UNIVERSIDAD TÉCNICA ESTATAL DE QUEVEDO

FACULTAD DE CIENCIAS DE LA COMPUTACION Y DISEÑO DIGITAL

CARRERA DE TELEMÁTICA

Trabajo de Integración Curricular previa la obtención del Grado Académico de Ingeniero en Telemática.

Proyecto de Investigación:

SEGURIDAD EN LA RED INTERNA DE LA UNIVERSIDAD TECNICA ESTATAL DE QUEVEDO

Autor:

JOSE GREGORIO LEON MOREIRA

Directora de Proyecto de Investigación:

Ing. PAOLA BENITEZ NAVARRETE, MSc

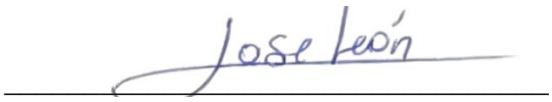
Quevedo – Los Ríos -Ecuador

2025

DECLARACIÓN DE AUTORÍA Y CESIÓN DE DERECHOS

Yo, **JOSE GREGORIO LEON MOREIRA,** declaro que la investigación aquí descrita es de mi autoría; que no ha sido previamente presentado por ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

La Universidad Técnica Estatal de Quevedo, puede hacer uso de los derechos correspondientes a este documento, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

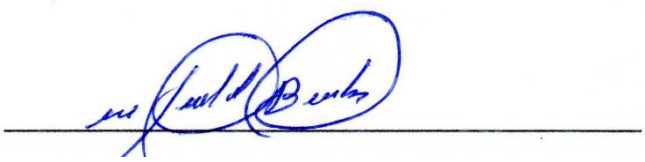


José Gregorio León Moreira

C.I. 0929414126

CERTIFICACIÓN DE CULMINACIÓN DEL PROYECTO DE INVESTIGACIÓN

La suscrita, **Paola Maribel Benítez Navarrete** Docente de la Universidad Técnica Estatal de Quevedo, certifica que el estudiante **León Moreira José Gregorio** realizó el Proyecto de Investigación de grado titulado **"Seguridad en la red interna de la Universidad Técnica Estatal de Quevedo"** previo a la obtención del **título de Ingeniero en Telemática**, bajo mi dirección, habiendo cumplido con las disposiciones reglamentarias establecidas para el efecto.



Ing. Paola Maribel Benítez Navarrete, MSc

DIRECTORA DEL PROYECTO DE INVESTIGACIÓN

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

La suscrita, **Paola Maribel Benítez Navarrete,** mediante el presente cumplo en presentar a usted el informe del proyecto de Investigación titulado **"Seguridad En La Red Interna de la Universidad Técnica Estatal de Quevedo"**, presentado por el estudiante **José Gregorio León Moreira**, egresado de la Carrera de Telemática que fue revisado bajo mi dirección según la resolución del Consejo Directivo de la Facultad de la Computación y Diseño Digital, que se ha desarrollado de acuerdo al Reglamento de la Unidad de Integración Curricular de la Universidad Técnica Estatal de Quevedo y cumple el requerimiento de análisis de COMPILATIO el cual avala los niveles de originalidad en un 95 % y similitud en 5 %, del trabajo investigativo. Valido este documento para que el estudiante siga con los trámites pertinentes de acuerdo como lo establece el Reglamento.


CERTIFICADO DE ANÁLISIS
magister

13 DEL 11 TESIS LEON MOREIRA OV ACTUALIZADO 009 (17-65)

5% Textos sospechosos

2% Similitudes
< 1 % similitudes entre comillas
0 % entre las fuentes mencionadas
3% Idiomas no reconocidos

Nombre del documento: 13 DEL 11 TESIS LEON MOREIRA OV ACTUALIZADO 009 (17-65).docx
ID del documento: f1590de51864eb4a4bb5a2d5eb9dcf4cf8a3518a
Tamaño del documento original: 1,78 MB
Autor: Tesis Leon Moreira Leon Moreira

Depositante: Tesis Leon Moreira Leon Moreira
Fecha de depósito: 16/11/2025
Tipo de carga: url_submission
fecha de fin de análisis: 16/11/2025

Número de palabras: 10.834
Número de caracteres: 74.704

Ing. Paola Maribel Benítez Navarrete, MSc.

DIRECTORA DEL PROYECTO DE INVESTIGACIÓN

UNIVERSIDAD TÉCNICA ESTATAL DE QUEVEDO

FACULTAD DE CIENCIAS DE LA COMPUTACIÓN Y DISEÑO DIGITAL

CARRERA DE TELEMÁTICA

PROYECTO DE INVESTIGACIÓN

CERTIFICADO DE APROBACIÓN POR TRIBUNAL DE SUSTENTACIÓN

Título:

"SEGURIDAD EN LA RED INTERNA DE LA UNIVERSIDAD TÉCNICA ESTATAL DE QUEVEDO"

Presentado al Consejo Directivo de la Facultad de Ciencias de la Computación y Diseño Digital como requisito previo a la obtención del título de Ingeniero en Telemática

Revisado por:

Ing. Anthony Limber Moran Cabezas, MSc.

PRESIDENTE DEL TRIBUNAL

Ing. Santiago Javier Meneses Narváez, MSc.

MIEMBRO DEL TRIBUNAL

Ing. Diego Fernando Intriago Rodríguez, M. Sc.

MIEMBRO DE TRIBUNAL

QUEVEDO – LOS RIOS- ECUADOR

2025

AGRADECIMIENTO

Quiero extender un sincero agradecimiento a todas las personas que contribuyeron de gran manera a la realización de este proyecto. A Dios por darme las fortalezas para lograr alcanzar esta meta. De igual manera a mis padres que siempre estuvieron a mi lado en cada paso que daba durante mi formación académica.

A la ingeniera Paola Benítez, al ingeniero Stalin Carreño por su liderazgo y conocimientos brindados para el correcto desarrollo de este proyecto. Gracias a la Universidad Técnica Estatal de Quevedo por abrirme sus puertas y brindarme la oportunidad de formarme como profesional.

A mi grupo de amigos, Francisco, Bryan, Raúl, Kevin, Wilmer, Adonis, Kenneth, Jair, por permitir que esta fase sea mucho más llevadera y por el apoyo brindado a lo largo de estos años académicos.

José Gregorio León Moreira

DEDICATORIA

A mi madre Carlina Moreira, y a mi padre Gregorio León por su apoyo incondicional, por sus palabras de amor, de que nunca me rindiera sin importar la circunstancia y que para todo existe solución.

A mis hermanas y hermano, especialmente a Jamilexy León, que siempre estuvo a mi lado brindándome su apoyo, Mostrando su preocupación, orgullo y apoyo incondicional pese a cualquier situación. A mi tía Mirian, a mi tío Lalo que desde el cielo me han acompañado en esta etapa.

A mi sobrino Gregory por darme un motivo mas para querer salir adelante, por haber sido un curita para el alma cuando menos lo esperaba y más lo necesitaba.

A Cinthya por todo el apoyo y cariño incondicional que me ha brindado a lo largo de estos años académicos, por su ayuda constante en esta meta de mi vida, sus palabras formaron un pilar fundamental para culminar esta etapa.

José Gregorio León Moreira

RESUMEN EJECUTIVO Y PALABRAS CLAVES

La presente investigación analizó la postura de ciberseguridad de la Universidad Técnica Estatal de Quevedo mediante un análisis sistemático de vulnerabilidades en su red cableada interna. Se implementó una metodología mixta que combinó revisión bibliográfica, análisis descriptivo y aplicación práctica de herramientas especializadas. Tras una evaluación comparativa, se seleccionó Nessus Professional como herramienta principal debido a su precisión en detección y capacidad de escaneos autenticados. Los hallazgos revelaron 573 vulnerabilidades distribuidas en 164 hosts activos, incluyendo 49 de severidad crítica concentradas principalmente en la zona DMZ. Las vulnerabilidades identificadas incluyen sistemas operativos desactualizados (CVE-2023-21554), configuraciones SNMP inseguras en 100 dispositivos y servicios SSH vulnerables. Se desarrolló un plan de mitigación estructurado en tres fases priorizadas por severidad, alineado con estándares ISO/IEC 27001 y NIST Cybersecurity Framework, proporcionando estrategias específicas para fortalecer la infraestructura tecnológica institucional.

Palabras claves: análisis, escaneo, infraestructura, ciberataques, mitigación

ABSTRACT AND KEYWORDS

This research evaluated the cybersecurity posture of the State Technical University of Quevedo through a systematic vulnerability analysis of its internal wired network. A mixed methodology combining bibliographic review, descriptive analysis, and practical application of specialized tools was implemented. Following comparative evaluation, Nessus Professional was selected as the primary tool due to its detection precision and authenticated scanning capabilities. Findings revealed 573 vulnerabilities distributed across 164 active hosts, including 49 critical severity vulnerabilities concentrated primarily in the DMZ zone. Identified vulnerabilities include outdated operating systems (CVE-2023-21554), insecure SNMP configurations on 100 devices, and vulnerable SSH services. A structured three-phase mitigation plan prioritized by severity was developed, aligned with ISO/IEC 27001 and NIST Cybersecurity Framework standards, providing specific strategies to strengthen the institutional technological infrastructure.

Keywords: analysis, scanning, infrastwructure, cyberattacks, mitigation

ÍNDICE

DECLARACIÓN DE AUTORÍA Y CESIÓN DE DERECHOS ii
CERTIFICACIÓN DE CULMINACIÓN DEL PROYECTO DE INVESTIGACIÓN iii
CERTIFICADO DEL REPORTE DE LA HERRAMIENTA DE PREVENCIÓN DE COINCIDENCIA Y/O PLAGIO ACADÉMICO iv
CERTIFICADO DE APROBACIÓN POR TRIBUNAL DE SUSTENTACIÓN v
AGRADECIMIENTO vi
DEDICATORIA vii
RESUMEN EJECUTIVO Y PALABRAS CLAVES viii
ABSTRACT AND KEYWORDS ix
ÍNDICE DE TABLAS xiii
ÍNDICE DE FIGURAS xiv
CÓDIGO DUBLÍN xv
INTRODUCCIÓN 1
CAPÍTULO I 2
CONTEXTUALIZACIÓN DE LA INVESTIGACIÓN 2
1.1. Problema de investigación 3
1.1.1. Planteamiento del problema 3
1.1.2. Formulación del problema 4
1.1.3. Sistematización del problema 4
1.2. Objetivos 5
1.2.1. Objetivo General 5
1.3. Justificación 5
CAPÍTULO II 6
FUNDAMENTACIÓN TEÓRICA DE LA INVESTIGACIÓN 6
2.1. Marco conceptual 7
2.1.1. Seguridad informática 7
2.1.2. Ciberseguridad 7
2.1.3. Vulnerabilidad 7
2.1.4. Exploits 7
2.1.5. Tipos de vulnerabilidades 7
2.1.6. Vulnerabilidades físicas 8
2.1.7. Vulnerabilidades lógicas 8
2.1.8. Análisis de vulnerabilidades 8
2.1.9. Intrusión 8

2.1.10. Integridad de datos 9
2.1.11. Disponibilidad 9
2.1.12. Red informática 9
2.1.13. Herramientas de ciberseguridad 9
2.1.13.1. Nmap (Network Mapper). 10
2.1.13.2. OpenVAS. 10
2.1.13.3. Nessus. 10
2.2. Marco referencial 10
2.3. Marco Legal y Normativo 12
CAPÍTULO III 14
METODOLOGÍA DE LA INVESTIGACIÓN 14
3.1. Localización 15
3.2. Tipo de investigación 15
3.2.1. Investigación bibliográfica 15
3.2.2. Investigación descriptiva 15
3.3. Métodos de investigación 16
3.3.1. Método inductivo 16
3.3.2. Método deductivo 16
3.4. Fuentes de recopilación de la información 16
3.5. Diseño de la investigación 17
3.6. Instrumentos de la investigación 18
CAPÍTULO IV 19
RESULTADOS Y DISCUSIONES 19
4.1. Resultados del primer objetivo 20
4.1.1. Esquema de conexión entre campus Central y La María 22
4.1.2. Esquema de conexión Campus Central 23
4.1.2.1. Servidores. 24
4.1.2.2. Medidas de seguridad del centro de datos. 24
4.1.3. Comparación de herramientas de escaneo de vulnerabilidades 25
4.1.3.2. Elección de Nessus como mejor herramienta 27
4.1.4. Discusión de objetivo específico 1 28
4.2. Resolución del segundo objetivo 29
4.2.1. Red propuesta para analizar vulnerabilidades 29
4.2.2. Herramienta Nessus Professional 30
4.2.5. Vulnerabilidades en hosts críticos 34

4.2.6. Escaneo de red interna (LAN) 36
4.2.6.1. Configuración de escaneo. 36
4.2.6.2. Resumen de hallazgos en red LAN. 37
4.2.6.3. Análisis por segmentos de red. 38
4.2.6.4. Vulnerabilidades Criticas Identificadas. 39
4.2.7. Correlación con estándares de seguridad 39
4.3. Resolución del tercer objetivo 40
4.3.1. Matriz de prioridad de eventos 41
4.3.2. Estrategias de mitigación para vulnerabilidades 42
4.3.2.1. Fase 1: Remediación inmediata (PRIORIDAD P1). 42
4.3.2.2. Fase 2: Fortalecimiento de servicios (PRIORIDAD P2). 42
4.3.2.3. Fase 3: Monitoreo continuo y prevención (PRIORIDAD P3) 42
4.3.3. Medidas técnicas para el fortalecimiento de la red cableada 43
4.3.4. Informe de resultados obtenidos del escaneo 45
CAPÍTULO V 48
CONCLUSIONES Y RECOMENDACIONES 48
5.1. Conclusiones 49
5.2. Recomendaciones 50
CAPÍTULO VI 51
BIBLIOGRAFÍA 51
6.1Bibliografía 52
CAPITULO VII 56
ANEXOS 56

ÍNDICE DE TABLAS

Tabla 1. Entrevista realizada al Líder del departamento de TIC de la UTEQ.....20
Tabla 2. Herramientas de análisis de vulnerabilidades 25
Tabla 3. Tabla comparativa de herramientas.....27
Tabla 4. Resumen global de vulnerabilidades en zona DMZ.....32
Tabla 5. Hosts Críticos DMZ 33
Tabla 6. Vulnerabilidades en DMZ.....34
Tabla 7. Distribución general de vulnerabilidades 37
Tabla 8. Segmentos de red.....38
Tabla 9. Matriz de priorización de vulnerabilidades.....41

ÍNDICE DE FIGURAS

Figura 1. Localización.....15
Figura 2. Diagrama de flujo diseño investigación.....18
Figura 3. Esquema de conexión entre campus central y la maría.....22
Figura 4. Equipo Firewall Hillstone SG-6000.....23
Figura 5. Esquema de conexión entre dispositivos.....23
Figura 6. Servidor HP Proliant DL360 24
Figura 7. Generador de electricidad SAI 24
Figura 9. Beneficios de Nessus 27
Figura 10. Cobertura de CVE entre Tenable y OpenVAS 28
Figura 11. Vista página principal de Nessus 30
Figura 12. Arquitectura defensa en profundidad 31
Figura 13. Arquitectura TCP/IP.....31
Figura 14. Gráfico de vulnerabilidades en DMZ.....32
Figura 15. Gráfico de vulnerabilidades por hosts.....33
Figura 16. Reincidencia de vulnerabilidad por SSL 34
Figura 17. Reincidencias de vulnerabilidades por HTTP/Trace Track 35
Figura 18. Reincidencias de vulnerabilidades por versión desactualizada de Apache 35
Figura 19. Horarios de escaneos.....36
Figura 20.Total de hosts y vulnerabilidades de red LAN 37
Figura 21. Diagrama radar de vulnerabilidades en red LAN 37
Figura 22. Mapa de calor sobre vulnerabilidades en red LAN 38

CÓDIGO DUBLÍN

Título:	"Seguridad en la red interna de la universidad técnica estatal de Quevedo"				
Autor:	José Gregorio León Moreira				
Palabras clave:	Análisis	Escaneo	Vulnerabilidades	Mitigación	Nessus
Fecha de publicación:	Noviembre, 2025				
Editorial:	Quevedo - UTEQ "Campus La Central", 2025				
Resumen:	La presente investigación analizó la postura de ciberseguridad de la Universidad Técnica Estatal de Quevedo mediante un análisis sistemático de vulnerabilidades en su red cableada interna. Se implementó una metodología mixta que combinó revisión bibliográfica, análisis descriptivo y aplicación práctica de herramientas especializadas. Tras una evaluación comparativa, se seleccionó Nessus Professional como herramienta principal debido a su precisión en detección y capacidad de escaneos autenticados. Los hallazgos revelaron 573 vulnerabilidades distribuidas en 164 hosts activos, incluyendo 49 de severidad crítica concentradas principalmente en la zona DMZ. Las vulnerabilidades identificadas incluyen sistemas operativos desactualizados (CVE-2023-21554), configuraciones SNMP inseguras en 100 dispositivos y servicios SSH vulnerables. Se desarrolló un plan de mitigación estructurado en tres fases priorizadas por severidad, alineado con estándares ISO/IEC 27001 y NIST Cybersecurity Framework, proporcionando estrategias específicas para fortalecer la infraestructura tecnológica institucional.				
Abstract:	This research evaluated the cybersecurity posture of the State Technical University of Quevedo through a systematic vulnerability analysis of its internal wired network. A mixed methodology combining bibliographic review, descriptive analysis, and practical application of specialized tools was implemented. Following comparative evaluation, Nessus Professional was selected as the primary tool due to its detection precision and authenticated scanning capabilities. Findings revealed 573 vulnerabilities distributed across 164 active hosts, including 49 critical severity vulnerabilities concentrated primarily in the DMZ zone. Identified vulnerabilities include outdated operating systems (CVE-2023-21554), insecure SNMP configurations on 100 devices, and vulnerable SSH services. A structured three-phase mitigation plan prioritized by severity was developed, aligned with ISO/IEC 27001 and NIST Cybersecurity Framework standards, providing specific strategies to strengthen the institutional technological infrastructure.				
Descripción	72 hojas: dimensiones 29 x 21 cm + CD ROM 6162				
URL:					

INTRODUCCIÓN

A nivel mundial, la ciberseguridad se ha consolidado como una prioridad estratégica fundamental en el siglo XXI. Las empresas e instituciones educativas enfrentan amenazas crecientes debido a la naturaleza sensible de la información que manejan datos personales de múltiples usuarios. Según un estudio reciente del Reino Unido, el 85% de las universidades han reportado incidentes de ciberseguridad en el último año [1].

Dentro de Latinoamérica, las universidades enfrentan desafíos particulares en materia de ciberseguridad. La misma presenta características específicas como limitaciones presupuestarias para inversión en tecnología, una creciente digitalización de procesos académicos y administrativos. Estos factores, combinados con el aumento de ciberataques dirigidos a instituciones educativas de la región, han evidenciado la necesidad urgente de fortalecer las capacidades de seguridad informática en el sector universitario latinoamericano.

Ecuador, como parte de esta realidad, ha experimentado un incremento significativo en las amenazas cibernéticas dirigidas a sus instituciones educativas superiores. Según un informe elaborado por Kaspersky Lab de amenazas en tiempo real, en junio del año 2017, Ecuador ocupó el primer lugar en América del Sur con el 2,8% y el quinto lugar a nivel mundial en ciberataques a redes [2].

El presente proyecto de integración curricular se encuentra estructurado en siete capítulos que abordan de manera sistemática el análisis de seguridad de la red interna de la UTEQ. Los primeros capítulos establecen la contextualización del problema y la fundamentación teórica necesaria, seguidos de la metodología empleada en el capítulo III. El capítulo IV presenta los resultados del análisis de vulnerabilidades utilizando la herramienta Nessus Professional, mientras que dentro del capítulo V desarrolla las conclusiones y estrategias de mitigación propuestas.

CAPÍTULO I

CONTEXTUALIZACIÓN DE LA INVESTIGACIÓN

1.1. Problema de investigación

1.1.1. Planteamiento del problema

En la actualidad, el ámbito de las instituciones de educación superior ha experimentado una transformación significativa debido al uso intensivo de tecnologías digitales, que ha modificado de manera profunda los procesos de gestión académica, administrativa e investigativa. Aunque esta dependencia tecnológica ha resultado beneficiosa para mejorar la eficiencia institucional, también ha incrementado la vulnerabilidad a riesgos cibernéticos. Según un informe del Reino Unido, el 85% de las universidades han informado haber tenido registros ciberataques en el último año [1].

A medida que los sistemas digitales se han convertido en pilares fundamentales en el desempeño de actividades dentro de entornos universitarios. Garantizar su seguridad deja de ser una opción y se transforma en una necesidad estratégica. En Ecuador, la autoridad competente en telecomunicaciones y sociedad de la información estableció el marco denominado Esquema Gubernamental de Seguridad de la Información (EGSI), un marco normativo obligatorio para las entidades públicas.

El esquema dado por el EGSI busca asegurar la confidencialidad, integridad y disponibilidad de la información, mediante la implementación de políticas y controles específicos[3]. Pese a estos lineamientos aún persisten distintas brechas importantes en su adopción y cumplimiento de manera efectiva, como los diversos análisis realizados en instituciones educativas [4].

La Universidad Técnica Estatal de Quevedo (UTEQ) se enfrenta al desafío de garantizar que su entorno de red se mantenga en condiciones óptimas de ciberseguridad. Además, es crucial que fortalezca sus medidas de seguridad mediante un análisis de las vulnerabilidades existentes, con el fin de obtener información detallada sobre el impacto de estas brechas y determinar las soluciones adecuadas para evitar que dichas vulnerabilidades den lugar a problemas mayores e irreparables.

Diagnóstico

En el escenario tecnológico actual de la UTEQ, se ha evidenciado un crecimiento considerable en la infraestructura de red. Este aumento, aunque responde a las necesidades operativas y académicas, también ha incrementado la exposición a posibles amenazas, especialmente por la incorporación no controlada de dispositivos no autorizados.Esta

problemática se intensifica debido a los extensos periodos que transcurren antes de detectar dichas vulnerabilidades, lo que permite la ocurrencia de accesos indebidos, intrusiones maliciosas y la posible pérdida de información relevante para la institución.

Pronóstico

La implementación de mecanismos de detección y seguimiento de vulnerabilidades en la red de la UTEQ fortalecerá significativamente la seguridad informática institucional, protegiendo la información confidencial de estudiantes y docentes. Se espera una reducción considerable en la exposición a amenazas cibernéticas y una mejora en la continuidad operativa de los servicios académicos y administrativos.

1.1.2. Formulación del problema

El presente estudio se orienta a examinar la siguiente problemática:

¿Cuál es el estado de la seguridad de la red cableada interna de la Universidad Técnica Estatal de Quevedo, a partir de un análisis realizado con la herramienta de escaneo de vulnerabilidades?

1.1.3. Sistematización del problema

¿Qué herramientas de análisis de vulnerabilidades son las más adecuadas para la red cableada interna de la UTEQ, considerando una revisión previa de su infraestructura?

¿Cuáles son las vulnerabilidades de seguridad identificadas al aplicar técnicas de análisis mediante el uso de herramientas de escaneo en la red cableada interna de la UTEQ?

¿Qué estrategias pueden proponerse para mitigar las vulnerabilidades identificadas en la red cableada interna de la UTEQ, basándose en los resultados obtenidos y en normativas de seguridad?

1.2. Objetivos

1.2.1. Objetivo General

- Analizar la seguridad de la red cableada interna de la Universidad Técnica Estatal de Quevedo, mediante el uso de herramienta de escaneo de vulnerabilidades, identificando debilidades dentro de la infraestructura tecnológica

1.2.2. Objetivos Específicos

- Identificar las herramientas de análisis de vulnerabilidades, mediante una revisión de infraestructura de red seleccionando la más adecuada para el estudio de seguridad.
- Aplicar la herramienta seleccionada mediante la ejecución de análisis en la red cableada interna, identificando vulnerabilidades existentes.
- Proponer estrategias de mitigación de las vulnerabilidades identificadas basándose en los resultados del análisis y normativas de seguridad, fortaleciendo la seguridad de la red cableada interna de la Universidad Técnica Estatal de Quevedo.

1.3. Justificación

Diversas investigaciones evidencian que las infraestructuras tecnológicas suelen estar expuestas a vulnerabilidades no detectadas, reduciendo el tiempo de reacción ante un riesgo inminente. Dentro de la UTEQ, el uso intensivo de servicios de internet y puntos de red es esencial para la accesibilidad de estudiantes y docentes a la red. Esto aumenta la superficie de ataque por esta razón es de suma importancia proteger la información de la institución mediante un correcto seguimiento y monitoreo de la red ante posibles vulnerabilidades.

Actualmente, la institución no dispone de monitoreo y análisis de vulnerabilidades por parte de personal propio de la UTEQ que permita identificar intentos de acceso no autorizado. Esta carencia limita la capacidad de respuesta ante posibles incidentes y comprometen la protección de información sensible. El análisis de vulnerabilidades mediante herramientas especializadas de seguridad informática en la red institucional permitirá beneficiar de forma directa a la institución, personal encargado del departamento de TIC permitiendo mantener el prestigio y reputación a nivel nacional de la institución [5].

CAPÍTULO II

FUNDAMENTACIÓN TEÓRICA DE LA INVESTIGACIÓN

2.1. Marco conceptual

2.1.1. Seguridad informática

La seguridad informática se lleva a cabo en la unión de conjunto de medidas, prácticas y herramientas las cuales están diseñadas para proteger sistemas informáticos, los datos que se almacenan dentro de este y la infraestructura por la cual está conformada. Su objetivo principal es garantizar dentro de la red la confidencialidad, integridad y disponibilidad de la información. La seguridad informática es la encargada de preservar la infraestructura tanto física como lógica frente a accesos no autorizados o alteraciones en la seguridad de la red [6].

2.1.2. Ciberseguridad

Dentro del ámbito de ciberseguridad, se conoce a una subdisciplina de la seguridad informática, esta se enfoca de forma puntual en la protección de sistemas conectados a la red, tanto hardware, software y datos. La ciberseguridad se enfoca en actuar antes del futuro problema, tratando de anticiparse, detectar y recuperarse frente a estos ataques [7].

2.1.3. Vulnerabilidad

Dentro de la ciberseguridad una vulnerabilidad es un punto crítico que puede ser explotada por una amenaza, esto lleva a cabo comprometer la seguridad de forma critica [8]. Estas vulnerabilidades se pueden dar en software como errores de programación, hardware (puertos abiertos) y/o humanas.

2.1.4. Exploits

En ciberseguridad, un exploit es un tipo de código conformado por una secuencia de comandos, esta es utilizada para aprovecharse de una vulnerabilidad especifica en un sistema o equipo para poder tomar el control de este y realizar acciones no autorizadas [9].

2.1.5. Tipos de vulnerabilidades

Existen dos variantes de vulnerabilidades, las lógicas y las físicas, las cuales son aprovechados por los atacantes para robar información.

2.1.6. Vulnerabilidades físicas

Este tipo de vulnerabilidad se ocasiona por infraestructura obsoleta o en mal estado, además se ocasionan por falta de protección a activos físicos en los cuales se encuentra alojado los sistemas informáticos e información, estas pueden conllevar grandes pérdidas y daños en el servicio [10].

2.1.7. Vulnerabilidades lógicas

Dentro de las vulnerabilidades lógicas, se encuentran amenazas que van a afectar de manera directa a la infraestructura y la disponibilidad de estos, estas pueden ser:

- Configuración
- Actualización
- Desarrollo

Dentro de las vulnerabilidades por configuración, estas nacen a partir de ajustes erróneos, configuraciones obsoletas o un sistema de acceso débil [11]. Las vulnerabilidades por actualización se dan a partir de hardware y software con faltas de actualizaciones periódicas, estas actualizaciones permiten corregir distintos fallos en versiones antiguas, de no percatarse de estas actualizaciones se está dejando a los equipos expuestos a exploits [12]. las fallas de desarrollo son introducidas en la creación de un software o sistemas, estas fallas radican en pequeños apartados que un programador o personal encargado de la creación de un sistema informático no se hayan percatado [13].

2.1.8. Análisis de vulnerabilidades

Es la realización de un proceso de forma sistemática, el cual permite identificar, cuantificar y priorizar vulnerabilidades dentro de un sistema. Para llevar a cabo este análisis, existen distintas herramientas como Nmap, OpenVAS y Nessus. Un análisis de esta magnitud es de suma importancia para prevenir accesos no autorizados y garantizar la seguridad en una red [8].

2.1.9. Intrusión

Se entiende por intrusión todo acceso no autorizado a un sistema informático. Estas pueden clasificarse en dos categorías: intrusiones pasivas, que consisten en la interceptación o

vigilancia de la información sin modificarla, e intrusiones activas, que implican la alteración o manipulación de datos. Según Garfinkel, muchas de estas intrusiones resultan complejas de detectar sin el uso de herramientas especializadas, como los Sistemas de Detección de Intrusos (IDS, por sus siglas en inglés) [14].

2.1.10. Integridad de datos

El principio de integridad garantiza que los datos se mantengan inalterados, asegurando que no hayan sido modificados sin autorización. Este componente es esencial en contextos donde la fidelidad a la información original resulta crítica [15]. La alteración indebida de los datos puede acarrear consecuencias legales y operativas significativas.

2.1.11. Disponibilidad

El principio de disponibilidad se refiere a la capacidad de un sistema para mantenerse operativo y accesible siempre que sea requerido. Esta propiedad puede verse comprometida por diversas amenazas, entre las más comunes se encuentran los ataques de denegación de servicio distribuido (DDoS) y las fallas en el hardware. De acuerdo con la International Organization for Standardization para asegurar la disponibilidad implica implementar estrategias de respaldo y mecanismos de continuidad operativa.

2.1.12. Red informática

Dentro de una red informática, se constituyen distintos dispositivos los cuales están interconectados, de esta manera facilita el intercambio de datos y compartir recursos como impresoras. Estas redes en su mayoría suelen estar conformadas por distintos dispositivos, ya sea computadoras, servidores, switches, routers, entre otros. Según la finalidad principal de una red es facilitar la comunicación eficiente y segura entre usuarios [16].

2.1.13. Herramientas de ciberseguridad

Las distintas herramientas existentes sobre ciberseguridad son aplicaciones tecnológicas diseñadas para proteger sistemas y redes informáticas frente a distintas amenazas que puedan existir en la red, el uso adecuado de estas herramientas de evaluación es fundamental para asegurar la integridad, disponibilidad y confidencialidad en las redes.

2.1.13.1. Nmap (Network Mapper).

Es una utilidad de código abierto la cual está diseñada para realizar tareas de exploración y evaluación de redes. Creada por Fyodor Lyon, esta herramienta permite facilitar la identificación de equipos activos. Nmap permite identificar debilidades o configuraciones de forma incorrecta antes de que se percaten de esto los atacantes [17].

2.1.13.2. OpenVAS.

Open Vulnerability Assessment System es una herramienta de escaneo de vulnerabilidades mantenida por Greenbone Networks, esta permite que el personal pueda realizar análisis de manera idónea sobre dispositivos para detectar algún percance en la seguridad. Como menciona. OpenVAS es una solución poderosa y de libre acceso para una correcta evaluación de vulnerabilidades [18].

2.1.13.3. Nessus.

Nessus es una herramienta ampliamente empleada para la detección de vulnerabilidades, además de ser útil en procesos de auditoría de seguridad. Permite obtener información detallada sobre configuraciones débiles, puertos abiertos o servicios con posibles fallos. Adicionalmente, brinda una visión más profunda del estado general de seguridad de los sistemas [19].

2.1.14. Riesgo informático

Potencial que las amenazas exploten vulnerabilidades existentes en infraestructuras de red de una organización o institución, agravando su situación de confidencialidad, integridad y disponibilidad [20].

2.2. Marco referencial

En el año 2023, Martha Cecilia Pantoja Mejía desarrolló una tesis titulada “Evaluación técnica informática de las vulnerabilidades en ciberseguridad en los laboratorios de computación de la Universidad Técnica del Norte con base en COBIT 2019”. Se centró en evaluar las vulnerabilidades presentes en el laboratorio de computación, mediante la identificación de activos críticos, el análisis de diversos riesgos. Como resultado, se obtuvo un diagnóstico que evidenció falencias en la gestión de accesos, el control físico y las

políticas de respaldo. Esta tesis constituye una referencia de gran utilidad para realizar evaluaciones estructuradas de vulnerabilidades en entornos universitarios [21].

Jorge Andrés Silva Terán, en el año 2021, elaboró la tesis titulada "Identificación de vulnerabilidades y amenazas de la red de la Unidad Educativa Gonzalo Zaldumbide" en la cual se llevó a cabo la identificación de las vulnerabilidades mediante distintas herramientas como Nmap y Whireshark, gracias a estas herramientas se pudo evidenciar brechas en distintas configuraciones inseguras, contraseñas de un carácter débil y la existencia de varios puertos abiertos sin ninguna finalidad, además se logró identificar las amenazas mediante categorías y realizo un plan de mitigación de acorde a recursos existentes dentro de la universidad [22].

El proyecto desarrollado por Henry David Quishpe Malla en el año 2016, titulado "Análisis de vulnerabilidades en la red LAN jerárquica de la Universidad Nacional de Loja, en el área de la Facultad de la Energía, las Industrias y los Recursos Naturales no Renovables", se enfocó en la utilización de escáneres de vulnerabilidades y la aplicación de pruebas prácticas, con el propósito de identificar riesgos potenciales. Entre los hallazgos se destacaron dispositivos desactualizados, contraseñas débiles y la falta de segmentación en la red. Como resultado de este estudio, se elaboró un informe técnico que incluyó recomendaciones específicas orientadas a fortalecer la arquitectura de red y los protocolos de acceso [23].

En el año 2021 Damián Nicolalde desarrolló su proyecto de integración curricular con el título ¨ Vulnerability Analysis of the Exposed Public IPs in a Higher Education Institution¨ dentro de este trabajo llevó a cabo la examinación a profundidad de una red universitaria, en el cual utilizó herramientas como advanced IP Scanner y Shodan, se clasificaron los hallazgos por gravedad y se puso en punto de mira los equipos inseguros y que mantenían una protección robusta. Su trabajo radica en la recomendación principal de que las auditorias periódicas son clave para reducir los peligros que surgen cuando las direcciones IP quedan al descubierto dentro del campus [24].

En el trabajo de titulación realizado por Juan Gabriel Espinoza, como requisito previo para la obtención del título de Máster en Seguridad de las Tecnologías de la Información y Comunicación, titulado "Aplicativo web para el análisis de vulnerabilidades de una red institucional integrando herramientas open source" se centró en la creación de una interfaz, permitiendo descubrir fallos en distintos dispositivos conectados a la red, asimismo permitió obtener un mapa claro de la exposición de cada servicio y dispositivos, estos hallazgos son

clasificados por orden de gravedad al entorno de red, la importancia de este trabajo radica en la importancia de esta herramienta para tener un monitoreo continuo en la red [25].

En el año 2019, Ilias Chalvatzis, Dimitrios Karras y Rallis Papademetriuo desarrollaron una investigación titulada "Evaluation of Security Vulnerability Scanners for Small and Medium Enterprises Business Networks Resilience towards Risk Assessment" Dentro de este trabajo se llevó a cabo una evaluación de escáneres de vulerabilidades aplicados en redes de pequeñas y medianas empresas, El estudio compraró la velocidad de escaneo, capacidad de descubrimiento de vulnerabilidades, presentación de resultados y opciones de cada herramienta. Los hallazgos de este estudio radican en que los tres escáneres evaluados son adecuados para el propósito de tener una herramienta de evaluación de riesgos, además destaca que Nessus de haber permanecido gratuito y de código abierto, habría sido la mejor opción general debido a su dominio en el mercado, documentación disponible y vasta base de datos de vulnerabilidades [26].

2.3.Marco Legal y Normativo

2.3.1. Ley orgánica de protección de datos personales (LOPDP)

"El articulo 4 tiene finalidad asegurar que los usuarios ejerzan su derecho a la protección de datos personales, estableciendo principios y obligaciones que aseguren una adecuada protección" [27].

"Dentro del articulo 43 presenta que, en caso de presentarse una vulneración en la seguridad de los datos personales de los usuarios, el responsable del tratamiento de dichos datos deberá notificar de inmediato tanto a la Autoridad de Protección de Datos Personales como a los titulares afectados. Su propósito es garantizar que cualquier filtración de información sea gestionada de manera adecuada"[27].

2.3.2. Política nacional de ciberseguridad del Ecuador (Acuerdo No. 006-2021)

"Dentro de la política pública de telecomunicaciones se establece un marco para la correcta protección de infraestructuras críticas y datos del estado, el cual recalca el desarrollo de capacidades de ciberseguridad institucional, la gestión de incidentes de seguridad cibernética y cooperación interinstitucional en materia de ciberseguridad"[28].

2.3.3. Esquema gubernamental de seguridad de la informacion (EGSI)

"El EGSI destaca la importancia de la confidencialidad, integridad y disponibilidad de la informacion, mediante la implementación de políticas y controles específicos obligatorios para entidades públicas mediante la evaluación de riesgos sobre sus activos de información críticos" [29].

CAPÍTULO III

METODOLOGÍA DE LA INVESTIGACIÓN

3.1. Localización

La presente investigación se llevó a cabo en el departamento de Tecnologías de la Información y Comunicación (TIC) en la Universidad Técnica Estatal de Quevedo campus Central, ubicada en Av. Quito km 11/2 vía Santo Domingo de los Tsáchilas.

Figura 1.

Localización

Nota: *Obtenido de Google Maps*

3.2. Tipo de investigación

3.2.1. Investigación bibliográfica

El presente trabajo de integración curricular se caracteriza por tener un importante componente bibliográfico, debido a que se basa en la recopilación de información de manera técnica, normativa y científica, la cual va relacionado conjunto a la ciberseguridad y seguridad informática, las distintas vulnerabilidades en redes institucionales y las distintas metodologías que existen para el análisis y detección. Asimismo, esta revisión teórica, permite que se logre establecer un marco conceptual el cual ayuda a fundamentar la selección de herramientas.

3.2.2. Investigación descriptiva

Dentro de la investigación el enfoque descriptivo consiste en validar los resultados obtenidos mediante diversas herramientas de seguridad informática aplicadas a la red de la institución. A través de una correcta interpretación de estos resultados, se logra una comprensión más profunda de las vulnerabilidades presentes en la red, así como una mejor evaluación del impacto que tiene la detección temprana y preventiva de estas vulnerabilidades para fortalecer la seguridad informática de la institución.

3.2.3. Investigación aplicada

La investigación aplicada en esta investigación se centra en utilizar la herramienta de seguridad informática óptima para analizar y mitigar vulnerabilidades presentes en la red interna de la UTEQ. Además, no solo consiste en realizar un análisis teórico, sino en la ejecución de evaluaciones de vulnerabilidades utilizando herramientas de escaneo de vulnerabilidades. A través de estas herramientas generar resultados tangibles que permitan observar presencia de amenazas o configuraciones inseguras y como solucionarlas.

3.3.Métodos de investigación

3.3.1. Método inductivo

Dentro de la presente investigación, se parte con un enfoque inductivo, el cual se refleja principalmente en la fase de análisis y diagnóstico de vulnerabilidades dentro de la red interna. En esta etapa se busca de manera directa identificar patrones comunes a partir de datos específicos obtenidos mediante herramientas de seguridad informática, para así tener una mayor noción sobre el estado de seguridad de la infraestructura tecnológica de la universidad.

3.3.2. Método deductivo

Este método se ve presente en varias fases de la investigación, se lleva a cabo conjunto a la aplicación de marcos teóricos, normativos y estándares internacionales, como ISO/IEC 27001 y la Ley Orgánica de Protección de Datos Personales, A través de estas normas se busca indagar e identificar brechas o incumplimientos que puedan representar riesgos para la seguridad de la red interna. Mediante este método se puede facilitar la interpretación de mejor manera el estado de seguridad de la red.

3.4. Fuentes de recopilación de la información

La fuente de recopilación de información utilizada dentro de este estudio se clasifica como “fuentes primarias”, debido a que se obtiene información de primera mano cómo resultados de herramientas y entrevistas a personal autorizado, además también se obtiene de “fuentes secundarias”, la cual se enfoca principalmente en libros y documentos que aporten valor significativo de la misma índole. La ejecución de una revisión bibliográfica de forma exhausta también permitió profundizar en fundamentos conceptuales y en las teóricas existentes dentro del campo de las vulnerabilidades y seguridad informática.

3.5. Diseño de la investigación

Dentro de esta investigación se empleó un diseño no experimental, ya que está centrado en el análisis de la seguridad de la red interna de la UTEQ, sin intervenir o manipular de forma directa las variables que afecten la red. Además, no se realizarán modificaciones o controles dentro de la infraestructura, el enfoque está basado en identificar, analizar y describir vulnerabilidades existentes mediante el uso de herramientas de detección de vulnerabilidades. A continuación, se muestran las etapas realizadas para llevar a cabo la investigación:

3.5.1. Etapa 1: Etapa de preparación y revisión bibliográfica

Dentro de esta primera etapa, se realizó una amplia revisión bibliográfica en relación con vulnerabilidades en la red, tipos de vulnerabilidades y los riegos que estas ocasionan dentro de una red institucional.

Además, también se investigaron distintas herramientas existentes las cuales se comparan y se seleccionan las más beneficiosas para el estudio presente además se indagó herramientas que brinden una amplia comprensión y un análisis de forma correcta sobre el estado de vulnerabilidades en equipos y dispositivos.

3.5.2. Etapa 2: Análisis y diagnóstico inicial de la red

Se llevó a cabo el diagnóstico inicial de la red en la cual se trabajó, para tener conocimiento de los equipos que se comunican entre sí, además de servidores que imparten conexión a la red y que equipos afectan de manera directa en caso de detectar una vulnerabilidad de alto riesgo.

Además, se mantuvo una conversación con personal de TIC, que proporciono información la cual aporta mayor relevancia a este estudio, como la falta de seguimiento del EGSI. Debido a la falta de personal dedicado a la seguridad de la información, un punto indispensable para tener un ambiente de ciberseguridad con un monitoreo constante.

3.5.3. Etapa 3: Selección de herramientas de análisis

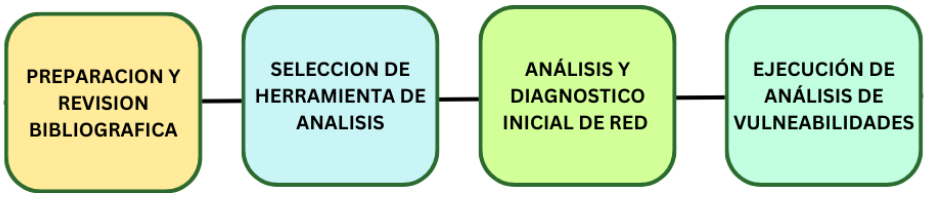
Luego de haber realizado una amplia revisión bibliográfica de distintas herramientas utilizadas para el análisis de vulnerabilidades en redes. Se seleccionará la herramienta óptima para la infraestructura de la red universitaria.

3.5.4. Etapa 4: Ejecución de análisis de vulnerabilidades

Una vez seleccionada las herramientas a utilizar en el presente estudio, se llevó a cabo el análisis de vulnerabilidades en equipos presentes dentro de la red del laboratorio de la UTEQ, para esto se conoció direcciones IP's de los servidores y equipos. Esta información es esencial para poder establecer conexión desde el software de análisis hacia el equipo a analizar.

Figura 2.

Diagrama de flujo diseño investigación



Nota: *Elaborado por Autor*

3.6. Instrumentos de la investigación

Para llevar a cabo esta investigación se utilizaron distintos instrumentos de investigación los cuales radican entre:

Observación Directa: se mantuvo presente la observación directa, de cómo funcionaban los distintos escaneos en las herramientas aplicadas, el cual incluye la revisión de nivel de peligrosidad de una vulnerabilidad, la solución frente a las distintas vulnerabilidades y que tanto afectaba esta vulnerabilidad hacia la red interna de la UTEQ.

Análisis de Documentación: Se analizaron los registros obtenidos luego de varios escaneos mediante las herramientas, el cual permite verificar el nivel de seguridad de la UTEQ, mediante un documento de auditoria arrojado por la propia herramienta.

Registros: Se mantuvieron registros de las distintas vulnerabilidades descubiertas, el cual permite crear una mejor propuesta de mejora en los distintos equipos de la Universidad.

CAPÍTULO IV

RESULTADOS Y DISCUSIONES

4.1. Resultados del primer objetivo

Para lograr el objetivo propuesto, se identificaron diversas herramientas de ciberseguridad destinadas al análisis de vulnerabilidades. Esta identificación se fundamentó en una revisión previa de la infraestructura de red, realizada a través de una entrevista con el Líder del departamento de TIC.

La elección de las nueve preguntas que se emplearon en la entrevista con el líder del Departamento de TIC se justificó en la congruencia del contenido con los controles más relevantes de la norma ISO/IEC 27001:2022. De los 93 controles existentes, se tomaron solamente los que se relacionan más con la gestión y protección de la red cableada interna, que es el enfoque de este trabajo.

Los controles seleccionados constituyen los elementos centrales para evaluar el nivel de madurez de la seguridad de la información en relación con la gestión de los activos de seguridad de la información, políticas de seguridad, segmentación de la red, control de vulnerabilidades, gestión de incidentes y responsabilidad. Esto hizo posible dirigir la entrevista a las áreas técnicas críticas que determinan directamente el nivel de riesgo de la infraestructura tecnológica institucional.

Tabla 1.

Entrevista realizada al Líder del departamento de TIC de la UTEQ

Preguntas	Si/No	Respuestas
Pregunta 1: Gestión de Activos (A.8.1): ¿Cuál es el número aproximado de dispositivos en la red cableada interna?	☒☒	Aprox. 180 dispositivos
Pregunta 2: Seguridad de Red (A.13.1): ¿Cómo está segmentada la red y cuáles son los rangos de IP principales?	☒☐	Segmentada en VLANs, con IPs públicas (190.15.134.1-30).
Pregunta 3: Gestión de Riesgos e Incidentes (A.6.1, A.16.1): ¿Qué tipos de ataques o incidentes preocupan más al Departamento de TIC para esta red interna?	☐☒	Los ataques que más son preocupantes se encuentran ransomware, robo de datos, la ingeniería social y bootnets que afecten la red.

Pregunta 4: Gestión de Incidentes (A.16.1): ¿Se han identificado vulnerabilidades o incidentes de seguridad relevantes en la red cableada interna en el pasado?	☒☐	Sí, incidentes de spam masivo en el pasado llevó a implementación de UTM
Pregunta 5: Gestión de Activos / Documentación (A.8.1, A.5.2) ¿Existen diagramas de red o inventarios de activos que podamos consultar?	☒☐	Sí, 80% del inventario de red desarrollado.
Pregunta 6: Políticas de Seguridad (A.5.1, A.18.2): ¿Hay alguna política de seguridad, norma interna o restricción que se deba conocer para realizar escaneos?	☐☒	No existen políticas, la única limitación es no generar escaneos en horarios laborables
Pregunta 7: Organización de la Seguridad de la Información (A.5.3, A.7.1): ¿Existe personal dedicado a la seguridad de la información?	☐☒	No, no hay personal dedicado a seguridad de la información.
Pregunta 8: Gestión de Vulnerabilidades (A.8.8): ¿Actualmente, la UTEQ utiliza alguna herramienta o plataforma para el escaneo de vulnerabilidades en su infraestructura de red o servidores?	☒☐	Sí, Nessus instalado, pero no gestionado por falta de personal.
Pregunta 9: Seguridad en el Desarrollo y Adquisición (A.8.2): ¿Existen páginas webs institucionales que se encuentren alojadas	☒☐	Si, las páginas webs de repositorio, biblioteca, página principal de la UTEQ se encuentran alojadas dentro de la red.

dentro de servidores de la Universidad?

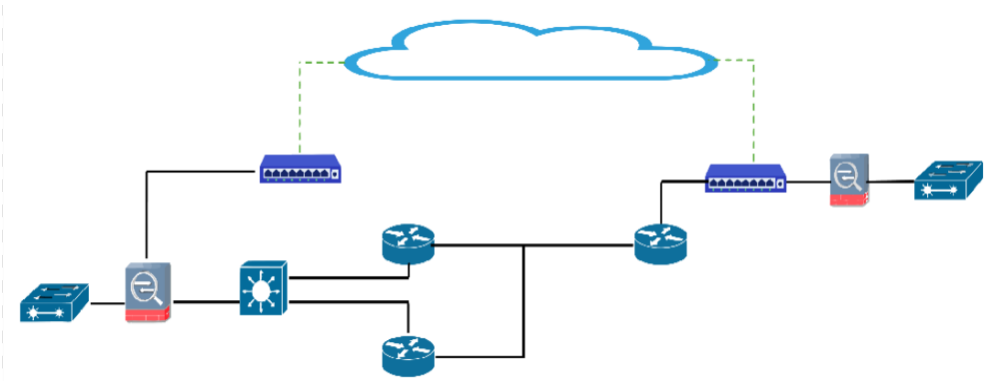
Nota: *Elaborado por Autor de acorde a normativa ISO 27001.*

La entrevista realizada al Líder del departamento de TIC permitió obtener un conocimiento profundo de la infraestructura. Gracias a su amplio dominio sobre el funcionamiento y la composición de la red, así como las principales deficiencias en la seguridad de la información, fue posible identificar la topología de red empleada por la UTEQ. Dicha topología facilita la distribución y administración de recursos entre sus dos campus, simulando una única infraestructura integrada.

4.1.1. Esquema de conexión entre campus Central y La María

Figura 3.

Esquema de conexión entre campus central y la maría



Nota: *Obtenido de informe de infraestructura Tecnológica UTEQ 2024*

La conexión entre ambos campus está configurada como una LAN extendida, esta permite que ambos campus se puedan administrar desde el departamento de TIC ubicado en su campus Central, esta red tiene la capacidad de 2.250 Gigabits por segundo (Gbps).

Dentro de esta topología se logra apreciar que las ultimas conexiones antes de llegar a los campus atraviesan un Firewall, en el caso del campus Central, el modelo del firewall es el Hillstone SG-6000, encargado de controlar el tráfico y/o bloquear conexiones, antivirus de Gateway, Filtrado de contenido, IDS/IPS, entre más opciones que permiten tener un entorno de red seguro en cuanto contenido que ingresa desde el exterior de la red.

Figura 4.

Equipo Firewall Hillstone SG-6000

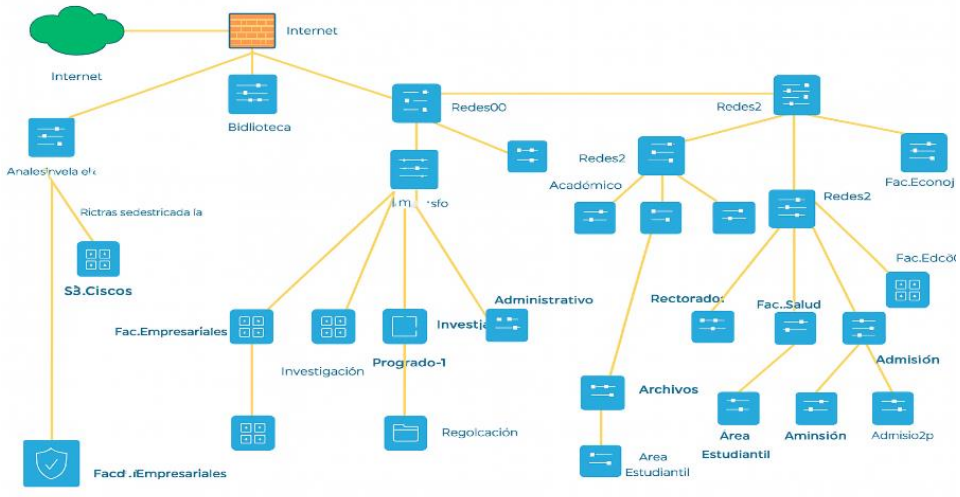
Nota: *Imagen referencial de equipo utilizado en red UTEQ*

Luego de reconocer como se encuentra conectada la arquitectura general de la red entre el proveedor de servicio de internet (CEDIA) y ambos campos de la UTEQ, el presente estudio se centró específicamente en el campus Central, esta decisión se basa en a que este campus alberga la mayor concentración de recursos tecnológico y es donde reside la infraestructura principal de la red, dentro del Departamento de TIC.

4.1.2. Esquema de conexión Campus Central

Figura 5.

Esquema de conexión entre dispositivos



Nota: *Topología utilizada entre edificios dentro de la red del campus Central*

La figura 5 describe como se encuentra segmentada la red del campus Central, en la cual se aprecia que se utiliza una topología tipo árbol, además resalta la presencia de sus principales conexiones y a que departamentos de la universidad provee de conexión a internet, esta segmentación por Vlans está pensada para cubrir de manera óptima cada área y tener una reducción de superficie de ataque, control de acceso y la contención de incidentes en la red.

4.1.2.1. Servidores.

La UTEQ cuenta con dos servidores HP modelo Proliant DL360 dentro de su red principal, estos servidores ofrecen diferentes servicios, además se imparte soporte a estudiantes y docentes de la institución para que puedan alojar aplicaciones web, utilizados en proyectos de investigación o vinculación. Los principales servicios que ofrecen estos servidores son:

- WEBUTEQ
- TOURVIRTUAL
- REVISTAS UTEQ
- DSPACE
- SERVICIOS TIC

Figura 6.

Servidor HP Proliant DL360

Nota: *Imagen referencial de servidores UTEQ*

4.1.2.2. Medidas de seguridad del centro de datos.

Dentro del centro de datos del departamento de TIC se encuentran alojados servidores, equipos de red y distintos equipos esenciales para un buen ambiente académico y laboral. Para garantizar la continuidad de este servicio sin interrupciones eléctricas, se cuenta con un sistema de respaldo el cual está compuesto por un generador a Diesel y un sistema de alimentación ininterrumpida (SAI) de 30kVA. Este sistema asegura la continuidad del funcionamiento de los servicios de red.

Figura 7.

Generador de electricidad SAI

Nota: *Imagen referencial de generador utilizado como SAI en red de la UTEQ*

4.1.3. Comparación de herramientas de escaneo de vulnerabilidades

Con la comprensión detallada de la infraestructura de la red cableada interna del Campus Central de la UTEQ, obtenida a través de la revisión previa y las perspectivas del personal de TIC, se procedió a la identificación y selección de las herramientas de análisis de vulnerabilidades más adecuadas para llevar a cabo el presente estudio.

Tabla 2.

Herramientas de análisis de vulnerabilidades

Tipo de herramienta	**OpenVAS**	**Nmap**	**Nessus Professional**
Tipo de análisis	Escaneo de vulnerabilidades	Descubrimiento de red e identificación de puertos	Escaneo de vulnerabilidades
Interfaz de usuario	Interfaz grafica	Líneas de comando	Interfaz gráfica intuitiva
Tipo de licencia	Código abierto (Gratuito)	Código abierto (Gratuito)	Comercial (Licencia de la UTEQ disponible)
Cobertura de vulnerabilidades	Amplia, con actualizaciones frecuentes	Limitada a scripts disponibles	Amplia, incluye configuraciones inseguras y software desactualizado
Actualizaciones de vulnerabilidades	Frecuente, gestionadas por Greenbone	Depende de la comunidad	Frecuentes, gestionadas por Tenable
Escaneo Autenticado	Si, robusto para sistemas operativos	Limitado	Sí, robusto y preciso

Nota: *Realizado por Autor basado en revisión previa de la infraestructura de la UTEQ*

Las herramientas mencionadas en la tabla 2 fueron seleccionadas de acuerdo con distintos estudios que utilizan estas aplicaciones como principales herramientas de escaneo de vulnerabilidades para un diagnóstico de seguridad en la red propuesta a estudiar.

De acuerdo con la comparación realizada se puede deducir que:

Nmap: se posiciona como una herramienta esencial para etapas iniciales del análisis, ya que permite identificar hosts activos, servicios en ejecución y puertos abiertos, proporcionando una visión clara de la superficie de exposición de la red. Aunque no está diseñada para realizar análisis avanzados de vulnerabilidades, su capacidad para detectar configuraciones irregulares o servicios inesperados la convierte en un recurso indispensable para obtener una base sólida del estado actual de la infraestructura.

OpenVAS: Ofrece un enfoque más profundo y completo, orientado específicamente a la detección y evaluación de vulnerabilidades. Su naturaleza de código abierto lo hace accesible, y su motor de escaneo permite identificar una gran variedad de fallas en sistemas y servicios. Sin embargo, su implementación y mantenimiento demandan mayor experiencia técnica, además de tiempos de escaneo más prolongados, lo que puede representar un desafío para instituciones con recursos limitados

Nessus Professional: destaca por su precisión, rapidez y amplio catálogo de plugins actualizados constantemente. Su capacidad para ejecutar escaneos autenticados, identificar configuraciones inseguras y correlacionar vulnerabilidades con soluciones propuestas le otorga una ventaja significativa frente a las demás herramientas evaluadas. Además, su interfaz intuitiva facilita la interpretación de los resultados incluso para personal con conocimientos intermedios.

4.1.3.1. Comparativa estadística de desempeño de herramientas.

Para tener una mejor perspectiva de cada herramienta se realizó una comparación basa en indicadores, las métricas están definidas según criterios como precisión, velocidad, cobertura, falsos positivos, facilidad de uso y actualización de vulnerabilidades.

Los valores ubicados en la tabla comparativa son considerados en base a estudios previos que evalúan el desempeño de cada una de estas herramientas [26][30][19].

Tabla 3.

Tabla comparativa de herramientas

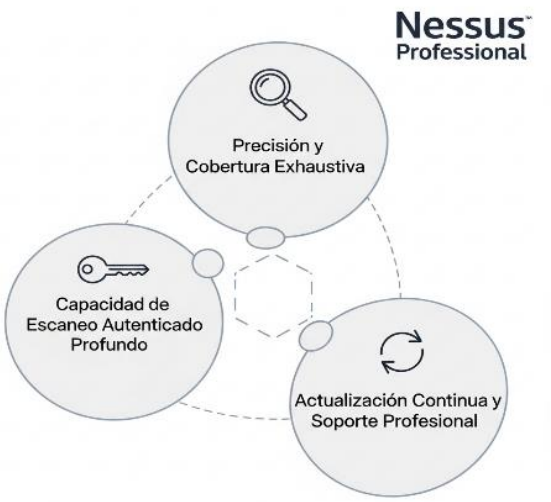
Criterio	Nmap	OpenVAS	Nessus Professional
Precisión de detección	68%	82%	96%
Falsos positivos	7%	9%	3%
Cobertura CVE	74%	88%	92%
Fallos de escaneo	7%	5%	2%

Nota: *Elaborado por Autor en base a distintos estudios*

4.1.3.2. Elección de Nessus como mejor herramienta

Figura 8.

Beneficios de Nessus



Nota: *Elaborado por Autor en base a estudio de evaluación de escáneres de vulnerabilidades*

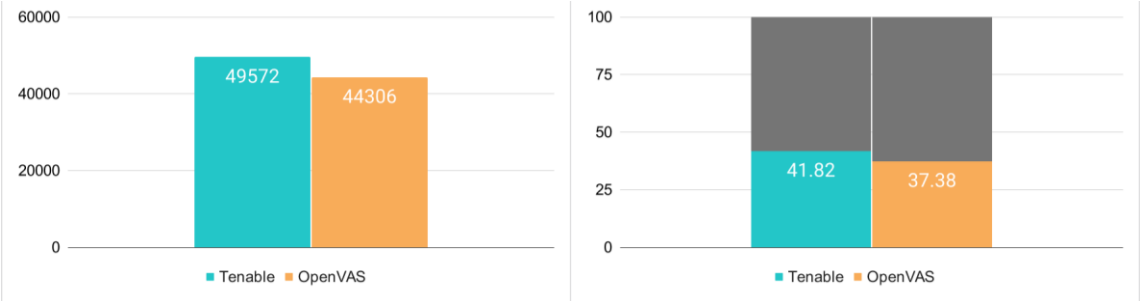
- **Cobertura y actualizaciones:** Nessus ofrece una amplia base de datos de vulnerabilidades y mantiene los plugins utilizados para detectar anomalías en una red actualizados de manera continua, permitiendo detectar nuevas vulnerabilidades que emergen [31].

La amplia cobertura de CVE de Nessus es comprobada en el análisis exhaustivo realizado por Andy Hornegold, indicando que la herramienta antes mencionada lleva una ventaja de

4.44% por delante de OpenVAS, este resultado (Figura 9) obtenido desde 2010 hasta la fecha en la que se publica este análisis en 2024 [31].

Figura 9.

Cobertura de CVE entre Tenable y OpenVAS



Nota: *Diferencia entre CVE de ambas herramientas*

- **Precisión:** Estudios recientes entre Nessus y OpenVAS, destacan que Nessus genera menos falsos positivos y tiene una tasa de detección verdadera mucho más elevada, reduciendo la revisión de alertas falsas.

  La comprobación de falsos positivos, comprobada elaborando laboratorios con vulnerabilidades simuladas en el cual Nessus detectó el 96% de manera correcta con solo 2 falsos positivos mientras que OpenVAS generó 5 falsos positivos [32].
- **Rendimiento:** Mediante un estudio que puso a prueba la velocidad de escaneo de Nessus, este completo el escaneo en 6 minutos se contrasta con más de 30 minutos que se tomó una herramienta convencional en realizar este mismo escaneo bajo las mismas condiciones [30].

4.1.4. Discusión de objetivo específico 1

La herramienta Nessus destaca en varios aspectos importantes, esto es respaldado en varios autores, Ilias Chalvatzis, Dimitrios Karras, Rallis Papedemetriou en su articulo “Evaluation of Security Vulnerability Scanners for Small and Medium Enterprises Business Networks Resilience towards Risk Assessment” también exponen el gran funcionamiento de esta herramienta comparada contra sus rivales, citando: “Su amplia documentación existente, extensa base de datos de vulnerabilidades la posiciona como una de las herramientas lideres en el mercado de la ciberseguridad, además de permitir al usuario tener una interfaz más intuitiva en el momento de realizar escaneos” [26].

La revisión previa de infraestructura mediante una entrevista estructurada alineada a normativas internacionales se alinea con la metodología de Pantoja, en la Universidad Técnica del Norte, quien también utilizó la interacción directa con los administradores de sus sistemas como fuente primaria de conocimiento [21]. Ambos estudios se alinean a reconocer que el conocimiento de personal técnico es fundamental para comprender la infraestructura.

4.2. Resolución del segundo objetivo

Esta fase de la investigación se enfocó en la aplicación de la herramienta de escaneo seleccionada mediante la ejecución de análisis en la red interna del departamento de TIC con el propósito de identificar vulnerabilidades existentes, para esto se utilizó Nessus Professional, la herramienta identificada y seleccionada en la etapa previa debido a sus capacidades de escaneo profundo y autenticado, así como la disponibilidad de su licencia en la UTEQ.

El alcance del objetivo presente se estableció para abarcar segmentos críticos de la red interna del campus central. Esto incluyó escaneos en la zona DMZ por su alta exposición, los servidores internos que alojan servicios institucionales esenciales y dispositivos de infraestructura de red central como switches. Para el análisis de esta configuración en equipos principales, fue coordinado con el personal de TIC de la UTEQ para asegurar un correcto escaneo y evitar interferencia en servicios de los usuarios.

4.2.1. Red propuesta para analizar vulnerabilidades

Con base a la entrevista que se mantuvo con personal del departamento de TIC y la facilitación de informacion sobre la infraestructura del campus Central de la UTEQ (Figura 5), se identificó distintos equipos de gran importancia para el análisis de vulnerabilidades existentes que podrían comprometer la funcionabilidad de sus servicios dentro del campus.

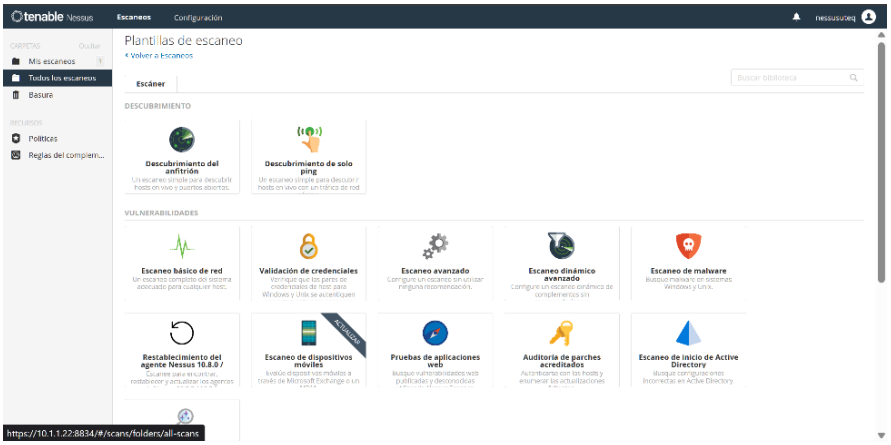
Entre estos equipos se encuentran:

- Servidores que alojan paginas importantes para la UTEQ
- Switches núcleo
- Switches de distribución
- Switches de acceso

4.2.2. Herramienta Nessus Professional

Figura 10.

Vista página principal de Nessus



Nota: *Página principal de herramienta Nessus antes de iniciar escaneo*

En la figura 11 se puede apreciar los distintos métodos de escaneos presentes en la herramienta Nessus, esta versión profesional, existe una gama más amplia de escaneos, la cual nos permite observar distintas falencias en las redes escaneadas.

Como principal método de escaneo se encuentra el de tipo avanzado, este método nos permite tener una vista mucho más detallada de las vulnerabilidades existentes dentro de una red, equipo o software.

Para la realización de estos escaneos se utilizaron plantillas las cuales se obtienen desde Nessus, permitiendo reconocer y abordar varias vulnerabilidades sin importar su procedencia.

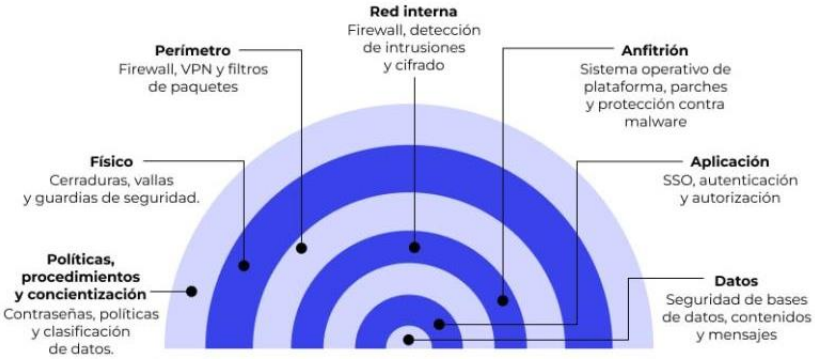
4.2.3. Arquitectura de ubicación de herramienta

Luego de seleccionar la herramienta Nessus como la más adecuada para el análisis de vulnerabilidades existentes dentro de la red, es indispensable entender el funcionamiento dentro de capas lógicas.

A nivel de arquitectura de seguridad, la herramienta Nessus Professional se ubica en la capa de Red interna, dentro del modelo de defensa en profundidad (Defence-in-depth). Debido a su funcionalidad que consiste en analizar vulnerabilidades en dispositivos finales e infraestructura de red.

Figura 11.

Arquitectura defensa en profundidad

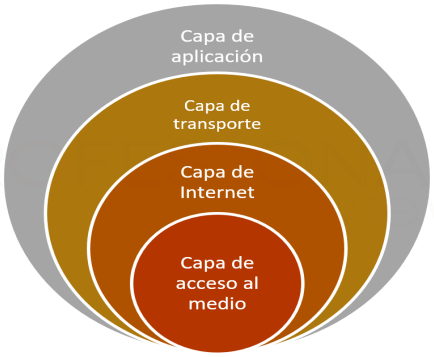


Nota: *Extraído de lab.wallarm.com*

Dentro de las arquitecturas TCP/IP y el modelo OSI, Nessus se encuentra ubicado en las capas de aplicación, transporte e internet. Realizando escaneos de vulnerabilidad en dispositivos y servicios críticos dentro de la infraestructura de red.

Figura 12.

Arquitectura TCP/IP



Nota: *Extraído de www.profesionalreview.com*

4.2.4. Escaneo de Zona Desmilitarizada (DMZ)

Los hallazgos significativos mediante el escaneo de la zona DMZ da a conocer un punto crítico dentro de la infraestructura, recalcando la alta cantidad de vulnerabilidades detectadas, especialmente las de severidad crítica y alta, esto refleja de manera directa una falta de seguimiento y monitoreo continuo en la red, debido a que la UTEQ no cuenta con personal dedicado a la seguridad de la información ni con políticas de seguridad que permitan la gestión y mitigación de estas vulnerabilidades.

Para lograr analizar esta DMZ, mediante la entrevista realizada al personal administrativo de TIC se pudo obtener esta dirección de red, la cual contiene distintos servicios que aloja la universidad dentro de su infraestructura, además de esto mediante este análisis se pudo observar que existen 32 servidores virtualizados.

Tabla 4.

Resumen global de vulnerabilidades en zona DMZ

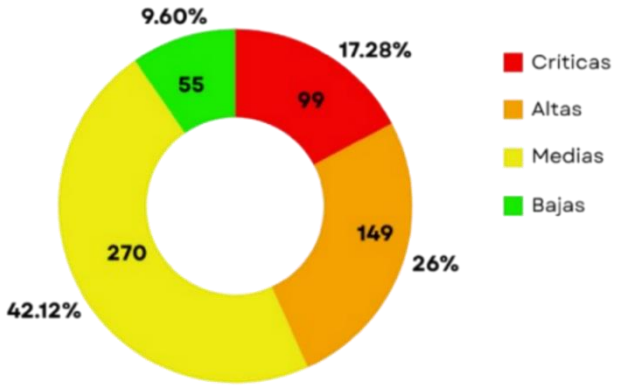
Nivel de Severidad	Vulnerabilidades totales	Porcentaje
Criticas	99	17.28%
Altas	149	14.9%
Medias	270	42.12%
Bajas	55	9.6%

Nota: *Elaborado por autor en base a reportes Nessus*

Mediante la tabla 4 se puede apreciar una gran afección a servicios alojados dentro de la infraestructura local del departamento de TIC, esto nos da una visión más amplia de cuan expuesto se encuentra la información en estos servidores. Para esto se eligió a los hosts más vulnerables los cuales son:

Figura 13.

Gráfico de vulnerabilidades en DMZ



Nota: *Elaborado por autor en base a tabla 4*

Tabla 5.

Hosts Críticos DMZ

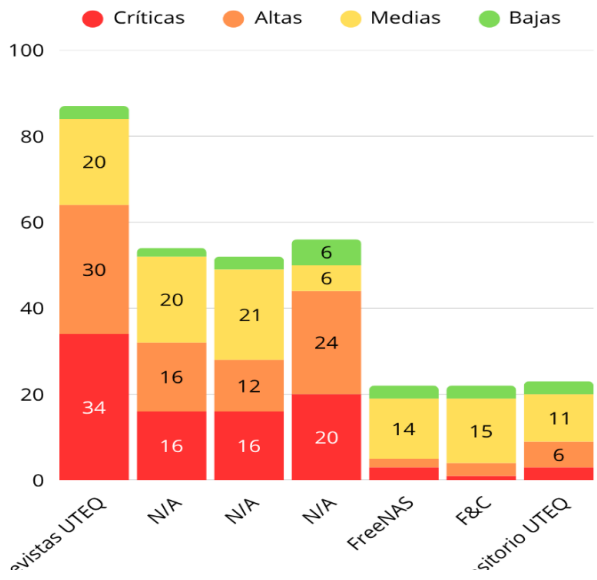
Host	Servicio	Criticas	Altas	Medias	Bajas
x.x.x.7	Revistas UTEQ	34	30	20	3
x.x.x.37	N/A	16	16	20	2
x.x.x.103	N/A	16	12	21	3
x.x.x.4	N/A	7	20	20	3
x.x.x.89	FreeNAS	3	2	14	3
x.x.x.41	F&C	1	3	15	3
x.x.x.200	Repositorio UTEQ	3	6	11	3

Nota: *Servidores críticos donde abarcan más vulnerabilidades*

Mediante la detección de 7 hosts más críticos que se encuentran dentro de la DMZ se puede comprobar la vulnerabilidad de 2 servicios propios de la UTEQ, tanto de las Revistas UTEQ y Repositorio UTEQ, además podemos observar que existen 3 hosts críticos los cuales no alojan un servicio disponible identificados como N/A (no activo), esto genera un punto de vulnerabilidad que puede ser explotado por atacantes, utilizándolo como un punto de pivote para realizar ataques internos, a distintos servidores que si alojan servicios críticos y de gran importancia.

Figura 14.

Gráfico de vulnerabilidades por hosts



Nota: *Elaborado en base a hallazgos en servidores críticos*

4.2.5. Vulnerabilidades en hosts críticos

En base al resumen global de las vulnerabilidades encontradas dentro de la DMZ, se procede a un análisis más profundo y detallado de estos 7 hosts críticos adjuntados en el punto anterior (tabla 4).

Para esto se presentará las principales fallas y vulnerabilidades de severidad crítica y alta encontradas en estos hosts, lo cual será de un punto de partida para la elaboración de un plan de mitigación efectivo.

Tabla 6.

Vulnerabilidades en DMZ

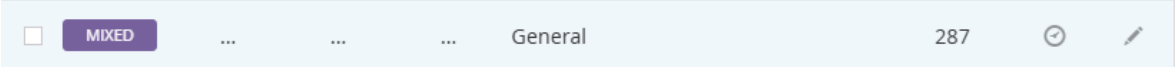
Caso	Severidad	Consecuencia
Versión desactualizada de Apache	Critica	Ataques DoS, Ejecución remota de código, filtración de información sensible
Versión desactualizada de OpenSSL	Critica	Ejecución de código remoto de atacante malicioso
Vulnerabilidad en HTTP TRACE/ TRACK	Media	Robo de información confidencial de usuarios mediante método TRACE

Nota: *Elaborado a partir de análisis de vulnerabilidades con mayor recurrencia*

Las vulnerabilidades seleccionadas en la presente tabla fueron seleccionadas debido a su alto nivel de reincidencia y nivel de afección a factores como disponibilidad de los datos en caso de ataque.

Figura 15.

Reincidencia de vulnerabilidad por SSL



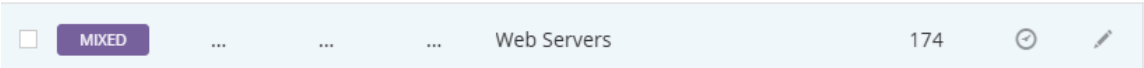
Nota: *Vulnerabilidades asociadas por versión desactualizada en OpenSSL*.

Dentro de la imagen se puede apreciar que está catalogado como Mixed, esto se debe a que, dentro de estas vulnerabilidades, existen vulnerabilidades de tipo crítico y alto relacionado

a versión obsoleta de OpenSSL, estas vulnerabilidades tienen una puntuación (CVSS) de 9, lo que lo cataloga como vulnerabilidad crítica.

Figura 16.

Reincidencias de vulnerabilidades por HTTP/Trace Track

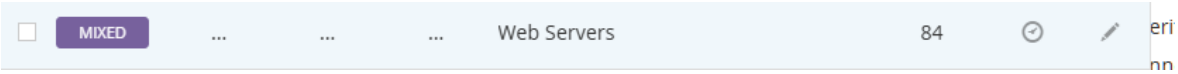


Nota: Se puede observar que 174 vulnerabilidades están asociadas a este método.

Estas vulnerabilidades por este método HTTP/Trace Track tiene como puntuación un CVSS de 6 esto las agrega en categoría de impacto medio.

Figura 17.

Reincidencias de vulnerabilidades por versión desactualizada de Apache



Nota: *Se observan 84 vulnerabilidades por Apache*

Entre estas vulnerabilidades derivadas de versiones obsoletas de Apache, se identifica una catalogada con un puntaje CVSS de 10, lo que la ubica como la más crítica y con el mayor número de reincidencias

De todas las vulnerabilidades encontradas dentro de este análisis a la zona DMZ se eligieron estas 3, debido a como se establece en la ISO/IEC27001:2022 en el control A.8.8 el cual trata sobre la gestión de vulnerabilidades, exige identificar, priorizar y tratar las debilidades que representen mayor exposición para la organización.

Asimismo, la normativa refuerza en su control A.8.9 (Gestión de parches) y A.8.21 (Seguridad de configuraciones) destaca la necesidad de corregir y mantener actualizados los servicios web y del sistema operativo.

El mismo fabricante de Apache reconoce la existencia y sus consecuencias de estas vulnerabilidades críticas en la red, como consecuencia de versiones obsoletas, su persistencia en el uso de estas expone a la infraestructura a graves consecuencias [33].

OpenSSL también ha publicado un aviso en el cual se enlistan 8 vulnerabilidades, 1 de severidad alta y 7 de severidad media, esto puede permitir que un atacante lea el contenido

de la memoria y provocar una denegación de servicio, además de descifrar los datos de la aplicación enviados y provocar fallos en la aplicación [34].

Las vulnerabilidades diagnosticadas como HTTP TRACE/TRACK son de severidad media, pese a esto puede provocar perdidas de información de gran valor, además permite la depuración malintencionada, permitiendo acceder a datos de confidenciales a personas equivocadas [35].

4.2.6. Escaneo de red interna (LAN)

La red interna de la UTEQ, es conformada por distintos switches los cuales están ubicados en zonas objetivas para poder brindar una buena comunicación entre edificios, estos switches conforman un tipo de topología árbol, al proceder de identificar las vulnerabilidades presentes en la red, permitió obtener una visión más amplia sobre el estado de la red interna de la UTEQ y las debilidades que asechan el compromiso de mantener confidencialidad y disponibilidad a los servicios prestados dentro de esta red.

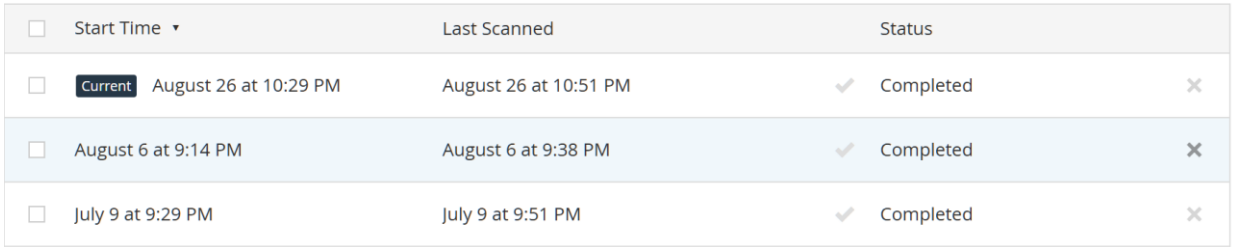
4.2.6.1. Configuración de escaneo.

El reporte obtenido desde la herramienta Nessus mediante el escaneo de tipo avanzado, se realizaron 3 escaneos, ejecutados a la dirección de red x.x.x.0/22 en distintas fechas, desde Julio hasta agosto del presente año que se realiza esta investigación.

Los escaneos se limitaron a 3 debido a que se observó que existió una grave afección en las redes correspondiente a su débil infraestructura que provocó colapso al momento de realizar escaneos que duró 6 minutos en volver a estar operativos todos los servicios.

Figura 18.

Horarios de escaneos

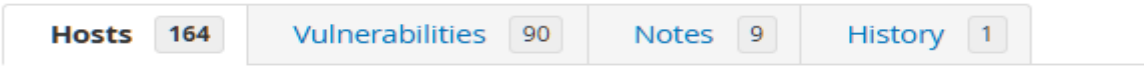


Nota: *Extraído de herramienta Nessus, fechas y horas de escaneos.*

Dentro de la herramienta se puede observar un resumen que presenta el total de hosts dentro de la red. Las vulnerabilidades existentes tomadas en cuenta por unidad sin repetición en hosts.

Figura 19.

Total de hosts y vulnerabilidades de red LAN



Nota: *Extraído de herramienta Nessus*

4.2.6.2. Resumen de hallazgos en red LAN.

El escaneo realizado a la red LAN de la UTEQ destaco un panorama en el cual se necesita acción y atención inmediata. Se identificaron 573 vulnerabilidades en un total de 164 hosts activos, lo cual deja como clara evidencia las brechas significativas en la postura de seguridad de la infraestructura de la red, la cual se encuentra alojada en el departamento de TIC y distribuido a los distintos edificios del campus.

Tabla 7.

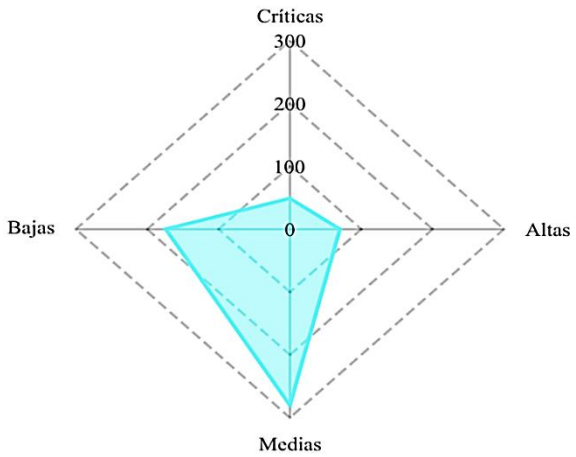
Distribución general de vulnerabilidades

Nivel de Severidad	Cantidad Total	Porcentaje
Críticas	49	8.55%
Altas	70	12.21%
Medias	280	48.8%
Bajas	174	30.3%

Nota: *Nivel de impacto por vulnerabilidades*

Figura 20.

Diagrama radar de vulnerabilidades en red LAN



Nota: *Se aprecia mayor cantidad de vulnerabilidades de categoría media.*

4.2.6.3. Análisis por segmentos de red.

Para poder tener una mejor percepción sobre el estado de estas vulnerabilidades, se procedió a separar por rango las direcciones IP debido a que dentro de la red antes mencionada hay 3 distintos rangos, x.x.24.x, x.x.25.x, x.x.27.x, obteniendo los distintos resultados de vulnerabilidades existentes.

Tabla 8.

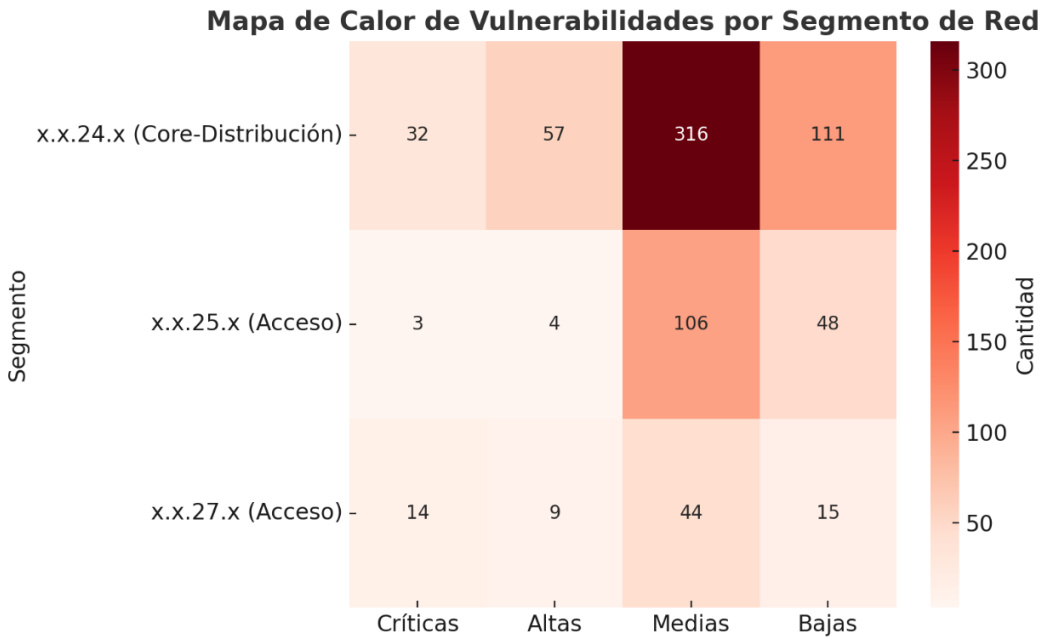
Segmentos de red

Host	Dispositivo	Criticas	Altas	Medias	Bajas
x.x.24.1 – x.x.24.254	Switch Core-Distribución	32	57	316	111
x.x.25.5 – x.x.25.103	Switches de Acceso	3	4	106	48
x.x.27.100 – x.x.27.255	Switches de Acceso	14	9	44	15

Nota: *Vulnerabilidades encontradas por segmentos de red.*

Figura 21.

Mapa de calor sobre vulnerabilidades en red LAN



Nota: *Se observa las zonas con mayor cantidad de vulnerabilidades*

De acuerdo con el análisis ejecutado en la red LAN y los hallazgos dado se puede observar distintas observaciones en los diferentes segmentos, dentro del rango .24 las principales afectaciones son switches cisco núcleo y servidores dentro de la infraestructura, en el rango .25 se encontró que existe una menor exposición debido a configuraciones más recientes, dentro del rango .27 se encuentran equipos con mayor antigüedad y falta de actualizaciones.

4.2.6.4. Vulnerabilidades Criticas Identificadas.

El análisis efectuado de las vulnerabilidades detectadas destaca patrones sistemáticos que requieren una atención estratégica para poder abordar y mitigar estas vulnerabilidades. Entre las vulnerabilidades más presentes en este análisis de la red LAN se encuentran:

1. **Sistemas operativos desactualizados**
   - CVE-2023-21554: Vulnerabilidad RCE en Microsoft message queuing
   - CVSS score: 9.8
   - Impacto: Ejecución remota de código no autenticado
2. **Protocolos de gestión inseguros**
   - Problema: Configuraciones SNMP con community strings por defecto
   - Hosts afectados: 100 dispositivos de red
   - Riesgo: Exposición de informacion sensible de configuración

3. **Servicios SSH vulnerables**
   - Vulnerabilidad: SSH con configuraciones débiles
   - Problemas: algoritmo de cifrados obsoletos, configuraciones de autenticación débiles, versiones desactualizadas de OpenSSH

4.2.7. Correlación con estándares de seguridad

Los hallazgos evidencian falencias significativas de acuerdo con las practicas establecidas por distintos marcos normativos nacionales e internacionales:

ISO/IEC 27001: 2022

- **A.8.8 (Gestión de vulnerabilidades):** Falta de proceso sistemático
- **A.13.1 (Controles de Red):** Configuraciones inseguras detectadas
- **A.12.2 (Protección contra Malware):** Sistemas sin protección actualizada

NIST Cybersecurity framework

- **Identify (ID):** Inventario incompleto de activos de red
- **Protect (PR):** Controles de acceso y actualizaciones insuficientes
- **Detect (DE):** Capacidad limitadas de monitoreo continuo

4.2.8. Discusión objetivo específico 2

La alta cantidad de vulnerabilidades detectadas en los servidores ubicados en la DMZ cifras que alcanzan valores acumulados superiores a los 200 hallazgos entre críticas y medias evidencia un incumplimiento directo del control A.8.8 de la ISO/IEC 27001:2022, que exige mantener un proceso continuo de identificación y tratamiento de vulnerabilidades.

Los resultados obtenidos de la DMZ, donde se identificaron varias vulnerabilidades criticas distribuidas en 32 distintos servidores virtualizados, tienen similitud con los hallazgos de Silva en la Unidad Educativa Gonzalo Zaldumbide, quien también identifico brechas significativas expuestas por configuraciones inseguras y la existencia de puertos abiertos sin funcionalidad especifica [22]. La similitud de estos resultados sugiere un patrón común en instituciones educativas ecuatorianas.

El análisis de la red interna reveló un total de 573 vulnerabilidades en 164 hosts identificados en la infraestructura, lo cual muestra una densidad mayor a la reportada por Nicolalde en su análisis de IP publicas expuestas en una institución de educación superior [24]. Esta diferencia se atribuye a que en el estudio presente involucro un análisis completo mientras que en la de Nicolalde se enfocó en la superficie de ataque externa.

4.3. Resolución del tercer objetivo

Luego de haber completado el análisis en busca de vulnerabilidades en la red propuesta a analizar, se logró identificar los principales riesgos y puntos débiles, para esto el presente objetivo se enfoca en proponer estrategias de mitigación. Las cuales se basan además de los resultados en normativas y estándares de seguridad reconocidos, asegurando que cada propuesta planteada sea viable para la institución.

Una estrategia que conlleva a una correcta protección está planteada por una serie de pasos que una organización puede tomar aumentar o mantener los niveles de seguridad en la red.

Dentro de la seguridad de redes el punto crítico que se debe de asegurar de primera mano es el factor humano, este por alto nivel de desconocimiento puede provocar la filtración de datos sensibles hacia cibercriminales. Para esto se plantea distintas estrategias de protección.

4.3.1. Matriz de prioridad de eventos

La asignación de prioridades dentro de la matriz de vulnerabilidades se fundamentó en criterios técnicos reconocidos internacionalmente, entre ellos el sistema de puntuación CVSS v3.1 (Common Vulnerability Scoring System), la norma ISO/IEC 27005 sobre gestión de riesgos y las directrices del NIST SP 800-30 Rev.1.

En función de estos parámetros, se estableció la categoría P1 (inmediata) para vulnerabilidades con severidad crítica, alta probabilidad de explotación externa e impacto directo en la disponibilidad de servicios institucionales, como los servidores alojados en la zona DMZ. Las vulnerabilidades P2 (urgentes) corresponden a fallas de severidad alta o media que, si bien poseen un impacto considerable, requieren acceso interno o autenticado para su explotación, como configuraciones inseguras de SNMP o SSH. Finalmente, las de P3 (importantes) fueron catalogadas como aquellas de bajo impacto operacional o probabilidad reducida de explotación, cuya mitigación puede realizarse de manera planificada.

Tabla 9.*Matriz de priorización de vulnerabilidades*

Categoría	Severidad	Impacto Operacional	Prioridad
Servidores DMZ	Crítica	Alto	P1-Inmediata
Protocolos SNMP	Media	Alto	P2-Urgente
Servicios SSH	Alta	Medio	P3-Importante
Sistemas operativos desactualizados	Crítica	Alto	P1-Inmediata

Nota: *Matriz de prioridad basada en directrices del NIST*

Para la mitigación de estas vulnerabilidades se proponen las siguientes estrategias especificas basadas en normas de fabricantes y puntos importantes de acuerdo con situación de red diagnosticada.

4.3.2. Estrategias de mitigación para vulnerabilidades

4.3.2.1. Fase 1: Remediación inmediata (PRIORIDAD P1).

Dentro de esta etapa se abordan las vulnerabilidades críticas con impacto directo en la disponibilidad de servidores institucionales.

- Actualización de Apache HTTP server a una versión estable recomendada por el fabricante (> 2.4.6) como medida de corrección de vulnerabilidades (CVE-2023-25690).
- Sustitución de openSSL por versiones mayores a 3.0.8 que corrigen fallos de ejecución remota de código.
- Implementación de monitoreo centralizado de logs en la zona DMZ con alertas automáticas.
- Desactivación de servidores innecesarios o sin función definida, evitando puntos de pivotes para ataques laterales

4.3.2.2. Fase 2: Fortalecimiento de servicios (PRIORIDAD P2).

La fase 2 se enfoca en reducir los vectores de ataque que resultan de configuraciones débiles y servicios inseguros.

- Reconfiguración de protocolos SNMP en todos los dispositivos de red utilizando community strings complejos y activando SNMPv3.
- Deshabilitar versiones obsoletas de SSH y forzar el uso de algoritmos criptográficos modernos.
- Implementar autenticación multifactor en los accesos administrativos a servidores críticos.
- Establecer un servidor de respaldo de configuraciones que permita la restauración ante alteraciones o incidentes.

4.3.2.3. Fase 3: Monitoreo continuo y prevención (PRIORIDAD P3)

Esta fase busca mantener la red bajo una observación constante y consolidar una cultura institucional de ciberseguridad.

- Automatizar escaneos semanales con Nessus y generar reportes comparativos.

- Integrar plataforma SIEM (Security Information and Event Management) para la correlación de eventos y detección temprana.
- Implementar políticas de gestión de vulnerabilidades y control de cambios donde cada parche o actualización sea documentado.
- Establecer indicadores de desempeño KPIs, como el tiempo promedio de respuesta y porcentaje de vulnerabilidades corregidas

4.3.3. Medidas técnicas para el fortalecimiento de la red cableada

El fortalecimiento de la seguridad de la red cableada interna de la UTEQ no solo es limitado a la mitigación de vulnerabilidades identificadas mediante escaneos, también se fundamenta mediante la implementación progresiva de controles técnicos, administrativos y operativos que garanticen la confidencialidad, integridad y disponibilidad de la información. Estos controles alineados con parámetros dentro de la norma ISO/IEC 27001:202 constituyen una base sobre la cual se consolida una configuración y fortalecimiento efectivo de la red.

4.3.3.1. Segmentación de red.

Luego de realizar los escaneos en la red interna, se identificó que la red utiliza una topología tipo árbol con varios segmentos conectados mediante switches núcleo y de acceso. El análisis mostró que el rango .24 donde se alojan servidores principales, abarca el 57% de las vulnerabilidades críticas detectadas.

Otro aspecto crítico identificado durante la evaluación es la presencia del protocolo SNMP configurado con la comunidad por defecto “public”, lo cual representa una vulnerabilidad significativa dentro del esquema actual de segmentación. Este tipo de configuración permite que cualquier usuario con acceso a la red interna pueda consultar información sensible del dispositivo, como tabla ARP, rutas, información del sistema y estadísticas de interfaz,

Como parte del proceso de mitigación, es prioritario deshabilitar comunidades por defecto, implementar SNMPv3 con autenticación y cifrado, y restringir el acceso únicamente a hosts autorizados dentro de la red de administración.

4.3.3.2.Control de acceso físico.

Durante la entrevista al líder del departamento de TIC se evidenció que no existen políticas formales de control físico para el ingreso al centro de datos, pese a que estos servidores almacenan información institucional.

La estrategia propuesta a aplicar consta de un sistema de control de acceso físico con registro biométrico y bitácora de ingreso para personal técnico autorizado, cumpliendo con el control A.11 de la ISO/IEC 27002. Permitiendo prevenir manipulaciones no autorizadas.

4.3.3.3. Autenticación y autorización.

El análisis de vulnerabilidades mostro la existencia de dispositivos con protocolos SNMP configurados con credenciales por defecto, así como servidores con SSH débil. Como estrategia a implementar está la aplicación de autentificación multifactorial y gestionar credenciales mediante un sistema centralizado.

4.3.3.4. Monitoreo y detección de intrusos.

Se constató que la UTEQ no dispone de monitoreo activo dentro de la institución, lo cual fue destacado en la entrevista previa a el líder TIC. Implementar un sistema de detección y prevención de intrusos (IDS/IPS) mediante software como snort o suricata, integrado con Nessus para la correlación de vulnerabilidades detectadas.

4.3.3.5. Actualización y parcheo de firmwares.

Los escaneos realizados evidenciaron 49 vulnerabilidades criticas asociadas a versiones desactualizadas de Apache HTTP server, openSSL y Microsoft message queuing. Para esto se plantea el establecimiento de un programa de gestión de parches con cronogramas mensuales, priorizando servidores expuestos de la DMZ. La ISO/IEC 27002 (A.8.8) exige que las organizaciones mantengan los sistemas actualizados para prevenir explotación de vulnerabilidades conocidas.

4.3.3.6. Políticas de uso y capacitación

Los resultados del diagnóstico inicial revelaron ausencia total de políticas internas de seguridad. Esto da como resultado planteado el desarrollo de una política institucional de

seguridad de la información (PISI) que establezca lineamientos para contraseñas, uso de recursos, gestión de incidentes y almacenamientos de datos. Estudios comprueban la efectividad de programas de concienciación de seguridad, se destaca que al entrenar al personal se reducen riesgos de errores humanos [36].

4.3.3.7. Auditorias y pruebas de penetración.

La ejecución de auditorías semanales y pruebas de penetración controladas utilizando herramientas especializadas. La ISO/IEC 27001, A.9.1. exige auditorías internas como mecanismos de mejora continua.

4.3.3.8. Redundancia y respaldo.

El análisis previo de la infraestructura de red permitió identificar que el centro de datos de la UTEQ cuenta con un solo punto de respaldo de energía, aunque se dispone de un sistema SAI de 30 kVA y un generador Diesel. Para fortalecer esto, se plantea el respaldo mediante copias de seguridad automáticas diarias y replicación de servidores principales de la UTEQ en máquinas virtuales espejo.

4.3.4. Informe de resultados obtenidos del escaneo

<table>
<tr><th colspan="3">INFORME FINAL DE ANALISIS DE RED INTERNA EN UTEQ</th></tr>
<tr><td colspan="3">Objetivo:</td></tr>
<tr><td colspan="3">Determinar el grado de exposición a vulnerabilidades dentro de la infraestructura de red de la UTEQ de acuerdo con criterios de seguridad definidos en ISO/IEC 27001 y EGSI, identificando riesgos y proponiendo medidas de mitigación.</td></tr>
<tr><td colspan="3">Alcance:</td></tr>
<tr><td colspan="3">Zona DMZ que abarca servidores institucionales, switches de núcleo, distribución y acceso de la red cableada. Se excluye redes inalámbricas y dispositivos finales de usuarios</td></tr>
<tr><td>Proceso</td><td>Descripción del hallazgo</td><td>Clasificación</td></tr>
<tr><td>Gestión de vulnerabilidades</td><td>Se identificaron 49 vulnerabilidades críticas, 70 altas en DMZ y configuraciones SNMP inseguras en 100 dispositivos.</td><td>M</td></tr>
</table>

Gestión de configuración	Se detectaron 39 hosts con SSH débil.	**M**
Procesos de monitoreo y respuesta	No existe personal dedicado a la reducción de las vulnerabilidades presentadas.	**O**
Gestión de incidentes	Existe un registro de incidentes y nuevas vulnerabilidades, pero no se abordan.	**O**

CLASIFICACIÓN

M = No conformidad mayor

m = No conformidad menor

O = Observación, área de mejora

4.3.5. Discusión objetivo específico 3

Las estrategias de mitigación propuestas, organizadas mediante una matriz la cual prioriza por severidad, se adoptan a un enfoque similar elaborado por Quishpe, quien elaboró un informe técnico el cual incluye recomendaciones específicas orientadas a fortalecer la arquitectura de red [23]. La similitud en ambos estudios valida la efectividad de marcos de priorización basado en riesgos de activos.

El presente estudio difiere significativamente de Silva en el enfoque de implementación. Mientras Silva propuso un plan de mitigación de acorde a los recursos existentes dentro de la universidad [22]. El presente estudio se basa en establecer fases de implementación que se consideran tanto los recursos disponibles como a estándares internacionales, proporcionando un marco más robusto para la gestión de vulnerabilidades existentes.

Es importante destacar que las vulnerabilidades técnicas identificadas en los hosts, la DMZ y los equipos de red guardan una relación directa con las nueve debilidades detectadas durante la entrevista del Objetivo Específico 1. Los hallazgos de Nessus como servicios desactualizados, configuraciones inseguras, puertos expuestos, SNMP por defecto y falta de segmentación efectiva.

Evidencian la ausencia de una adecuada gestión de vulnerabilidades (Control A.8.8), la inexistencia de políticas claras de configuración segura (Control A.8.21) y una deficiente administración de parches (Control A.8.9). Asimismo, la recurrencia de fallas en múltiples

equipos confirma las brechas previamente identificadas en control de accesos, monitoreo, inventario y capacitación del personal. Esto demuestra que las vulnerabilidades técnicas no son hechos aislados, sino el resultado de problemas estructurales ya señalados en las nueve preguntas iniciales.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

- El análisis comparativo elaborado entre las distintas herramientas de escaneo de vulnerabilidades reveló que la herramienta Nessus Profesional es la opción más viable para la infraestructura de la UTEQ al integrar unas funcionalidades avanzadas de escaneo. La revisión de red institucional evidencio la ausencia de políticas de seguridad, personal de seguridad de la informacion. La selección de Nessus se justifica por la disponibilidad de una licencia profesional y extensa base de plugins gestionados por Tenable, lo cual permite realizar escaneos profundos en distintos dispositivos de red.
- El diagnóstico realizado mediante la herramienta seleccionada en la red cableada interna del departamento de TIC evidenció una gran exposición a vulnerabilidades tanto críticas, altas, medias y bajas, demostrando un total de 573 vulnerabilidades en 164 hosts. De estas, el 8,55% corresponden a vulnerabilidades de severidad crítica y el 12,21% a vulnerabilidades de severidad alta y el 48,87% de severidad media. Asimismo, la zona DMZ se concentraron vulnerabilidades criticas asociadas a software obsoleto y versiones desactualizadas de bases de datos incrementando exposición de servicios institucionales alojados en la UTEQ.
- Las estrategias de mitigación de vulnerabilidades permitieron transformar los hallazgos de los análisis previos en un modelo integral de fortalecimiento de la red cableada interna de la UTEQ, basado en ocho ejes estratégicos que integran controles técnicos, administrativos y humanos. Este objetivo evidenció que la seguridad no depende solo de la tecnología, sino de la interacción entre procesos, personal capacitado y políticas institucionales bien estructuradas. Con ello, la UTEQ avanza hacia un esquema de defensa en profundidad, capaz de reducir más del 80 % de las vulnerabilidades críticas detectadas y consolidar una cultura organizacional orientada a la ciberseguridad sostenible.

5.2. Recomendaciones

- Se sugiere a la Universidad Técnica Estatal de Quevedo establecer formalmente un Sistema de Gestión de Vulnerabilidades (SGV) que incorpore la metodología de priorización por matriz de severidad validada en este estudio. Este sistema debe incluir la designación de al menos un profesional especializado en seguridad de la información dentro del organigrama institucional, la definición de procedimientos estandarizados para la gestión de incidentes según los SLAs propuestos, y la automatización de escaneos mediante la herramienta Nessus Professional ya disponible. La implementación debe seguir las fases progresivas establecidas (P1, P2, P3) para optimizar el uso de recursos limitados y garantizar la continuidad operativa durante los procesos de remediación.
- La UTEQ debe invertir en el desarrollo de capacidades técnicas del personal del Departamento de TIC mediante programas de capacitación especializados en gestión de vulnerabilidades, análisis de riesgos cibernéticos y implementación de controles de seguridad basados en estándares internacionales ISO/IEC 27001:2022 y NIST Cybersecurity Framework. Se sugiere establecer alianzas estratégicas con universidades o instituciones especializadas en ciberseguridad para facilitar la transferencia de conocimiento y la certificación del personal técnico. Esta iniciativa debe complementarse con la creación de documentación técnica interna que permita la institucionalización del conocimiento y la continuidad de los procesos de seguridad.
- Es pertinente institucionalizar la Política de Seguridad de la Información y ejecutar de manera gradual las ocho estrategias propuestas, priorizando la segmentación de red, autenticación multifactor y actualización continua de firmware. Asimismo, se debe fortalecer la capacidad técnica del personal TIC mediante formación en gestión de vulnerabilidades, implementar auditorías semestrales con herramientas automatizadas y mantener esquemas de respaldo y redundancia que aseguren la continuidad operativa. Finalmente, se aconseja establecer indicadores de desempeño que midan la eficacia de los controles implementados, permitiendo a la UTEQ evolucionar hacia un modelo preventivo, medible y conforme a estándares internacionales de seguridad informática.

CAPÍTULO VI

BIBLIOGRAFÍA

6.1Bibliografía

[1] Jesús Diaz Ruiz, “El 85% de las universidades ha sufrido ciberataques en el último año,” Nov. 2023.

[2] Kapersky Lab, “Empresas latinoamericanas reciben un promedio de dos ataques de ransomware por minuto, señala Kaspersky,” https://latam.kaspersky.com/about/press-releases/empresas-latinoamericanas-reciben-un-promedio-de-dos-ataques-de-ransomware-por-minuto-senala-kaspersky.

[3] ARCOTEL, “Implementación del Esquema Gubernamental de Seguridad de la Información (EGSI) en la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL),” 2015.

[4] R. Domínguez Domínguez, O. Flores Laguna, and J. A. Del Valle López, “Evaluation of an information security management system at a Mexican higher education INSTITUTION.”

[5] Daniel Fernando Yánez Guevara, “‘Sistema de detección y prevención de intrusos para el control de la vulnerabilidad en los servidores de la facultad de ingeniería en sistemas, electrónica e industrial de la universidad técnica de Ambato”,Universidad Técnica de Ambato, Ambato, 2013.

[6] WIlliam Stallings, “Computer Security: Principles and Practice,” Upper Saddle River, New Jersey, 2012.

[7] Allan Friedman, “Cybersecurity and Cyberwar: What Everyone needs to know ,” Oxford University , New York, 2014.

[8] Karen Scarfone, Murugiah Souppaya, and Amanda Cody, “Technical Guide to Information Security Testing and Assessment (NIST SP 800-115),” National Institute of Standards and Technology (NIST), Gaithersburg, 2008.

[9] Mariana Sofia Monsalve Gualteros, “Capacidades técnicas legales y de gestión para equipos red team & blue team,” Universidad Nacional Abierta y a Distancia- UNAD, Cauca, 2024.

[10] F. Andrade-Logroño and J. C. Cobos-Torres, “Vulnerabilidades y ciberseguridad en sistemas SCADA: Análisis de riesgos y estrategias de protección en infraestructuras

críticas," *MQRInvestigar*, vol. 9, no. 1, p. e289, Mar. 2025, doi: 10.56048/MQR20225.9.1.2025.e289.

[11] Luis Vicente Vite Constante, "Hacking ético en dispositivos PLC de control industrial conectados a red," Universidad Tecnica de Ambato, Ambato, 2017.

[12] Jaime Fabricio Malla and Diego Mauricio Narváez, "Implementación de un Framework de pentesting para el laboratorio de Micro-Red de la Universidad de Cuenca," Universidad de Cuenca, 2024.

[13] Jorge Eliecer Amorocho, "Diseño de estrategias de mitigación a las vulnerabilidades del entorno virtual metasploitable ," Barrancabermeja, 2020.

[14] Simson Garfinkel and Gene Spafford, "Practical Unix and Internet Security," Sebastopol, California, 2002.

[15] Kenneth Laudon and Jane Laudon, "Management Information Systems: Managing the Digital Firm," *Pearson*, 2015.

[16] Behrouz Forouzan, "Data Communications and Networking," New York, 2017.

[17] Gordon Fyodor Lyon, "Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning," 2009.

[18] Greenbone Networks GmbH, "OpenVAS 9 Documentation," 2020.

[19] Inc. Tenable Network Security, "Nessus Documentation," 2021.

[20] R. Sabillón and J. Cano, "Auditorías en Ciberseguridad: Un modelo de aplicación general para empresas y naciones," *Revista lbérica de Sistemas y Tecnologías de Información*, 2016.

[21] Martha Cecilia Pantoja Mejía, "Evaluación técnica informática de las vulnerabilidades en ciberseguridad en los laboratorios de computación de la Universidad Técnica del Norte con base en COBIT 2019," Universidad Técnica del Norte, Ibarra, 2023.

[22] Jorge Andrés Silva Terán, "Identificación de vulnerabilidades y amenazas de la red de la Unidad Educativa Gonzalo Zaldumbide," Universidad de los Andes, Ambato, 2021.

[23] Henry David Quishpe Malla, “Análisis de vulnerabilidades en la red LAN jerárquica de la Universidad Nacional de Loja, en el área de la Facultad de la Energía, las Industrias y los Recursos Naturales no Renovables,” Universidad Nacional de Loja, Loja, 2016.

[24] A. Chancusi, P. Diestra, and D. Nicolalde, “Vulnerability Analysis of the Exposed Public IPs in a Higher Education Institution,” in *2020 the 10th International Conference on Communication and Network Security*, New York, NY, USA: ACM, Nov. 2020, pp. 83–90. doi: 10.1145/3442520.3442523.

[25] Juan Gabriel Espinoza Calle, “Aplicativo web para el análisis de vulnerabilidades de una red institucional integrando herramientas open source,” Universitat Oberta de Catalunya, Catalunya, 2021.

[26] I. Chalvatzis, D. A. Karras, and R. C. Papademetriou, “Evaluation of Security Vulnerability Scanners for Small and Medium Enterprises Business Networks Resilience towards Risk Assessment,” in *2019 IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA)*, IEEE, Mar. 2019, pp. 52–58. doi: 10.1109/ICAICA.2019.8873438.

[27] Asamblea Nacional del Ecuador, “Ley Organica de Proteccion de Datos Personales,” May 2021.

[28] MINISTRA DE INCLUSIÓN ECONÓMICA Y SOCIAL, “ACUERDO MINISTERIAL No. 006-2021,” 2021.

[29] MINISTERIO DE TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓ, “Ministerio De Telecomunicaciones Y De La Sociedad De La Información:”.

[30] Kushe, “COMPARATIVE STUDY OF VULNERABILITY SCANNING TOOLS: NESSUS VS RETINA,” *INTERNATIONAL SCIENTIFIC JOURNAL “SECURITY & FUTURE”*.

[31] A. Hornegold, “OpenVAS vs. Nessus: un análisis exhaustivo,” https://www.intruder.io/blog/openvas-vs-nessus.

[32] S. Toyin, “COMPARATIVE ANALYSIS OF SECURITY VULNERABILITY SCANNERS (NESSUS AND OPENVAS) IN CLOUD ENVIRONMENT,” University of Bolton, 2023.

[33] Apache Software Foundation, “Apache HTTP Server 2.4 vulnerabilities,” https://httpd.apache.org/security/vulnerabilities_24.html.

[34] S2GRUPO, “Múltiples vulnerabilidades en OpenSSL,” https://s2grupo.es/multiples-vulnerabilidades-en-openssl/#:~:text=OpenSSL%20ha%20publicado%20un%20aviso%20que%20recoge%208,conexi%C3%B3n%20o%20provocar%20un%20fallo%20en%20la%20aplicaci%C3%B3n.

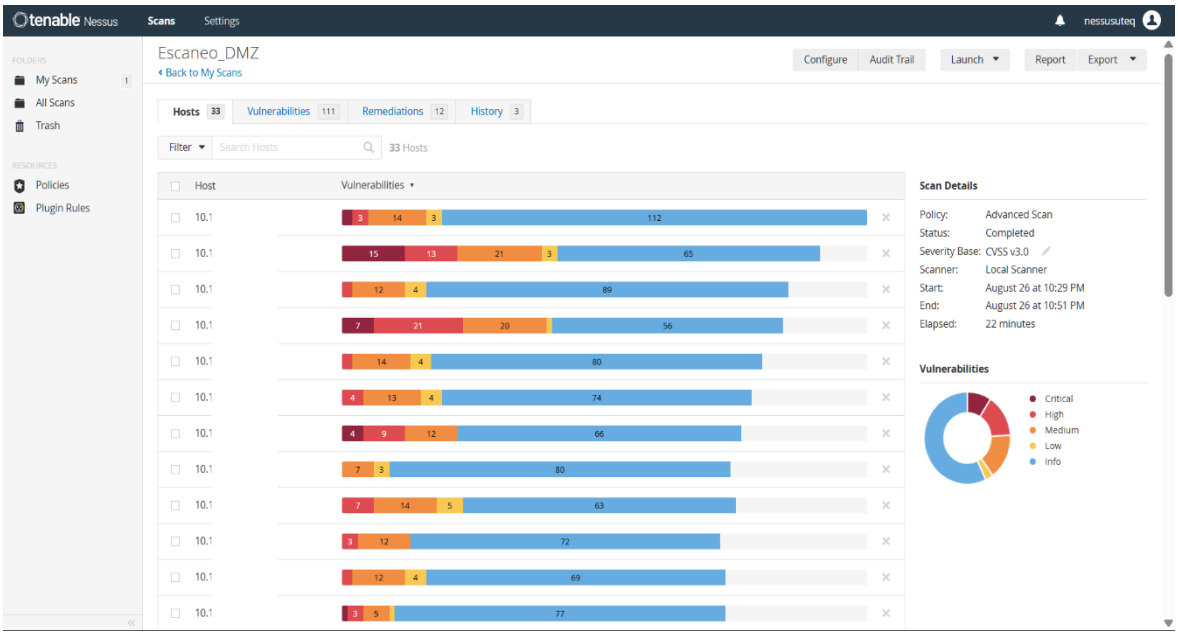
[35] B. Martínez, “AUDITORÍA DE SEGURIDAD WEB COMO HERRAMIENTA DE DIAGNÓSTICO DE VULNERABILIDADES DE LA PÁGINA WEB DEL CENTRO DE TRANSFERENCIA DE TECNOLOGÍA - TALLERES TECNOLÓGICOS DE LA FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL ,” UNIVERSIDAD TÉCNICA DE AMBATO , Ambato, 2025.

[36] J. Haney and W. Lutters, “Security Awareness Training for the Workforce: Moving Beyond ‘Check-the-Box’ Compliance,” *Computer (Long Beach Calif)*, vol. 53, no. 10, pp. 91–95, Oct. 2020, doi: 10.1109/MC.2020.3001959.

CAPITULO VII

ANEXOS

Anexo 1.*Escaneo de DMZ*



Anexo 2. *Escaneo de red LAN TIC*