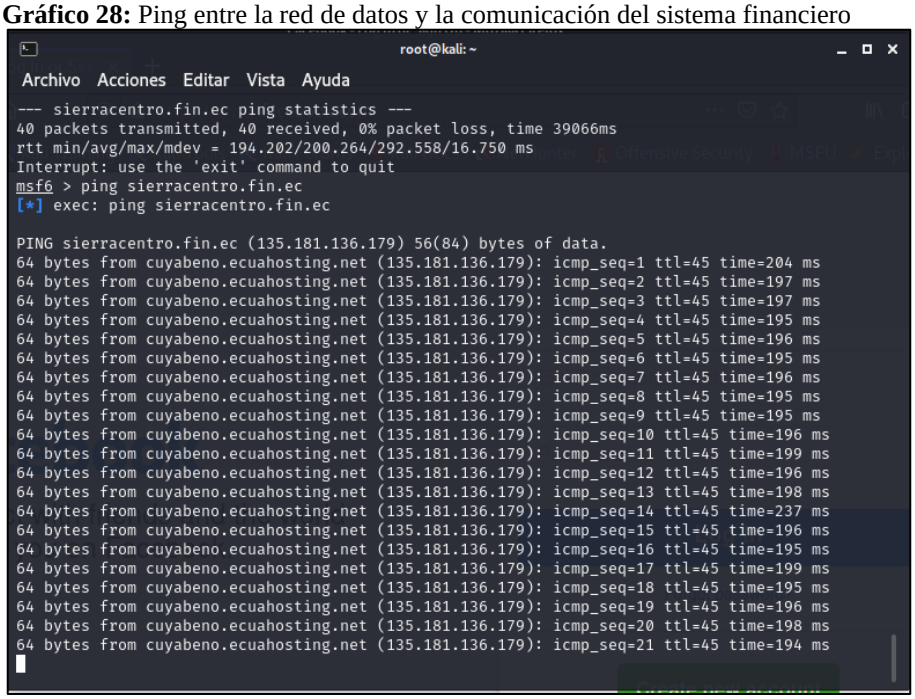


Fuente: Elaborado por las Investigadoras

El dominio detectado tiene como nombre sierracentro.fin.ec, alojado en un servidor VPS denominado ecuahosting ubicado en la ciudad de Guayaquil; en base a la estadística de Metasploit el rendimiento de la IP de una red de datos arroja 40 paquetes de transmisión, 40 recibidos y perdidas de paquetes 0, dando como conclusión un tiempo de respuesta de

39066ms lo cual quiere decir que el estado de la red responde adecuadamente en la entidad.

Gráfico 28: Ping entre la red de datos y la comunicación del sistema financiero



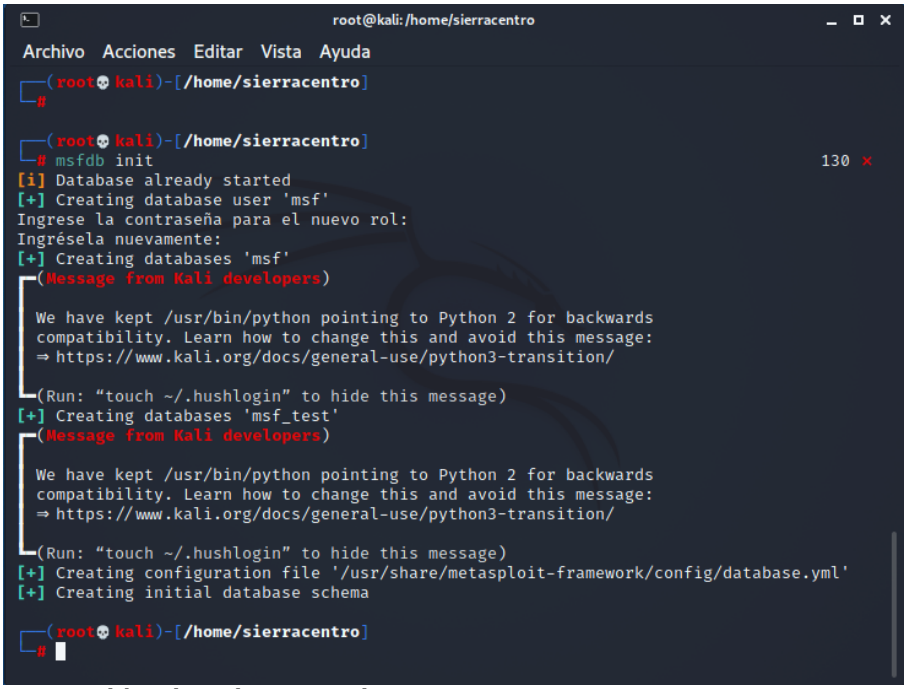
Fuente: Elaborado por las Investigadoras

13.5.2. Aplicación de NMAP en redes de datos

A continuación, se procederá a escanear la red de datos de la cooperativa SIERRA CENTRO SUCURSAL LA MANÁ, PROVINCIA DE COTOPAXI, desde Metasploit con la herramienta NMAP, lo cual se genera un espacio de trabajo para el proceso de autoría de la red. El primer paso para la aplicación del escaneo para detección de equipos vinculados a la red es ejecutar el servicio Metasploit con el comando msfconsole en la ruta de la maquina donde se ejecutará la sintaxis /etc/init.d/postgresql.

Ejecutado el servicio para la detección de las redes y las maquinas asociados, se procede hacer la conexión y creación de la base de datos para la comunicación Metasploit y los elementos de la red de la entidad, teniendo en cuenta que la maquina denominada con la ruta /home/sierracentro, es donde se procederá a levantar la configuración en base a la instalación y creación del espacio de trabajo.

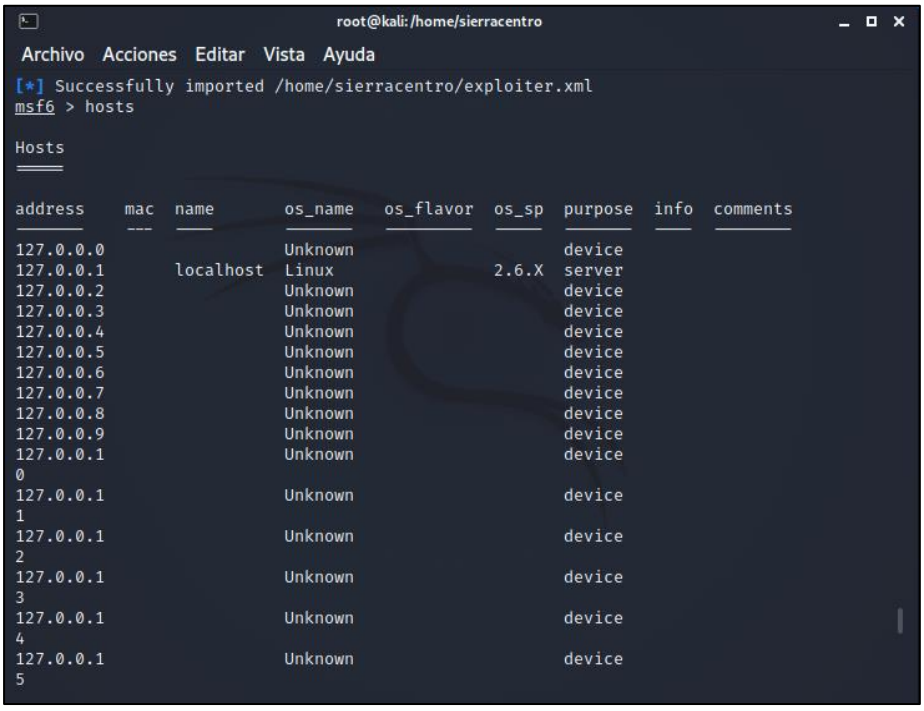
Gráfico 29: Entorno de configuración del área de trabajo para el escaneo de la red



Fuente: Elaborado por las Investigadoras

Ejecutado el escáner, se obtiene la siguiente información de toda la red dependiendo de los nodos que tendremos a disposición lo cual tomará su tiempo. Ahora para exportar la base de datos de los hosts encontrados se debe declarar la sintaxis db_import exploiter.xml, esto detalla de manera técnica y precisa.

Gráfico 30: Listado completo de host en la red de datos

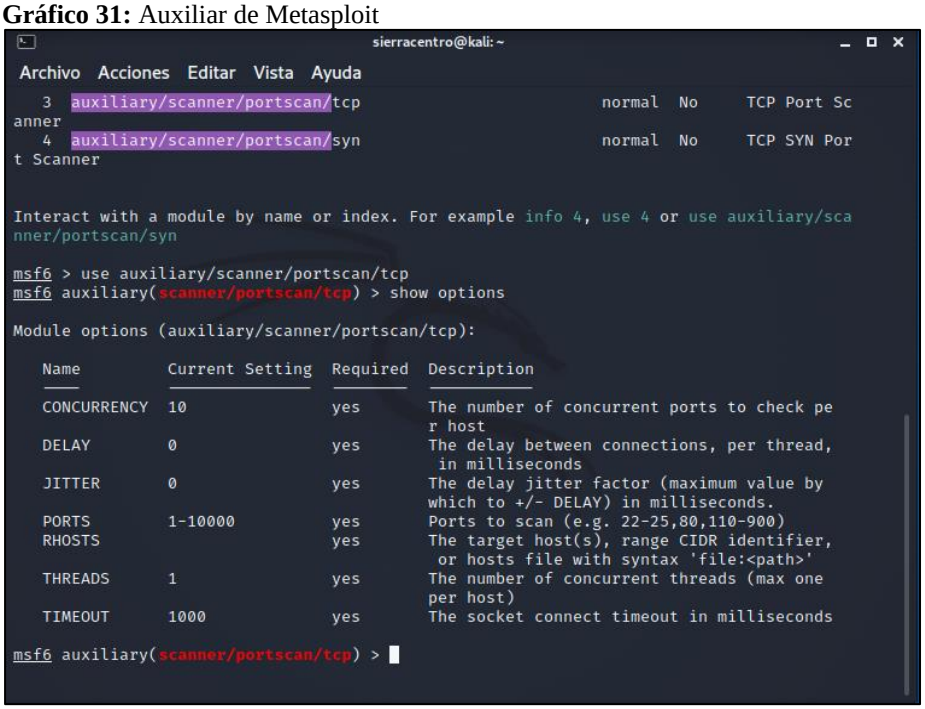


Fuente: Elaborado por las Investigadoras

13.5.3. Escaneo auxiliar para la red de datos de la cooperativa

Identificado los hosts anclados a la red de datos de datos, se procede a implementar el escaneo auxiliar a la red de datos, para el proceso de la identificación de la base de datos anclada con la red mediante el target use/auxiliary/scanner/portscan/.El target use/auxiliary/scanner/portscan/, nos permite aplicar el pentest al entorno del socket donde implementaremos la identificación del objetivo, en este caso la evaluación de la red de datos de la cooperativa SIERRA CENTRO SUCURSAL LA MANÁ, PROVINCIA DE COTOPAXI.

Gráfico 31: Auxiliar de Metasploit



Fuente: Elaborado por las Investigadoras

Identificado el objetivo, se instaura el procedimiento mediante RHOST apuntado a la dirección IP con la numeración y nomenclatura 192.168.100.102 de la red de tipo TCP (Protocolo de transmisión) para el escaneo de todo el rango con el set del puerto de la red que se identifica con la máscara /24, mencionando que los 32 bits constituyen a dicha dirección y el hilo de comunicación aplicado al set THREADS 30 ejecuta el escaneo auxiliar para la aplicación del pentesting y evaluación en la red de tipo LAN.

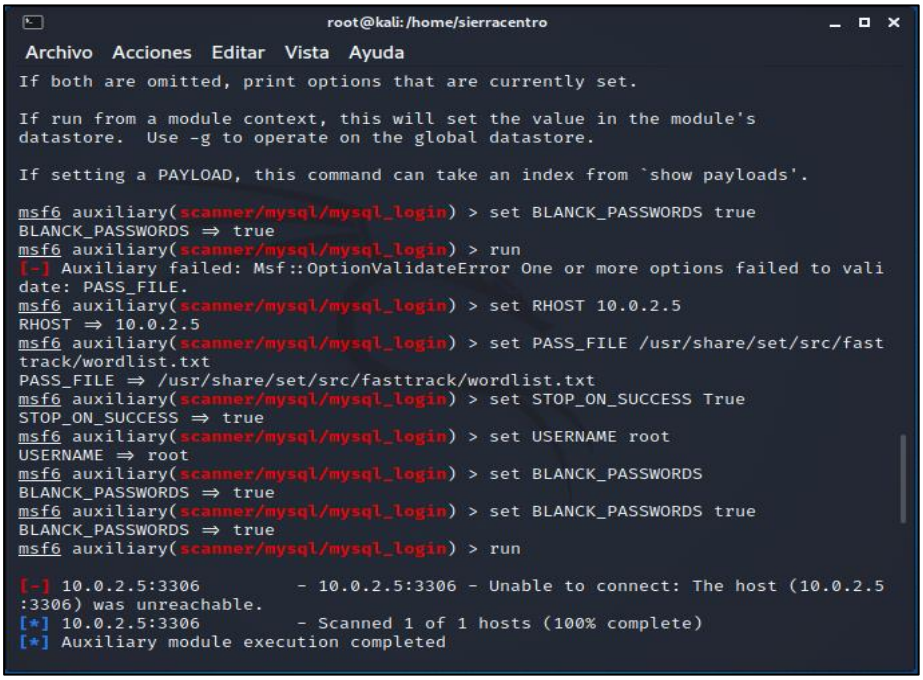
13.5.4. Ataque de fuerza bruta para la detección y evaluación de vulnerabilidades

Para la evaluación de la red de datos de la cooperativa, se aplicó la técnica de ataque basado en fuerza bruta con Metasploit y Metalpreter, lo que permitirá la aplicación de pentesting a la red, en donde no solo se hará el ataque de fuerza bruta a la red de datos, si

no en que su aplicación también se basará en la inyección de Payload para que ejecute la vulnerabilidad a la red de comunicación con un número de elementos de 1800 exploits o conocidos como ataques, forzando así el acceso y control de toda la comunicación de la entidad financiera y poder determinar la evaluación de la red de datos y el estado que se encuentra y cómo responderá a un posible ataque externo en la extracción de datos en el futuro. A continuación, se procederá a ingresar a los módulos de la red de datos, mediante el uso de la sintaxis auxiliary, permitiendo que la configuración de la IP o el Host de la red objetivo para el ataque de fuerza, lo cual contiene lo siguiente:

- La ejecución se realiza mediante conexión física, estableciendo comunicación entre router y máquina virtual.
- El laboratorio de análisis de la red es en base al home de la máquina sierracentro ya configurada.
- Se aplican rangos distintos de IP para poder identificar de varias alternativas las redes que tienen altas posibilidades de ser atacadas para proceder a su análisis.

Gráfico 32: Preparación de entorno para el ataque mediante Metasploit

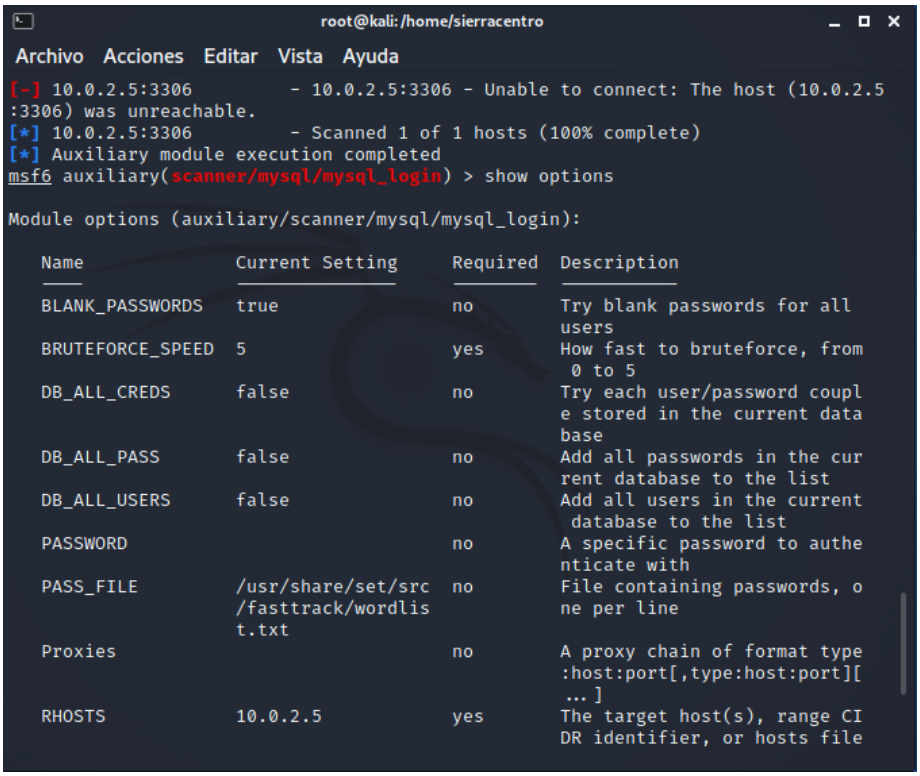


Fuente: Elaborado por las Investigadoras

En este caso se procede a setear el SET_RHOST 10.0.2.5 con una puerta de enlace Gateway de la maquina cliente 192.168.100.1 que va hacer el objetivo de ataque de fuerza bruta, condicionando así la penetración a la red. Considerando que se puede escanear la IP objetivo, condicionamos mediante el set PASS_FILE el diccionario de acceso a los host o puertos de la red de datos que posiblemente tengan que evaluarse mediante un

ataque y analizar sus falencias, considerando que una vez se tenga el control de las comunicaciones procedemos a tomar el control de la dirección de la red de datos objetivo en base a la dirección IP de la puerta de enlace completando así el análisis de la maquina host.

Gráfico 33: Host analizado con vulnerabilidad en la red de datos



Fuente: Elaborado por las Investigadoras

Dentro del análisis de los hosts vinculados a la red de datos, observamos que la IP que apunta con puerto de enlace 192.168.100.1 y RHOST 10.0.2.5 está disponible para que sea marcada como objetivo de pentesting para el análisis de la vulnerabilidad en base a un ataque forzado, ejecutándose de manera automática el lanzamiento de los exploits en cada puerto de la red para su ataque hasta que encuentre la red que está fraccionada.

La aplicación del ataque de fuerza bruta mediante Payload permitió al momento del análisis identificar de manera correcta la red donde sufría vulnerabilidad, teniendo en cuenta que se tiene el control de la conexión física de la entidad de la maquina cliente; siendo que el Payload se utilizó para la penetración en el objetivo en él envió de paquetes de datos, dando como efecto el bajo rendimiento de la conexión en las oficinas donde recorre la infraestructura LAN; obteniendo como resultado que el Metalpreter se ejecute de manera correcta en las comunicaciones de estaciones de trabajo.

13.5.5. Resultados de la aplicación de pentesting

Para la evaluación de resultados, se detalla a continuación la información del registro de puertos franqueables y vulnerables de las redes de datos de la cooperativa SIERRA CENTRO SUCURSAL LA MANÁ, PROVINCIA DE COTOPAXI.

Tabla 12: Resultado de la aplicación de Pentesting en la red de datos

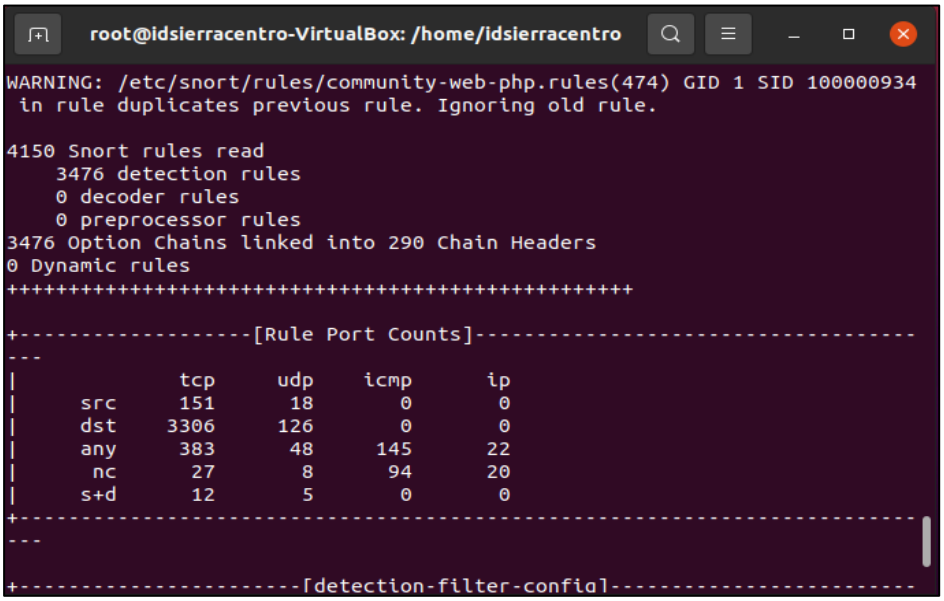
IP Maquina DHCP	Payload de ataque Metasploit	Tipo de Configuración	Estado actual de la Red
192.168.100.1 (Getway)	MSFPC	No configurada	Vulnerable
192.168.100.102 (Maquina)	MSFvenom	No configurada	Vulnerable

Fuente: Elaborado por las Investigadoras

13.5.6. Configuración de reglas en la red de datos

Se establece el IDS como sistema de detección de intrusos mediante la gestión y monitorización del tráfico de la red de datos, basándonos en el resultado obtenido de la aplicación del pentesting de la comunicación de la entidad financiera, teniendo así varias brechas vulnerables identificadas. A continuación, se procede a ingresar como usuario root a la maquina cliente denominada (IDSierraCentro) con dirección física 08:00:27:EA:77:F2 donde se implementará el IDS para la red de datos donde lo cual se aplicó la evaluación, el acceso a ello es de tipo root y se procede con la instalación del IDS llamado Snort con la sentencia apt-get install.

Gráfico 34: Instalación de snort



Fuente: Elaborado por las Investigadoras

Ejecutada la sentencia mediante el comando gedit /etc/snort/snort/.conf, procedemos a configurar el fichero de la red de datos de la entidad mediante la red 192.168.100.1/24.

13.5.7. Aplicación de reglas y seguridad para la red de datos

Una vez implementado el IDS instalado en la configuración interna de la red de datos, procederemos a la creación de un archivo o folder personalizado para la creación de las reglas personalizadas en la red para que se alerte de algún tráfico de red malintencionado. Para la creación del archivo se establece la siguiente escritura de comandos snort -T -c /etc/snort/snort.conf -i enp0s3, esto configura la interfaz de red enp0s3, manteniendo a disposición las reglas de alerta en el tráfico de red externo.

Gráfico 35: Reglas personalizadas para la protección de la red de datos

```
46 # Note to Debian users: this value is overriden when starting
47 # up the Snort daemon through the init.d script by the
48 # value of DEBIAN_SNORT_HOME_NET s defined in the
49 # /etc/snort/snort.debian.conf configuration file
50 #
51 #REGLA PERSONALIZADA PARA MAQUINA IDSierraCentro en la configuracion de
   la puerta de enlace GATEWEY EN LA APLICACION DE PROTECCION DE TRAFICO
   INTRUSO
52
53 ipvar HOME_NET 192.168.100.1/24
54
55 #ESTADO DE RUTA IDS PERSONALIZADA
56 # such as:  c:\snort\rules
57 var RULE_PATH /etc/snort/rules
58 var SO_RULE_PATH /etc/snort/so_rules
59 var PREPROC_RULE_PATH /etc/snort/preproc_rules
60
61
62 # Set up the external network addresses. Leave as "any" in most
   situations
63 ipvar EXTERNAL_NET any
64 # If HOME_NET is defined as something other than "any", alternative,
   you can
65 # use this definition if you do not want to detect attacks from your
   internal
```

Texto plano ▾ Anchura del tabulador: 8 ▾ Ln 55, Col 21 ▾ INS

Fuente: Elaborado por las Investigadoras

La regla no es determina o por defecto. Con la última versión de Snort se tiene que declarar la variable HOME NET más la dirección GATEWAY que está a disposición para ser vulnerable, teniendo en cuenta las rutas para levantar el servicio del IDS. Creado el directorio para las alertas mediante el sistema IDS, se procede a definir dos variables para el correcto uso de la monitorización de la red que son HOME_NET y EXTERNAL_NET basada en la red que se va a proteger, en este caso la 192.168.100.1/24.

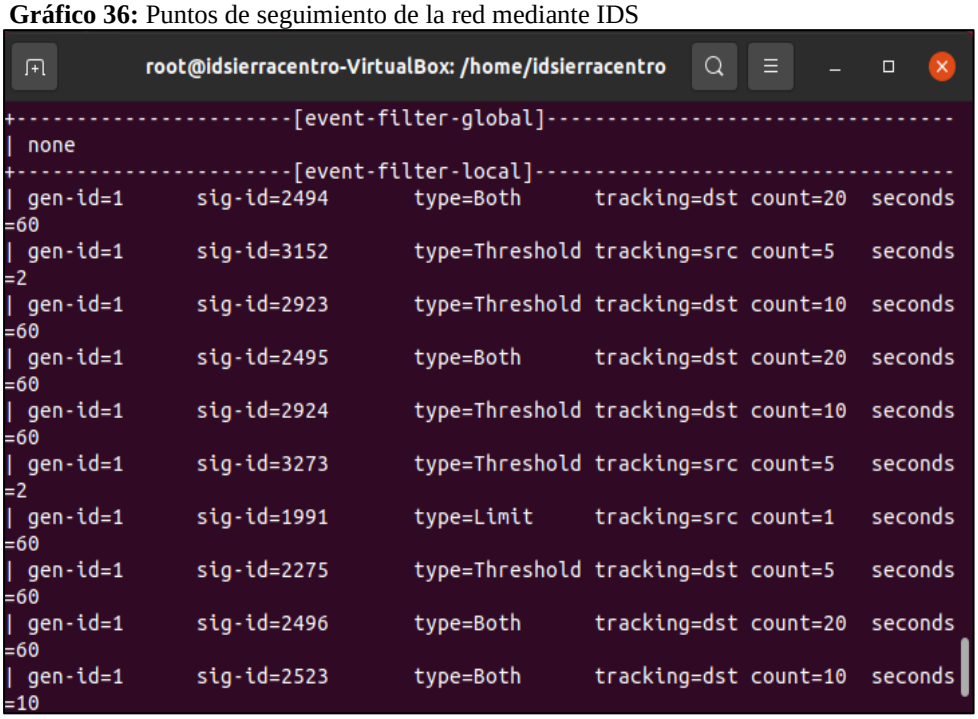
13.5.8. Puntos de seguimientdo de la regla IDS

Se consideró que al momento de que las comunicaciones de los paquetes proviniendo de una maquina externa para que establezca una regla de 10000, estos valores pueden ser

por defecto o dependiendo de la cantidad de paquetes que se requiera, La personalización de la regla mediante el IDS Snort permitirá que el tráfico de red sea detectado en base a posibles ataques entrantes, considerando que al momento de utilizar reglas personalizadas pueden funcionar, pero que a su vez estas reglas pueden generar más alertas de falsos positivos detrás de un desbordamiento en comunicaciones.

Una vez establecidas las variables de red de la monitorización ante ataques, asignamos el rol de que en sí todo el tráfico TCP venga de una red externa mediante la asignación $HOME_NET en el puerto estándar 24, en este caso se mostrará una alerta (msg: "´Potentially Bad Traffic") abarcando el tráfico que está fuera de lo común y que es potencialmente indicativo de un sistema comprometido, así la monitorización nos alertará ante ataques o intrusos en la red de datos.

Gráfico 36: Puntos de seguimiento de la red mediante IDS



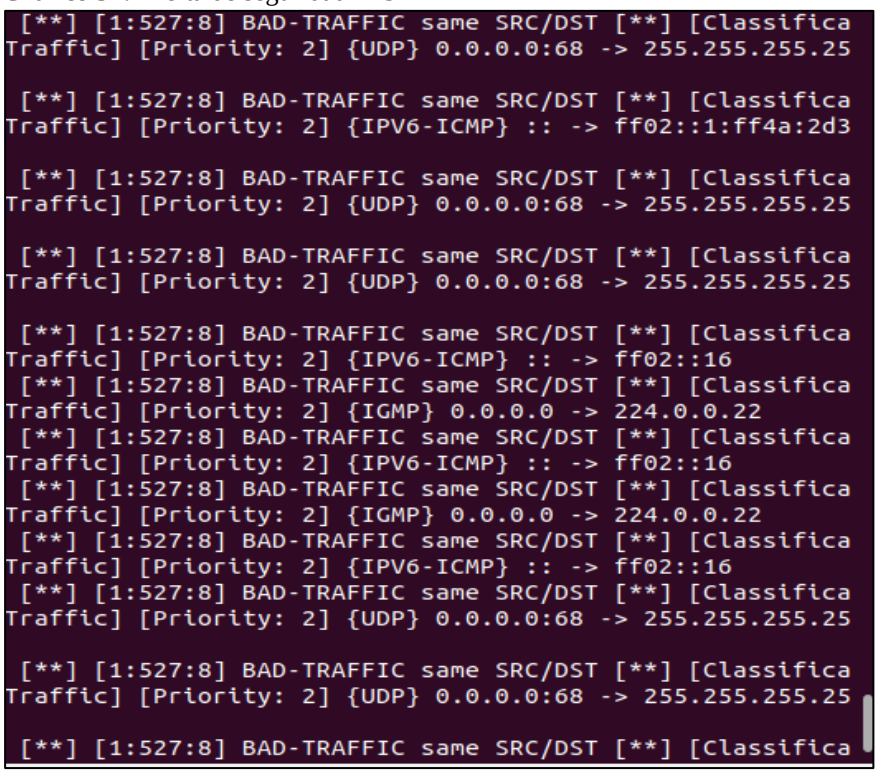
Fuente: Elaborado por las Investigadoras

13.5.9. IDS implementado alerta en la red de datos de la cooperativa

Establecida las reglas de tráfico donde se asignó la configuración del TCP previamente configurado, visualizamos si existe una alerta, la regla establecida menciona que si existe tráfico desde una IP con denominación 192.168.100.102 con una interfaz de red eth0. Entonces se procede a observar la consola donde está configurada la protección mediante el IDS snort, ejecutado en tiempo real el control y bloqueo del tráfico potencial hacia la red 192.168.100.1 donde esta implementada la seguridad, previniendo así el tráfico externo que ataca a la red de datos en base al mapeo de conexiones, recordar que dentro

del IDS implementado para la seguridad de la red contiene una regla personalizada habilitada para su uso.

Gráfico 37: Alerta de seguridad IDS



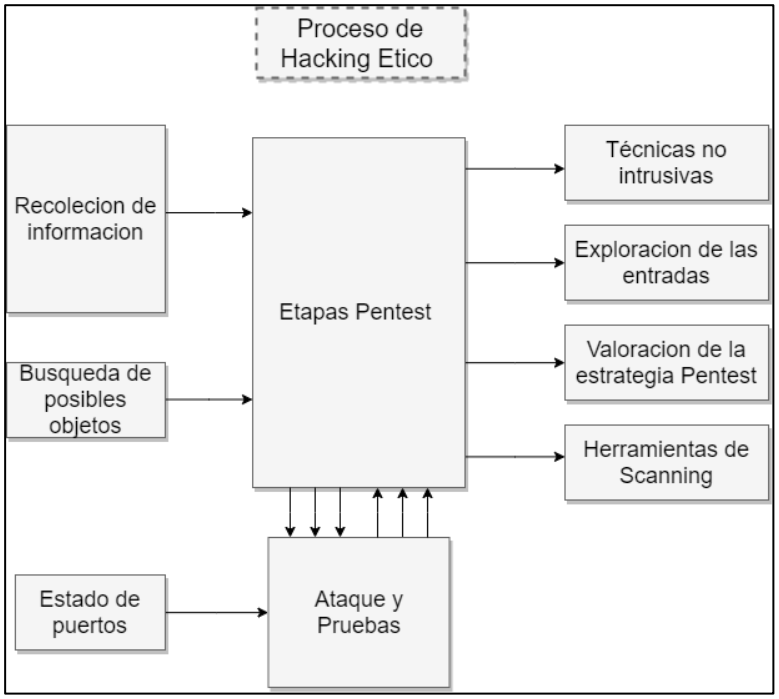
Fuente: Elaborado por las Investigadoras

Aplicado el IDS obtendremos como resultado que la comunicación de la red en la cooperativa SIERRA CENTRO SUCURSAL LA MANÁ, PROVINCIA DE COTOPAXI, se encuentra en estado activo todos los servicios ejecutados para la protección de ataques informáticos con identificación de red IP 192.168.100.1/24 estática; Manteniendo así la estabilidad de la comunicación empresarial con éxito, libre de tráfico externo potencial.

13.5.10. Proceso de hacking ético caja blanca

Para la aplicación del análisis técnico en la evaluación de las redes de datos de la cooperativa SIERRA CENTRO, se realizó la búsqueda de vulnerabilidades con el fin de tomar medidas preventivas en la comunicación de la entidad financiera, sin embargo para las pruebas de penetración orientadas a la seguridad informática se estableció el proceso de hacking ético de caja blanca, lo cual permitió en el proceso investigativo definir los procedimientos que se llevan a cabo para la aplicación de Pentest.

Gráfico 38: Etapas aplicadas de hacking ético caja blanca



Fuente: Elaborado por las Investigadoras

Dentro de las etapas del hacking ético de caja blanca se consideró lo siguiente:

- Realizar el debido proceso de escanear puertos y buscar vulnerabilidades mediante herramientas que permitan la obtención de posibles objetos.
- Utilizar técnicas no intrusivas con el fin de atraer y analizar ataques realizados por boots o ataques externos.
- Rastrear y examinar instalaciones de parches de seguridad, asegurando que estos complementos no puedan ser explotados.
- Aplicar de manera ética las etapas de caja blanca complementando con la normativa ISO 27001.

13.6. Informe técnico del análisis en las redes de datos

UNIVERSIDAD TÉCNICA DE COTOPAXI

FACULTAD DE CIENCIAS DE LA INGENIERÍA Y APLICADA

CARRERA DE INGENIERÍA SISTEMAS

13.6.1. Cargo del grupo

Tabla 13: Grupo de Estudiantes

Cargo	Nombre y Apellido
Director de análisis técnico	García Vega Ana Rebeca
Coordinador técnico informático	Morales Baren Dayana Jamileth

Fuente: Elaborado por las Investigadoras

13.6.2. Actividades de planificación de los resultados en la aplicación de pentesting informática de la cooperativa sierra centro sucursal la maná

Tabla 14: Actividades de la planificación

Actividad	Responsable de Ejecución	Responsable de seguimiento
Conformación del Equipo Auditor	Director de análisis técnico	Director de análisis técnico
Definición del Alcance y Objetivos	Coordinador técnico informático	Director de análisis técnico
Trámites en la Empresa	Coordinador técnico informático	Director de análisis técnico
Formalización de la Auditoría en la Organización	Coordinador técnico informático	Director de análisis técnico
Estructura de negocio de la entidad	Coordinador técnico informático	Director de análisis técnico
Antecedentes del Cooperativa Sierra Centro Sucursal La Maná	Coordinador técnico informático	Director de análisis técnico
Determinación del área por auditar de la Cooperativa Sierra Centro Sucursal La Maná.	Coordinador técnico informático	Director de análisis técnico
Definición de Áreas Críticas	Director de análisis técnico	Director de análisis técnico
Objetivo de la Revisión y Materia a Examinar	Director de análisis técnico	Director de análisis técnico
Normativa General	Coordinador de análisis técnico en Informática	Director de análisis técnico
Programa de Pruebas	Director de análisis técnico	Director de análisis técnico y Coordinador técnico informático

Ejecución del Plan del informe técnico en Informática	Director de análisis técnico y Coordinador técnico informático	Auditor de análisis informático
Evaluación del control Interno Informático	Coordinador técnico informático	Director de análisis técnico y Coordinador técnico informático
Recopilación de Información de la Organización	Coordinador técnico informático	Director de análisis técnico y Coordinador técnico informático
Análisis del Informe de la Organización	Coordinador técnico informático	Director de análisis técnico y Coordinador técnico informático
Recopilación de Información Operacional	Coordinador técnico informático	Director de análisis técnico y Coordinador técnico informático
Análisis de la Información Operacional	Coordinador técnico informático	Director de análisis técnico y Coordinador técnico informático
Recopilación de Información Detallada	Coordinador técnico informático	Director de análisis técnico y Coordinador técnico informático
Análisis de Información Detallada	Coordinador técnico informático	Director de análisis técnico y Coordinador técnico informático
Confirmar programa de pruebas	Coordinador técnico informático	Director de análisis técnico y Coordinador técnico informático
Ejecutar programa de pruebas	Coordinador técnico informático	Director de análisis técnico y Coordinador técnico informático
Reunión de cierre de equipo de auditoría	Coordinador técnico informático	Director de análisis técnico y Coordinador técnico informático
Presentación del Plan a la alta Dirección	Coordinador técnico informático	Director de análisis técnico y Coordinador técnico informático

Fuente: Elaborado por las Investigadoras

13.6.3. Objetivo

Evaluar al personal del departamento de Tecnología y Sistemas de la **Cooperativa Sierra Centro Sucursal La Maná** sobre los procesos, manipulación de los equipos de cómputo, para valorar su funcionamiento, detectar deficiencias, evaluación de la red de datos para así proponer aspectos principales para mejorar su eficiencia, funcionalidad y productividad de la entidad financiera.

13.6.4. Etapas

13.6.4.1. Análisis

En esta fase se determinará los objetivos del análisis técnico que se realizará al personal del departamento de Tecnología y Sistemas de la Cooperativa Sierra Centro Sucursal La Maná, después se debe realizar un inventario de todos los aspectos concernientes a los sistemas y usos informáticos en la empresa, con la colaboración entre gerente, empleados y técnicos informáticos.

13.6.4.2. Planificación

Luego de tener establecidos los objetivos del análisis técnico informático y los componentes informáticos que existen, así como los usos más habituales dentro de la empresa, se planificará análisis técnico a través de herramientas de análisis. Teniendo en cuenta cómo se va a evaluar cada uno de los puntos que ha analizar y con qué criterios.

13.6.4.3. Determinación de riesgos e incidencias

El mantenimiento preventivo y predictivo es clave en toda auditoría informática para analizar los posibles riesgos que existen de que se produzca un problema en el futuro. Por lo cual se prevén estos problemas mediante unas prácticas de mantenimiento efectivas, como método de seguridad informática.

13.6.4.4. Ejecución

En esta fase, se tomarán o aplicarán medidas ejecutivas para resolver los problemas actuales en los sistemas y equipos de cómputo y prevenir los riesgos que se podrían producir. Se debe elaborar un presupuesto con los puntos que habría que corregir para que se cumplan los objetivos de la empresa para mejorar la seguridad informática o adecuar sus sistemas a un determinado objetivo de productividad.

13.6.5. Entrevista dirigida al personal del departamento de tecnología y sistemas de la cooperativa sierra centro sucursal la maná

Se utilizará el método de entrevista de comprobación, la cual permitirá comprobar la información recopilada durante la evaluación, colaborar o rectificar los datos, percepciones, profundizar reforzar o cambiar en la evaluación.

Tabla 15: Entrevista al personal del departamento de tecnología Sierra Centro

CONCEPTO	CATEGORÍAS	INDICADOR	ÍTEMS
Recopilar y evaluar evidencias de la auditoría a realizar al personal del departamento de Tecnología y Sistemas de la Cooperativa Sierra Centro Sucursal La Maná.	**Recurso**	**Humano**	1. ¿El Depto. ¿De Tecnología cuenta con el personal suficiente para cubrir las necesidades de la institución? 2. ¿Se capacita al personal entorno al ámbito tecnológico? 3. ¿Se siente seguro en el área de trabajo? 4. ¿Cuenta usted con los recursos necesarios para ejercer su trabajo? 5. ¿Cree que el departamento cuenta con las medidas necesarias de seguridad? 6. ¿Existe una buena relación con su equipo de trabajo? 7. ¿Cree que el personal que labora en este departamento cuenta con la capacidad para ejercer su trabajo? 8. ¿Cumple con el horario de ingreso y salida establecidos? 9. ¿Ha tenido inconvenientes con alguien de su equipo de trabajo?
	Evidencias	**Control de Acceso**	10. ¿Existe control de acceso a los computadores para usuarios no autorizados? 11. ¿Existe un control de acceso de personal al departamento de Sistemas? 12. ¿Realizan copias o respaldos de información en caso

	Sistemas de Información	**Fallas Tecnológicas**	de presentar fallas en los sistemas o equipos de cómputo? 13. ¿Realizan mantenimientos preventivos y correctivos a los equipos de cómputo periódicamente? 14. ¿El Sistema operativo se encuentra operando en óptimas condiciones? 15. ¿El Sistema Informático cuenta con una licencia de pago? 16. ¿Los departamentos cuentan con claves de seguridad de cada máquina? 17. ¿Se mantienen programas y procedimientos de detección de virus para la seguridad de la información y los sistemas?
	Proceso	**Plan de Contingencia**	18. ¿La institución posee planes de contingencia ante cualquier eventualidad?

Fuente: Elaborado por las Investigadoras

13.6.6. Nivel de riesgos

La estimación del impacto de los activos tecnológicos es de manera cualitativa, lo cual se considera cada elemento tecnológico de gran importación en base a una determinada información que manipula; sin embargo, la pérdida de confiabilidad, disponibilidad e integridad de los activos tecnológicos afectan de manera prolongada con el trabajo de la entidad financiera.

Los niveles de riesgo establecidos son:

- **Nivel Alto:** Se requiere que su ejecución sea fuerte en la toma de acciones correctivas y preventivas para la empresa.
- **Nivel Medio:** Acción de ejecuciones necesarias en base a un plan desarrollado para la implementación de acciones en periodos no establecidos.
- **Nivel Bajo:** Observar un riesgo, pero no se determina si en la evaluación mediante el informe técnico tomará acciones correctivas o preventivas sobre los alcances de riesgos.

Tabla 16: Probabilidad de impacto

Vulnerabilidades	Nivel de Probabilidad	Principio de seguridad	Nivel de riesgo
Redes inalámbricas.	Alta	Confidencial	Alto
Control nulo en las redes de comunicación.	Alta	Disponibilidad	Alto
Falta de control en la asignación de IP.	Medio	Disponibilidad	Medio
Descarga de recursos externos mediante la red.	Alta	Disponibilidad	Alto
Poco mantenimiento a los activos tecnológicos.	Alta	Disponibilidad	Alto
Protocolos de red inseguros por falta de políticas de uso.	Alta	Confidencialidad Integridad Disponibilidad	Alto
Falta de políticas en el uso del VPS.	Alta	Confidencialidad Integridad Disponibilidad	Alto
No existen respaldos en la nube de la información.	Medio	Integridad	Alto
Uso de la misma clave de acceso a máquinas de oficina.	Alta	Confidencialidad Integridad Disponibilidad	Alto
Contraseñas no robustas.	Alta	Integridad	Alto
Uso de IP dinámica en las	Medio	Disponibilidad	Medio

máquinas de oficina.			
Inexistencia en el cifrado de información financiera en discos duros.	Alta	Confidencialidad Integridad Disponibilidad	Alto
Administración de VPS no periódica.	Alta	Disponibilidad	Medio
Vulnerabilidad TCP	Alta	Confidencialidad Integridad	Alto
Malas prácticas para el almacenamiento de información financiera.	Medio	Disponibilidad	Alto
Daño físico de la infraestructura de la red de comunicaciones LAN.	Bajo	Disponibilidad	Medio
Control en máquinas portables de la entidad financiera.	Alta	Confidencialidad Integridad	Alto
Bajo monitoreo de la red de datos de la entidad financiera.	Alta	Confidencialidad Integridad Disponibilidad	Alto
Personal a falta de capacitación sobre medidas de seguridad informática.	Medio	Confidencialidad Integridad Disponibilidad	Alto
Actualizaciones de software de terceros.	Medio	Disponibilidad	Medio
Errores en el cableado de red.	Medio	Disponibilidad	Medio
Falta de Configuración de firewall en la red de datos	Alta	Confidencialidad Integridad Disponibilidad	Alto
Uso de protocolos inseguros.	Alta	Confidencialidad Integridad Disponibilidad	Alto

Uso de ejecutables externos no confiables	Alta	Integridad	Alto
Brechas de seguridad vulnerables en el sistema financiero.	Alta	Confidencialidad Integridad	Alto
Políticas ante el uso de activos tecnológicos.	Medio	Disponibilidad	Bajo
Uso de versiones anteriores de software propietario.	Medio	Disponibilidad	Bajo
Sistemas operativos en ejecución sin licencia oficial.	Alta	Integridad	Alto
Fallas de conexión del proveedor de internet.	Bajo	Disponibilidad	Bajo
Falta de activación de Firewall en máquinas.	Alta	Confidencialidad Integridad Disponibilidad	Alto
Errores de cambios en la configuración de equipos activos.	Bajo	Disponibilidad	Bajo

Fuente: Elaborado por las Investigadoras

Realizado el levantamiento de activos tecnológicos, posibles amenazas y los niveles de riesgos como probabilidad e impacto, se estableció en el informe de probabilidades en la evaluación de riesgos lo siguiente:

- **Minimizar riesgos:** se deben implementar controles ante posibles tanto como los activos tecnológicos a nivel de hardware y redes de datos para las comunicaciones.
- **Trasladar riesgo:** en base al proceso evaluativo en análisis al riesgo, se debe contemplar la posibilidad de controles realizados por terceros, esto reduce costos.
- **Aceptar los niveles de riesgo:** ser conscientes y tener el conocimiento de los riesgos a los que se está expuesto ante alguna posibilidad de amenaza tanto interna como externa.

- **Evitar los niveles de riesgo:** estas acciones están contempladas en base al análisis de la probabilidad de impacto de una actividad en particular.

13.6.7. Diseño de la seguridad lógica informática en la red de datos de la cooperativa de ahorro y crédito sierra centro sucursal la maná

En base a la evaluación de la red de datos en la entidad financiera aplicando hacking ético mediante el test de penetración (Pentesting) se pudo determinar los puertos y brechas aperturada como puntos débiles de los estados de comunicación, con la presente información es factible realizar un estudio en el diseño de la seguridad lógica para la seguridad informática.

A continuación, se aplica el desarrollo de las medidas para la seguridad lógica en base a la normativa de estandarización internacional ISO 27001 como gestor de la seguridad de información; como complemento para el diseño lógico se aplica la metodología NIST que se utilizó al momento de analizar las vulnerabilidades en la red de datos.

13.6.8. Alcance de la propuesta para el diseño de la seguridad lógica en la red de datos

Para la implementación del diseño de la seguridad lógica en la red de datos se debe tener en cuenta que controles de seguridad puedan mitigar las vulnerabilidades en los canales de comunicación, lo cual serán señalados para su implementación en el plan de mitigación lo que ayudará a reducir el nivel de impacto a nivel de seguridad informática.

13.6.9. Esquema de seguridad lógica tipo firewall

- **Firewall de tipo perimetral:** Delimitará la salida del internet hacia el exterior en base a la configuración de reglas filtradas mediante el requerimiento del servicio de la entidad.
- **Proxy:** Se recomienda instalar proxy de software libre mediante la suite de Kali Linux para su configuración.
- **IDS:** Establecer el sistema de monitorización Snort como soporte de la penetración de intrusos, este complemento ya se encuentra instalado en el análisis y protección de la red de datos.

Como resultado se obtendrá la elaboración de un correcto sistema de gestión en la seguridad de la información, teniendo en cuenta que elementos que restringe de carácter

no técnico, sin embargo, se establecerá un marco lo cual se debe limitar; este contempla decisiones de gerencia de la entidad financiera como:

- Se dependerá de los recursos asignados por la entidad financiera.
- Planificación de gasto en base al presupuesto asignado.
- Cultura interna dentro del trabajo.

13.6.10. Mecanismos en el control de la seguridad lógica

Para la aplicación de los mecanismos de mitigación en base a la seguridad informática se aplicará la metodología NIST para el correcto análisis de los controles en la red de datos, mostrando así una lista de control que servirán para planificación y reestructuración de una red de datos, teniendo en cuenta que estos mecanismos son para minimizar o eliminar probabilidades de una amenaza o ataque externo antes brechas de seguridad vulnerables.

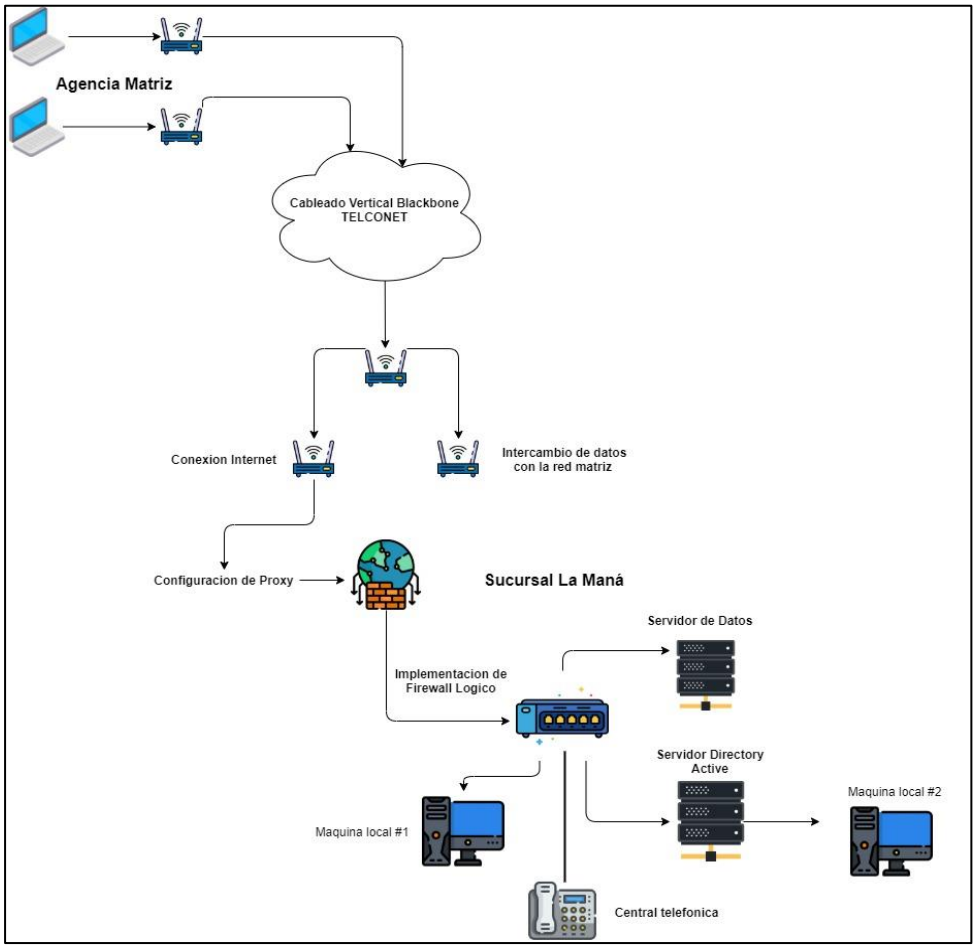
Tabla 17:Controles de seguridad en la red de datos

Vulnerabilidades	Nivel de Riesgo	Sugerencia para el control
Redes inalámbricas aperturadas	Alto	Hospot
Escaso control sobre las redes inalámbricas y ethernet	Alto	Hospot, Servidor
Falta de mecanismo para el control de la red	Alto	Firewall, Proxy
Falta de protocolos inseguros	Alto	Firewall, Proxy
Inexistencia de políticas de seguridad para la red de datos	Alto	Políticas de configuración de equipos activos
Falta de mantenimiento del servidor VPS	Alto	Hospot, Servidor
Inexistencia del respaldo de la información financiera	Alto	Concientización en temas de seguridad
Uso de los mismos (Accesos) por largos periodos a largo tiempo	Alto	Concientización en temas de seguridad
Contraseñas no robustas	Alto	Concientización en temas de seguridad
Uso de IP para los usuarios	Alto	Concientización en temas de seguridad
Inexistencia de cifrados en discos duros de la entidad	Alto	Cifrado
Vulnerabilidad TCP/IP	Medio	Políticas de monitorización
Fuga de información de la entidad financiera	Medio	Políticas de confidencialidad
Control de acceso débil en aplicaciones externas	Alta	Capacitación del personal técnico

Falta de mantenimiento en los equipos	Alta	Mantenimiento preventivo y correctivo
Uso de protocolos de comunicación inseguros	Alta	Implementación de comunicación cifrada

Fuente: Elaborado por las Investigadoras

Gráfico 39: Esquema de seguridad lógica de la red de datos de la cooperativa



Fuente: Elaborado por las Investigadoras

Para la implementación de seguridad informática se recomienda establecer bases metodológicas mediante estándares internacionales, el proyecto de investigación se basa en aplicar la norma ISO 27001, esto se debe al control de acceso que debe cumplir, cabe recalcar que esta norma cuenta con controles previamente establecidos, no es obligatorio acatarlos; sin embargo, esto se centrará en aquellos que nos permitan diseñar e implementar seguridad informática en la red de datos de la cooperativa.

13.6.11. Control para la red de datos aplicando la norma 27001

En base al análisis de las vulnerabilidades ya detectadas en la red de datos de la entidad financiera, es necesario hacer uso de la metodología NIST para determinar mecanismos adecuados para mitigar brecha vulnerable pertinente a la red donde se aplicó el pentesting.

Tabla 18: Declaración de estado de factibilidad

Objetivo del control	Control	Factibilidad	Justificación
Organización de la interna financiera	Control de políticas para la seguridad de la información	Objetivo factible	Como entidad financiera se deben establecer políticas de administración, control y configuración de los activos tecnológicos.
Responsabilidad en los activos tecnológicos de la entidad financiera	Inventario de los activos informáticos	Objetivo factible	Se debe tener en conocimiento los activos declarados mediante documentación de los mismos, asignando a los responsables de dichos equipos
Gestión de acceso a los usuarios de los equipos de aplicaciones financieras de la entidad financiera.	Uso de información confidencial de la empresarial	Objetivo factible	En la actualidad es necesario establecer políticas de seguridad para el control de las Tics, de esa manera se evita que personas externas accedan a información confidencial.
Gestión de la seguridad en la red de datos	Control de redes Mecanismo de seguridad Optimización de redes	Objetivo factible	Para definir la gestión en seguridad, es importante establecer los mecanismos que permitan aplicar la seguridad necesaria para sus comunicaciones; definir segmentos óptimos de red en base a requerimientos a las necesidades de la infraestructura tecnológica.
Requerimientos de seguridad de la red de datos y sistemas de información	Seguridad de las comunicaciones accesibles mediante red privada	Objetivo factible	Los mecanismos implementados resguardaran las comunicaciones establecidas direccionando al internet y el acceso al VPS de la cooperativa.
Seguridad de la información mediante los suministros de comunicación.	Políticas de seguridad para la información de suministros	Objetivo factible	Se recomienda establecer políticas para la adquisición de activos tecnológicos por terceros

			para definir así riesgos que se puedan presentar sus servicios.
Gestión en los incidentes que pueden ser causados por falta de seguridad de la información	Responsabilidades la asignación de procedimientos Notificación de puntos débiles de la seguridad	Objetivo factible	Necesario e imperativo estar al constante control de las medidas en seguridad, sin embargo, el cumplimiento de políticas se establece para el resguardo de la información confidencial.

Fuente: Elaborado por las Investigadoras

13.6.12. Políticas de acceso en el control de la información

Los recursos importantes dentro de una organización financiera es la información por la que se tiene que resguardar para el correcto desarrollo de la actividad. Las políticas giran en torno a la seguridad de la información siendo así un mecanismo operacional de los sistemas informáticos y redes de comunicación, para cumplir con lo mencionado; se deben establecer objetivos de la entidad financiera Sierra Centro para así minimizar el riesgo al daño de cualquier tipo.

Se deben establecer compromisos internos dentro de la institución para que la difusión y complimiento de la misma sea la correcta mediante una política direccionada a salvaguardar la información:

13.6.12.1. Objetivos de políticas de acceso

- Respaldar la información que genera el ente financiero y a su vez los recursos físicos de Tics, frente a amenazas externas de cualquier tipo. De esta manera se asegura la confiabilidad, integridad y disponibilidad de los datos financieros.
- Instaurar directrices para los procedimientos y requerimientos necesarios para asegurar la información mediante protecciones que respondan oportunamente mediante los recursos Tics de la cooperativa Sierra Centro.

13.6.12.2. Alcance de las políticas de acceso

La investigación y documentación está direccionada al personal de la cooperativa de ahorro y crédito Sierra Centro, manifestando las políticas, normas y procedimientos que genera la cooperativa mediante la operación de servicios a nivel tecnológico. El no cumplir con los lineamientos en las políticas de acceso establecidas tendrá como resultado

medidas severas. Las políticas se establecen a nivel centralizado para resguardar la seguridad de la información, la protección de las redes de datos y sus comunicaciones a través de la red, procedimientos y requerimientos necesarios para implementar mecanismos de seguridad de la cooperativa; al mismo tiempo el uso de los servicios de correo corporativo.

13.6.13. Seguridad informática a nivel lógico

13.6.13.1. Identificar

Para establecer el acceso a la información, debe ser emitido mediante escrito un procedimiento de manera formal y de manera escrita que exija al acceso de la información dependiendo de sus requerimientos con los siguientes atributos:

- Identificación del ID establecido en el carnet de la cooperativa.
- Nombres y Apellidos completos.
- Área donde labora.
- Justificar el motivo o razón por la cual requiere la información.

13.6.14. Seguridad a nivel de red de datos y telecomunicaciones

13.6.14.1. Topología de la red de datos

- Disponibilidad de la documentación sobre las topologías de la red realizadas por la entidad que realizó la configuración de la infraestructura de la red de datos
- Disponibilidad de medios de transmisión dado el caso que alguna contingencia afecte a elementos de comunicación primarios

13.6.14.2. Red de Datos

Las redes de datos de la cooperativa Sierra Centro son esenciales para la comunicación, cuál función debe recopilar determinada información como:

- Ancho de banda asignado y utilizado.
- Tráfico de red interna y externa.
- Recursos que utilizan las máquinas.
- Intentos de Intrusión mediante tráfico SSH.
- Uso de protocolos externos para acceder a la red de datos de manera ilegal.

13.6.14.3. Uso de los sistemas de comunicación

Los sistemas de comunicación de la entidad financiera deben utilizarse para las actividades de suma importancia. El uso formal o personal es necesario siempre y cuando se respete los límites de tiempo y recursos, lo cual estos no pueden interferir con la productividad de los empleados de la cooperativa.

13.6.14.4. Conexiones externas de la red de datos

- Los servicios de red implementados en la cooperativa se usan sólo con propósitos relacionados con la comunicación financiera mediante previa autorización de la gerencia.
- El tráfico de red interno y externo debe ser filtrado por un Firewall lógico prohibiendo así el paso al que no se encuentre autorizado.
- El uso de la conexión a internet debe ser analizado y monitoreado constantemente para así evitar que las conexiones entrantes penetren en la vulneración de la red de datos.

13.6.14.5. Firewall

El firewall que se implemente a futuro para la entidad financiera debe presentar una postura de negación en base a sus reglas y configuraciones lo cual prohíba el acceso de los protocolos TCP y servicios de conexiones entrantes externas hacia la red de datos. El personal asignado para el mantenimiento de la red de datos tiene que documentar el proceso de actividades como resultados, manifestando a continuación:

13.6.14.6. Ataques a la red de datos

- La red de datos debe ser monitoreada con herramientas de software libre, recomendable utilizar Kali Linux con la suite que viene en el paquete de instalación.
- La red debe disminuir en respuesta ante ataques DoS de manera lógica para así disminuir el riesgo de phishing.
- Los archivos y gestores de contraseña deben ser encriptados mediante estrictos controladores en base al acceso lógico para así disminuir el riesgo de pistas que se pueden dar como información valiosa para el atacante externo.

13.6.15. Seguridad en software de terceros

13.6.15.1. A nivel de software

La cooperativa tiene que contar con licencia de software original, adquirida dependiendo del proveedor y herramienta a utilizar, esto se traduce en obtener la serie original numérica para evitar sufrir sanciones o limitantes al momento de ejecutar los programas en los dispositivos electrónicos como las computadoras.

Obtener la licencia original de cada herramienta es garantía de soporte de parte del proveedor identificando, así como un software autorizado. Sin embargo, la entidad también puede hacer uso de programas sin licencia, pero con la responsabilidad en que estas herramientas no cuentan con soporte son descargas externas y obtenidos por terceros lo cual representa un problema a futuro para la empresa.

13.6.15.2. Manipulación y control de las máquinas

- Se debe aplicar el correcto procedimiento apegado al plan establecido en el control de seguridad de software de terceros, para que este se ejecute de acuerdo al perfil de cada usuario.
- Los cambios en configuraciones en los perfiles de usuario se deben hacer mediante respaldos de información y de una configuración existente.
- Se deberá documentar los procedimientos de instalación tanto de una configuración, mantenimiento y reparación.
- Realizar un comunicado por escrito a la entidad financiera sobre cualquier cambio de producto o software antes de adquirir; justificar el cambio en los equipos de las oficinas.

13.6.15.3. Gestión y control de datos en las aplicaciones instaladas

Para la gestión y protección de controles al acceso de información y recursos compartidos como carpetas distribuidas en la red. Solo el administrador de la oficina de Tics es el encargado de manipular y obtener el acceso a ellas, con respecto al convenio de terceros para el desarrollo de aplicaciones dependiendo de la necesidad de la entidad financiera debe hacer entrega de una previa documentación y archivos que son los siguientes:

- Aplicación ejecutable; Si es para su ejecución en entornos de escritorio es indispensable montar el gestor de base de datos y la última versión del aplicativo desarrollado.
- Aplicación de tipo web: Debe entregar al departamento el código fuente, documentación de ejecución y uso detallado de los servidores donde está montado el software.
- Documentar la utilización de software proveniente de terceros para la entidad, este tiene que ser analizado y firmado por la gerencia de la cooperativa.

13.6.16. Seguridad física de la entidad financiera

Los recursos como los activos tecnológicos tanto físicos como lógicos deben solo emplearse en ambientes seguro como lo son a continuación:

- Ambiente seguro sin impactar las medidas de control para la protección del hardware, software y manipulación de datos.
- Por políticas establecidas en el informe de auditoría, queda prohibido el consumo de comida y consumo de tabaco en las estaciones de trabajo.
- Se deberán proteger los activos tecnológicos de riesgos que provocan el medio ambiente como el polvo y salpicaduras de agua.
- La pérdida o sustracción de los componentes debe ser reportada por el encargado de Tics.

13.6.16.1. Gestión y control del acceso físico de equipos de cómputo

- Asegurar que las personas que ingresen a la oficina donde se gestionan los activos tecnológicos y áreas restringidas de la entidad financiera deberá ser escoltado por el encargado de la oficina para que este sea autorizado a ingresar.
- Las personas que ingresan deben de cumplir con los elementos de identificación, que sean autenticados y aprobados por el gerente de la entidad financiera para poder ingresar.
- Los servidores VPS tienen que tener establecidas reglas de acceso para su configuración o para realizar mantenimiento preventivo.

13.6.17. Gestionar respaldo de información de la cooperativa

13.6.17.1. Recuperar información extraviada

La persona asignada en la seguridad de la información de la entidad financiera es el máximo responsable que gestiona la tarea de realizar backup o copias de seguridad de la información empresarial, debe tener en cuenta que al momento de realizar respaldos debe recurrir al informe técnico de auditoría que menciona lo siguiente:

- El responsable debe almacenar la ubicación de las copias más recientes generadas ya sea de una máquina local o respaldo de una determinada información del servidor que se esté utilizando.
- Asignar determinada información a un nivel de protección tanto lógica como física y ambiental, según las normas establecidas. Resguardar los controles aplicados para la extracción de información de los dispositivos vinculados a red la de datos.
- Verificar de manera periódica el procedimiento de backup y restauración de información garantizando así el cumplimiento del rol asignado en base a la tarea de gestionar respaldos a través de la recuperación de documentación o información de gran relevancia mediante procesos operativos tecnológicos.

13.6.18. Protección ante ataques y penetración de software malicioso

Para la protección ante ataques maliciosos y penetración a las máquinas de la entidad financiera se debe tener en cuenta las nuevas políticas establecidas por el análisis técnico realizado:

- No utilizar software no autorizado por la entidad financiera.
- Actualizar el gestor de la base de datos del antivirus de manera continua.
- Revisar de manera periódica el contenido del software para los equipos de procesamiento en base a los activos no aprobados o modificaciones no autorizadas sin contemplar lo que menciona la recomendación del análisis.
- Realizar la gestión de configuración del Firewall para la prohibición de acceso de una red externa a los canales de información.
- Verificar la presencia de virus mediante el mantenimiento correctivo y preventivo, gestionar los correos electrónicos empresariales de manera correcta para prevenir infecciones de enlaces externos no autorizados.

- Redactar cada procedimiento para la verificación de información que represente semejanza con algún tipo de software malicioso, garantizando así las alertas que se pueden dar.
- Generar conciencia al personal que labora en la entidad financiera, asesorar con charlas técnicas para el conocimiento de los virus informáticos y cuál es su afectación y causas que pueden generar.

13.6.19. Gestionar la seguridad en la red de datos

La persona asignada para la gestión de la seguridad en la red de datos debe documentar de manera técnica las normas establecidas en base a la auditoría realizada que se muestran a continuación:

- Integridad y confiabilidad de la información que genera la red de datos.
- Implementar aspectos técnicos como controles especiales en base a la asignación de reglas para mantener la disponibilidad de los servicios en red.
- El responsable del cargo debe garantizar mediante las actividades de supervisión y controles que sean aplicados para el procesamiento de información en la red de datos.
- Reportar y documentar de manera técnica accesos de terceros ante posibles ataques informáticos a la red de datos.

13.6.19.1. Gestionar medios removibles

- Realizar una correcta eliminación de contenidos que influyan en el rendimiento de las comunicaciones en las oficinas operativas de la entidad financiera.
- Aplicar el almacenamiento de recursos tecnológicos en un ambiente seguro y protegido.

13.6.19.2. Servicios en la red de datos

Las conexiones a la red de datos de la cooperativa no son seguras, esto puede afectar a la productividad laboral, por lo tanto, mediante el presente informe de auditoría se asignará el control de acceso a los servicios de la red, tanto internos como externos. Es necesario que se garantice la funcionalidad al acceso a la red y todos sus servicios.

El administrador encargado de la red debe responder ante la otorgación de los servicios, únicamente mediante un pedido formal a los representantes de la entidad financiera, este

control de los servicios en la red de datos es importante por las conexiones de la red que están ancladas a las aplicaciones financieras que procesan información de gran relevancia. Por ello, se establecerá punto a considerar para la activación en los accesos a la red de datos, estos son los siguientes:

- Identificar y examinar las redes de datos en base a su protocolo TCP.
- Aplicar la norma ISO 27001 para la realización de procedimientos en la modificación de las comunicaciones.
- Realizar procedimientos de autorización para asignar a personas, redes de datos, permisos a los cuales se otorgará el acceso.
- Establecer privilegios para el control en la implementación de la seguridad lógica de la red de datos para su proceso de análisis, configuración y ejecución.

13.6.20. Declaración de analís técnico

Nosotras García Vega Ana Rebeca y Morales Baren Dayana Jamileth, como equipo auditor informático se aplicó el siguiente informe técnico mediante la investigación: SEGURIDAD INFORMÁTICA MEDIANTE HACKING ÉTICO EN LA APLICACIÓN DE PENTESTING PARA EL ANÁLISIS DE VULNERABILIDADES EN LAS REDES DE DATOS DE LA COOPERATIVA SIERRA CENTRO SUCURSAL LA MANÁ, PROVINCIA DE COTOPAXI, notificando al gerente de la sucursal; Ing. Wilmer Alcaciega Guanín; sobre los problemas que existen en la entidad financiera en los procesos de comunicación de las redes de datos y sus altos niveles de inseguridad ante posibles ataques informáticos, manifestando los correctivos necesarios para que sean implementados de acuerdo a la toma de las decisiones gerenciales en base al informe técnico informático.

14. IMPACTO DEL PROYECTO

14.1. Impacto técnico

Se realizó la aplicación de un test de penetración (Pentesting) basado en las normativas ISO 27001, las cuales servirán para evaluar los riesgos y amenazas ante ataques informáticos que pueden suceder a futuro en la cooperativa de ahorro y crédito Sierra Centro, sucursal La Maná, permitiendo así brindar protección, confidencialidad, integridad y disponibilidad de la información de la entidad financiera.

14.2. Impacto social

Las políticas de seguridad informática orientadas a las normativas ISO 27001 aplicadas en las empresas son de gran importancia, lo cual permite proteger los activos tecnológicos como empresa y económicos de los socios afiliados a la entidad financiera para así hacer frente a situaciones que conjeturé una amenaza, permitiendo controlar el acceso a los equipos informáticos y sistemas de comunicación como las redes de datos, reduciendo así amenazas externas y riesgos presentes en una institución.

14.3. Impacto económico

Por medio del diseño de una evaluación de las redes de datos orientadas a nuevas políticas de seguridad de la información en la entidad financiera, se podrán reducir los costos o pérdidas de información relevante, problemas que se suscitan con equipos de comunicación y dispositivos electrónicos; los costos asociados en solucionar este tipo de inconvenientes se generan a través de un contrato dirigido al personal especializado lo cual mediante en la aplicación del desarrollo de la investigación generó un ahorro de inversión en mano de obra de $3.355 dólares.

15. PRESUPUESTO PARA LA PROPUESTA DEL PROYECTO

Tabla 19: Presupuesto del proyecto de investigación

RECURSOS			
Gastos Directos	**Cantidad**	**Precio Unitario**	**Total**
Mano de obra	2 personas	260,00 (3 Meses)	1560.00
Internet	6 meses	35,00	210.00
Pendrive	1	10,00	10.00
Sub- total			**1780.00**
Servicios			
ZAP	3 meses	75,00	225.00
Subtotal			**225.00**
TOTAL			**2005.00**

Fuente: Elaborado por las Investigadoras

- En la utilización del apartado tecnológico para la realización del análisis técnico mediante software libre como: VirtualBox y el sistema operativo de ofensiva Kali Linux perteneciente a la distribución de CENTOS, permitieron ahorrar costos ya que son programas o distribuciones de licencia gratuita. Por lo tanto, se generar $0.00 costos para la cooperativa de ahorro y crédito “Sierra Centro”.

- Para la aplicación de las evaluaciones en las redes de datos de la entidad financiera se debe considerar que los costos asociados en solucionar este tipo de análisis se generan a través de un contrato dirigido al personal especializado, teniendo en cuenta que el valor total de la mano de obra tiene un costo de $5.360, pero mediante la aplicación del desarrollo de la investigación se generó un ahorro de inversión en mano de obra de $3.355 dólares.

16. CONCLUSIONES Y RECOMENDACIONES

16.1. Conclusiones

- La investigación permitió identificar mecanismos y herramientas en la aplicación de pentesting en el análisis y evaluación de una red de datos, obteniendo como resultado la detección de brechas vulnerables en la red mediante los puertos de comunicación, aplicando así las normativas de la organización internacional de normalización ISO 27001.

- El análisis de las redes de datos, permitió aplicar los procesos que se llevan a cabo ante las pruebas realizadas en diversos métodos de implementación como la utilización de scanner de conmutadores mediante NMAP; y a su vez obtener los resultados esperados mediante el uso de entornos de virtualización de software libre.

- La aplicación de seguridad informática mediante pentesting permitió en el desarrollo de la investigación, implementar de manera correcta diversos mecanismos entre los cuales se encuentra la configuración de seguridad básica en el uso de IDS (Intrusion Detection System), teniendo como resultado la protección de la red interna.

16.2. Recomendaciones

- Es significativo identificar los aspectos que intervienen en la aplicación de la metodología adecuada para el estudio de pentesting orientado a la detección y evaluación de vulnerabilidades tanto de información como de equipo tecnológico, esto permitirá en el proceso investigativo identificar que normas de la organización de normalización ISO implementar en seguridad informática.

- Dentro del análisis técnico es recomendable detallar y documentar los procesos operativos, lo cual permitirá listar las tareas basadas en mantenimientos previstos en la recuperación de procedimientos, tanto en la explotación de vulnerabilidades hasta contratiempos y análisis de seguridad ante futuros incidentes.

- Es recomendable realizar análisis periódicos y monitorización continua en las redes de datos para así evitar vulnerabilidades ante futuros ataques de información de la entidad, lo cual tiene que ser un proceso continuo de acciones puntuales basadas en la implementación de la norma ISO 27001.

17. BIBLIOGRAFÍA

- Garces, S. (2015). Seguridad informática para la red de datos en la cooperativa de ahorro y crédito unión popular ltda. 23-09-2021, de Universidad técnica de Ambato Sitio web: http://repositorio.uta.edu.ec/handle/123456789/8654
- Rojas, A. (2018). Hacking ético para analizar y evaluar la seguridad informática en la infraestructura de la empresa plasticaucho industrial s.a. 23-09-2021, de Universidad Técnica De Ambato Sitio web: http://repositorio.uta.edu.ec/handle/123456789/28102
- Lino, C. (2019). Diseño de un plan de seguridad informática para la cooperativa de ahorro y crédito "por el pan y el agua" de la ciudad de jipijapa. 22-11-2021, de universidad estatal del sur de Manabí Sitio web: http://repositorio.unesum.edu.ec/bitstream/53000/1543/1/UNESUM-ECU-SIATEMAS-2019-09.pdf
- Borbor, R. (2020). Análisis proactivo de amenazas de la seguridad informática y de la información para la infraestructura de servidores y red de la dirección de TIC de un GAD Municipal. 22-11-2021, de Universidad estatal península de santa elena Sitio web: https://repositorio.upse.edu.ec/xmlui/bitstream/handle/46000/5649/UPSE-TIN-2020-0015.pdf?sequence=1&isAllowed=y
- Zatán, L. (2017). Plan de seguridad informática basada en la norma ISO 27002 para el control de accesos indebidos a la red de Uniandes puyo. 23-09-2021, de UNIANDES Sitio web: https://dspace.uniandes.edu.ec/handle/123456789/6762
- Mancheno, T., & Robles, I. (2013). Vulnerabilidades y seguridad en redes tcp/ip. 23-09-2021, de UCSG Sitio web: http://201.159.223.180/bitstream/3317/1399/1/T-UCSG-PRE-TEC-ITEL-13.pdf
- Bonilla, M. (2016). Análisis y diseño de un sistema de seguridad de red perimetral en la Empresa Aseguradora del Sur. 23-09-2021, de Pontificia Universidad Del Ecuador Sitio web: http://repositorio.puce.edu.ec/handle/22000/11158
- Valencia., Orozco, M. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27001.Colombia: ScieloPortugal.http://www.scielo.mec.pt/scielo.php?script=sci_arttext&pid=S1646-98952017000200006&lng=en&tlng=en
- Freire, F. (2014). Implementación del modelo de gestión de la seguridad de la información aplicando iso 27001 en la empresa coka tours, ambato – ecuador. 4 de

Julio Del 2020, De Universidad Central Del Ecuador Sitio Web: Http://Www.Dspace.Uce.Edu.Ec/Bitstream/25000/4244/1/T-UCE-0011-55.Pdf

- Corporación de Estudios y Publicaciones. (2008). Constitución De La República Del Ecuador. Ecuador: CEP Corporación de Estudios y Publicaciones.https://elibro.net/es/ereader/utcotopaxi/115730?page=676
- Gómez, A. (2014). Seguridad en Equipos Informáticos. España: RA-MA Editorial https://elibro.net/es/ereader/utcotopaxi/62466
- Ficarra, F. (2002). Antivirus y Seguridad Informática. Ecuador: Editorial Chasqui https://elibro.net/es/ereader/utcotopaxi/17919
- Primicias. (16 De septiembre). Empresa Ecuatoriana protagoniza filtración de datos. Quito. Primicia.Ec Recuperado de https://www.primicias.ec/noticias/tecnologia/datos-17-millones-ecuatorianos-fueron-filtrados/
- Patiño, I. (1 De octubre del 2019). Masiva filtración de datos habría afectado a 200 millones en Android y iOS. []. Recuperado de https://socialgeek.co/tech/filtran-200-millones-datos-usuarios-ios-android/
- Uleam.Ec. (2015). Política de seguridad de la información. Ecuador. Uleam.Ec Recuperado de https://www.uleam.edu.ec/wp-content/uploads/2016/10/Politica-de-seguridad-de-la-informacion.pdf
- Chávez, J. (2016). Análisis y modelos de datos de redes para seguridad informática. 22-11-2021, de universidad de chile facultad de ciencias físicas y matemáticas ´ departamento de ingeniería eléctrica Sitio web: https://repositorio.uchile.cl/bitstream/handle/2250/138269/Analisis-y-modelos-de-datos-de-redes-para-seguridad-informatica.pdf?sequence=1&isAllowed=y
- López, Y. (2009). Los virus informáticos: una amenaza para la sociedad. Cuba: Editorial Universitaria Cuba: https://elibro.net/es/ereader/utcotopaxi/71403
- Costas, J. (2014). Seguridad informática. España: RA-MA, S.A Editorial y Publicaciones: https://elibro.net/es/lc/utcotopaxi/titulos/62452
- Guillen, L. (2017). Introducción al pentesting. 25-09-2021, de Universidad De Barcelona Sitio web: http://diposit.ub.edu/dspace/bitstream/2445/124085/2/memoria.pdf
- Alvarado, J. (2017). Análisis de las vulnerabilidades en seguridad informática de los equipos de cómputo y redes de la Municipalidad Distrital de Independencia, mediante

el uso de phishing. 22-11-2021, de Universidad Señor Sipán Sitio web: https://repositorio.uss.edu.pe/handle/20.500.12802/8170

- Baca, G. (2016). Seguridad Informática. México: Grupo Editorial Patria.
- Fernández, Y. (2020). VirtualBox. 26-09-2021, de Xataka Sitio web: https://www.xataka.com/basics/virtualbox-que-como-usarlo-para-crear-maquina-virtual-windows-u-ot
- Rubén, A. (2016). Herramientas de seguridad informática y Kali Linux. 26-09-2021, de computerhoy Sitio web: https://computerhoy.com/paso-a-paso/software/que-es-kali-linux-que-puedes-hacer-41671
- De la Fuente, J. (2018). Herramientas de seguridad informática. 26-09-2021, de Marindelafuente Sitio web: https://www.marindelafuente.com.ar/que-es-nmap-por-que-necesitas-este-mapeador-de-red/
- Espinoza, O. (2019). Tutoriales de Internet Qué es y para qué sirve Whois. 26-09-2021, de redeszone Sitio web: https://www.redeszone.net/tutoriales/internet/que-es-whois/
- Deyimar, A. (2020). Cómo usar el comando Dig en Linux. 26-09-2021, de Hostinger Sitio web: https://www.hostinger.es/tutoriales/comando-dig-linux
- Esteban, S. (2016). Burp Suite: Potente herramienta para Pentesting Web. 26-09-2021, de backtrackacademy Sitio web: https://backtrackacademy.com/articulo/burp-suite-potente-herramienta-para-pentesting-web
- Sánchez, C., & Piattini, M. (2012). Modelo para el gobierno de las Tics basadas en las normas ISO. España: AENORediciones.
- Ayala, J. (2016). Metodología de Pruebas de Penetración Issaf. 17-02-2022, de Scrib Sitio web: https://es.scribd.com/document/93966058/Metodologia-de-pruebas-de-penetracion-issaf
- COIP. (2014). Código Orgánico Integral Penal. 17-02-2022, de Asamblea Nacional De La Republica Del Ecuador Sitio web: https://tbinternet.ohchr.org/Treaties/CEDAW/Shared%20Documents/ECU/INT_CEDAW_ARL_ECU_18950_S.pdf

18. ANEXOS

Anexo 1: Curriculum Vitae Docente tutor MSc. Najarro Quintero Rodolfo

UNIVERSIDAD TÉCNICA DE COTOPAXI

DATOS PERSONALES

APELLIDOS: Najarro Quintero
NOMBRES: Rodolfo
ESTADO CIVIL: Casado
CEDULA DE CIUDADANÍA: 172523456-9
NÚMERO DE CARGAS FAMILIARES: 2
LUGAR Y FECHA DE NACIMIENTO: Cuba/ 14/07/1971
DIRECCIÓN DOMICILIARIA: El Guayacán, Quevedo.
TELÉFONO CONVENCIONAL: ----
TELÉFONO CELULAR: 0987309973
EMAIL INSTITUCIONAL: rodolfo.najarro@utc.edu.ec
TIPO DE DISCAPACIDAD: Ninguna
 # DE CARNET CONADIS: -----

ESTUDIOS REALIZADOS Y TÍTULOS OBTENIDOS

NIVEL	TITULO OBTENIDO	FECHA DE REGISTRO	CÓDIGO DEL REGISTRO CONESUP O SENESCYT
TERCER	INGENIERO MECÁNICO	04/julio/2008	CU-08-1186
CUARTO	MAGISTER EN CONECTIVIDAD Y REDES DE ORDENADORES	11/septiembre /2015	1014-15-86067819

HISTORIAL PROFESIONAL

INSTITUCION	DEPENDENCIA	CARGO
Fab.Filtros,Juntas y Accesorios Aulet y Casals	Producción	Ingeniero Especialista Técnico
Fab.Filtros,Juntas y Accesorios Aulet y Casals	Ventas	Jefe de Departamento de Ventas
Transtur	Mantenimiento	Ingeniero Especialista en Mantenimiento
Cubacar	Producción	Jefe de Taller
Cubacar	Producción	Asesor Técnico
Dekorando	Producción	Jefe de Planta
Scotland School	Educación	Docente
Tekquimik	Ventas	Asesor Técnico
Fundación Augusto Cesar Saltos	Educación	Docente
Univ. Técnica Estatal de Quevedo	Educación	Docente
SNNA UTEQ	Educación	Docente
ESCUTEQ	Educación	Docente

Instituto Tecnológico Superior Siete de Octubre	Educación	Docente
Univ. Técnica Estatal de Quevedo	Educación	Docente
Universidad Técnica de Cotopaxi	Educación	Docente

UNIDAD ADMINISTRATIVA O ACADÉMICA EN LA QUE LABORA: Facultad de Ciencias de la Ingeniería y Aplicadas

ÁREA DEL CONOCIMIENTO EN LA CUAL SE DESEMPEÑA: Sistemas de Información

FECHA DE INGRESO A LA UTC: 14/04/2017

Anexo 2: Curriculum Vitae Autora García Vega Ana Rebeca

CURRICULUM VITAE

INFORMACIÓN PERSONAL

Nombres y Apellidos: Ana Rebeca García Vega

Cédula de Identidad: 120528338-3

Lugar y fecha de nacimiento: Los Ríos – Valencia 16/08/1997

Estado Civil: Soltero

Tipo de Sangre: O+

Domicilio: Valencia–Ciudadela La Moderna

Teléfonos: 0988259160

Correo electrónico: ana.garcia3383@utc.edu.ec

ESTUDIOS REALIZADOS

Primer Nivel:

- Escuela Fiscal Mixta Víctor Manuel Rendón

Segundo Nivel:

- Unidad Educativa Lcdo. Manuel Viteri Camacho

Tercer Nivel:

- Universidad Técnica de Cotopaxi Extensión La Maná

TÍTULOS

- Bachiller en Aplicaciones Informativas, 11 de marzo del 2015
- Suficiencia en Ingles (Nivel B1)

IDIOMAS

- Español (nativo)
- Suficiencia en el Idioma Inglés Nivel B1

CURSOS DE CAPACITACIÓN :

- Primera Jornada Científica Internacional de Informática – UTC La Maná 2016
  Dictado: Universidad Técnica de Cotopaxi

  Lugar y fecha: La Maná 06 hasta el 08 de julio del 2016

  Tiempo: 40 horas

- II Jornadas Informáticas - UTC La Maná
  Dictado: Universidad Técnica de Cotopaxi

  Lugar y fecha: La Maná 12 hasta el 14 de julio del 2017

  Tiempo: 40 horas

- III Jornadas Informáticas - UTC La Maná
  Dictado: Universidad Técnica de Cotopaxi

  Lugar y fecha: La Maná 10 hasta el 12 de julio del 2018

  Tiempo: 40 horas

- IV Congreso Internacional De Investigación Científica - UTC La Maná
  Dictado: Universidad Técnica de Cotopaxi

  Lugar y fecha: La Maná 08 hasta el 10 de mayo del 2019

  Tiempo: 40 horas

- Capacitación Académica de Ingeniería en Sistema de Información 2020 – UTC La Maná **Dictado:** Universidad Técnica de Cotopaxi
  Lugar y fecha: La Maná 03 hasta el 07 de agosto del 2020

  Tiempo: 40 horas

- V Congreso Internacional De Investigación Científica - UTC La Maná
  Dictado: Universidad Técnica de Cotopaxi

  Lugar y fecha: La Maná 02 hasta el 04 de diciembre del 2020

  Tiempo: 40 horas

- VI Congreso Internacional De Investigación Científica - UTC La Maná

  Dictado: Universidad Técnica de Cotopaxi

  Lugar y fecha: La Maná 17 hasta el 21 de enero del 2022

  Tiempo: 40 horas

REFERENCIAS PERSONALES

- ING. EDUARDO CATOTA TLF: 0979034823
- ING. CRISTIAN ANGULO TLF: 0992197361

Anexo 3: Curriculum Vitae Autora Morales Baren Dayana Jamileth

CURRICULUM VITAE

INFORMACIÓN PERSONAL

Nombres y Apellidos: Dayana Jamileth Morales Baren

Cédula de Identidad: 120826209-5

Lugar y fecha de nacimiento: Los Ríos – Valencia 31/07/1997

Estado Civil: Soltero

Tipo de Sangre: O+

Domicilio: Valencia–Parroquia La Unión-Lotización San Antonio

Teléfonos: 0988524891

Correo electrónico: Dayana.morales2095@utc.edu.ec

ESTUDIOS REALIZADOS

Primer Nivel:

- Escuela Mixta Municipal Las Mercedes

Segundo Nivel:

- Unidad Educativa Nicolás Infante Díaz

Tercer Nivel:

- Universidad Técnica de Cotopaxi Extensión La Maná

TÍTULOS

- Bachiller en Ciencias, 23 de febrero del 2016
- Suficiencia en Ingles (Nivel B1)

IDIOMAS

- Español (nativo)
- Suficiencia en el Idioma Inglés Nivel B1

CURSOS DE CAPACITACIÓN

- Primera Jornada Científica Internacional de Informática – UTC La Maná 2016
  Dictado: Universidad Técnica de Cotopaxi

  Lugar y fecha: La Maná 06 hasta el 08 de julio del 2016

  Tiempo: 40 horas

- II Jornadas Informáticas - UTC La Maná
  Dictado: Universidad Técnica de Cotopaxi

Lugar y fecha: La Maná 12 hasta el 14 de julio del 2017

Tiempo: 40 horas

- III Jornadas Informáticas - UTC La Maná
  Dictado: Universidad Técnica de Cotopaxi

  Lugar y fecha: La Maná 10 hasta el 12 de julio del 2018

  Tiempo: 40 horas

- IV Congreso Internacional De Investigación Científica - UTC La Maná
  Dictado: Universidad Técnica de Cotopaxi

  Lugar y fecha: La Maná 08 hasta el 10 de mayo del 2019

  Tiempo: 40 horas

- Capacitación Académica de Ingeniería en Sistema de Información 2020 – UTC La Maná **Dictado:** Universidad Técnica de Cotopaxi
  Lugar y fecha: La Maná 03 hasta el 07 de agosto del 2020

  Tiempo: 40 horas

- V Congreso Internacional De Investigación Científica - UTC La Maná
  Dictado: Universidad Técnica de Cotopaxi

  Lugar y fecha: La Maná 02 hasta el 04 de diciembre del 2020

  Tiempo: 40 horas

- VI Congreso Internacional De Investigación Científica - UTC La Maná

  Dictado: Universidad Técnica de Cotopaxi

  Lugar y fecha: La Maná 17 hasta el 21 de enero del 2022

  Tiempo: 40 horas

REFERENCIAS PERSONALES

- ING. JENIFFER SOLORZANO ALMEIDA TLF: 0994136332
- ING. OSWALDO CRUZ CHÁVEZ TLF: 0994288358

Anexo 4: Formato de la entrevista aplicada

UNIVERSIDAD TÉCNICA DE COTOPAXI

EXTENSIÓN - LA MANÁ

Entrevistadores: García Vega Ana Rebeca y Morales Baren Dayana Jamileth

Entrevistado: Ing. Wilmer Alcaciega Guanín.

Cargo: Gerente.

Lugar: La Maná.

1.- ¿Es necesario realizar monitoreos constantes en los activos tecnológicos de las entidades financieras?

2.- ¿Cuál importante es implementar seguridad informática en las cooperativas de ahorro y crédito?

3.- ¿Las empresas financieras deben invertir en seguridad informática?

4.- ¿Qué procesos viene llevando la cooperativa de ahorro y crédito sierra centro en la gestión de la información para que esta no sea extraída por terceros?

5.- ¿La implementación de seguridad informática orientada a la red de datos permitirán imponer una brecha de seguridad para la no extracción de información financiera?

Anexo 5: Entrevista aplicada al Ing. Wilmer Alcaciega Guanín gerente de la cooperativa de ahorro y crédito sierra centro sucursal la Maná

Descripción: Se desarrolló la entrevista con el gerente de la cooperativa de ahorro y crédito sierra centro sucursal La Maná, lo cual se trataron de temas de seguridad informática y que procesos viene llevando la entidad financiera sobre la gestión de información de sus socios.

Anexo 6: Formato de encuesta aplicada al personal de la cooperativa

UNIVERSIDAD TÉCNICA DE COTOPAXI

EXTENSIÓN - LA MANÁ

ENCUESTA DIRIGIDA A LA COOPERATIVA DE AHORRO Y CREDITO SIERRA CENTRO

Instrucciones:

En los siguientes enunciados responda según su criterio y marque con una (X).

1.- ¿Es necesario implementar mecanismos de seguridad informática para evitar futuros ataques en la extracción de información financiera?

Si ☐ No ☐

2.- ¿Ha escuchado mencionar sobre los ataques informáticos que se dan hoy en día a las entidades bancarias mediante técnicas de extracción de información por terceros?

Sí ☐ No ☐

3.- ¿Cómo trabajador ha tenido experiencia en detectar fallas o avisos sobre ataques informáticos en la entidad?

Buena ☐ Regular ☐ Mala ☐

4.- ¿Conoce usted sobre la importancia de las redes de datos a nivel comunicacional en una entidad privada basadas en las normativas ISO 27001?

Sí ☐ No ☐

5.- ¿Considera usted que se implemente seguridad informática a la red de datos de la cooperativa de ahorro y crédito sierra centro?

Si ☐ No ☐

Anexo 7: Entrevista al personal de la cooperativa de ahorro y crédito sierra centro sucursal La Maná

Descripción: Desarrollo de la encuesta aplicada al personal que labora en la cooperativa de ahorro y crédito sierra centro sucursal La Maná.

Anexo 8: Revisión de la encuesta de tabulación de resultados

TABLA DE ENCUESTAS

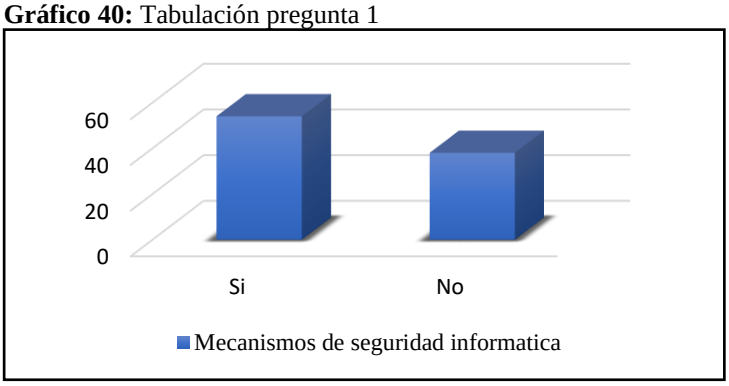
1. **¿Es necesario implementar mecanismos de seguridad informática para evitar futuros ataques en la extracción de información financiera?**

Tabla 20: Tabulación pregunta 1

Detalle	Frecuencia	Porcentaje
Si	54	65%
No	38	35%
TOTAL	92	100%

Elaborado Por: Las Investigadoras

Gráfico 40: Tabulación pregunta 1



Elaborado Por: Las Investigadoras

Análisis e interpretación: Del 100% de la población encuestada el 65% cree necesario aplicar mecanismos de seguridad informática, mientras el 35% no está de acuerdo en aplicar procedimientos de seguridad en las empresas financieras. Los resultados reflejan que se implementen soluciones que hagan referencia a la seguridad informática para evitar la extracción de información.

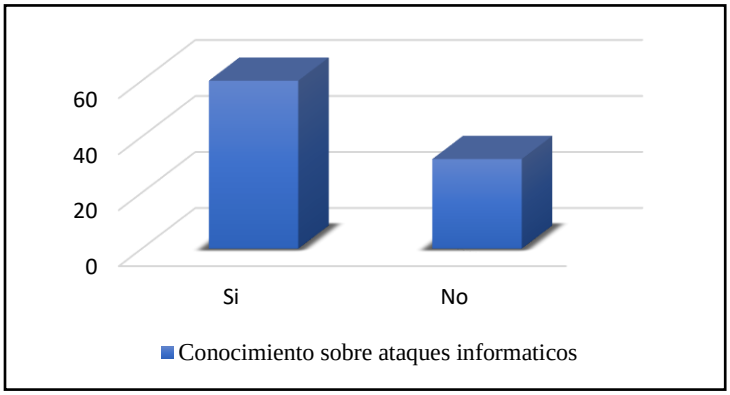
2. **¿Ha escuchado mencionar sobre los ataques informáticos que se dan hoy en día a las entidades bancarias mediante técnicas de extracción de información por terceros?**

Tabla 21: Tabulación de pregunta 2

Detalle	Frecuencia	Porcentaje
Si	60	85%
No	32	15%
TOTAL	92	100%

Elaborado Por: Las Investigadoras

Gráfico 41: Tabulación de pregunta 2



Elaborado Por: Las Investigadoras

Análisis e interpretación: Del 100% de la población encuestada el 60% tiene conocimientos sobre los ataques informáticos en las entidades financieras, mientras que el 32% manifiesta que no ha escuchado mencionar sobre aquello. Los resultados reflejan

que existe conocimiento en la gestión de la seguridad informática en las entidades financieras.

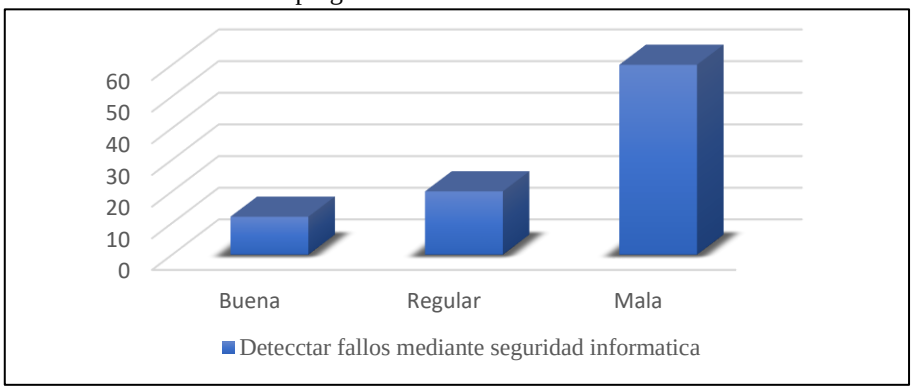
3. **¿Cómo trabajador ha tenido experiencia en detectar fallas o avisos sobre ataques informáticos en la entidad?**

Tabla 22: Tabulación de pregunta 3

Detalle	Frecuencia	Porcentaje
Buena	12	20%
Regular	20	23%
Mala	60	49%
TOTAL	92	100%

Elaborado Por: Las Investigadoras

Gráfico 42: Tabulación de pregunta 3



Elaborado Por: Las Investigadoras

Análisis e interpretación: Del 100% de la población encuestada el 20% al detectar fallas informáticas fue buena; el 23% fue regular en la detección de vulnerabilidades de seguridad; mientras que el 49% ha tenido una mala experiencia. Esto refleja que existe desconocimiento en la gestión de seguridad informática y activos tecnológicos

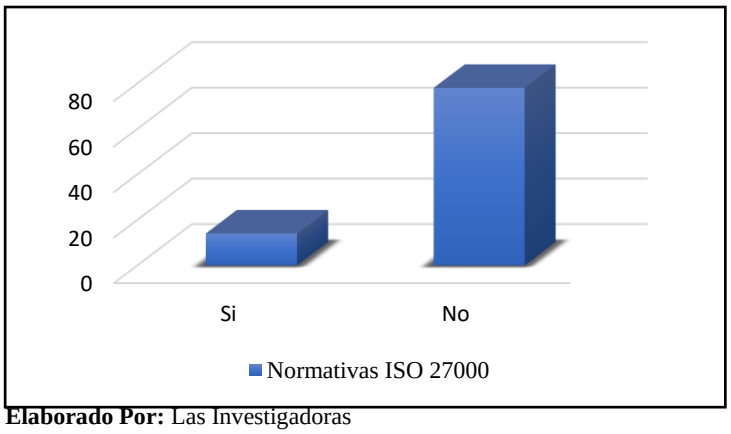
4. **¿Conoce usted sobre la importancia de las redes de datos a nivel comunicacional en una entidad privada basadas en las normativas ISO 27001**

Tabla 23: Tabulación de pregunta 4

Detalle	Frecuencia	Porcentaje
Si	14	20%
No	78	80%
TOTAL	92	100%

Elaborado Por: Las Investigadoras

Gráfico 43: Tabulación de pregunta 4



Elaborado Por: Las Investigadoras

Análisis e interpretación: Del 100% de la población encuestada el 20%, conoce la importancia de la aplicación de la normativa ISO como estándar mundial, mientras que el 80% manifiesta que no ha escuchado mencionar sobre las normas de estandarización ISO 27001 orientadas a las redes de datos.

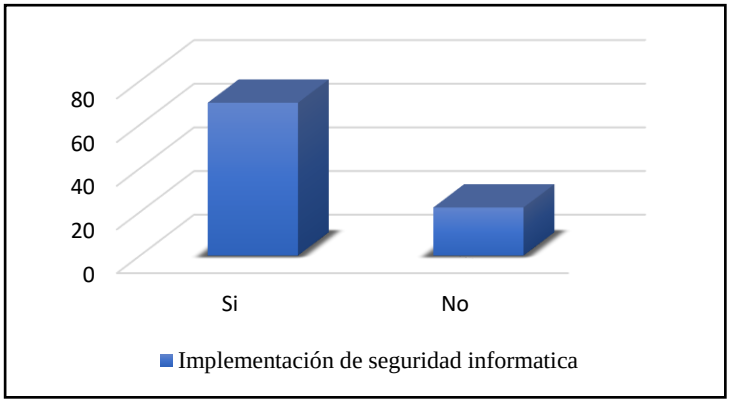
5. ¿Considera usted que se implemente seguridad informática a la red de datos de la cooperativa de ahorro y crédito sierra centro?

Tabla 24: Tabulación de pregunta 5

Detalle	Frecuencia	Porcentaje
Si	70	80%
No	22	20%
TOTAL	92	100%

Elaborado Por: Las Investigadoras

Gráfico 44: Tabulación de pregunta 5



Elaborado Por: Las Investigadoras

Análisis e interpretación: Del 100% de la población encuestada el 80% cree que es importante la implementación de seguridad informática en las redes de datos basándose en la aplicación de la normativa internacional ISO 27001, mientras que el 20% manifiesta

que no es necesario. Los resultados reflejan que es necesario implementar seguridad en las redes de datos para el análisis y evaluación de la misma.

Anexo 9: Configuración de consola para mostrar los resultados de pentesting

Elaborado Por: Las Investigadoras

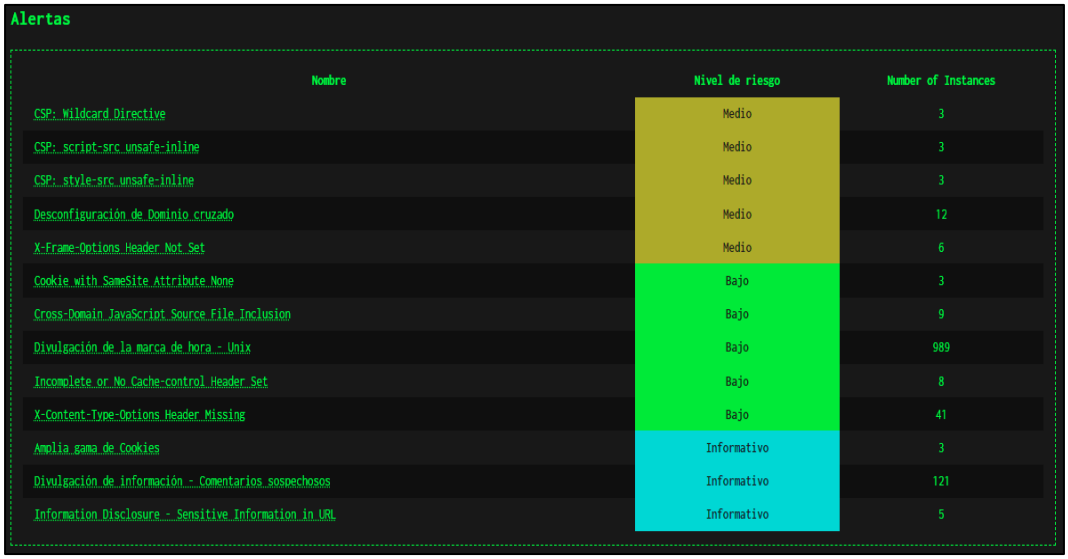
Descripción: Configuración de la consola mediante el uso del sistema operativo Kali Linux para mostrar los resultados del pentesting.

Anexo 10: Evaluación del resultado de la aplicación de pentesting al gerente de la cooperativa sierra centro sucursal La Maná

Elaborado Por: Las Investigadoras

Descripción: Se mostró ante el gerente de la cooperativa los resultados de la aplicación de pentesting y evaluación dentro del análisis técnico informático.

Anexo 11: Resultados en base alertas del software ZAP



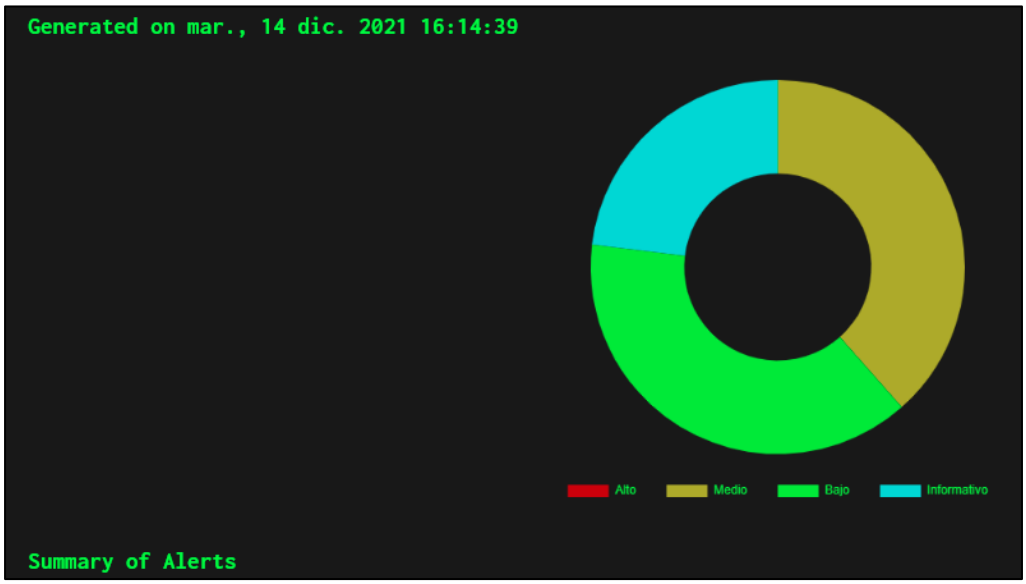
Alertas

Nombre	Nivel de riesgo	Number of Instances
CSP: Wildcard Directive	Medio	3
CSP: script-src unsafe-inline	Medio	3
CSP: style-src unsafe-inline	Medio	3
Desconfiguración de Dominio cruzado	Medio	12
X-Frame-Options Header Not Set	Medio	6
Cookie with SameSite Attribute None	Bajo	3
Cross-Domain JavaScript Source File Inclusion	Bajo	9
Divulgación de la marca de hora - Unix	Bajo	989
Incomplete or No Cache-control Header Set	Bajo	8
X-Content-Type-Options Header Missing	Bajo	41
Amplia gama de Cookies	Informativo	3
Divulgación de información - Comentarios sospechosos	Informativo	121
Information Disclosure - Sensitive Information in URL	Informativo	5

Elaborado Por: Las Investigadoras

Descripción: Resultados de la aplicación de pentesting en base a la utilización del software gratuito ZAP, capturando así los niveles de riesgo que contiene la aplicación web financiera y el número de instancias afectadas.

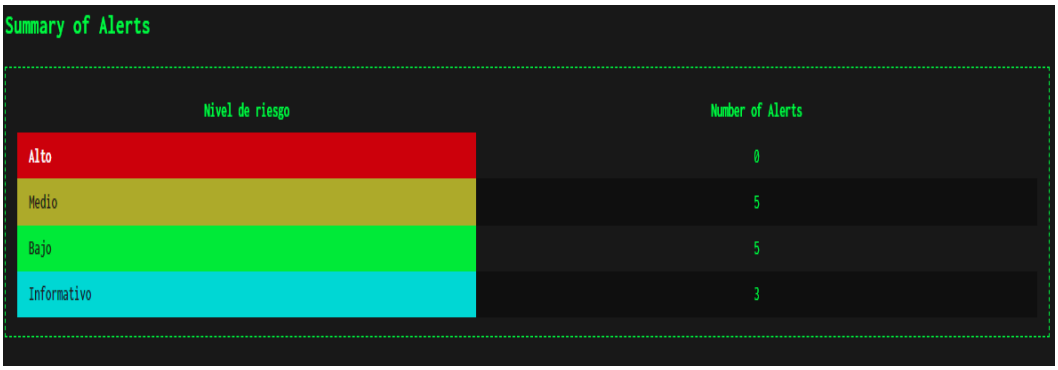
Anexo 12: Resultados generados mediante la evaluación con ZAP del 14 de diciembre



Elaborado Por: Las Investigadoras

Descripción: Sumario de alertas generado, la evaluación de resultados fue el 14 de diciembre del 2021 con hora 16:14 representando así un gráfico pastel en base a los niveles de alto, medio y bajo.

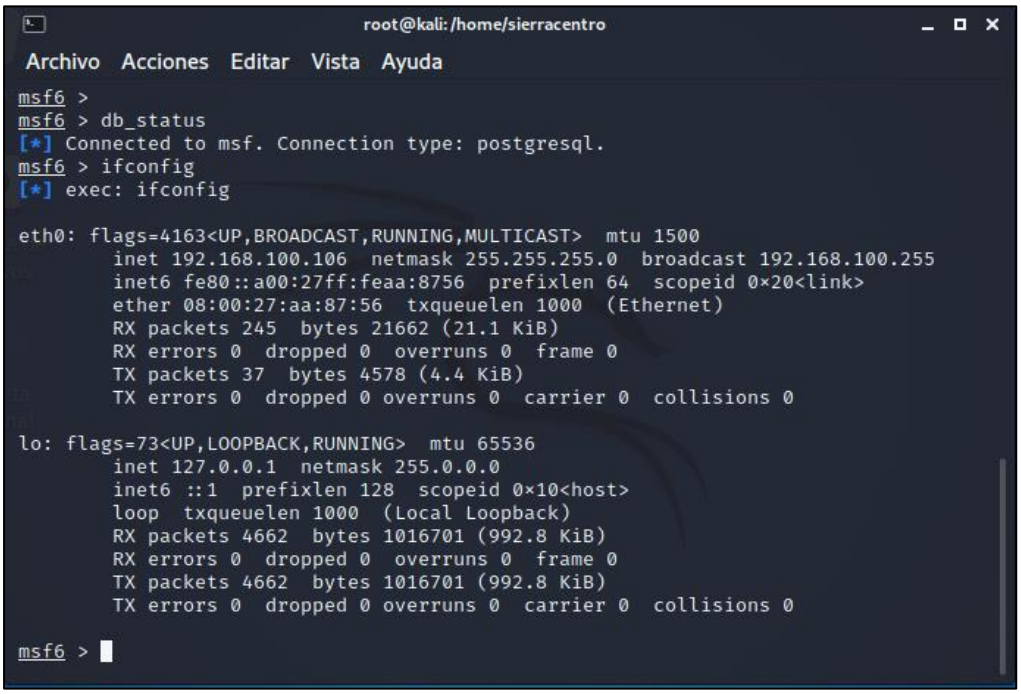
Anexo 13: Resultados del nivel de riesgo de los números de alertas



Elaborado Por: Las Investigadoras

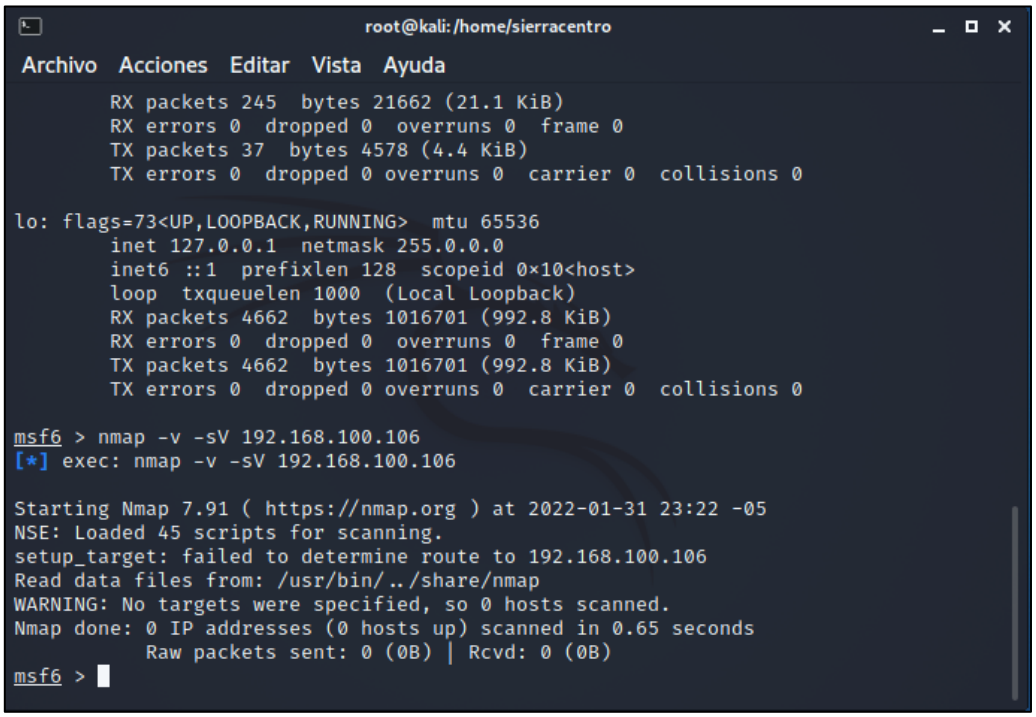
Descripción: Resultado sobre los números de objetos, enumerando así cada nivel de alerta generado con el software ZAP desde los niveles altos hasta componentes informativos.

Anexo 14: Comprobación de IP de la cooperativa sierra centro anclado mediante puente de conexión bridge.



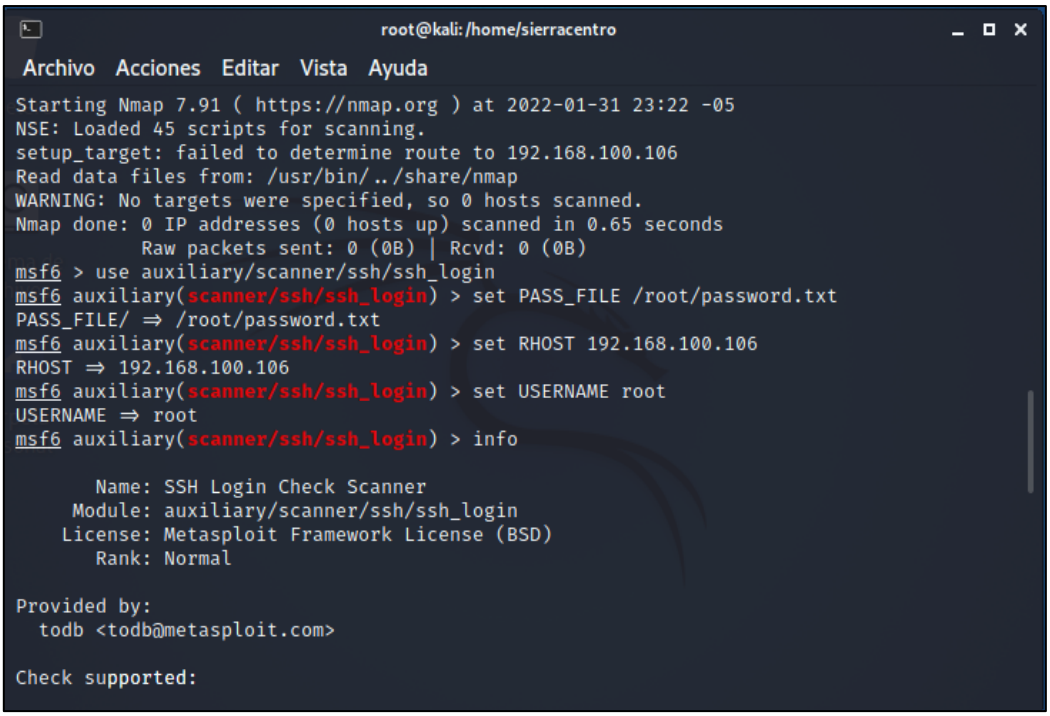
Descripción: Para proceder la aplicación de pentesting se capturó la IP de la entidad financiera para que esta sea evaluada mediante los servicios de Metasploit en el sistema de Kali Linux.

Anexo 15: Aplicación de NMAP para apertura de conexiones TCP



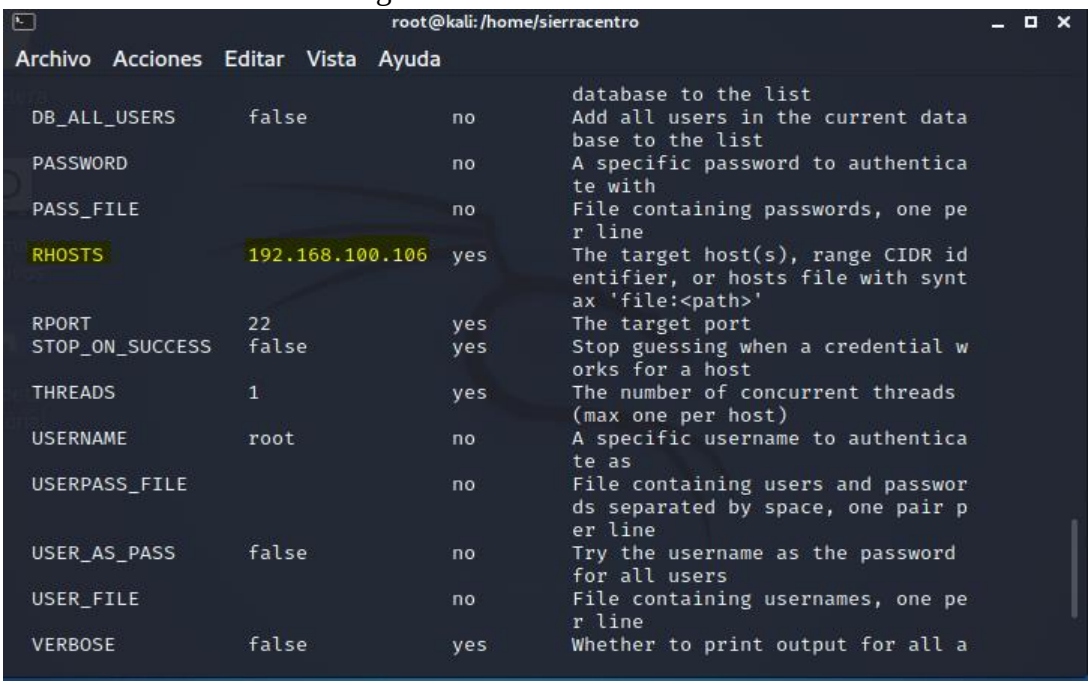
Descripción: Se aplicó NMAP para rastrear de manera adecuada los filtros de conexiones de red y a su vez evaluar la seguridad de las redes de datos de la entidad financiera.

Anexo 16: Evaluación y apertura de brecha en la penetración de la red de datos



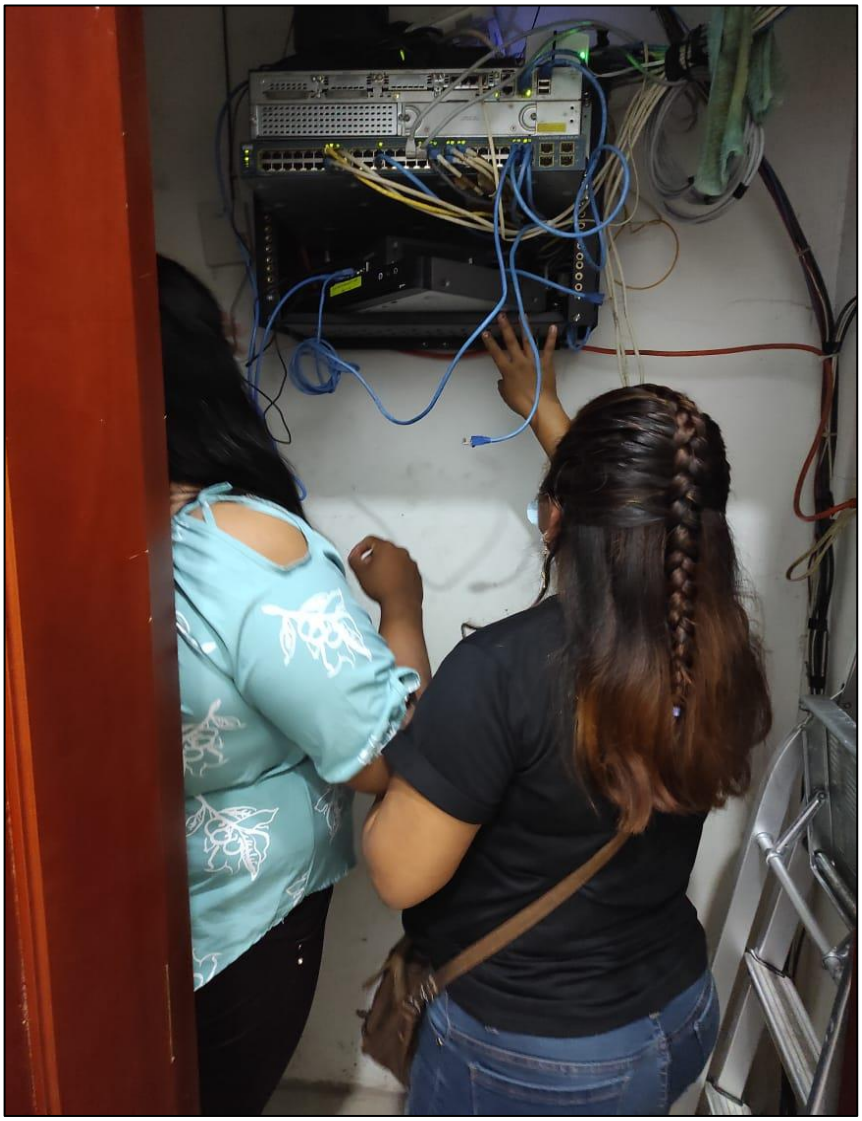
Descripción: Penetración de la red de datos en base a los comandos de Seteo como PASS_ set USERNAME para obtener información del TCP objetivo y evaluar el estado de la red.

Anexo 17: Información del target TCP a atacar



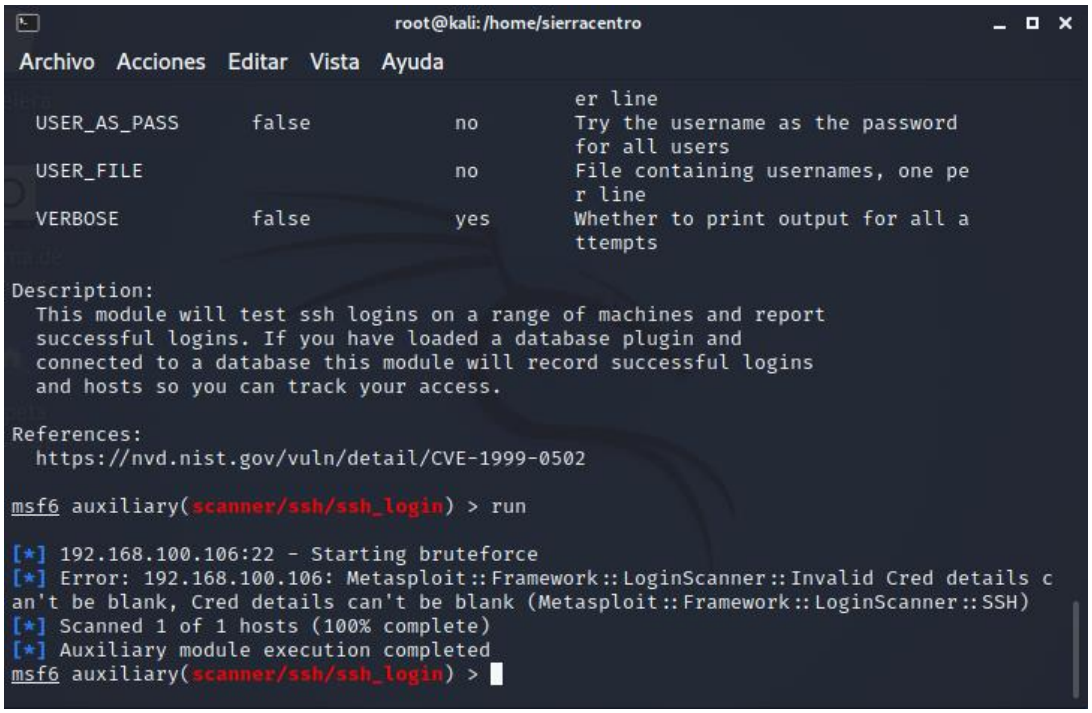
Descripción: Aplicando el comando info mediante usuario root, se obtiene la información del TCP o puerto de la red de datos direccionando de manera automática un ataque mediante Metasploit de tipo bruteforce. Cabe recordar que esta acción aplicada a la evaluación de la red de datos permite obtener objetivos en concreto para la vulneración tanto como acceso a la información y alteración en el consumo del rendimiento en la comunicación de determinada tipografía de red.

Anexo 18: Inspección del sistema de cableado de la red de datos de la cooperativa sierra centro



Descripción: Para la implementación de seguridad informática se realizó la evaluación del RACK de la cooperativa, por lo tanto, desde el análisis del mismo se recomienda establecer bases metodológicas mediante estándares internacionales en la distribución del cableado; lo que a su vez no cumple con estas normas. El proyecto de investigación se basa en aplicar la norma ISO 27001, esto se debe al control de acceso que debe cumplir, cabe recalcar que esta norma cuenta con controles previamente establecidos, no es obligatorio acatarlos; sin embargo, esto se centrará en aquellos que nos permitan diseñar e implementar seguridad informática en la red de datos de la cooperativa.

Anexo 19: Vulneración de la red de datos



Descripción: Obtendremos como resultado la vulneración de la red de datos en la cooperativa SIERRA CENTRO SUCURSAL LA MANÁ, PROVINCIA DE COTOPAXI, se encuentra en estado activo todos los servicios ejecutados para la protección de ataques informáticos en el RHOST con identificación de red IP 192.168.100.168 estática; aplicando ataque de tráfico externo mediante los procesos de Metasploit y bruteforce.

Anexo 20: Certificado de investigación realizada en la cooperativa de ahorro y crédito sierra centro sucursal La Maná

COOPERATIVA DE AHORRO Y CRÉDITO
SIERRA CENTRO

La Maná, 1 de Febrero del 2022

CERTIFICADO

Quien suscribe Sr. **ALCACIEGA GUANIN WILMER REINALDO** con C.I, 050367819-5 luego de revisar los archivos correspondientes que reposan en la oficina en nuestro cargo, Certificamos que las estudiantes GARCÍA VEGA ANA REBECA con C.I.: : 1205283383 y con MORALES BAREN DAYANA JAMILETH C.I.: 1208262095 estudiantes de la carrera de Ingeniería en Informática y Sistemas Computacionales de la Universidad Técnica de Cotopaxi-Extensión La Maná, se encuentran desarrollando e implementando el proyecto con el tema: **"SEGURIDAD INFORMÁTICA MEDIANTE HACKING ÉTICO EN LA APLICACIÓN DE PENTESTING PARA EL ANÁLISIS DE VULNERABILIDADES EN LAS REDES DE DATOS DE LA COOPERATIVA SIERRA CENTRO SUCURSAL LA MANÁ, PROVINCIA DE COTOPAXI."**

Atentamente,

Alcaciega Guanin Wilmer Reinaldo
C.I.1050367819-5
GERENTE

19. CERTIFICADO DE REPORTE DE LA HERRAMIENTA DE PREVENCIÓN DE COINCIDENCIA Y/O PLAGIO ACADÉMICO

Curiginal

Document Information

Analyzed document	Tesis-Garcia-Morales.docx (D132981022)
Submitted	2022-04-07T20:48:00.0000000
Submitted by	
Submitter email	johnny.bajana@utc.edu.ec
Similarity	1%
Analysis address	jaime.cajas.utc@analysis.urkund.com

Sources included in the report

SA	**Formato-T_EvenSuescumV3.pdf** Document Formato-T_EvenSuescumV3.pdf (D111717551)	1
SA	**final tesis 2021.pdf** Document final tesis 2021.pdf (D107940302)	2
W	URL: https://1library.co/document/q5wv6p7q-diseno-sistema-gestion-seguridad-informacion-direccion-cocharcas-chincheros.html Fetched: 2022-04-07T21:32:34.5770000	1
SA	**Indice.docx** Document Indice.docx (D13939905)	1
SA	**TESIS 1.docx** Document TESIS 1.docx (D16072333)	2
SA	**MT_carolina.docx** Document MT_carolina.docx (D43885964)	1
W	URL: http://www.scielo.org.pe/scielo.php?pid=S2307-79992020000400011&script=sci_arttext Fetched: 2021-11-06T23:47:33.2730000	2
W	URL: https://repositorio.uisrael.edu.ec/bitstream/47000/2019/1/UISRAEL-EC-MASTER%20-%20TELEM-378.242-2019-007.pdf Fetched: 2022-04-07T21:32:36.3330000	2