UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ

TRABAJO DE TITULACIÓN

MODALIDAD PROYECTO INTEGRADOR

TÍTULO:

"SISTEMA DE DETECCIÓN DE INTRUSOS EN LA RED DE COMUNICACIÓN DE LA UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ EXTENSIÓN CHONE."

AUTOR:

JESUS SIMON DELGADO MACIAS

UNIDAD ACADÉMICA:

EXTENSIÓN CHONE

CARRERA:

TECNOLOGÍAS DE LA INFORMACIÓN

TUTOR:

ING. JORGE LUIS MENDOZA LOOR

CHONE – MANABÍ – ECUADOR

JUNIO 2026

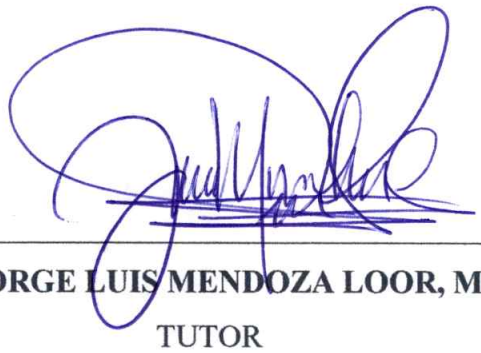
CERTIFICCERACICÓN DEL TUTOR

Ing. Jorge Luis Mendoza Loor, Mg.; docente de la Universidad Laica "Eloy Alfaro" de Manabí, Extensión Chone, en calidad de Tutor(a) del Proyecto.

CERTIFICO:

Que el presente Proyecto Integrador con el título "Sistema de detección de intrusos en la red de comunicación de la Universidad Laica Eloy Alfaro de Manabí Extensión Chone." ha sido exhaustivamente revisado en varias sesiones de trabajo, las opciones y conceptos vertidos en este Proyecto son fruto de la perseverancia y originalidad de su autor: Jesus Simon Delgado Macias, siendo de su exclusiva responsabilidad.

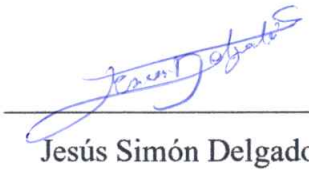
Chone, junio de 2026



Ing. JORGE LUIS MENDOZA LOOR, Mag.
TUTOR

DECLARACIÓN DE AUTORÍA

Quien suscribe la presente: Jesús Simon Delgado Macias, estudiante de la Carrera de Tecnologías de la información, ULEAM Extensión Chone, declaro bajo juramento que el siguiente proyecto cuyo título: "Sistema de detección de intrusos en la red de comunicación de la Universidad Laica Eloy Alfaro de Manabí Extensión Chone.", previa a la obtención del Título de Ingeniero en Tecnologías de la Información, es de autoría propia y ha sido desarrollado respetando derechos intelectuales de terceros y consultando las referencias bibliográficas que se incluyen en este documento.



Jesús Simón Delgado Macias

NUI: 1314337674

APROBACIÓN DEL TRABAJO DE TITULACIÓN

Los miembros del Tribunal Examinador aprueban el Trabajo de Titulación con Modalidad Proyecto Integrador, titulado: "Sistema de detección de intrusos en la red de comunicación de la Universidad Laica Eloy Alfaro de Manabí Extensión Chone.", bajo la autoría de: Jesus Simon Delgado Macias, estudiante de la Carrera de Tecnologías de la Información y la tutoría del Ing. Jorge Luis Mendoza Loor, Mg.

Chone, junio de 2026

Lcda. Lilia del Rocío Bermúdez Cevallos, Mg.
DECANA

Ing. Jorge Luis Mendoza Loor, Mg.
TUTOR

Lector 1
MIEMBRO DEL TRIBUNAL

Lector 2
MIEMBRO DEL TRIBUNAL

Leda. Indira Zambrano Cedeño, Mg.
SECRETARIA

AGRADECIMIENTO

En primer lugar, mi más profundo agradecimiento es para Dios, fuente de fortaleza y esperanza en cada paso de este recorrido. Ha sido mi guía en los momentos de incertidumbre y mi refugio en los días difíciles. Reconozco que todo logro alcanzado es también fruto de su amor y de las bendiciones que ha derramado sobre mi vida.

A mis padres, les debo más de lo que las palabras pueden abarcar. Gracias por su esfuerzo incansable, por los sacrificios silenciosos, por creer en mí incluso cuando yo dudaba, y por enseñarme con su ejemplo que la constancia y la honestidad son la base de cualquier meta alcanzada. Este triunfo es tan suyo como mío.

Mi gratitud también es para la Universidad Laica Eloy Alfaro de Manabí, Extensión Chone, por brindarme no solo una educación de calidad, sino también experiencias y aprendizajes que han contribuido a mi crecimiento personal y profesional. Cada desafío superado en estas aulas ha dejado una huella en mi manera de ver y enfrentar la vida.

A mis docentes, gracias por su dedicación, paciencia y compromiso, más allá de los conocimientos académicos, me han enseñado que el verdadero valor de la educación está en la pasión por transmitirla y en el ejemplo que se deja en los estudiantes.

A mis amigos y compañeros de camino, gracias por compartir largas horas de estudio, momentos de tensión, risas y celebraciones, su apoyo constante y su compañía hicieron que este trayecto fuera más ameno y memorable, sin duda, la amistad que hemos forjado es uno de los tesoros más valiosos que me llevo de esta etapa.

Jesus Simon Delgado Macias

DEDICATORIA

Dedico este trabajo, en primer lugar, a Dios, por ser la luz que ha guiado mi camino y la fuerza que me sostuvo en los momentos más difíciles. Sin Su presencia, nada de esto habría sido posible.

A mis padres, que con amor, paciencia y sacrificio me enseñaron a luchar por mis sueños y a no rendirme ante las adversidades. Este logro es el reflejo de todo lo que me han inculcado y del inmenso apoyo que siempre me han brindado.

A mi familia, por estar siempre ahí con una palabra de aliento, un consejo oportuno y un abrazo sincero. A mis amigos, que con su compañía hicieron de este recorrido una experiencia más llevadera, llenando de alegría incluso los días de mayor esfuerzo.

Y a todas aquellas personas que, de una u otra forma, han dejado su huella en esta etapa de mi vida, les dedico este logro con gratitud y cariño.

Jesus Simon Delgado Macias

ÍNDICE DE CONTENIDOS

Contenido

ÍNDICE DE GRAFICAS E ILUSTRACIONES

ÍNDICE DE TABLAS

RESUMEN

La Universidad Laica Eloy Alfaro de Manabí, Extensión Chone, surge como respuesta a la creciente necesidad de proteger los recursos tecnológicos y la información institucional frente a amenazas cibernéticas, en los servicios en línea y aplicaciones móviles en el entorno universitario, la exposición a ataques como accesos no autorizados, malware, robo de credenciales y fuga de datos ha aumentado significativamente. El proyecto tiene como propósito implementar un mecanismo que permita monitorear de forma continua el tráfico de la red, detectar comportamientos anómalos y generar alertas tempranas para una respuesta rápida ante incidentes, para su desarrollo, se aplicó una metodología mixta que combinó recolección de datos mediante encuestas y entrevistas con personal técnico, análisis documental de normativas y políticas de seguridad, y pruebas prácticas utilizando herramientas de detección y análisis como Snort, Suricata y Wireshark. La arquitectura propuesta del IDS contempla módulos para análisis de paquetes en tiempo real, registro detallado de eventos, integración con firewalls, autenticación reforzada y cifrado de datos de red, fomentando una cultura de ciberseguridad dentro de la institución. La estrategia se fundamentó en estándares internacionales como ISO/IEC 27001 y las directrices nacionales sobre protección de datos personales, asegurando que las medidas adoptadas cumplan con las mejores prácticas del sector. Como resultado, se logró una solución escalable y adaptable a las necesidades del campus, fortaleciendo la resiliencia de la red ante amenazas internas y externas, y minimizando el impacto de posibles incidentes de seguridad.

Palabras claves: Desarrollo del Sistema de Detección de Intrusos (IDS) para la red de comunicación

CAPITULO I: INTRODUCCIÓN

1.1. Introducción

Los Sistemas de Detección de Intrusos (IDS) han experimentado importantes avances en los últimos años gracias a la incorporación de algoritmos de aprendizaje automático (Machine Learning) y técnicas de inteligencia artificial, permitiendo incrementar la precisión en la identificación de amenazas y adaptarse a nuevos tipos de ataques, especialmente aquellos conocidos como ataques de día cero. Entre las innovaciones más destacadas se encuentra el uso de Redes Generativas Antagónicas (GAN), las cuales permiten simular escenarios de ataque para fortalecer la capacidad de detección de tráfico malicioso, incluso cuando los atacantes intentan evadir los mecanismos tradicionales de seguridad.

A nivel mundial, los IDS desempeñan un papel fundamental en la protección de las infraestructuras tecnológicas, ya que permiten detectar actividades sospechosas, accesos no autorizados y posibles vulneraciones de seguridad. Su implementación contribuye a la protección de la información y de los recursos tecnológicos utilizados por estudiantes, docentes, personal administrativo y demás usuarios que hacen uso de los servicios de red dentro de las instituciones educativas. De esta manera, los sistemas de detección de intrusos se han convertido en una herramienta indispensable para fortalecer la seguridad informática y garantizar la continuidad de los servicios tecnológicos.

En Ecuador, el crecimiento de la transformación digital y el aumento de las amenazas cibernéticas han impulsado la adopción de mecanismos avanzados de protección tanto en organizaciones públicas como privadas. Diversas entidades han incorporado sistemas de detección de intrusos basados en análisis de comportamiento, firmas e inteligencia artificial, con el propósito de prevenir incidentes de seguridad y reducir los riesgos asociados al acceso no autorizado a la información. Estas acciones evidencian la necesidad de implementar soluciones tecnológicas que permitan fortalecer la protección de las redes de comunicación y los activos informáticos.

La Universidad Laica Eloy Alfaro de Manabí, Extensión Chone, depende de su infraestructura tecnológica para el desarrollo de actividades académicas, administrativas y de

comunicación, sin embargo, el incremento de los riesgos cibernéticos hace necesario fortalecer los mecanismos de seguridad existentes mediante la implementación de herramientas que permitan identificar oportunamente posibles amenazas, por ello, la presente investigación tiene como objetivo general implementar un Sistema de Detección de Intrusos (IDS) en la red de comunicación de la institución, con el fin de mejorar la seguridad informática y contribuir a la protección de los recursos tecnológicos institucionales.

En este contexto, la presente investigación se desarrolla dentro de la línea de investigación Tecnologías de la Información y las Comunicaciones (TIC), la cual promueve el estudio, desarrollo e implementación de soluciones tecnológicas orientadas a mejorar la gestión, transmisión y protección de la información mediante el uso eficiente de las tecnologías digitales, asimismo, se vincula con la sub línea Seguridad Informática y Redes de Comunicación, debido a que aborda el análisis, monitoreo y protección de infraestructuras de red frente a amenazas y vulnerabilidades que puedan afectar la integridad, confidencialidad y disponibilidad de la información institucional.

Para alcanzar este propósito, se plantea analizar la infraestructura actual de la red para identificar vulnerabilidades y riesgos de seguridad, seleccionar las herramientas y tecnologías más adecuadas para la implementación del sistema, un IDS que permita monitorear el tráfico de red y detectar actividades sospechosas, evaluar su funcionamiento mediante pruebas de detección de amenazas y, finalmente, proponer recomendaciones que contribuyan al fortalecimiento continuo de la seguridad informática dentro de la Universidad Laica Eloy Alfaro de Manabí, Extensión Chone.

Para el desarrollo de este proyecto se adopta un enfoque metodológico mixto, integrando, técnicas cuantitativas y cualitativas con el propósito de obtener una visión integral de la situación actual de la red de comunicación de la Universidad Laica Eloy Alfaro de Manabí, Extensión Chone, el estudio se enmarca en una investigación de tipo aplicada, ya que busca desarrollar e implementar una solución tecnológica orientada a fortalecer la seguridad informática institucional mediante un Sistema de Detección de Intrusos (IDS), asimismo, presenta un nivel descriptivo y explicativo, debido a que permite identificar y analizar las vulnerabilidades existentes en la infraestructura de red, así como comprender las causas y efectos de los riesgos de seguridad detectados.

Para la recopilación de información se emplearán métodos exploratorios, observación directa, permitiendo obtener datos relevantes sobre el estado actual de la red y fundamentar el diseño, implementación y evaluación de la solución propuesta, este enfoque metodológico contribuirá al cumplimiento de los objetivos planteados y permitirá determinar la efectividad del sistema en la detección y mitigación de posibles amenazas informáticas.

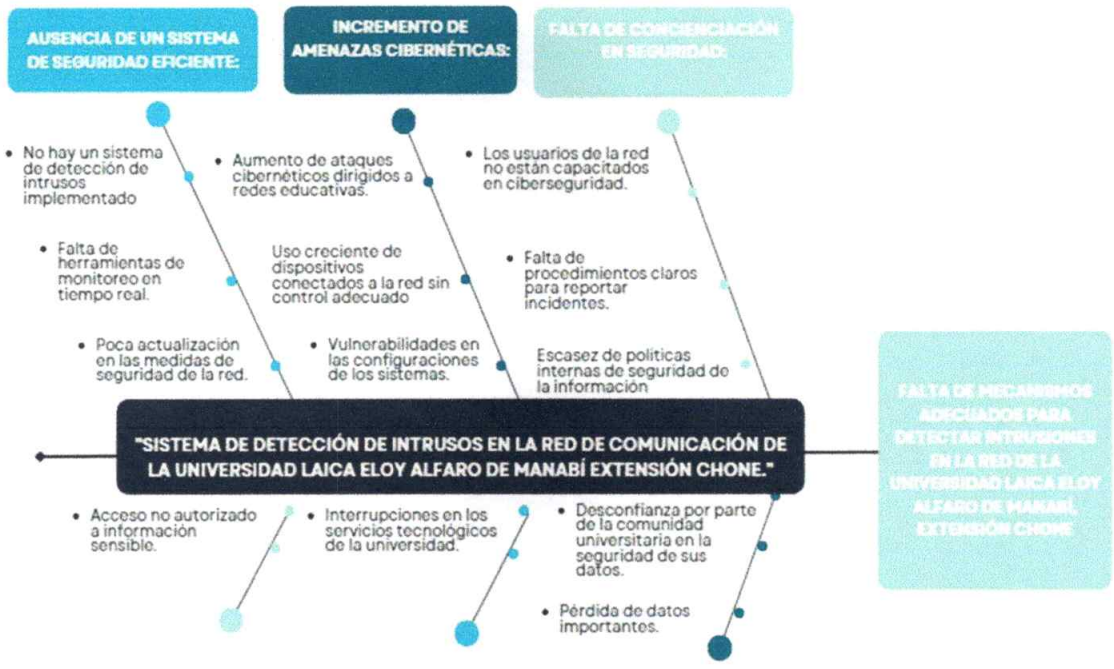
Se espera que la implementación del Sistema de Detección de Intrusos (IDS) en la red de comunicación de la Universidad Laica Eloy Alfaro de Manabí, Extensión Chone, permita identificar las principales vulnerabilidades presentes en la infraestructura tecnológica institucional y detectar oportunamente actividades sospechosas o accesos no autorizados, asimismo, se prevé que el sistema proporcione información relevante sobre el comportamiento del tráfico de red, facilitando el monitoreo continuo y fortaleciendo los mecanismos de seguridad existentes, como resultado, se espera mejorar la capacidad de respuesta ante incidentes de seguridad informática, reducir los riesgos asociados a posibles ataques cibernéticos y contribuir a la protección de la información académica, administrativa y tecnológica de la institución.

Con base en los objetivos planteados, se espera concluir que la implementación de un Sistema de Detección de Intrusos constituye una alternativa eficaz para fortalecer la seguridad de la red de comunicación de la Universidad Laica Eloy Alfaro de Manabí, Extensión Chone., Se prevé demostrar que el análisis previo de las vulnerabilidades permitió seleccionar e implementar una solución adecuada a las necesidades institucionales, mejorando la detección de amenazas y el monitoreo de la red. Finalmente, se espera evidenciar que la incorporación de herramientas de detección de intrusos contribuye significativamente a la protección de los activos tecnológicos, garantizando una mayor integridad, confidencialidad y disponibilidad de la información, así como la continuidad de los servicios de comunicación de la universidad.

1.2. Diagrama causa – efecto

Se encuentran la ausencia de un sistema de seguridad eficiente, el incremento de las amenazas cibernéticas y la falta de concienciación en seguridad informática. Estas deficiencias pueden generar consecuencias como accesos no autorizados a información sensible, interrupciones en los servicios tecnológicos y pérdida de datos importantes.

Ilustración 1: Diagrama casusa y efecto



Elaborado por: Autor del Proyecto

1.3. Planteamiento y Formulación del Problema

La Universidad Laica Eloy Alfaro de Manabí, Extensión Chone, depende de una red de comunicación que facilita la gestión académica, administrativa y el acceso a recursos digitales. Sin embargo, esta red está expuesta a múltiples amenazas cibernéticas, como accesos no autorizados e intentos de intrusión, que ponen en riesgo la confidencialidad y la integridad de la información sensible, y la falta de un sistema de detección de intrusos (IDS) eficiente ha aumentado la vulnerabilidad de la universidad, lo que podría derivar en la pérdida de datos, interrupciones de servicios y potenciales daños a la reputación institucional.

El problema se localiza en la red de comunicación de la Universidad Laica Eloy Alfaro de Manabí, Extensión Chone, Provincia de Manabí, Ecuador, la extensión universitaria carece de un sistema robusto para detectar y prevenir intrusiones en su red la cual tiene la necesidad de implementar este tipo de sistemas para mayor seguridad de los que conforman la institución, lo que pone en riesgo la confidencialidad, integridad y disponibilidad de la información. La universidad enfrenta un escenario de vulnerabilidad creciente debido a la falta de un sistema adecuado de detección de intrusos (IDS). Este vacío en la infraestructura de seguridad de la red

podría permitir el acceso no autorizado a datos críticos, comprometiendo la privacidad de estudiantes, profesores y personal administrativo. La ausencia de un monitoreo en tiempo real, junto con el aumento de ciber amenazas en el sector educativo, agrava esta situación.

El origen del problema radica en la creciente dependencia de la universidad en sus redes de comunicación y la falta de medidas proactivas para protegerlas, con la expansión de servicios digitales, el aumento de dispositivos conectados y la falta de actualización de las políticas de seguridad, la red de la universidad se ha convertido en un blanco atractivo para ataques cibernéticos, hasta ahora, no se ha priorizado la implementación de un sistema integral de detección de intrusos en la red de la Uleam extensión Chone. Actualmente, la red de comunicación de la universidad no cuenta con mecanismos suficientes para detectar de manera proactiva intentos de intrusión o accesos no autorizados, esto ha resultado en un ambiente de riesgo donde los ataques cibernéticos pueden pasar desapercibidos , y tener riegos a recibir manipulación y ataques mediante datos o software maliciosos, lo que podría afectar gravemente las operaciones diarias de la universidad de los estudiantes y comprometer la integridad de sus datos.

Formulación del Problema: ¿Cómo puede la Universidad Laica Eloy Alfaro de Manabí, Extensión Chone, implementar un sistema de detección de intrusos (IDS) que permita monitorear, detectar y mitigar los intentos de intrusión en su red de comunicación, ¿garantizando la seguridad y protección de los datos sensibles ante las crecientes amenazas cibernéticas?

1.4. Objetivos

1.4.1. Objetivo General

Implementar un Sistema de Detección de Intrusos (IDS) en la red de comunicación de la Universidad Laica Eloy Alfaro de Manabí, Extensión Chone, para fortalecer la seguridad informática mediante la identificación y mitigación de amenazas que puedan comprometer la integridad, confidencialidad y disponibilidad de la información.

1.4.2. Objetivos Específicos

- Analizar el estado actual de la infraestructura de red de la Universidad Laica Eloy Alfaro de Manabí, Extensión Chone, para identificar vulnerabilidades y riesgos de seguridad.

- Seleccionar las herramientas y tecnologías más adecuadas para la implementación de un Sistema de Detección de Intrusos acorde con las necesidades institucionales.
- Diseñar e implementar un IDS que permita monitorear el tráfico de red y detectar actividades sospechosas o accesos no autorizados.
- Evaluar el funcionamiento y la efectividad del sistema implementado mediante pruebas de detección de amenazas y análisis de resultados.

1.5. Justificación e impactos esperados

Según (Stallings, 2021) la implementación de un sistema de detección de intrusos en la red de comunicación de la Universidad Laica Eloy Alfaro de Manabí, Extensión Chone, es una medida esencial para proteger los datos sensibles y garantizar la seguridad de la infraestructura digital de la institución, en un entorno donde las ciber amenazas son cada vez más sofisticadas, resulta crucial contar con herramientas que permitan identificar ataques en tiempo real y responder de manera rápida y eficaz, un IDS ayudará a prevenir posibles vulneraciones, reduciendo el riesgo de pérdida de datos, interrupción de servicios y daños.

El impacto tecnológico será significativo, según (Vacca, 2021) la implementación de un sistema de detección de intrusos proporcionará a la universidad una infraestructura de seguridad más robusta y avanzada, este sistema permitirá a los administradores de red monitorear continuamente el tráfico de la red, detectar amenazas y mitigar posibles ataques en tiempo real, también se integrarán procedimientos automatizados para la gestión de incidentes, mejorando la eficiencia de la respuesta ante ciber amenazas. Desde el punto de vista social de (Martínez, 2022), el proyecto beneficiará directamente a los estudiantes, profesores y personal administrativo de la universidad, quienes podrán utilizar los servicios en línea y acceder a los recursos digitales de manera segura, el aumentar la protección de los datos personales y académicos.

El impacto ecológico no es directo, la optimización del uso de la infraestructura digital puede generar un impacto positivo al reducir el consumo innecesario de recursos, mediante un sistema de detección de intrusos bien gestionado puede prevenir ataques que podrían comprometer equipos y sistemas, evitando que se tengan que reemplazar o reparar dispositivos afectados por malware u otras amenazas, lo que indirectamente contribuye a un menor consumo de hardware y energía (Marcaibo, . 2009)

CAPITULO II: MARCO TEÓRICO DE LA INVESTIGACIÓN

2.1. Sistemas de Detección de Intrusos (IDS)

La seguridad en las redes de comunicación ha adquirido una importancia significativa en el ámbito académico, empresarial y gubernamental debido al crecimiento constante de las tecnologías de la información y al aumento de las amenazas cibernéticas. Actualmente, las instituciones dependen de redes informáticas para el almacenamiento, procesamiento y transmisión de grandes volúmenes de información, lo que incrementa la necesidad de implementar mecanismos que garanticen la protección de los datos y de la infraestructura tecnológica, en el entorno universitario, donde se gestionan datos académicos, administrativos y personales, resulta indispensable contar con herramientas que permitan prevenir, detectar y responder oportunamente ante posibles incidentes de seguridad.

Los Sistemas de Detección de Intrusos (IDS) constituyen una de las principales soluciones para fortalecer la seguridad de las redes de comunicación, estos sistemas están diseñados para monitorear continuamente el tráfico de red y las actividades que se desarrollan dentro de los sistemas informáticos, con el propósito de identificar comportamientos anómalos, intentos de acceso no autorizados, ataques informáticos y otras acciones que puedan comprometer la integridad, confidencialidad y disponibilidad de la información.

2.1.1. Antecedentes de los IDS

Los antecedentes de los IDS se remontan a la década de 1980, cuando surgió la necesidad de contar con herramientas capaces de detectar actividades sospechosas dentro de los sistemas computacionales, desde entonces, estas tecnologías han evolucionado considerablemente, pasando de mecanismos básicos basados en firmas y reglas predefinidas a soluciones avanzadas que incorporan inteligencia artificial, aprendizaje automático y análisis de comportamiento.

Mediante el monitoreo constante del tráfico de datos y la detección temprana de actividades sospechosas, será posible identificar vulnerabilidades, prevenir accesos no autorizados y proteger los activos tecnológicos de la universidad, de esta manera, los IDS se

convierten en una herramienta fundamental para fortalecer la infraestructura de red y contribuir a la continuidad y confiabilidad de los servicios tecnológicos institucionales. En la cual el autor (Antonio J. M., 2011) en su estudio "Retos y oportunidades en materia de ciberseguridad de América Latina frente (Antonio, 2021) analiza el contexto global de ciber amenazas a la seguridad nacional y política exterior" analiza las deficiencias en el desarrollo de políticas nacionales de ciberseguridad en la región, el estudio destaca la necesidad de construir capacidades para enfrentar las amenazas cibernéticas que afectan la seguridad nacional y la política exterior, concluye que América Latina debe mejorar significativamente en la construcción de una política de ciberseguridad robusta y en la formación de ciber capacidades

El Banco Interamericano de Desarrollo y la Organización de los Estados Americanos (2020) publicaron un reporte detallado sobre las políticas y prácticas de ciberseguridad en América Latina y el Caribe, este informe examina la madurez cibernética de cada país y destaca las brechas en las capacidades de seguridad cibernética, los autores enfatizan la importancia de la ciberseguridad para el crecimiento económico y la sostenibilidad, y proponen políticas para aumentar la resiliencia cibernética en la región (Banco Interamericano de Desarrollo & Organización de los Estados Americanos, 2020)

2.1.2. Análisis de los Ciberataques Realizados en América Latina

Un estudio reciente analiza los ciberataques en América Latina y su impacto en la región. Este análisis proporciona información valiosa sobre las estrategias de defensa que pueden adoptar los países latinoamericanos para protegerse contra delitos cibernéticos, los autores sugieren que la colaboración regional y la inversión en tecnologías avanzadas son cruciales para mejorar la ciberseguridad en América Latina. (Leyva-Méndez A. E., 2021) En cuanto al análisis realizó un análisis exhaustivo de las políticas públicas de seguridad cibernética en Ecuador, en su estudio, destaca la importancia de desarrollar políticas robustas para proteger la infraestructura crítica del país, utilizando una metodología cualitativa basada en la revisión documental, el autor concluye que Ecuador necesita fortalecer sus estrategias de ciberseguridad para enfrentar las amenazas actuales y futuras

En 2011 (Maldonado, 2021) llevó a cabo una revisión sistemática sobre el estado de la ciberseguridad en las empresas del sector público en Ecuador, el estudio identifica las

principales vulnerabilidades y propone soluciones para mejorar la seguridad tecnológica en estas instituciones, el autor (Maldonado, 2021) subraya la necesidad de implementar medidas preventivas para proteger los recursos del estado y la información sensible. Este estudio analiza los ciberataques en organizaciones públicas de Ecuador y sus impactos administrativos, los autores examinan casos específicos de ciberataques y discuten las medidas adoptadas para mitigar estos incidentes en el estudio "Análisis de Políticas Públicas de Seguridad Cibernética en Ecuador" realizado por (Leyva-Méndez A. E., 2021), se obtuvieron varios resultados importantes:

- Deficiencias en la Estrategia Nacional: El estudio identificó que la Estrategia Nacional de Seguridad Cibernética de Ecuador presenta deficiencias significativas en su implementación y alcance. Aunque existen políticas establecidas, su aplicación práctica es limitada debido a la falta de recursos y capacitación adecuada (Leyva-Méndez, 2023)
- Necesidad de Capacitación y Concienciación: Se destacó la necesidad urgente de programas de capacitación y concienciación en ciberseguridad para el personal de las instituciones públicas. La falta de conocimiento y habilidades en ciberseguridad es un obstáculo importante para la protección efectiva de la infraestructura crítica (Leyva-Méndez, 2023)
- Colaboración Internacional: En estudio subrayó la importancia de la colaboración internacional para mejorar la ciberseguridad en Ecuador. La cooperación con otros países y organizaciones internacionales puede proporcionar acceso a mejores prácticas, tecnologías avanzadas y recursos adicionales (Leyva-Méndez, 2021) analiza que estos resultados son un gran avance
- Marco Legal y Normativo: Se identificó la necesidad de actualizar y fortalecer el marco legal y normativo relacionado con la ciberseguridad. (Leyva-Méndez, 2021) sugiere que las leyes actuales no son suficientes para abordar las amenazas cibernéticas modernas y recomienda la creación de nuevas regulaciones específica
- Inversión en Tecnología: El estudio de la investigación donde nos dice ((Leyva-Méndez), 2021) concluye que es crucial aumentar la inversión en tecnologías de ciberseguridad.

2.1.3. Principales amenazas a la seguridad de redes en instituciones educativas

a) Relevancia de la seguridad de redes en entornos universitarios

b) Fundamentos de los sistemas de detección de intrusos (IDS)

c) Tipos de sistemas IDS (basados en firmas, anomalías, etc.)

d) Técnicas y herramientas más utilizadas en la detección de intrusiones

e) Comparación entre IDS y otros mecanismos de seguridad

f) Relación entre los sistemas de detección de intrusos y la seguridad de la red

g) Impacto de los IDS en la protección de redes

h) Integración de IDS con otras medidas de seguridad

i) Casos de estudio en universidades con implementación de IDS

j) Aplicaciones en la red de comunicación de la ULEAM

k) Evaluación de la red actual de la ULEAM, Extensión Chone

l) Descripción de vulnerabilidades presentes

m) Propuesta de un IDS específico para cubrir las necesidades de seguridad

2.1.4. Definiciones conceptuales Variable Independiente: Sistemas de Detección de Intrusos (IDS)

Un Sistema de Detección de Intrusos (IDS) es una solución diseñada para monitorear y analizar el tráfico de red o actividades en un sistema, con el fin de identificar posibles intrusiones, es decir, actividades maliciosas o no autorizadas. Los IDS se clasifican en dos tipos principales:

- IDS basados en red (NIDS): Monitorean el tráfico de red y analizan patrones que puedan indicar intentos de intrusión.
- IDS basados en host (HIDS): Monitorean actividades específicas en un solo sistema, como registros o archivos críticos.

Según el autor en su análisis (García-Teodoro) los IDS desempeñan un papel crucial en la arquitectura de seguridad de cualquier organización, ya sea institución pública o privada, permitiendo la identificación temprana de amenazas y ayudando a mitigar el daño antes de que se produzcan o se incrementen las intrusiones serias. Los primeros IDS surgieron en la década de 1980 como herramientas básicas de monitoreo. Sin embargo, a lo largo de los años, estas tecnologías han evolucionado para incorporar técnicas más avanzadas, como el uso de algoritmos de aprendizaje automático y la inteligencia artificial (AI). Según (Mell S. y., 2007), la evolución de los IDS ha seguido una tendencia hacia una mayor automatización y capacidad de detección proactiva, lo que ha permitido a los IDS modernos adaptarse a nuevas formas de

ataques, como el ransomware y las amenazas persistentes avanzadas (APT)

Hoy en día, los IDS más modernos no solo se limitan a detectar posibles intrusiones, sino que también integran herramientas de respuesta automática a incidentes. Sistemas como Snort y Suricata utilizan firmas predefinidas y heurísticas para identificar comportamientos sospechosos en tiempo real (Roesch, 1999) Además, las tecnologías IDS han comenzado a trabajar en conjunto con los Sistemas de Prevención de Intrusos (IPS), añadiendo una capa adicional de protección frente a amenazas potenciales.

Los avances recientes hechos por (Álvarez, 2020) en este campo integran el uso de Machine Learning Inteligencia Artificial, estas técnicas permiten a los IDS adaptarse y aprender del comportamiento normal de la red, lo que facilita la identificación de amenazas desconocidas o sin firma previa. La combinación de análisis estadístico y modelos de aprendizaje automático ha demostrado ser eficaz para detectar ataques complejos que pueden evadir sistemas tradicionales.

En los entornos académicos, las redes de comunicación son esenciales para la enseñanza, la investigación y la colaboración entre diferentes instituciones, los objetivos atractivos para los atacantes debido a la gran cantidad de información confidencial que manejan, como datos personales de estudiantes y profesores, así como investigaciones no publicadas, de acuerdo con (Alotaibi, 2019) las universidades deben prestar especial atención a la implementación de medidas de seguridad eficaces, incluyendo IDS, para proteger estos recursos críticos.

Un caso interesante es el de la Universidad de California, que sufrió un ataque de ransomware en 2020, comprometiendo una gran cantidad de datos sensibles (Gressin, 2020) En respuesta, la institución mejoró significativamente sus mecanismos de detección de intrusos, incorporando herramientas de detección basadas en comportamiento y monitoreo continuo de sus redes, lo que ayudó a evitar futuros incidentes. Los sistemas de detección de intrusos (IDS) emergieron como respuesta a la creciente necesidad de protección en redes frente a amenazas como accesos no autorizados y ataques cibernéticos.

En entornos académicos, como ULEAM, su implementación ha permitido proteger datos sensibles y mitigar riesgos en tiempo real, ellos destacan (López R. M., 2023) la

importancia del monitoreo constante y la integración de IDS como una medida proactiva para reducir vulnerabilidades en redes internas y externas. Además, su correcta implementación requiere alinearse con estándares internacionales como ISO 27001. De acuerdo al análisis de (Zambrano, 2023) Los componentes de un IDS incluyen sensores que monitorean el tráfico de la red, servidores que analizan los datos recolectados y consolas de administración para gestionar alertas. En ULEAM, estos componentes han sido adaptados para su infraestructura académica, garantizando que los sistemas puedan identificar tanto amenazas conocidas como nuevos patrones de comportamiento sospechoso

2.1.5. Métodos de Detección

Esta implementación sigue lineamientos como los establecidos en la norma ISO 27001 para asegurar la protección de la información:

- Basado en firmas: Compara el tráfico con una base de datos de patrones de ataques ya conocidos.
- Basado en anomalías: Detecta comportamientos no esperados en la red, lo que ayuda a identificar nuevas amenazas.

La investigación en ULEAM de acuerdo a los autores (Coello, 2023) ha adoptado una combinación de estos dos métodos para maximizar la efectividad y minimizar los falsos positivos, utilizando análisis comparativo de tráfico normal y anormal en las redes universitarias, la implementación de un IDS en ULEAM ha requerido un análisis exhaustivo de la infraestructura tecnológica de la universidad. El sistema fue configurado para asegurar que se balancee el rendimiento con la seguridad, y se realizaron capacitaciones al personal sobre el uso adecuado del sistema. Además (Pinargote, 2023), analiza que el monitoreo y las actualizaciones del sistema son constantes para mantenerse al día con las amenazas emergentes.

La seguridad de la red es fundamental para proteger la integridad, confidencialidad y disponibilidad de la información en organizaciones e instituciones, en universidades como ULEAM, la adopción de sistemas de detección de intrusos (IDS) se ha vuelto esencial para prevenir accesos no autorizados y mitigar riesgos. Investigaciones como las de (López R. M., 2023) enfatizan la necesidad de monitoreo constante, implementación de normas ISO 27001 y

el uso de herramientas de detección avanzada para garantizar la protección integral de los recursos digitales.

La seguridad de red basada en Sistemas de Detección de Intrusos (IDS) se enfoca en monitorear y proteger infraestructuras informáticas ante posibles amenazas externas e internas. Los IDS permiten identificar patrones de ataque o comportamientos inusuales dentro de una red, generando alertas para que los administradores puedan actuar rápidamente y minimizar daños. La incorporación de un IDS refuerza la política de seguridad de las instituciones, como la Universidad Laica Eloy Alfaro de Manabí (ULEAM), asegurando el cumplimiento de normativas y evitando accesos no autorizados, nos dice (Asia, 2024)

Estos sistemas se clasifican en dos tipos principales: los NIDS (Network-based Intrusion Detection Systems), que operan a nivel de red, y los HIDS (Host-based Intrusion Detection Systems), que se centran en la actividad de equipos individuales. Los NIDS son esenciales para detectar amenazas como ataques de denegación de servicio, propagación de malware y abusos de protocolos críticos como HTTP o DNS. A través de esta vigilancia continua, los IDS no solo detectan actividad maliciosa, sino que también identifican problemas de configuración que podrían comprometer la seguridad de la red (UOC, 2012)

La gestión eficiente de un IDS requiere una infraestructura complementaria, cuando a los autores (Information Security Asia & UOC, 2024) como firewalls y sistemas de gestión de eventos de seguridad (SIEM), para correlacionar las alertas y reducir la incidencia de falsos positivos. En entornos académicos, como la ULEAM, el uso de herramientas IDS permite prevenir incidentes que comprometan datos críticos o afecten el desempeño de los servicios.

La medición de la seguridad en redes se realiza mediante auditorías que identifican vulnerabilidades y evalúan el cumplimiento de estándares internacionales de acuerdo a lo analizado por (Coello, 2023) Las auditorías comprenden el análisis de tráfico, pruebas de penetración, y la implementación de metodologías como MAGERIT, que permite gestionar riesgos tecnológicos, este proceso garantiza una visión clara de las brechas de seguridad en las infraestructuras digitales.

2.2. Implementación de sistemas de detección de intrusos en redes universitarias

En la investigación actual y el estudio de (López G. y., 2020), se exploró la implementación de un sistema de detección de intrusos (SDI) en la red de una universidad pública en México, enfocándose en la prevención de ataques cibernéticos dirigidos a servicios académicos y administrativos, los autores destacaron la efectividad del sistema basado en Snort para identificar patrones anómalos de tráfico y proteger datos sensibles. Además, el estudio resalta la importancia de capacitar al personal técnico para interpretar las alertas generadas por el sistema.

El uso de IDS tiene un impacto significativo en la seguridad de las redes, ya que mejora la detección temprana de amenazas y minimiza los tiempos de respuesta (Zambrano, 2023) Estos sistemas permiten identificar ataques en tiempo real y tomar medidas inmediatas para mitigar riesgos, lo que fortalece la infraestructura informática y aumenta la confiabilidad del sistema, estos sistemas trabajan bajo dos enfoques principales: basados en firmas (detección de ataques conocidos) y en anomalías (comportamientos no habituales en la red).

Según la investigación de (Mendoza C. , 2022) Los Sistemas de Detección de Intrusos (IDS) desempeñan un papel fundamental en la protección de la infraestructura de red, dado que permiten detectar accesos no autorizados y comportamientos anómalos que podrían comprometer la seguridad del sistema Implementar un IDS contribuye significativamente a la mejora de la seguridad, ya que actúa como una capa adicional de protección más allá de los cortafuegos, identificando amenazas que podrían pasar desapercibidas por otros sistemas de defensa. Los estudios realizados en la ULEAM y otras universidades muestran que la implementación de IDS ha reducido incidentes de seguridad en más de un 40%. Además, investigaciones previas en redes académicas, como las de (Pinargote, 2023), resaltan cómo los IDS permiten monitorear el comportamiento de los usuarios y detectar patrones inusuales de tráfico, mejorando la seguridad general de la red.

2.2.1. Análisis de vulnerabilidades en redes locales

Dentro del análisis realizado por (Ramírez, 2019) realizaron un análisis detallado de vulnerabilidades en la red de una institución educativa de Colombia, empleando herramientas

de escaneo como Nmap y Wireshark. Su investigación identificó debilidades críticas, como configuraciones inseguras y falta de monitoreo continuo, que podrían ser explotadas por atacantes externos. Posteriormente, los autores implementaron un sistema de detección de intrusos híbrido, combinando técnicas de análisis basado en firmas y comportamientos.

2.2.2. Importancia de los Sistemas de Detección de Intrusos en Entornos Universitarios

Las universidades utilizan redes de comunicación para gestionar procesos académicos, administrativos y de investigación, permitiendo el intercambio constante de información entre estudiantes, docentes y personal administrativo. Debido a la gran cantidad de datos que circulan por estas redes, existe un mayor riesgo de sufrir ataques informáticos, accesos no autorizados y otras amenazas que pueden comprometer la seguridad de la información, en este contexto, los Sistemas de Detección de Intrusos (IDS) se han convertido en una herramienta fundamental para la protección de los recursos tecnológicos, ya que permiten monitorear continuamente el tráfico de red e identificar actividades sospechosas que puedan afectar el funcionamiento normal de la infraestructura tecnológica.

La implementación de un IDS en entornos universitarios contribuye a fortalecer la seguridad informática mediante la detección temprana de amenazas y vulnerabilidades. Además, facilita la supervisión de las actividades realizadas dentro de la red, permitiendo a los administradores actuar de manera oportuna ante posibles incidentes de seguridad. De esta forma, las instituciones de educación superior pueden garantizar una mayor protección de la información académica y administrativa, así como la continuidad de los servicios tecnológicos que apoyan los procesos de enseñanza, aprendizaje e investigación.

2.2.3. Beneficios de la Implementación de un IDS en Redes Universitarias

La implementación de un Sistema de Detección de Intrusos en redes universitarias ofrece importantes beneficios para la gestión y protección de la infraestructura tecnológica. Entre ellos destaca la capacidad de identificar accesos no autorizados, detectar comportamientos anómalos y generar alertas sobre posibles amenazas que puedan poner en riesgo la seguridad de la red. Asimismo, estos sistemas permiten recopilar información detallada sobre el tráfico de datos, facilitando el análisis de eventos de seguridad y la

identificación de posibles vulnerabilidades. Beneficio relevante es el fortalecimiento de la confidencialidad, integridad y disponibilidad de la información institucional. Al contar con mecanismos de monitoreo permanente, las universidades pueden reducir el impacto de los ataques cibernéticos y mejorar su capacidad de respuesta ante incidentes de seguridad, en el caso de la Universidad Laica Eloy Alfaro de Manabí, Extensión Chone, la implementación de un IDS permitiría optimizar la protección de los recursos tecnológicos, mejorar el control sobre la red de comunicación y contribuir al desarrollo de un entorno digital más seguro para toda la comunidad universitaria.

Los sistemas de detección de intrusos (IDS, por sus siglas en inglés) constituyen un componente crítico en la arquitectura de ciberseguridad de las redes universitarias, las cuales presentan desafíos operativos únicos debido a su naturaleza intrínsecamente abierta, masiva y heterogénea. A diferencia de las redes corporativas tradicionales que operan bajo perímetros estrictamente controlados, las instituciones de educación superior deben equilibrar la accesibilidad constante y el intercambio libre de información con la protección de datos altamente sensibles, tales como registros académicos, información financiera y propiedad intelectual de investigaciones en curso (Mwangala, 2025). En este entorno, caracterizado por la adopción de políticas de "trae tu propio dispositivo" (BYOD), infraestructuras de nube y fluctuaciones masivas de tráfico concurrente, un IDS actúa como una capa de defensa indispensable. Estos sistemas monitorizan pasiva y continuamente el tráfico de la red para identificar actividades sospechosas, exploraciones de puertos no autorizadas o firmas de malware, permitiendo a los administradores aislar y mitigar amenazas antes de que comprometan la integridad de los servicios educativos (Ring et al., 2019).

Para hacer frente a la creciente sofisticación de los ciberataques en estos ecosistemas académicos, la tecnología subyacente de los IDS ha evolucionado desde arquitecturas puramente basadas en firmas hacia modelos híbridos y de detección de anomalías impulsados por inteligencia artificial. Históricamente, los sistemas tradicionales generaban un alto volumen de falsos positivos en las universidades debido a la legitimidad del tráfico atípico originado por experimentos computacionales o simulaciones de estudiantes e investigadores. La integración contemporánea de algoritmos de aprendizaje automático (Machine Learning) y redes neuronales profundas en los IDS permite establecer una línea base dinámica del comportamiento normal de la red institucional (Fotiadou et al., 2021).

CAPITULO III: DISEÑO METODOLÓGICO

3.1. Tipo de la Investigación

El proyecto "Sistema de detección de intrusos en la red de comunicación de la Universidad Laica Eloy Alfaro de Manabí, Extensión Chone" se clasifica como una investigación aplicada y de nivel descriptivo-explicativo, la investigación es de tipo aplicada porque busca utilizar conocimientos teóricos y prácticos para desarrollar una solución específica: un sistema de detección de intrusos adaptado a las necesidades de la red de comunicación de la universidad. Este enfoque, según (al. H.-S. e., 2018) tiene como propósito resolver problemas concretos mediante el diseño e implementación de soluciones tecnológicas.

La investigación se enmarca como aplicada, ya que se orienta a resolver un problema específico relacionado con la protección de la red institucional mediante la implementación de un SDI, este tipo de estudio no solo identifica vulnerabilidades, sino que propone soluciones prácticas y directas, adaptadas a las características técnicas y operativas de la ULEAM, Extensión Chone, la aplicación de un SDI busca abordar ataques cibernéticos recurrentes, como accesos no autorizados o intentos de accesos maliciosos, demostrando su eficacia en tiempo real, según el autor (Tamayo, 2011) Al centrarse en la solución de problemas concretos, esta investigación busca un impacto inmediato y sostenible en la seguridad informática del entorno universitario.

3.2. Nivel de la Investigación

El proyecto se clasifica en un nivel descriptivo y explicativo, ya que permite describir el estado actual de la red de comunicación de la Universidad Laica Eloy Alfaro de Manabí (ULEAM), Extensión Chone, y detalla cómo las vulnerabilidades presentes afectan su seguridad, además, busca explicar el impacto que tendría la implementación de un sistema de detección de intrusos (SDI) en la mejora de la protección de los datos y servicios institucionales. Este nivel de investigación es clave para comprender tanto las causas como las posibles soluciones a los problemas de seguridad detectados (Mendoza H.-S. &., 2018). Al combinar ambos enfoques, el estudio abarca tanto la identificación de riesgos actuales como la propuesta de una solución basada en tecnología de vanguardia.

3.3. Enfoque de la Investigación

El enfoque de esta investigación es cuantitativo, ya que se centra en la medición y análisis de datos para evaluar la efectividad del sistema de detección de intrusos en la red de la ULEAM. Esto implica la recopilación de métricas como la frecuencia de intentos de acceso no autorizados, la identificación de patrones de tráfico anómalo y la clasificación de los ataques detectados, este enfoque permite obtener resultados objetivos y confiables que apoyen la toma de decisiones respecto a la seguridad de la red (Bernal, 2020), los resultados cuantitativos facilitan la comparación entre el estado de la red antes y después de la implementación del sistema, aportando evidencia sólida sobre los beneficios alcanzados.

3.4. Métodos de la Investigación

En este estudio se emplean los métodos descriptivo y experimental, cada uno con un propósito específico dentro del desarrollo del proyecto, el método descriptivo se utiliza para analizar los ataques y vulnerabilidades existentes en la red, proporcionando un panorama claro de los riesgos actuales, por otro lado, el método experimental permite probar el sistema de detección de intrusos en entornos controlados, verificando su efectividad en escenarios simulados y reales (Lee K. &., 2002) Al combinar ambos métodos, la investigación asegura tanto la comprensión de los problemas actuales como la validación de las soluciones propuestas. Según el autor (Creswell S., 2024) nos dice que este enfoque permite integrar datos numéricos con análisis descriptivo, proporcionando una comprensión más completa del fenómeno estudiado, en cuanto se utilizó el método exploratorio para identificar vulnerabilidades en la red, tal como sugieren (al. G. e., 2018) en estudios sobre seguridad informática.

3.5. Técnicas e Instrumentos de la investigación

Entre las técnicas utilizadas, destaca el uso de simulaciones de ataques para evaluar la capacidad del sistema ante diversas amenazas, como ataques de fuerza bruta o intentos de inyección SQL, además, se realiza un análisis de tráfico de red, que permite identificar patrones de comportamiento malicioso y prevenir posibles intrusiones, finalmente, se aplican encuestas

al personal universitario, enfocadas en medir su percepción de seguridad antes y después de la implementación del sistema (Brown S. &., 2020) estas técnicas no solo contribuyen a validar el sistema, sino que también involucran a los usuarios en el proceso de mejora continua de la seguridad.

El monitoreo de red es una técnica esencial para evaluar el rendimiento y la seguridad de los sistemas informáticos. Según (Wetherall T. y., 2019), este proceso implica observar y registrar el flujo de paquetes de datos en tiempo real para detectar anomalías o fallos en la red, los paquetes de datos, que contienen información sobre los dispositivos conectados y los servicios utilizados, son capturados mediante herramientas especializadas, como Wireshark, que permiten desglosar el tráfico por protocolos, IP y puertos. Este método es especialmente útil para identificar ataques de denegación de servicio (DoS) o accesos no autorizados.

Las entrevistas a expertos son una técnica cualitativa que facilita el entendimiento de problemas complejos de seguridad en redes. De acuerdo con (Poth C. y., 2018) las entrevistas semiestructuradas permiten recopilar información detallada y contextualizada sobre vulnerabilidades específicas, en este caso, los encargados de TI pueden aportar conocimientos sobre brechas en los sistemas, estrategias actuales de mitigación y desafíos recurrentes. Este enfoque asegura una comprensión integral de los riesgos desde la perspectiva operativa y estratégica.

El análisis de tráfico de red se enfoca en monitorear y examinar los paquetes de datos que circulan en la infraestructura para identificar patrones sospechosos o comportamientos anómalos. Herramientas como Wireshark y Zeek pueden ser utilizadas para realizar este tipo de análisis, proporcionando información sobre intentos de intrusión y posibles brechas de seguridad. (Wetherall T. y., 2021) destacan que esta técnica es esencial en la detección de amenazas persistentes avanzadas, ya que permite diferenciar el tráfico legítimo del malicioso. En el caso de la ULEAM, este análisis facilitará la creación de reglas personalizadas para el SDI, mejorando su capacidad de respuesta ante ataques específicos.

Las encuestas dirigidas al personal administrativo y técnico de la universidad permiten medir la percepción de seguridad antes y después de la implementación del SDI. Este enfoque cualitativo busca evaluar si las medidas adoptadas generan confianza en los usuarios y si están alineadas con sus expectativas en términos de protección de la red, de acuerdo a lo que

menciona (Mendoza H.-S. y., 2018) las encuestas son herramientas efectivas para recopilar información sobre el impacto de las soluciones tecnológicas en los usuarios. En este contexto, los resultados obtenidos podrán guiar futuras mejoras, asegurando que el sistema no solo sea técnicamente eficaz, sino también aceptado y respaldado por quienes lo utilizan.

3.6. Procedimientos de la investigación

Los procedimientos inician con un estudio de vulnerabilidades, identificando las principales debilidades en la infraestructura de la red mediante herramientas especializadas. Posteriormente, se lleva a cabo la implementación del sistema de detección de intrusos, seleccionando software como Snort o Suricata para proteger los segmentos más críticos. Luego, se realizan pruebas de efectividad, donde el sistema es evaluado bajo condiciones reales y simuladas para medir su rendimiento y capacidad de detección, nos dice (Wetherall T. &., 2021) Finalmente, se establece un proceso de monitoreo continuo, que permite realizar ajustes y garantizar la sostenibilidad del sistema implementado.

El primer procedimiento consiste en realizar un análisis detallado de las vulnerabilidades presentes en la red de comunicación de la Universidad Laica Eloy Alfaro de Manabí, Extensión Chone, este paso implica el uso de herramientas como Nmap o Nessus para identificar configuraciones inseguras, puertos abiertos, y posibles brechas explotables por atacantes, según (Mell S. y., 2007) un diagnóstico inicial es fundamental para priorizar las áreas críticas que requieren intervención inmediata, este procedimiento sienta las bases para la implementación de medidas correctivas y el diseño del sistema de detección de intrusos, asegurando que se adapte a las necesidades específicas de la red.

Implementación del sistema de detección de intrusos: La implementación del SDI se realiza configurando software especializado, como Snort o Suricata, en los segmentos más vulnerables de la red. Este procedimiento incluye la instalación, personalización de reglas, y configuración de alertas para detectar actividades sospechosas. (Brown S. S., 2020) la correcta implementación de un SDI permite no solo identificar intrusiones en tiempo real, sino también generar registros detallados para análisis posteriores, en el caso de la ULEAM, este procedimiento asegura que el sistema pueda operar en armonía con la infraestructura existente, minimizando interrupciones en los servicios

Pruebas de efectividad: Una vez implementado el SDI, se realizan pruebas para evaluar su desempeño en condiciones reales y simuladas, estas pruebas incluyen simulaciones de ataques cibernéticos, monitoreo de tráfico en tiempo real, y evaluación de falsos positivos y negativos, donde (Wetherall T. y., 2021) afirman que estas pruebas son cruciales para garantizar que el sistema sea capaz de diferenciar el tráfico legítimo del malicioso y responder de manera eficiente.

Monitoreo y evaluación continua: Se establecerá un proceso de monitoreo constante de la red, utilizando las capacidades del SDI para detectar y registrar nuevas amenazas. Este procedimiento incluye la actualización regular de reglas de detección y la capacitación del personal técnico para interpretar los registros generados, según (Bernal, 2020) un monitoreo continuo no solo asegura la eficacia del sistema a largo plazo, sino que también permite anticipar ataques emergentes y proteger la red de manera proactiva.

Herramientas: Wireshark es una herramienta líder en análisis de paquetes, utilizada ampliamente en la gestión y seguridad de redes. Según (Ross K. y., 2021) este software permite visualizar, en tiempo real, la actividad en la red, incluyendo detalles como las cabeceras de los protocolos y el contenido de los paquetes. Su capacidad de filtrar y clasificar información lo convierte en una herramienta invaluable para identificar patrones de comportamiento anómalo, como intentos de intrusión o tráfico inusual. **Snort,** por otro lado, es un sistema de detección de intrusos (IDS) que opera analizando el tráfico de red en busca de actividades sospechosas. (Mell R. y., 2020) destacan su efectividad para implementar reglas de detección personalizadas, que alertan sobre amenazas específicas como intentos de explotación de vulnerabilidades. Su integración con sistemas de análisis lo convierte en un aliado esencial para la protección de redes complejas

3.7. Descripción de la Población y Diseño de la Muestra

La población objeto de estudio está conformada por los usuarios y responsables de la infraestructura tecnológica de la Universidad Laica Eloy Alfaro de Manabí, Extensión Chone, quienes utilizan o administran la red de comunicación institucional. Esta población incluye personal del área de Tecnologías de la Información, autoridades administrativas, docentes y personal que hace uso de los recursos tecnológicos de la institución. Su participación es

fundamental para obtener información relacionada con las condiciones actuales de seguridad de la red, las vulnerabilidades existentes y la necesidad de implementar un Sistema de Detección de Intrusos (IDS).

La población objetivo del estudio está conformada por usuarios de la red de comunicación de la Universidad Laica Eloy Alfaro de Manabí, Extensión Chone. Dentro de este universo se encuentran diferentes segmentos:

- Estudiantes: Son el grupo más numeroso y utilizan la red institucional para acceso a plataformas educativas, recursos digitales y actividades académicas.
- Docentes: Emplean la red para actividades didácticas, entrega de materiales, uso de plataformas virtuales y comunicaciones académicas.
- Personal administrativo: Dependen de la conectividad para procesos administrativos, gestión interna y servicios a la comunidad universitaria.
- Técnicos de TI: Responsables del soporte, mantenimiento y monitoreo de la infraestructura tecnológica institucional.

La población total identificada es de 885 personas, desglosada aproximadamente así: Diseño de la Muestra y Método de Muestreo. Se aplicó un muestreo probabilístico estratificado. Este método asegura que cada grupo o estrato (estudiantes, docentes, administrativos y técnicos de TI) esté representado proporcionalmente en la muestra, reflejando adecuadamente la diversidad de la comunidad universitaria. El tamaño de la muestra fue de 338 personas, determinado utilizando la fórmula para poblaciones finitas, considerando:

- Nivel de confianza: 95%
- Margen de error: 5%
- Proporción máxima de variabilidad: $p = 0.5$; $q = 0.5$

Esta cantidad se seleccionó para asegurar la representatividad estadística de los datos recogidos. En la Distribución Proporcional por Estrato, la muestra de 338 personas se asignó de manera proporcional a cada estrato, según su peso relativo sobre el total de la población:

Tabla 1: Distribución Proporcional de la Muestra por Estrato

Estrato	Población	Participación (%)	Tamaño de la muestra
Estudiantes	800	90.4	306
Docentes	60	6.8	23
Administrativos	20	2.3	8
Técnicos de TI	5	0.5	1
Total	885	100	338

Nota de tabla: Muestra del total de botos en estudiantes y su porcentaje

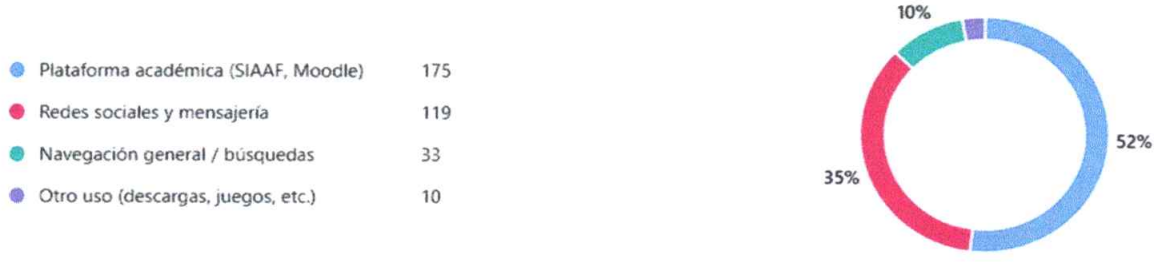
Se tomaron en cuenta que los procedimientos se dieron:

- Dentro de cada estrato, los encuestados se seleccionaron de forma aleatoria.
- Las encuestas y entrevistas se aplicaron tanto en formato presencial como digital, facilitando la participación de todos los grupos considerados.
- Esto asegura que los resultados capturen fielmente la percepción y necesidades respecto al sistema de detección de intrusos y la seguridad digital de la red institucional.

3.8. Análisis y descripción de los resultados

3.8.1. Descripción y Análisis de los resultados de la Encuesta

Ilustración 2: Uso principal al conectarte a la red universitaria.



Nota: Elaborado por Autor del Proyecto

La mayoría de los usuarios (52%) utiliza la red universitaria con fines académicos, lo que confirma su efectividad como herramienta educativa. No obstante, un 48% la emplea para actividades no académicas como redes sociales, búsquedas o entretenimiento. Esto evidencia la necesidad de establecer políticas de uso responsable y mecanismos de control para garantizar un buen rendimiento y priorizar el acceso a recursos académicos. En conjunto, estos datos

resaltan la importancia de establecer mecanismos de gestión y control del tráfico en la red, con el fin de asegurar el rendimiento óptimo de los servicios académicos, al mismo tiempo que se permite un uso equilibrado para otras necesidades.

Ilustración 3: Comportamientos anómalos al usar la red, redirecciones extrañas, bloqueos, avisos sospechosos

Nota: Elaborado por: Los autores del proyecto

El 77% de los encuestados afirma haber notado comportamientos anómalos en la red institucional en alguna ocasión, mientras que un 8% lo ha experimentado con frecuencia. Solo un 15% (sumando "rara vez" y "nunca") afirma no haberlos percibido de forma significativa. Este resultado indica que existen indicios constantes de posibles vulnerabilidades o irregularidades en la red, como redirecciones extrañas, bloqueos o avisos sospechosos. Por ello, es urgente implementar mecanismos de monitoreo, detección de intrusos y fortalecimiento de la seguridad en la red para garantizar su integridad y confianza por parte de los usuarios

Ilustración 4: Formación sobre seguridad o uso seguro de redes en la universidad

Nota: Elaborado por: Los autores del proyecto

El 51% de los encuestados indica haber recibido formación en ciberseguridad solo por su cuenta, mientras que apenas un 11% lo ha hecho de forma académica en varias asignaturas y un 17% de manera puntual. Además, un 20% afirma no haber recibido ninguna formación.

Estos resultados reflejan una falta de formación institucional estructurada en temas de ciberseguridad, lo que representa una debilidad significativa frente a las amenazas digitales. La mayoría de los estudiantes ha tenido que buscar esta formación por iniciativa propia, lo que evidencia la necesidad urgente de incorporar contenidos sobre seguridad digital en la malla curricular y desarrollar programas de capacitación formal para toda la comunidad universitaria

Ilustración 5: Sistema que detecte accesos no autorizados en la red universitaria

Nota: Elaborado por: Los autores del proyecto

Este resultado evidencia una alta conciencia entre los estudiantes sobre la importancia de la ciberseguridad, y refuerza la urgencia de implementar programas formativos en esta área dentro del entorno universitario, la demanda clara por parte de la comunidad estudiantil justifica la inclusión de contenidos de seguridad digital en la malla curricular y en actividades extracurriculares. El 89% de los encuestados considera que es necesario o totalmente necesario recibir formación sobre ciberseguridad en la universidad (63% lo considera necesario y 26% totalmente necesario). Solo un 9% lo considera poco necesario y apenas un 1% lo ve innecesario.

Ilustración 6: Monitoreo del tráfico de red con fines de protección y mejora de la seguridad

Nota: Elaborado por: Los autores del proyecto

El 91% de los encuestados estaría dispuesto a aceptar el monitoreo del tráfico de red con fines de protección y mejora de la seguridad, aunque con ciertas condiciones: un 50% lo acepta solo si se informa previamente, un 41% en parte, y solo un 8% lo acepta totalmente. Apenas un 1% se opone por completo. Estos resultados reflejan una actitud mayoritariamente favorable pero cautelosa frente al monitoreo de red. La aceptación está condicionada a la transparencia y comunicación previa, lo que resalta la importancia de establecer protocolos claros de consentimiento e información al implementar medidas de seguridad digital, esto permitiría proteger la red institucional sin comprometer la confianza ni la privacidad de los usuarios.

Ilustración 7: Proyectos que fortalezcan la seguridad digital en la universidad

Nota: Elaborado por: Los autores del proyecto

El 90% de los encuestados considera que el tema es relevante o muy relevante mostrando que el (62% relevante y 28% muy relevante) y solo un 9% lo ve como poco relevante, y apenas un 1% lo califica de irrelevante. Este resultado evidencia un alto nivel de interés y valoración por parte de los usuarios hacia el tema consultado (presumiblemente relacionado con ciberseguridad, formación o monitoreo de red). La percepción general destaca la importancia de abordar esta temática en la planificación académica e institucional, y justifica su inclusión como prioridad en estrategias educativas, de concienciación y de seguridad en el entorno universitario.

CAPITULO IV: EJECUCIÓN DE LA PROPUESTA

4.1. Descripción del proyecto

El proyecto tiene como objetivo implementar un Sistema de Detección de Intrusos en la red de comunicación de la Universidad Laica Eloy Alfaro de Manabí, extensión Chone. Este sistema permitirá realizar un monitoreo constante y automatizado de todos los dispositivos y usuarios que accedan a la red, identificando patrones de comportamiento anómalos, accesos no autorizados, intentos de vulneración y otras posibles amenazas. La propuesta busca fortalecer la seguridad informática institucional, minimizando riesgos de ataques informáticos, robo de información, o mal uso de los recursos tecnológicos. Además, se documentarán y clasificarán las amenazas detectadas, facilitando una mejor toma de decisiones en el ámbito de la ciberseguridad

4.2. Fases de la propuesta

La ejecución del proyecto se divide en fases secuenciales que permiten estructurar el desarrollo técnico y operativo del sistema de detección de intrusos en la red institucional. Cada fase está diseñada para cumplir con objetivos específicos, desde el diagnóstico inicial hasta la capacitación del personal y la implementación en producción. Según el autor Creswell (2024) sugiere que los proyectos tecnológicos deben seguir una ruta metodológica que combine análisis, diseño, implementación, validación y evaluación, garantizando así una transición lógica y controlada entre las distintas etapas, asimismo, según Poth et al. (2018), los proyectos de seguridad requieren fases de simulación y pruebas controladas que permitan evaluar la efectividad del sistema antes de su puesta en marcha definitiva, esta metodología asegura no solo la viabilidad técnica del IDS, sino también su integración adecuada con la infraestructura de red existente, optimizando recursos y reduciendo el margen de error.

4.2.1. Fase 1: Planificación

Esta fase establece el alcance, los recursos necesarios y el cronograma formal para asegurar la viabilidad del Sistema de Detección de Intrusos (IDS).

1. Objetivo de la fase: Establecer los lineamientos técnicos, administrativos y operativos para la implementación de un Sistema de Detección de Intrusos (IDS) que permita fortalecer la seguridad de la infraestructura de red de la Universidad Laica Eloy Alfaro de Manabí Extensión Chone.

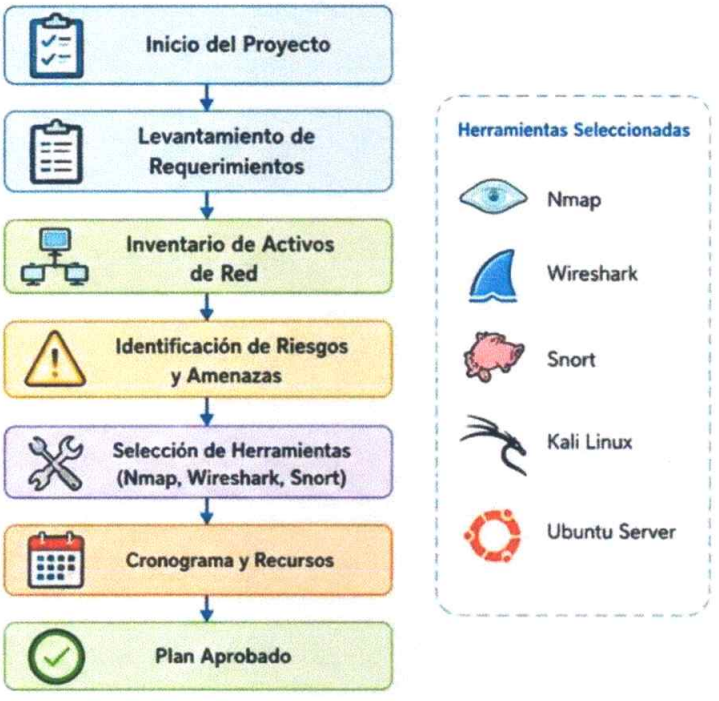
2. Periodo de ejecución: septiembre 2025 – febrero 2026

3. Estándares utilizados:

- ISO/IEC 27001:2022
- ISO/IEC 27002
- NIST Cybersecurity Framework
- NIST SP 800-94
- OWASP Top 10 (referencia para amenazas)

4. Esquema de la fase:

Ilustración 8: Esquema de la fase de proyecto



5. Actividades desarrolladas: Durante este período de cinco meses se definió el alcance del IDS, priorizando los segmentos de red más críticos de la ULEAM Extensión Chone (Servidores de Moodle, Base de Datos Académica y Red Administrativa). Se gestionaron los recursos de hardware (servidores dedicados o entornos virtualizados) y software (evaluación de licencias de código abierto como Snort o Suricata). Se estructuró la matriz de roles y responsabilidades del equipo de TI.

a) Levantamiento de información: Se realizaron reuniones con el personal encargado del área tecnológica para identificar:

- Estructura actual de la red.
- Equipos críticos.
- Servicios institucionales.
- Segmentos de red.
- Vulnerabilidades conocidas.

b) Inventario de activos: Se identificaron:

Tabla 2 Inventario de Activos

Activo	Descripción
Servidor Académico	Sistema de gestión académica
Servidor Administrativo	Gestión financiera
Equipos docentes	Laboratorios
Switches	Distribución de red
Router principal	Conectividad WAN

Elaborado por: Autor del Proyecto

c) Definición de herramientas: Se seleccionaron las siguientes herramientas:

Tabla 3 Definición de herramientas

Herramienta	Función
Nmap	Descubrimiento de hosts y puertos
Wireshark	Captura y análisis de tráfico
Snort	Motor IDS
Kali Linux	Pruebas de seguridad
VirtualBox	Entorno de pruebas

Elaborado por: Autor del Proyecto

d) Entregables:

- Inventario de activos.
- Cronograma.
- Requerimientos funcionales.
- Requerimientos de seguridad.

4.2.2. Fase 2: Análisis de la propuesta

Fase orientada a entender el estado actual del tráfico de red de la universidad y determinar los requerimientos técnicos del sistema.

1. Objetivo: Analizar el estado actual de la red institucional y detectar posibles vulnerabilidades que justifiquen la implementación del IDS.

2. Estándares utilizados:

- NIST SP 800-115
- CVSS v3.1
- CIS Controls

3: Esquema de la fase:

Ilustración 9: Diagnostico Situacional

4. Actividades desarrolladas:

Se realizó un diagnóstico situacional mediante el análisis de la topología de red actual de la extensión.

Se capturaron muestras de tráfico (línea base) para identificar el flujo de datos normal y detectar posibles cuellos de botella, se definieron los requerimientos funcionales (capacidad de alertas en tiempo real, inspección profunda de paquetes) y no funcionales

5. Uso de Nmap: Nmap permitió identificar:

- Hosts activos.
- Puertos abiertos.
- Servicios ejecutándose.
- Sistemas operativos detectados.

Escaneo realizado: nmap -sS -sV -O 192.168.1.0/24

Parámetros:

Tabla 4: Detección del sistema

Parámetro	Descripción
-sS	TCP SYN Scan
-sV	Detección de versiones
-O	Detección de sistema operativo

Resultados obtenidos:

Equipo	IP	Puertos
Servidor Académico	192.168.1.10	80,443,3306
Servidor Administrativo	192.168.1.20	443,3389
Router Principal	192.168.1.1	22,80

Nota: Elaborado por Autor del Proyecto

6. Uso de Wireshark: Se capturó tráfico en diferentes segmentos de red para identificar:

- Protocolos más utilizados.
- Tráfico anómalo.
- Intentos de conexión sospechosos.

Filtros utilizados:

- tcp.port==80
- tcp.port==443
- ip.addr==192.168.1.10

Hallazgos:

- Elevado tráfico HTTP.
- Múltiples intentos de acceso SSH.
- Conexiones repetitivas desde direcciones IP externas.

Vulnerabilidades detectadas:

Tabla 5: Vulnerabilidades de riesgo

Vulnerabilidad	Riesgo
Puertos abiertos innecesarios	Alto
Falta de monitoreo continuo	Alto

Ausencia de IDS	Crítico
Segmentación limitada	Medio

Nota: Elaborado por Autor del Proyecto

4.2.3. Fase 3: Diseño y Construcción

En esta etapa se modela la arquitectura técnica del IDS y se configuran las reglas de detección iniciales.

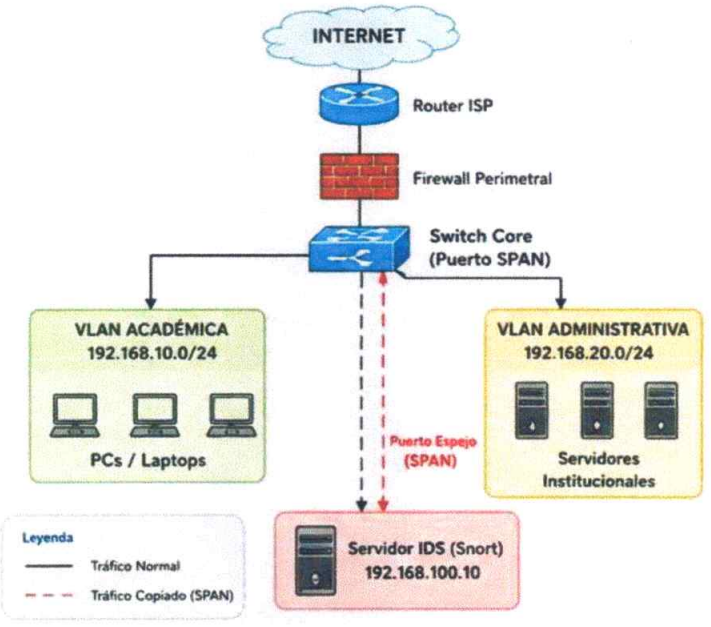
1. Objetivo: Diseñar la arquitectura del IDS e implementar el entorno tecnológico necesario para su funcionamiento.

2. Estándares utilizados:

- NIST SP 800-94
- ISO 27033 (Seguridad en Redes)

3. Diseño de la topología de red: Se propuso una arquitectura basada en un IDS de red (NIDS) utilizando Snort.

Ilustración 10 Diseño de la topología de red



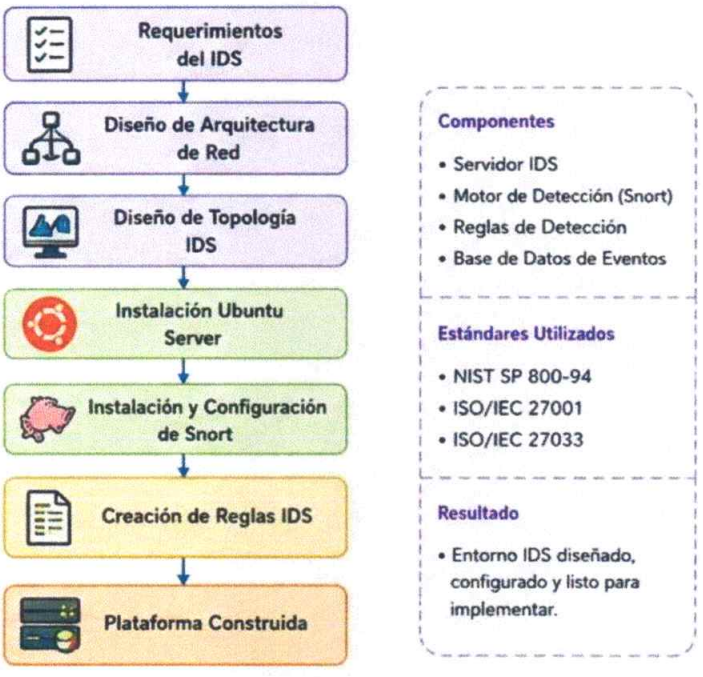
4. Actividades desarrolladas:

Se diseñó la arquitectura lógica del sistema, determinando que el sensor principal se ubicará mediante un puerto espejo (SPAN/Mirror) en el switch central de la universidad para no interrumpir el tráfico.

Se configuró el motor del IDS (por ejemplo, Suricata/Snort) y se construyó el conjunto de reglas personalizadas orientadas a mitigar ataques comunes en entornos educativos (como inyecciones SQL en portales, escaneos de puertos maliciosos o denegación de servicios DoS).

5. Topología propuesta en la fase:

Ilustración 11 Configuración de switch principal



6. Justificación técnica: El IDS se conecta mediante un puerto espejo (SPAN Port) configurado en el switch principal. Las ventajas fueron:

- No afecta el rendimiento.
- Monitoreo pasivo.
- Captura de tráfico en tiempo real.

7. Construcción del entorno

Hardware:

Tabla 6: Especificaciones de Hardware

Recurso	Especificación
CPU	Intel Core i5
RAM	8 GB
Disco	500 GB SSD
NIC	Gigabit Ethernet

Nota: Elaborado por Autor del Proyecto

Sistema Operativo: Ubuntu Server 24.04 LTS

Instalación de Snort:

- sudo apt update
- sudo apt install snort

Configuración inicial:

- sudo nano /etc/snort/snort.conf

Definición de red protegida:

- ipvar HOME_NET 192.168.1.0/24

Reglas implementadas

Detección de escaneo Nmap:

- alert tcp any any -> $HOME_NET any
- (msg:"NMAP Scan Detectado";
- flags:S;
- sid:1000001;)

Detección de intentos SSH:

- alert tcp any any -> $HOME_NET 22
- (msg:"Acceso SSH";
- sid:1000002;)

4.2.4. Fase 4: Implementación

Despliegue físico o virtual del sistema dentro de la infraestructura tecnológica de la ULEAM Chone.

1. Objetivo: Desplegar el IDS dentro de la infraestructura institucional y realizar pruebas de funcionamiento.

2. Actividades desarrolladas: Se instaló el sistema operativo base (por ejemplo, Ubuntu Server) en el hardware seleccionado, procediendo con el despliegue del software IDS y su

consola de gestión (como el entorno Web o la integración con un SIEM tipo Wazuh/ELK). Se activaron las interfaces de red en modo promiscuo para la escucha pasiva del tráfico y se integró el sistema de alertas tempranas vía correo electrónico o canales de comunicación del departamento de TI.

3. Esquema de la fase:

Ilustración 12 Pruebas de funcionamiento

4. Integración con la red: Se configuró el switch principal para replicar todo el tráfico hacia el servidor IDS.

Configuración conceptual SPAN:

Puerto 1-24 ——▶ Puerto 48 (IDS)

5. Pruebas de funcionamiento:

Prueba 1: Escaneo con Nmap

- Desde Kali Linux: nmap -A 192.168.1.10
- Resultado: Snort generó alerta inmediata.

Prueba 2: Fuerza bruta SSH

- Herramienta: hydra
- Resultado: Generación de alertas y Registro del evento.

Alertas generadas:

Tabla 7: Información sobre alertas generales

Evento	Estado
Escaneo de puertos	Detectado
Fuerza bruta SSH	Detectado
Conexiones sospechosas	Detectado

Nota: Elaborado por Autor del Proyecto

4.2.5. Etapa V: Evaluación y Mantenimiento

Verificación del correcto funcionamiento del IDS mediante pruebas de penetración controladas y análisis de falsos positivos.

1. Objetivo: Determinar la efectividad del sistema IDS implementado.

2. Estándares utilizados

- NIST SP 800-94
- ISO 27004
- CIS Controls

3. Esquema de la fase:

Ilustración 13 Criterios de Evaluación

4. Actividades desarrolladas: Se ejecutaron pruebas de intrusión controladas y simuladas (Ethical Hacking básico) desde segmentos externos e internos para verificar si el IDS detectaba y alertaba correctamente las anomalías de acuerdo con las reglas construidas.

Se midió la tasa de falsos positivos y falsos negativos, procediendo a realizar el "tuning" (ajuste fino) de las reglas para asegurar que el sistema sea eficiente y no sature al administrador de red con alertas innecesarias.

5. Indicadores evaluados:

Tabla 8: Indicador de alertas

Indicador	**Fórmula**
Tasa de detección	Alertas detectadas / Ataques realizados
Precisión	Alertas válidas / Total alertas
Falsos positivos	Alertas incorrectas / Total alertas
Disponibilidad	Tiempo activo / Tiempo total

6. Resultados obtenidos:

Indicador	**Resultado**
Detección de escaneos	100%
Detección SSH	95%
Falsos positivos	4%
Disponibilidad	99.5%

Nota: Elaborado por Autor del Proyecto

7. Beneficios obtenidos:

- Monitoreo permanente de la red institucional.
- Detección temprana de amenazas.
- Reducción del riesgo de intrusiones.
- Generación de evidencia para auditorías.
- Mejora de la postura de ciberseguridad institucional.

La implementación del Sistema de Detección de Intrusos basado en Snort permitió establecer un mecanismo de vigilancia continua sobre la infraestructura de red de la Universidad Laica Eloy Alfaro de Manabí Extensión Chone. Las pruebas realizadas mediante Nmap, Wireshark y Kali Linux demostraron que el sistema es capaz de identificar actividades sospechosas, escaneos de red e intentos de acceso no autorizados, proporcionando información

monitoreo en tiempo real expone a la universidad a accesos no autorizados, especialmente en horarios no laborales o en puntos de acceso público como las zonas Wi-Fi.

4.3.1. Recursos Económicos

El recurso económico es un componente estratégico del proyecto, ya que permite costear la adquisición de tecnología, contratación de servicios especializados y capacitación técnica, la sostenibilidad de un sistema de seguridad de red depende en gran medida de una inversión inicial bien planificada y de un presupuesto asignado para mantenimiento y actualización continua.

En base a lo que va a realizar Según (Laudon L. &., (2022)) los proyectos de tecnología en instituciones educativas deben contemplar no solo los gastos de implementación, sino también los asociados a la capacitación del personal y a la renovación tecnológica periódica, el Centro de Estudios de Ciberseguridad de América Latina (BID-OEA, 2020) recomienda destinar fondos para pruebas de penetración y análisis forense, que ayuden a prevenir incidentes cibernéticos antes de que generen daños.

En este sentido, se plantea una inversión razonable que combine la adquisición de equipos robustos con el aprovechamiento de herramientas de software libre, reduciendo costos sin comprometer la calidad del proyecto. También se incluye presupuesto para formación técnica continua, que es esencial para mantener operativo el sistema en el largo plazo.

4.3.2. Recursos Humanos

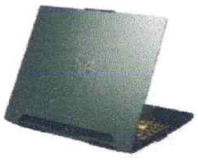
- Director del proyecto: Responsable de supervisar el cumplimiento del cronograma y los objetivos del sistema.
- Ingeniero en Redes: Encargado de diseñar y configurar el IDS dentro de la infraestructura de red actual.
- Especialista en Seguridad Informática: Evalúa amenazas, define políticas de seguridad y analiza los eventos detectados.
- Técnico de soporte: Brinda apoyo en la instalación física, configuración de equipos y pruebas.

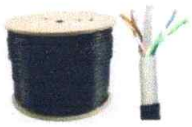
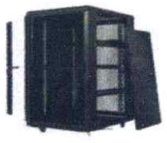
- Pasantes o estudiantes de último nivel: Apoyan en la documentación, pruebas de intrusión controlada y levantamiento de información

4.3.3. Recursos materiales

Los recursos materiales abarcan todos los elementos físicos y digitales necesarios para implementar el sistema de detección de intrusos. Incluyen servidores, switches, routers, computadoras, cableado estructurado, UPS, racks, software especializado como Snort o Wireshark, y manuales técnicos. Estos componentes permiten montar la infraestructura que soporta la recolección y análisis del tráfico de red, la calidad de estos materiales influye directamente en la eficiencia y precisión del sistema. Su correcta selección e instalación aseguran un entorno robusto, escalable y funcional para proteger la red institucional.

Tabla 9: Cuadro de materiales con precios completos

N.º	Material	Cantidad	Precio Unitario (USD)	Costo Total (USD)
1	Servidor de monitoreo (con SSD, 16GB RAM, Xeon) *Servidor de monitoreo (con SSD, 16GB RAM, Xeon)*	1 	1,500	1,500
2	Switch gestionable de 24 puertos (con VLAN y SNMP)	2 	250	500
3	Computadora para análisis y visualización (Core i7)	1 	600	600
4	Router empresarial con firewall integrado	1 	300	300

5	Cableado estructurado (UTP Cat6, rollo de 305m)	1 	150	150
6	Sistema de alimentación ininterrumpida (UPS 1500VA	1 	250	250
7	Rack metálico para equipos de red (22U) *Ilustración 14*	 1	200	200
8	Software IDS (Snort / Suricata - valor de uso estimado*)	1 SURICATA	200	200
9	Software de análisis (Wireshark / Zeek - valor estimado*)	1 Wireshark	150	150
10	Manuales y guías impresas (formato A4, encuadernados)	5 	10	50
	Total, estimado del equipamiento			**3,900**

CAPÍTULO IV: CONCLUSIONES, RECOMENDACIONES, BIBLIOGRAFÍA

5.1. Conclusiones

La identificación de vulnerabilidades en la red de la Universidad Laica Eloy Alfaro de Manabí, Extensión Chone, permitió evidenciar debilidades relacionadas con la seguridad informática, tales como configuraciones inadecuadas, falta de monitoreo continuo y posibles accesos no autorizados que comprometen la información de los docentes. Este diagnóstico inicial permitió determinar la necesidad de implementar mecanismos de protección orientados a fortalecer la seguridad de la red institucional, cumpliendo así con el primer objetivo específico planteado.

El diseño e implementación del sistema de detección de intrusos (IDS), mediante herramientas como Snort y Wireshark, permitió monitorear el tráfico de red en tiempo real, detectar actividades sospechosas y generar alertas frente a posibles intentos de intrusión. La implementación del IDS contribuyó al fortalecimiento de la seguridad de la información de los docentes, permitiendo un mayor control sobre los eventos de red y cumpliendo con el segundo objetivo específico de la investigación.

El desarrollo de una metodología de seguimiento y control continuo permitió evaluar el funcionamiento y efectividad del sistema IDS dentro del entorno tecnológico de la ULEAM Extensión Chone. A través del monitoreo constante, actualización de reglas y análisis periódico de eventos de seguridad, se logró establecer un mecanismo de prevención y respuesta ante nuevas amenazas informáticas. De esta manera, se cumplió el objetivo general de realizar el control y seguimiento del sistema de detección de intrusos para proteger la información institucional.

Finalmente, se concluye que la seguridad informática no depende únicamente de herramientas tecnológicas, sino también de la capacitación y compromiso del personal encargado de administrar la infraestructura de red. La implementación del IDS, acompañada de procesos de formación y concientización, fortalece la cultura de ciberseguridad institucional y mejora la capacidad de respuesta frente a incidentes informáticos.

5.2. Recomendaciones

Se recomienda a la Universidad Laica Eloy Alfaro de Manabí, Extensión Chone, realizar evaluaciones periódicas de vulnerabilidades en la infraestructura de red, con el propósito de identificar nuevas amenazas o debilidades que puedan ser aprovechadas por intrusos. Estas revisiones deben incluir auditorías técnicas, análisis de tráfico y verificación de configuraciones de seguridad en los dispositivos de red.

Es importante mantener actualizado el sistema de detección de intrusos (IDS), incorporando nuevas reglas y firmas de detección que permitan enfrentar amenazas emergentes. Asimismo, se recomienda monitorear constantemente el tráfico de red y generar reportes periódicos que faciliten el seguimiento y control del funcionamiento del sistema implementado.

Se sugiere establecer procedimientos y protocolos de respuesta ante incidentes de seguridad informática, definiendo responsabilidades y acciones específicas para actuar de manera rápida y eficiente frente a posibles accesos no autorizados o ataques cibernéticos que comprometan la información de los docentes y de la institución.

Finalmente, se recomienda fortalecer la capacitación del personal de tecnología y desarrollar programas permanentes de concientización dirigidos a docentes, administrativos y estudiantes sobre buenas prácticas de seguridad informática, esto permitirá reducir riesgos asociados a errores humanos y contribuirá al fortalecimiento de una cultura institucional orientada a la protección de la información y al uso seguro de los recursos tecnológicos.

5.3. Bibliografía

Alotaibi, B. (2019). Cybersecurity challenges in higher education institutions. *International Journal of Advanced Computer Science and Applications, 10*(5), 1–8.

Bernal, C. A. (2020). *Metodología de la investigación: Administración, economía, humanidades y ciencias sociales* (4.ª ed.). Pearson Educación.

Brown, S., & Wilson, T. (2020). Network security monitoring and intrusion detection in academic environments. *Journal of Information Security, 11*(3), 145–158.

Cisco Systems. (2023). *Cisco annual cybersecurity report 2023*. Cisco.

Creswell, J. W., & Creswell, J. D. (2024). *Research design: Qualitative, quantitative, and mixed methods approaches* (6th ed.). SAGE Publications.

Fotiadou, A., Velivassaki, T. H., Vassilakis, V. G., & Logothetis, M. D. (2021). Machine learning techniques for intrusion detection systems. *Future Internet, 13*(5), 1–25.

International Organization for Standardization. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. ISO.

International Organization for Standardization. (2022). *ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls*. ISO.

Lee, W., & Stolfo, S. J. (2000). A framework for constructing features and models for intrusion detection systems. *ACM Transactions on Information and System Security, 3*(4), 227–261.

Mell, P., & Scarfone, K. (2007). *Guide to intrusion detection and prevention systems (IDPS) (NIST Special Publication 800-94)*. National Institute of Standards and Technology.

NIST. (2024). *Cybersecurity framework (CSF) 2.0*. National Institute of Standards and Technology.

Northcutt, S., & Novak, J. (2002). *Network intrusion detection* (3rd ed.). New Riders Publishing.

Poth, C. N. (2018). *Innovation in mixed methods research: A practical guide to integrative thinking with complexity*. SAGE Publications.

Roesch, M. (1999). Snort: Lightweight intrusion detection for networks. In *Proceedings of the 13th USENIX Conference on System Administration (LISA '99)* (pp. 229–238). USENIX Association.

Ross, K. W., Kurose, J. F., & Ross, K. (2021). *Computer networking: A top-down approach* (8th ed.). Pearson.

Scarfone, K., & Mell, P. (2007). Guide to intrusion detection and prevention systems (IDPS). *NIST Special Publication 800-94.*

Singh, A., Sharma, P., & Kumar, R. (2022). Network intrusion detection using machine learning techniques: A survey. *Journal of Network and Computer Applications, 203*, 103376.

Stallings, W. (2021). *Network security essentials: Applications and standards* (7th ed.). Pearson.

Stallings, W. (2023). *Cryptography and network security: Principles and practice* (9th ed.). Pearson.

Suricata. (2024). *Suricata user guide*. Open Information Security Foundation.

Tamayo y Tamayo, M. (2011). *El proceso de la investigación científica* (5.ª ed.). Limusa.

Tanenbaum, A. S., & Wetherall, D. J. (2019). *Computer networks* (6th ed.). Pearson.

Vacca, J. R. (2021). *Computer and information security handbook* (3rd ed.). Elsevier.

Wireshark Foundation. (2024). *Wireshark user guide*. Wireshark Foundation.

Zeek Project. (2024). *Zeek network security monitor documentation*. Zeek Project.

Bace, R. G., & Mell, P. (2001). Intrusion detection systems. *NIST Special Publication 800-31*. National Institute of Standards and Technology.

Bishop, M. (2018). *Computer security: Art and science* (2nd ed.). Addison-Wesley.

Kizza, J. M. (2020). *Guide to computer network security* (6th ed.). Springer.

Kim, D., & Solomon, M. G. (2018). *Fundamentals of information systems security* (3rd ed.). Jones & Bartlett Learning.

Whitman, M. E., & Mattord, H. J. (2022). *Principles of information security* (7th ed.). Cengage Learning.

Organization of American States. (2020). *State of cybersecurity in Latin America and the Caribbean*. OAS.

Banco Interamericano de Desarrollo. (2020). *Ciberseguridad: Riesgos, avances y el camino a seguir en América Latina y el Caribe*. BID.

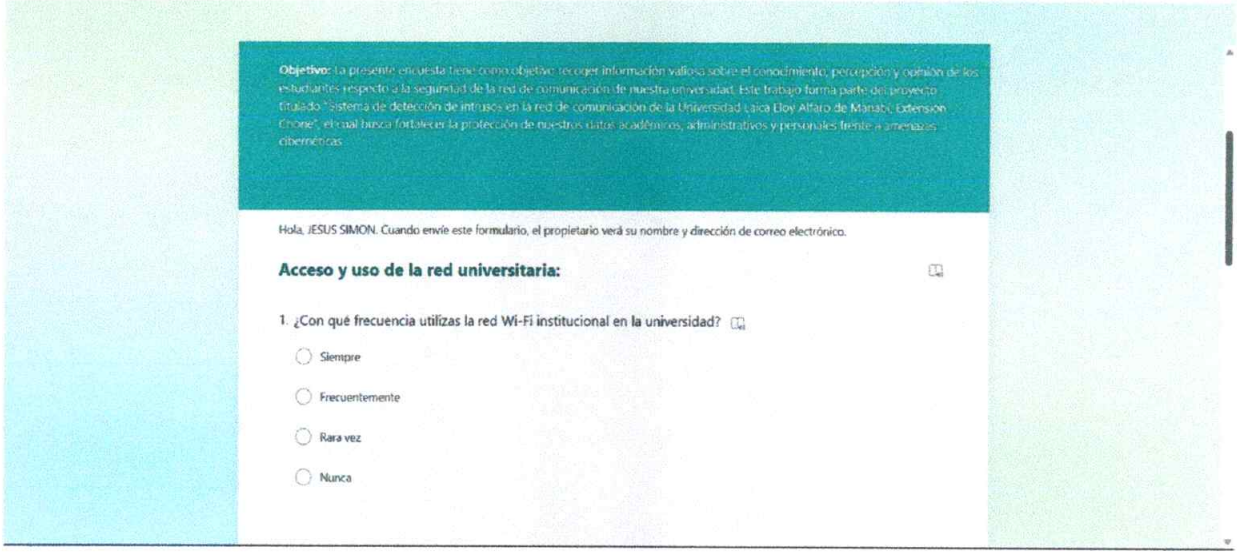
OWASP Foundation. (2024). *OWASP Top 10: The ten most critical web application security risks*. OWASP Foundation.

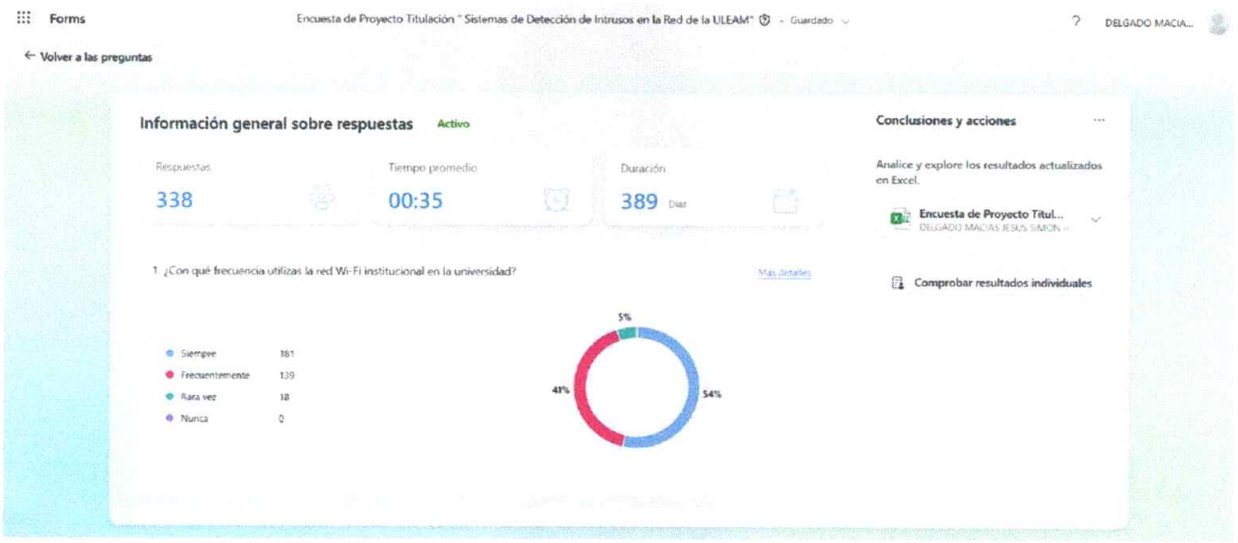
Bejtlich, R. (2013). *The practice of network security monitoring*. No Starch Press.

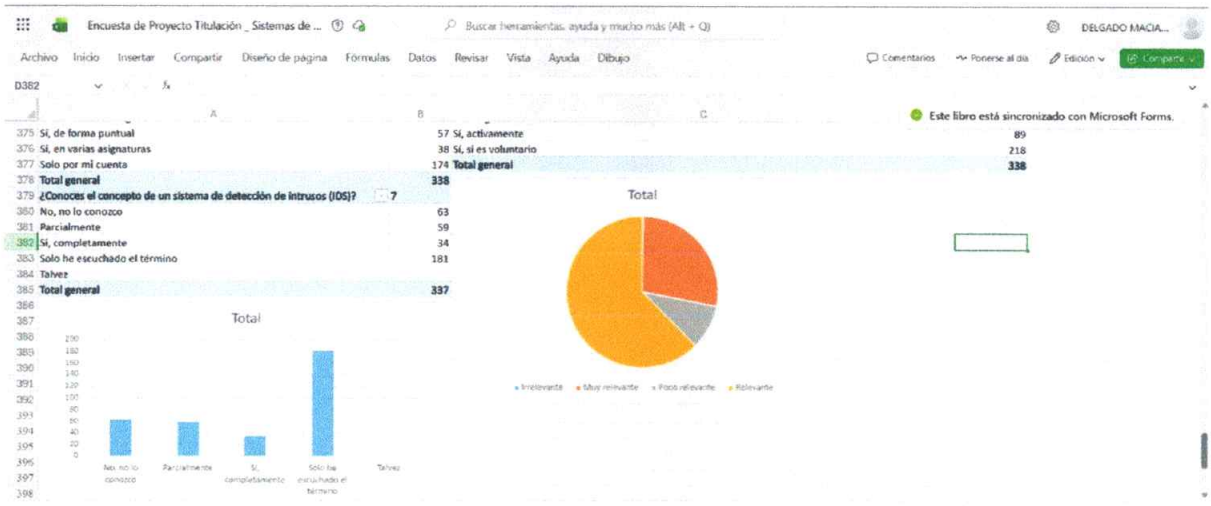
Cheswick, W., Bellovin, S., & Rubin, A. (2014). *Firewalls and internet security: Repelling the wily hacker* (2nd ed.). Addison-Wesley.

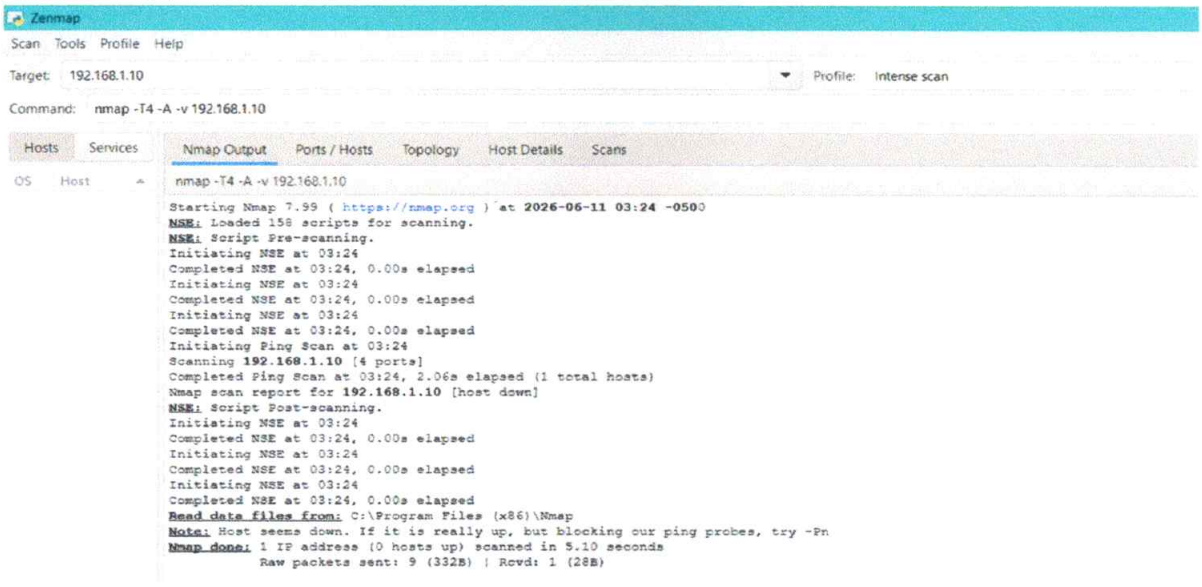
Anexos

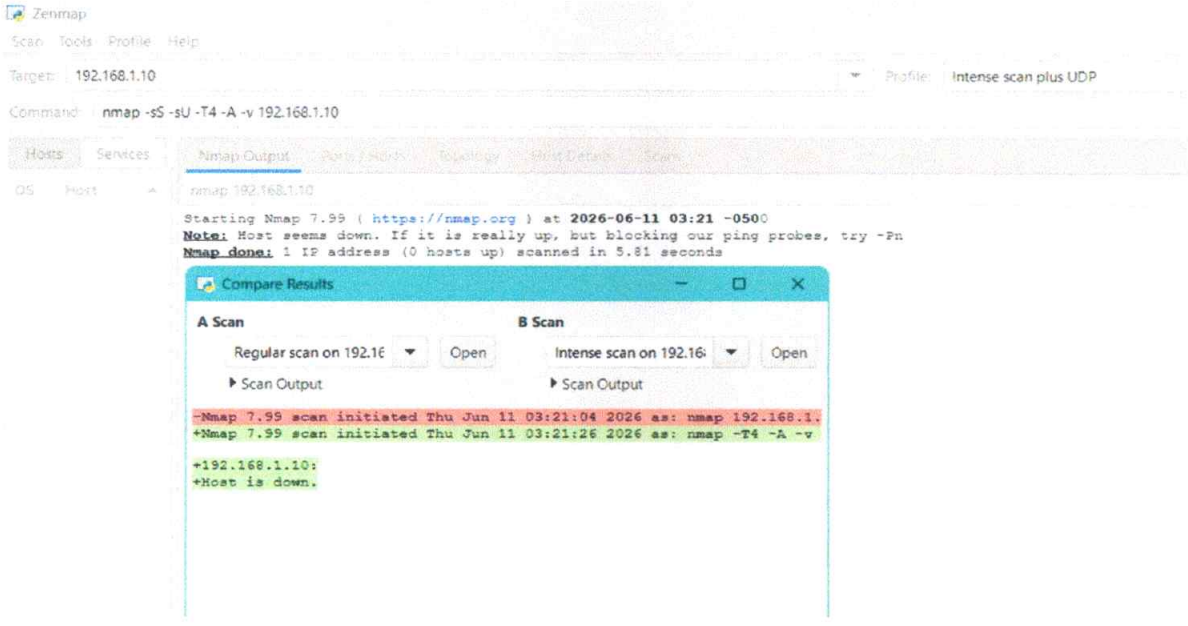

Forms
Encuesta de Proyecto Titulación " Sistemas de Detección de Intrusos en la Red de la ULEAM"
Guardado
DELGADO MACIA...
Estilo
Configuración
Vista previa
Recopilar respuestas
Ver respuestas
338
Presentar
Uleam
Plantillas
Encuesta de Proyecto Titulación " Sistemas de Detección de Intrusos en la Red de la ULEAM"
Esta encuesta esta dirigida a los estudiantes de la ULEAM extensión Chone ,sobre la importancia de los Sistemas de Detección de Intrusos (IDS) en la seguridad informática a través del estudio e implementación de estas tecnologías, se busca fortalecer el conocimiento en ciberseguridad y promover buenas prácticas para proteger los recursos informáticos dentro del entorno universitario.
Objetivo: La presente encuesta tiene como objetivo recoger información valiosa sobre el conocimiento, percepción y opinión de los estudiantes respecto a la seguridad de la red de comunicación de nuestra universidad. Este trabajo forma parte del proyecto titulado "Sistema de detección de intrusos en la red de comunicación de la Universidad Laica Eloy Alfaro de Manabí, Extensión Chone", el cual busca fortalecer la protección de nuestros datos académicos, administrativos y personales frente a amenazas cibernéticas.
Sección 1
Atrás
PC
Móvil

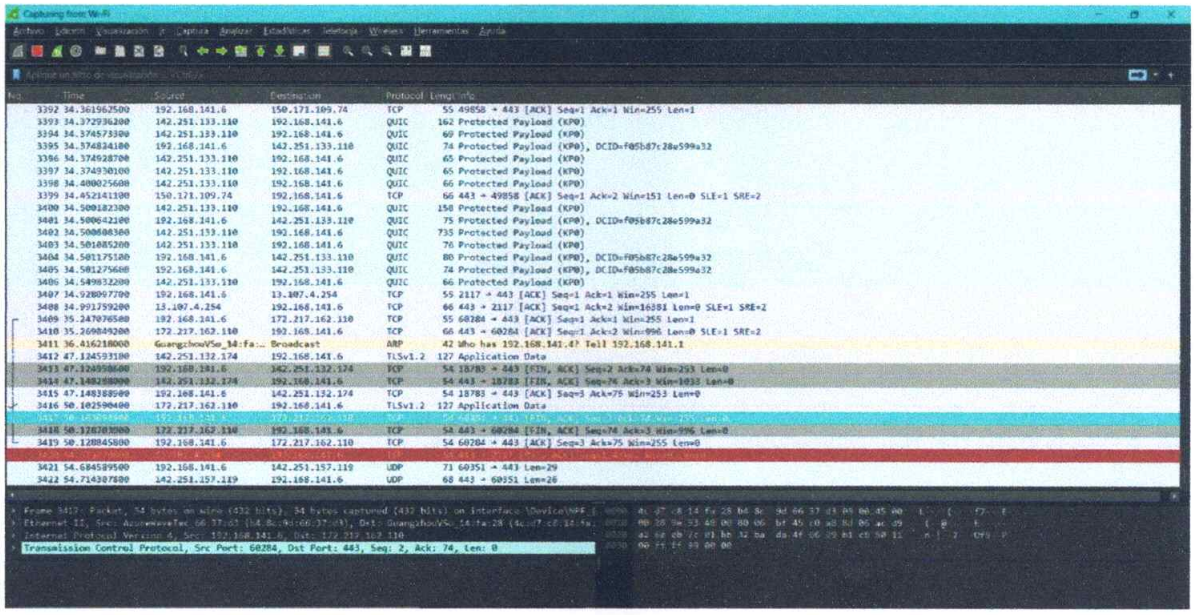

Objetivo: La presente encuesta tiene como objetivo recoger información valiosa sobre el conocimiento, percepción y opinión de los estudiantes respecto a la seguridad de la red de comunicación de nuestra universidad. Este trabajo forma parte del proyecto titulado "Sistema de detección de intrusos en la red de comunicación de la Universidad Laica Eloy Alfaro de Manabí, Extensión Chone", el cual busca fortalecer la protección de nuestros datos académicos, administrativos y personales frente a amenazas cibernéticas.
Hola, JESUS SIMON. Cuando envíe este formulario, el propietario verá su nombre y dirección de correo electrónico.
Acceso y uso de la red universitaria:
1. ¿Con qué frecuencia utilizas la red Wi-Fi institucional en la universidad?
Siempre
Frecuentemente
Rara vez
Nunca

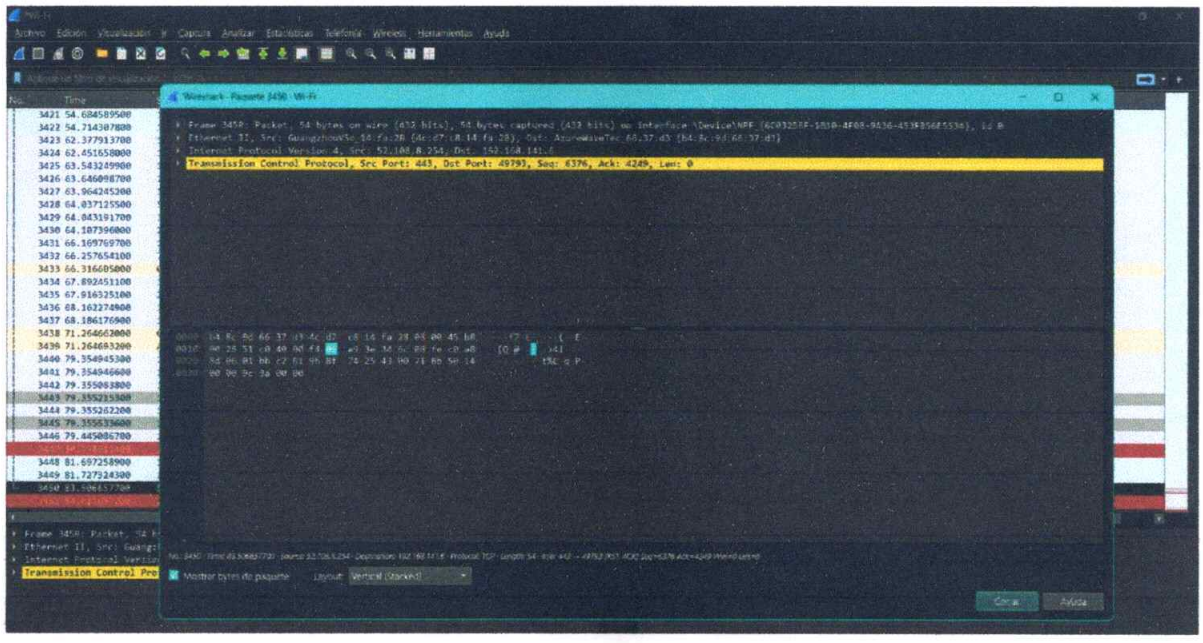

Forms
Encuesta de Proyecto Titulación " Sistemas de Detección de Intrusos en la Red de la ULEAM"
Guardado
DELGADO MACIA...
Volver a las preguntas
Información general sobre respuestas
Activo
Respuestas
338
Tiempo promedio
00:35
Duración
389 Días
Conclusiones y acciones
Analice y explore los resultados actualizados en Excel.
Encuesta de Proyecto Titul...
DELGADO MACIAS JESUS SIMON
Comprobar resultados individuales
1. ¿Con qué frecuencia utilizas la red Wi-Fi institucional en la universidad?
Más detalles
Siempre 161
Frecuentemente 139
Rara vez 18
Nunca 0
5%
41%
54%


Encuesta de Proyecto Titulación _ Sistemas de ...
Archivo Inicio Insertar Compartir Diseño de página Fórmulas Datos Revisar Vista Ayuda Dibujo
Este libro está sincronizado con Microsoft Forms.
Total
Total


Zenmap
Scan Tools Profile Help
Target: 192.168.1.10
Profile: Intense scan
Command: nmap -T4 -A -v 192.168.1.10
Hosts Services
Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
nmap -T4 -A -v 192.168.1.10
Starting Nmap 7.99 (https://nmap.org) at 2026-06-11 03:24 -0500
NSE: Loaded 158 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 03:24
Completed NSE at 03:24, 0.00s elapsed
Initiating NSE at 03:24
Completed NSE at 03:24, 0.00s elapsed
Initiating NSE at 03:24
Completed NSE at 03:24, 0.00s elapsed
Initiating Ping Scan at 03:24
Scanning 192.168.1.10 [4 ports]
Completed Ping Scan at 03:24, 2.06s elapsed (1 total hosts)
Nmap scan report for 192.168.1.10 [host down]
NSE: Script Post-scanning.
Initiating NSE at 03:24
Completed NSE at 03:24, 0.00s elapsed
Initiating NSE at 03:24
Completed NSE at 03:24, 0.00s elapsed
Initiating NSE at 03:24
Completed NSE at 03:24, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 5.10 seconds
Raw packets sent: 9 (332B) | Rcvd: 1 (28B)


Zenmap
Target: 192.168.1.10
Profile: Intense scan plus UDP
Command: nmap -sS -sU -T4 -A -v 192.168.1.10
Starting Nmap 7.99 (https://nmap.org) at 2026-06-11 03:21 -0500
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 5.81 seconds
Compare Results
A Scan
B Scan
Regular scan on 192.16
Intense scan on 192.16
Open
Scan Output
-Nmap 7.99 scan initiated Thu Jun 11 03:21:04 2026 as: nmap 192.168.1.
+Nmap 7.99 scan initiated Thu Jun 11 03:21:26 2026 as: nmap -T4 -A -v
+192.168.1.10:
+Host is down.





1. ¿Con qué frecuencia utilizas la red Wi-Fi institucional en la universidad?

- ◯ Siempre
- ◯ Frecuentemente
- ◯ Rara vez
- ◯ Nunca

2. ¿Cuál es tu uso principal al conectarte a la red universitaria?

- ◯ Plataforma académica (SIAAF, Moodle)
- ◯ Redes sociales y mensajería
- ◯ Navegación general / búsquedas
- ◯ Otro uso (descargas, juegos, etc.)

3. ¿Con qué frecuencia experimentas lentitud o desconexiones en la red institucional?

- ◯ Muy frecuente
- ◯ Ocasional
- ◯ Rara vez
- ◯ Nunca

4. ¿Has notado comportamientos anómalos al usar la red institucional (ej. redirecciones extrañas, bloqueos, avisos sospechosos)?

- ◯ Sí, muchas veces
- ◯ Algunas veces
- ◯ Rara vez
- ◯ Nunca

Conocimientos sobre seguridad en redes

5. ¿Qué nivel de conocimiento tienes sobre seguridad en redes?

- ◯ Alto
- ◯ Medio
- ◯ Bajo
- ◯ Nulo

6. ¿Has recibido formación sobre ciberseguridad o uso seguro de redes en la universidad?

- ◯ Sí, en varias asignaturas
- ◯ Sí, de forma puntual
- ◯ Solo por mi cuenta
- ◯ No he recibido ninguna

7. ¿Conoces el concepto de un sistema de detección de intrusos (IDS)?

- ◯ Sí, completamente
- ◯ Parcialmente
- ◯ Solo he escuchado el término
- ◯ No, no lo conozco

Opinión sobre la seguridad de la red institucional

8. ¿Consideras que la red de la ULEAM Extensión Chone es segura actualmente?

- Sí, es muy segura
- Algo segura
- Poco segura
- Nada segura

9. ¿Crees necesario implementar un sistema que detecte accesos no autorizados en la red universitaria?

- Totalmente necesario
- Necesario
- Poco necesario
- Innecesario

Lector inmersivo

10. ¿Aceptarías el monitoreo del tráfico de red con fines de protección y mejora de la seguridad?

- Sí, totalmente
- En parte
- Solo si se informa previamente
- No

Opinión adicional sobre la propuesta

11. ¿Te sientes expuesto a riesgos de ciberataques al usar la red institucional? *

- Sí, constantemente
- Algunas veces
- Rara vez
- No me siento en riesgo

12. ¿Te parece relevante que los estudiantes participen en proyectos que fortalezcan la seguridad digital en la universidad? *

- Muy relevante
- Relevante
- Poco relevante
- Irrelevante

13. ¿Estarías dispuesto a apoyar iniciativas tecnológicas estudiantiles relacionadas con ciberseguridad? *

- Sí, activamente
- Sí, si es voluntario
- No tengo interés
- No