Seminario de Investigación — Entrega Final

«Diseño e implementación de un sistema inteligente de detección de intrusiones para el monitoreo y análisis de amenazas en redes locales»

Autores:
Lina María Sánchez Mina
Erick Javier Castro Sánchez
Luis Ernesto Bogota Guzman

Universidad EAN
Facultad de Ingeniería
Especialización en Gerencia en Ciberseguridad
Seminario de Investigación
Docente: Ricardo Andres Villalba Rivera
Bogotá D.C., Colombia — 2026

RESUMEN

Colombia registró 36 mil millones de intentos de ciberataques durante los primeros once meses de 2024, posicionándose como el cuarto país con más ataques en América Latina (ERC Colombia, 2024; ACIS, 2025). En este contexto, las redes de área local (LAN) de instituciones educativas y organizaciones de pequeña y mediana escala representan objetivos vulnerables, pues frecuentemente carecen de mecanismos especializados de monitoreo y detección temprana de intrusiones.

El presente estudio evalúa la efectividad del sistema de detección de intrusiones (IDS) implementado con la herramienta de código abierto Snort 3.x en la identificación y generación de alertas ante ataques informáticos simulados —escaneo de puertos, fuerza bruta, denegación de servicio (DoS) y propagación de malware— en la red local de laboratorio de la Universidad EAN durante el primer semestre de 2026. La investigación adopta un diseño cuasiexperimental con enfoque mixto de predominancia cuantitativa y alcance explicativo-evaluativo.

La metodología combina la medición de tres indicadores cuantitativos —tasa de detección (TD%), tasa de falsos positivos (TFP%) y tiempo medio de detección (TMD en segundos)— con análisis cualitativo complementario de los registros de logs y evaluación del cumplimiento del estándar NIST SP 800-94. La muestra comprende N = 1.200 eventos de ataque distribuidos en cuatro categorías (300 por tipo) más 300 eventos de tráfico legítimo de referencia, calculados con la fórmula de Cochran (1977) con nivel de confianza del 95% y margen de error del 5%.

Se espera demostrar que Snort 3.x alcanza una tasa de detección global ≥ 75%, con TFP < 15% y cumplimiento de al menos el 70% de los controles NIST SP 800-94, contribuyendo a fortalecer los mecanismos de protección en infraestructuras tecnológicas de pequeña escala.

Palabras clave: ciberseguridad, detección de intrusiones, Snort 3.x, redes LAN, tasa de detección, falsos positivos, NIST SP 800-94, diseño cuasiexperimental, Colombia.

ABSTRACT

Colombia recorded 36 billion cyberattack attempts in the first eleven months of 2024, ranking fourth in Latin America for cyber incidents (ERC Colombia, 2024). Local area networks (LANs) in educational institutions and small-to-medium organizations remain particularly vulnerable, as they frequently lack specialized monitoring and intrusion detection mechanisms.

This study evaluates the effectiveness of the open-source intrusion detection system (IDS) Snort 3.x in identifying and generating alerts against simulated cyberattacks —port scanning, brute force, denial of service (DoS), and malware propagation— within the laboratory LAN at Universidad EAN during the first semester of 2026. The research employs a quasi-experimental design with a mixed-methods approach (quantitative predominant) and an explanatory-evaluative scope.

Three quantitative indicators are measured: detection rate (DR%), false positive rate (FPR%), and mean time to detect (MTTD). A qualitative component complements the study through log analysis and NIST SP 800-94 compliance evaluation. The sample comprises N = 1,500 events (300 per attack type × 4 + 300 baseline), calculated using Cochran's formula (1977) at 95% confidence.

Keywords: cybersecurity, intrusion detection, Snort 3.x, LAN networks, detection rate, false positives, NIST SP 800-94, quasi-experimental design, Colombia.

INTRODUCCIÓN

El vertiginoso avance de las tecnologías de la información y la comunicación ha transformado la manera en que las organizaciones gestionan sus procesos, servicios y recursos digitales. Las redes de área local (LAN) constituyen hoy la columna vertebral de la operación tecnológica en instituciones educativas, empresas y entidades públicas de todo el mundo. Sin embargo, esta dependencia creciente de las infraestructuras de red también ha ampliado la superficie de ataque disponible para actores maliciosos, quienes explotan vulnerabilidades técnicas y humanas para comprometer la confidencialidad, integridad y disponibilidad de la información —la denominada triada CIA (Stallings, 2018).

En Colombia, el escenario es especialmente preocupante: durante los primeros once meses de 2024 se registraron 36 mil millones de intentos de ciberataques, consolidando al país como el cuarto más afectado en América Latina (ERC Colombia, 2024; ACIS, 2025). Colombia enfrenta una creciente amenaza digital que exige invertir en estrategias robustas de ciberseguridad para proteger a las organizaciones. Adicionalmente, las pérdidas promedio por brecha de seguridad superan 1,1 millones de dólares según el IBM Cost of a Data Breach Report 2024, y el 74% de las brechas involucran credenciales comprometidas, según el Verizon DBIR 2024. Esta realidad obliga a instituciones de todos los tamaños —incluidas las educativas— a fortalecer sus capacidades de detección y respuesta.

En este contexto, los Sistemas de Detección de Intrusiones (IDS) representan una de las herramientas más eficientes y accesibles para monitorear el tráfico de red en tiempo real e identificar comportamientos maliciosos antes de que causen daño significativo (Scarfone & Mell, 2007). Snort, desarrollado originalmente por Roesch (1999) y mantenido actualmente por Cisco Talos en su versión 3.x con un nuevo motor de detección basado en aprendizaje automático (Cisco Snort Blog, 2024), es el IDS de código abierto más ampliamente adoptado en entornos académicos, corporativos y gubernamentales a nivel mundial. Snort ha sido modificado y mejorado en numerosas ocasiones desde su creación, expandiendo sus funcionalidades hasta convertirse en uno de los sistemas de detección de intrusiones más exitosos disponibles, utilizado por innumerables personas, empresas y la mayoría de las agencias gubernamentales.

A pesar de su disponibilidad, muchas organizaciones de pequeña escala e instituciones educativas en Colombia aún no han implementado mecanismos formales de monitoreo de red. La falta de parches de seguridad oportunos, configuraciones inadecuadas y la ausencia de monitoreo continuo facilitan intrusiones que pueden pasar desapercibidas durante meses mientras los atacantes extraen información valiosa o preparan ataques más devastadores. Esta brecha entre la amenaza real y las capacidades defensivas instaladas constituye el problema central que motiva la presente investigación.

La investigación evalúa sistemáticamente la efectividad de Snort 3.x mediante un experimento controlado en el laboratorio de redes de la Universidad EAN, simulando cuatro tipos de ataques representativos de las amenazas más frecuentes en redes LAN: escaneo de puertos (Nmap), fuerza bruta sobre SSH/HTTP (Hydra), denegación de servicio —DoS— (hping3) y propagación de malware simulado (Metasploit Framework). Los resultados se contrastarán con los parámetros del estándar NIST SP 800-94, aportando evidencia empírica sobre la capacidad defensiva de soluciones de bajo costo para organizaciones con recursos tecnológicos limitados.

PLANTEAMIENTO DEL PROBLEMA

Las organizaciones modernas dependen de manera creciente de las redes de área local para ejecutar sus operaciones administrativas, académicas y de servicio. Esta dependencia genera una exposición constante a amenazas informáticas cuya sofisticación aumenta año tras año. Según Stallings (2018), las redes LAN son vulnerables a múltiples vectores de ataque, entre los que se destacan el escaneo de puertos, los ataques de fuerza bruta, el acceso no autorizado, la propagación de malware y los ataques de denegación de servicio. El NIST señala que gran parte de estas organizaciones carece de mecanismos adecuados para monitorear su tráfico de red y detectar actividades maliciosas en tiempo real (Scarfone & Mell, 2007).

En el contexto colombiano, esta problemática adquiere una dimensión crítica. El Centro de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT) identificó 22.086 vulnerabilidades en 2024, lo que muestra un volumen inmenso de riesgos con consecuencias potencialmente graves para las organizaciones. El diagnóstico de ERC Colombia revela que este incremento exponencial responde a una combinación de bajo presupuesto en ciberseguridad, falta de formación del personal, sistemas desactualizados y una digitalización acelerada que ha superado la preparación técnica de muchas organizaciones (ERC Colombia, 2024). Para el primer semestre de 2026, se prevé la intensificación de ataques dirigidos contra infraestructura crítica mediante el uso de inteligencia artificial generativa, afectando especialmente los sectores de salud, educación y gobierno (MobileTime, 2026).

En este escenario, las instituciones educativas ocupan una posición de particular vulnerabilidad: sus redes LAN conectan decenas o cientos de dispositivos de usuarios con diferentes perfiles de conocimiento en seguridad, gestionan información sensible de estudiantes y personal, y frecuentemente operan con presupuestos de TI reducidos que no contemplan soluciones de seguridad propietarias. La ausencia de sistemas IDS en estas redes permite que los ataques pasen desapercibidos durante periodos prolongados, con consecuencias que incluyen pérdida de información, interrupción de servicios académicos y compromisos en la privacidad de datos personales regulada por la Ley 1581 de 2012.

Ante este escenario, resulta pertinente investigar en qué medida la implementación de un IDS basado en Snort 3.x puede mejorar la capacidad de detección de ataques informáticos en una

red LAN institucional, evaluando su efectividad mediante indicadores cuantitativos verificables y comparando los resultados con el estándar internacional de referencia para sistemas IDS/IPS: el NIST SP 800-94 (Scarfone & Mell, 2007).

PREGUNTA DE INVESTIGACIÓN E HIPÓTESIS

Pregunta de Investigación

¿En qué medida la implementación de un sistema de detección de intrusiones basado en Snort 3.x mejora la identificación y el monitoreo de ataques informáticos simulados dentro de una red local de laboratorio, en términos de tasa de detección, tasa de falsos positivos y tiempo medio de detección, según los criterios del estándar NIST SP 800-94?

Hipótesis General (HG)

HG: La implementación del sistema IDS Snort 3.x con reglas personalizadas en la red LAN de laboratorio de la Universidad EAN logrará, durante el primer semestre de 2026:

(a) una tasa de detección (TD%) global ≥ 75% ante los cuatro tipos de ataque simulados;

(b) una tasa de falsos positivos (TFP%) < 15% sobre el total de alertas generadas; y

(c) un índice de cumplimiento del estándar NIST SP 800-94 ≥ 70%.

Hipótesis Específicas

#	Hipótesis Específica	OE Asociado	Indicador de Verificación
HE1	Los ataques de escaneo de puertos serán detectados con TD ≥ 85%, dado que Snort dispone de firmas ampliamente documentadas para patrones Nmap (Beale, Baker & Caswell, 2015).	OE2–OE3	TD escaneo puertos (%)
HE2	La tasa de falsos positivos del sistema IDS configurado será inferior al 15%, mediante el ajuste de umbrales y la personalización de reglas.	OE3	TFP = alertas FP / total alertas × 100
HE3	El IDS implementado cumplirá al menos el 70% de los controles de detección especificados en el NIST SP 800-94 para sistemas NIDS.	OE4	% cumplimiento NIST SP 800-94

1. OBJETIVO GENERAL Y OBJETIVOS ESPECÍFICOS

Objetivo General

Evaluar la efectividad del sistema de detección de intrusiones (IDS) implementado con la herramienta Snort 3.x —como variable independiente— en la identificación y generación de alertas ante ataques informáticos simulados —como variable dependiente— en la red local de laboratorio de la Universidad EAN, durante el primer semestre de 2026, para determinar su capacidad de protección frente a los cuatro tipos de ataque más frecuentes en redes LAN institucionales en Colombia.

Análisis de los elementos del Objetivo General

Elemento requerido (Hernández-Sampieri, 2018)	Contenido en el OG
Verbo en infinitivo — nivel cognitivo alto (Bloom)	EVALUAR — nivel 5 de la taxonomía revisada (Anderson & Krathwohl, 2001): emitir juicio fundamentado en criterios y evidencia empírica
Fenómeno concreto de estudio	Sistema IDS implementado con Snort 3.x en entorno de laboratorio LAN
Variable Independiente (VI)	Implementación del IDS Snort 3.x (configuración, reglas personalizadas, cobertura de amenazas)
Variable Dependiente (VD)	Capacidad de detección: TD%, TFP%, TMD en segundos; cumplimiento NIST SP 800-94
Unidad de análisis	Red local de laboratorio de la Universidad EAN (eventos de tráfico y alertas IDS)
Alcance temporal	Primer semestre de 2026 (febrero–mayo 2026)
Alcance espacial	Laboratorio de Redes — Facultad de Ingeniería — Universidad EAN, Bogotá D.C.

Objetivos Específicos

OE	Enunciado	Verbo Bloom	Nivel	Indicador verificable	Técnica anticipada
OE1	Identificar y clasificar los principales tipos de ataques informáticos que afectan las redes LAN institucionales —escaneo de puertos, fuerza bruta, denegación de servicio y propagación de malware— mediante	IDENTIFICAR / CLASIFICAR	Recordar-Comprender (Bloom N.°1-2)	Matriz taxonómica con ≥ 8 ataques clasificados por tipo, vector, protocolo afectado e impacto CIA	Revisión documental sistemática (Scopus, IEEE Xplore, ACM DL, 2015–2026)

OE	Enunciado	Verbo Bloom	Nivel	Indicador verificable	Técnica anticipada
	revisión documental sistemática de la literatura científica especializada en ciberseguridad (2015-2026).				
OE2	Implementar el sistema IDS Snort 3.x con reglas de detección personalizadas para los cuatro tipos de ataque identificados en OE1, en un entorno de red local controlado y documentado con topología definida, verificando la cobertura de reglas activas.	IMPLEMENTAR	Aplicar (Bloom N.°3)	Índice de cobertura = N° reglas activas / N° tipos de ataque × 100% (meta: 100%)	Experimento controlado en laboratorio (implementación técnica documentada)
OE3	Analizar el desempeño del IDS implementado mediante la ejecución de 1.200 escenarios de ataque controlado, calculando la tasa de detección (TD%), la tasa de falsos positivos (TFP%) y el tiempo medio de detección (TMD) para cada tipo de amenaza simulada.	ANALIZAR	Analizar (Bloom N.°4)	TD%, TFP% y TMD por tipo de ataque; comparación entre categorías mediante ANOVA de un factor	Observación técnica estructurada + análisis automático de logs Snort + captura Wireshark
OE4	Evaluar la efectividad global del sistema IDS Snort 3.x comparando el Índice de Efectividad Global (IEG) obtenido con los parámetros de referencia del estándar NIST SP 800-94, e identificar oportunidades de mejora en la configuración de reglas.	EVALUAR	Evaluar (Bloom N.°5)	IEG = TD% promedio − TFP%; % cumplimiento NIST SP 800-94; N° recomendaciones documentadas	Análisis comparativo con estándar NIST + lista de cotejo + análisis de logs (componente cualitativo)

2. DISEÑO METODOLÓGICO

2.1 Paradigma y Enfoque

La investigación se inscribe en el paradigma pragmático (Creswell & Creswell, 2018), que permite combinar métodos cuantitativos y cualitativos según la naturaleza del problema, sin compromisos ontológicos rígidos. Esta elección se justifica desde dos perspectivas:

Desde la perspectiva epistemológica, el problema investigado requiere medir objetivamente el comportamiento de un sistema tecnológico (positivismo) —cuántas alertas genera, con qué precisión y en qué tiempo— pero también interpretar cualitativamente los patrones de los registros de eventos y evaluar el cumplimiento normativo (constructivismo). Ningún paradigma único resulta suficiente.

Desde la naturaleza de las variables, la Variable Independiente —configuración del IDS Snort 3.x— es manipulable y sus efectos sobre la Variable Dependiente —capacidad de detección— son medibles con escalas de razón (TD%, TFP%, TMD en segundos). Esto exige métodos cuantitativos como componente principal. El análisis interpretativo de los logs y la evaluación NIST añaden un componente cualitativo complementario indispensable para responder plenamente la pregunta de investigación.

ENFOQUE ADOPTADO: Mixto con predominancia cuantitativa — diseño Explicativo Secuencial (CUAN → cual)

Creswell & Plano Clark (2018, Cap. 3) definen el diseño Explicativo Secuencial como aquel en que primero se recogen y analizan los datos cuantitativos (Fase 1), y luego los resultados guían la selección de qué aspectos profundizar con métodos cualitativos (Fase 2). Para este proyecto:

FASE 1 — CUANTITATIVA (predominante): Experimento controlado — medición de TD%, TFP% y TMD
mediante 1.200 escenarios de ataque simulado + 300 eventos de tráfico legítimo (N=1.500 total).

FASE 2 — cualitativa (complementaria): Análisis de logs Snort + evaluación Lista de Cotejo NIST SP 800-94 + análisis temático (Braun & Clarke, 2006) de patrones no capturados por indicadores numéricos.

PUNTO DE INTEGRACIÓN: Los tipos de ataque con TD% más baja o TFP% más alta en Fase 1 se seleccionan como casos para análisis cualitativo profundo en Fase 2.

2.2 Tipo de Diseño y Alcance

El diseño de investigación es CUASIEXPERIMENTAL de serie temporal (Campbell & Stanley, 1966, Diseño N.°7). Esta determinación se fundamenta en que los investigadores introducen deliberadamente cuatro tipos de ataques simulados como condiciones experimentales controladas —manipulación de la Variable Independiente— y miden la respuesta del IDS en cada escenario —Variable Dependiente—. El entorno de laboratorio cerrado provee control sobre variables extrañas, pero la ausencia de aleatorización plena de condiciones lo distingue del diseño experimental puro.

La afirmación del documento original —"no se manipulan variables de forma deliberada"— es factualmente incorrecta: los ataques simulados representan la manipulación deliberada y controlada de la Variable Independiente. Campbell & Stanley (1966) son explícitos en que la manipulación de la VI, aun sin aleatorización plena, define un diseño cuasiexperimental y no observacional.

Característica metodológica	Diseño experimental puro	Diseño cuasiexperimental (ADOPTADO)	Diseño no experimental
Manipulación de la VI	Sí	Sí	No
Aleatorización plena	Sí	No — condiciones predefinidas	No aplica
Control del ambiente	Total	Parcial — laboratorio	Observación natural
Validez interna	Alta	Media-alta	Baja a media
¿Aplica a este proyecto?	No — no hay aleatorización de grupos	**SÍ — manipulación VI + laboratorio controlado**	No — los ataques SE manipulan deliberadamente

El alcance del estudio es EXPLICATIVO-EVALUATIVO (Hernández-Sampieri & Mendoza, 2018, Cap. 5). Es explicativo porque determina en qué medida la VI (IDS Snort 3.x configurado) afecta la VD (capacidad de detección), estableciendo relaciones causales verificables entre la configuración de reglas y los indicadores de desempeño. Es evaluativo porque contrasta los resultados empíricos con el estándar normativo NIST SP 800-94 mediante criterios predefinidos y medibles.

3. TÉCNICAS DE RECOLECCIÓN DE DATOS

3.1 Población, Universo y Muestra

Nivel	Definición	Aplicación al proyecto
UNIVERSO	Todos los eventos de tráfico y ataques en redes LAN organizacionales	Totalidad de eventos en redes LAN de instituciones educativas y organizaciones en Colombia
POBLACIÓN	Subconjunto accesible con características comunes (Hernández-Sampieri, 2018)	Todos los eventos de tráfico generados en la red LAN de laboratorio de la U. EAN durante el primer semestre de 2026
MUESTRA	Subconjunto representativo o justificado de la población	N = 1.500 eventos: 300 por cada tipo de ataque (×4) + 300 de tráfico legítimo como línea base

Cálculo del Tamaño de Muestra — Fórmula de Cochran (1977)

$n = Z^2 \times p \times q / e^2$

$n = (1{,}96)^2 \times 0{,}75 \times 0{,}25 / (0{,}05)^2 = 3{,}8416 \times 0{,}1875 / 0{,}0025 = 288{,}12 \approx 300$ eventos por tipo de ataque

Parámetros utilizados:

- $Z = 1{,}96 \rightarrow$ Nivel de confianza del 95% (estándar en investigación de ingeniería de sistemas)
- $p = 0{,}75 \rightarrow$ Tasa de detección esperada (75%) según hipótesis general HG
- $q = 0{,}25 \rightarrow q = 1 - p$
- $e = 0{,}05 \rightarrow$ Margen de error del 5% (aceptable para estudios de laboratorio controlado)

N total adoptado = 300 × 4 tipos de ataque + 300 tráfico legítimo = 1.500 eventos

3.2 Técnicas para el Componente Cuantitativo (Montgomery, 2017)

El componente cuantitativo sigue los principios del Diseño de Experimentos (DOE) de Montgomery (2017). Se adopta un diseño factorial de un factor (tipo de ataque) con cuatro niveles (escaneo de puertos, fuerza bruta, DoS, malware simulado) y medición repetida de tres respuestas (TD%, TFP%, TMD). Las variables de bloqueo son: hora de la sesión, versión de Snort y carga de CPU del nodo IDS, que se controlan documentando su estado en cada sesión mediante la bitácora BTC-02.

Técnica cuantitativa	Descripción	Variable que mide	Referente
Experimento controlado en laboratorio — implementación de la VI	Instalación y configuración de Snort 3.x con reglas personalizadas para 4 tipos de ataque. El investigador manipula deliberadamente la VI activando/desactivando reglas y ejecutando ataques.	VI: Implementación IDS Snort 3.x (cobertura de reglas, integridad de configuración)	Montgomery (2017), Cap. 2
Observación técnica estructurada — medición instrumental automatizada	Captura automática de alertas por Snort durante los escenarios de ataque. Sin intervención humana en la captura: los logs se generan en tiempo real y se exportan a CSV.	VD: TD%, TFP% — número y tipo de alertas generadas	Ñaupas et al. (2019), Cap. 7; Montgomery (2017)
Medición instrumental de timestamps	Captura simultánea del tráfico con Wireshark (.pcap) para calcular el tiempo entre el primer paquete de ataque y la generación de la alerta Snort.	VD: TMD — tiempo medio de detección en segundos	Montgomery (2017): medición instrumental reduce sesgo
Análisis de registros (logs) cuantitativo	Procesamiento automatizado de alert_fast.txt: conteo de VPs y FPs por tipo de ataque, cálculo de TD%, TFP% y TMD. Herramienta: Python (pandas + scipy).	VD: Todos los indicadores cuantitativos	Ñaupas et al. (2019)

3.3 Técnicas para el Componente Cualitativo (Flick, 2019)

Técnica cualitativa	Descripción	Variable que cubre	Referente
Revisión documental sistemática	Búsqueda y análisis de literatura científica en Scopus, IEEE Xplore, ACM Digital Library (2015–2026) para clasificar los 4 tipos de ataque seleccionados y documentar tasas de detección reportadas en estudios comparables.	V. contextual: tipos de ataques LAN (OE1)	Bernal (2016), Cap. 7; Flick (2019), Cap. 12
Análisis de registros (logs) — componente interpretativo	Lectura e interpretación de patrones en los logs de Snort no reducibles a indicadores numéricos: análisis de los tipos de eventos que generan más FPs, identificación de patrones de evasión.	V. evaluativa: efectividad cualitativa del IDS	Flick (2019), Cap. 15
Evaluación con lista de cotejo — juicio experto	Aplicación de la Lista de Cotejo NIST SP 800-94 (LCN-03) por dos investigadores de forma independiente sobre los resultados experimentales. Escala ordinal:	V. evaluativa: cumplimiento NIST SP 800-94 (OE4)	Flick (2019): análisis documental de estándares

Técnica cualitativa	Descripción	Variable que cubre	Referente
	Cumple (2) / Cumple parcialmente (1) / No cumple (0).		

3.4 Triangulación de Datos (Denzin, 1978)

TRIANGULACIÓN METODOLÓGICA (Denzin, 1978) — uso de múltiples técnicas para medir los mismos indicadores:

• TD% y TMD: medidos por (1) log automático Snort + (2) captura Wireshark de forma independiente

• TFP%: clasificación automática del sistema validada por revisión manual de dos investigadores

• Efectividad global: evaluada por (1) indicadores cuantitativos (IEG) + (2) Lista de Cotejo NIST

TRIANGULACIÓN DE FUENTES (Denzin, 1978):

• Los resultados propios se contrastan con tasas de detección reportadas en estudios previos comparables

(Islam & Islam, 2024; Robbani et al., 2025; Gaddam & Nandhini, 2017) y con los parámetros NIST SP 800-94.

Justificación: la triangulación reduce el sesgo de método único y fortalece la validez interna del estudio

(Flick, 2019, Cap. 28; Hernández-Sampieri & Mendoza, 2018, p. 453).

Tabla Maestra de Técnicas e Instrumentos

Variable	Técnica	Instrumento	Fuente	Triangulación
VI: IDS Snort 3.x	Experimento controlado	Bitácora técnica BTC-02	Primaria	Fuentes: config. vs. doc. Snort.org
VD: TD%	Obs. técnica estructurada	Log Snort (alert_fast.txt) + verificación Wireshark	Primaria	Metodológica: 2 instrumentos independientes
VD: TFP%	Análisis de registros	Log Snort + clasificación manual VP/FP — FRAS-01	Primaria	Metodológica: automático validado por manual
VD: TMD	Medición instrumental	Wireshark .pcap + timestamps Snort — FRAS-01	Primaria	Metodológica: 2 fuentes de tiempo

Variable	Técnica	Instrumento	Fuente	Triangulación
V. Evaluativa: NIST	Análisis documental + juicio experto	Lista de cotejo LCN-03 (25 controles)	Secundaria	Fuentes: resultados vs. estándar internacional
V. Contextual: Ataques LAN	Revisión documental sistemática	Ficha bibliográfica FCA-04	Secundaria	Teórica: múltiples fuentes IEEE + Scopus + NIST

4. INSTRUMENTOS DE RECOLECCIÓN

4.1 Tabla de Especificaciones (Kerlinger & Lee, 2002)

Variable	Dimensión	Indicador operacional	Ítem / Medición	Escala (Stevens, 1946)
VI: IDS Snort 3.x	Configuración	Índice de cobertura: N° reglas activas / N° tipos ataque × 100	T-01: Registrar reglas .rules activadas por categoría de ataque en BTC-02	Razón (%)
VI: IDS Snort 3.x	Instalación	Modo promiscuo activo + Snort en modo IDS (S/N)	T-02: Verificar ifconfig y snort --version	Nominal dicotómica
VI: IDS Snort 3.x	Integridad	Hash SHA-256 del archivo snort.conf (coincide pre/post sesión: S/N)	T-03: sha256sum snort.conf al inicio y cierre de cada sesión	Nominal dicotómica
VD: Detección	Tasa de detección	Alertas VP / Total ataques simulados × 100	T-04: Cruzar registros de alertas con registro de ataques ejecutados	Razón (%)
VD: Detección	Falsos positivos	Alertas FP / Total alertas generadas × 100	T-05: Clasificar cada alerta en FRAS-01: VP (verdadero positivo) / FP (falso positivo)	Razón (%)
VD: Detección	Tiempo medio de detección	Promedio de (timestamp alerta Snort − timestamp primer paquete ataque Wireshark)	T-06: Calcular diferencia de timestamps por evento en FRAS-01	Razón (segundos)
VD: Detección	Eficacia por tipo	TD% individualizada por cada una de las 4 categorías de ataque	T-07 a T-10: una fila de resultado por categoría en tabla de análisis	Razón (%) por categoría
V. Evaluativa	Cumplimiento NIST	N° controles cumplidos / N° controles NIST × 100	T-11: Evaluar cada uno de los 25 controles aplicables del NIST SP 800-94 con LCN-03	Ordinal (0–2 por control)

4.2 Fichas Técnicas de Instrumentos

INSTRUMENTO 1 — Ficha de Registro de Alertas Snort (FRAS-01)

FICHA TÉCNICA — FRAS-01: Registro de Alertas y Métricas del IDS	
Nombre completo	Ficha de Registro de Alertas Snort y Métricas de Desempeño (FRAS-01)
Tipo de instrumento	Registro mixto: captura automática (log Snort) + validación manual (clasificación VP/FP)

FICHA TÉCNICA — FRAS-01: Registro de Alertas y Métricas del IDS	
Variables que mide	VD: TD%, TFP%, TMD — capacidad de detección y generación de alertas del IDS Snort 3.x
Escala de medición (Stevens, 1946)	RAZÓN para TD%, TFP%, TMD — existe cero absoluto real (0% detección = ninguna alerta ante ataques). Las operaciones aritméticas son válidas: media, DE, comparación porcentual.
Campos / ítems (12 campos)	N° evento | Timestamp ataque (inicio) | Timestamp alerta Snort | Diferencia TMD (seg) | Tipo de ataque | Herramienta ejecutada | Regla Snort activada | IP origen | IP destino | Clasificación VP/FP | Observación | Firma investigador
Precisión de timestamps	Milisegundos (formato Unix epoch de Snort 3.x — resolución ms)
Rango de indicadores	TD%: 0–100% | TFP%: 0–100% | TMD: 0 – ∞ segundos (esperado < 5 s en LAN)
Frecuencia de aplicación	Una ficha por escenario de ataque: 20 escenarios por tipo × 4 tipos = 80 fichas (cada ficha acumula 15 eventos)
Modo de aplicación	Automático (alert_fast.txt generado por Snort 3.x) + revisión manual post-sesión por investigador designado para clasificación VP/FP
Referente metodológico	Kerlinger & Lee (2002): cada ítem rastrea a un indicador operacional específico. DeVellis (2017): trazabilidad ítem → indicador → variable.

INSTRUMENTO 2 — Bitácora Técnica de Configuración y Laboratorio (BTC-02)

FICHA TÉCNICA — BTC-02: Bitácora Técnica de Sesiones de Laboratorio	
Nombre completo	Bitácora Técnica de Configuración, Control de Sesiones y Diario de Campo (BTC-02)
Tipo de instrumento	Registro manual estructurado — instrumento cualitativo-documental (Flick, 2019; Taylor & Bogdan, 1987)
Variables que cubre	VI: implementación del IDS. Variable de control: condiciones del experimento por sesión.
Escala de medición (Stevens, 1946)	NOMINAL para verificaciones dicotómicas (S/N) + RAZÓN para versiones y duraciones + TEXTO ABIERTO para incidencias
Campos (16 campos)	Fecha-hora inicio | Investigador responsable | Versión Snort (snort --version) | Versión SO | N° reglas .rules activas | N° categorías cubiertas | Modo promiscuo S/N | Hash SHA-256 snort.conf | IP nodo IDS | IP máquina atacante | IP máquina víctima | Tipo de ataque ejecutado | Herramienta y versión | Duración sesión (min) | Incidencias y decisiones tomadas | Firma investigador
Verificación de integridad	Hash SHA-256 del archivo snort.conf garantiza reproducibilidad de la configuración entre sesiones
Frecuencia de aplicación	Una entrada al inicio y una al cierre de cada sesión de laboratorio (6 sesiones × 2 = 12 registros)

FICHA TÉCNICA — BTC-02: Bitácora Técnica de Sesiones de Laboratorio	
Modo de aplicación	Manual por el investigador coordinador (Erick Castro). Revisión cruzada por segundo investigador al cierre.
Referente metodológico	Flick (2019): la bitácora es esencial para la auditoría y replicabilidad del estudio. Taylor & Bogdan (1987): el diario de campo estructura la memoria metodológica.

INSTRUMENTO 3 — Lista de Cotejo NIST SP 800-94 (LCN-03)

FICHA TÉCNICA — LCN-03: Lista de Cotejo de Controles NIST SP 800-94	
Nombre completo	Lista de Cotejo de Controles NIST SP 800-94 para Sistemas NIDS (LCN-03)
Tipo de instrumento	Lista de cotejo estructurada — instrumento cualitativo-evaluativo
Variable que mide	V. evaluativa: porcentaje de cumplimiento de controles NIST SP 800-94 aplicables a sistemas NIDS
Escala de medición (Stevens, 1946)	ORDINAL de 3 niveles con definiciones operacionales explícitas: 2 = Cumple: el control se verifica completamente con evidencia observable 1 = Cumple parcialmente: el control se satisface en parte, con limitaciones documentadas 0 = No cumple: el control no se verifica o la evidencia es inexistente
Controles evaluados	25 controles aplicables de la Sección 4 del NIST SP 800-94 para NIDS, incluyendo: capacidad de detección por firma, alertas en tiempo real, registro de eventos, gestión de reglas, cobertura de protocolos, tiempo de respuesta, y tasa de falsos positivos aceptable
Número de ítems	25 controles, cada uno con campos: N° control | Descripción NIST | Evidencia observada en Snort | Calificación (0/1/2) | Observación | Recomendación de mejora
Frecuencia de aplicación	Una vez, al finalizar la Fase 1 cuantitativa (semana 7-8, sesión S5)
Confiabilidad	Evaluación independiente por dos investigadores + porcentaje de acuerdo ≥ 85% (DeVellis, 2017). Discrepancias resueltas por docente supervisor.
Referente metodológico	Scarfone & Mell (2007), NIST SP 800-94, Sección 4. DeVellis (2017): trazabilidad ítem → indicador.

INSTRUMENTO 4 — Ficha de Clasificación de Ataques LAN (FCA-04)

FICHA TÉCNICA — FCA-04: Ficha de Clasificación de Ataques en Redes LAN	
Nombre completo	Ficha de Análisis Bibliográfico y Clasificación de Ataques Informáticos en Redes LAN (FCA-04)
Tipo de instrumento	Ficha de análisis documental estructurada (instrumento de revisión sistemática)

FICHA TÉCNICA — FCA-04: Ficha de Clasificación de Ataques en Redes LAN	
Variable que mide	V. contextual: tipos de ataques informáticos en redes LAN (OE1)
Escala de medición (Stevens, 1946)	NOMINAL: categoría de ataque, vector, protocolo, herramienta de simulación. ORDINAL: impacto CIA (Alto/Medio/Bajo). ORDINAL: frecuencia en literatura (Alta/Media/Baja)
Campos (8 campos)	Autor/año | Nombre del ataque | Categoría (taxonomía CIA) | Vector de ataque | Protocolo afectado | Impacto CIA (C/I/D: Alto/Medio/Bajo) | Herramienta de simulación ética | Frecuencia reportada en literatura
Número mínimo de registros	≥ 8 tipos de ataque clasificados (indicador de OE1)
Modo de aplicación	Manual por investigador (Luis Bogota) durante la revisión documental sistemática en Scopus, IEEE Xplore y ACM DL
Referente metodológico	Hernández-Sampieri & Mendoza (2018, Cap. 9): instrumento adecuado representa fielmente los conceptos teóricos. Bernal (2016): ficha bibliográfica estandarizada.

5. PROCEDIMIENTO

5.1 Descripción del Entorno Experimental

Componente	Especificación técnica	Función en el experimento
Máquina IDS (Nodo IDS)	Ubuntu Server 22.04 LTS — Snort 3.x (última versión estable) — 4 GB RAM — tarjeta de red en modo promiscuo	Captura y analiza todo el tráfico del segmento LAN; genera logs de alertas
Máquina atacante	Kali Linux 2024.x — Nmap 7.x — Hydra 9.x — hping3 — Metasploit Framework 6.x	Ejecuta los 4 tipos de ataques simulados según el protocolo de cada sesión
Máquina víctima	Ubuntu Server 22.04 LTS — servicios SSH, HTTP (Apache), FTP activos	Objetivo de los ataques simulados; tráfico capturado por el nodo IDS
Switch de red	Switch gestionable con puerto espejo (SPAN) configurado al nodo IDS	Permite que el nodo IDS capture todo el tráfico del segmento
Herramienta de apoyo	Wireshark 4.x instalado en nodo IDS	Captura simultánea .pcap para verificación de timestamps (triangulación)
Segmento de red	192.168.100.0/24 — aislado de internet y redes externas durante las sesiones	Garantiza el control total del entorno y la exclusión de tráfico no controlado

5.2 Protocolo de Recolección de Datos — Paso a Paso

Paso 1 — Preparación y revisión documental (Semanas 1-2, febrero 2026)

- Revisión documental sistemática en Scopus, IEEE Xplore y ACM DL: identificar y clasificar ≥ 8 tipos de ataques LAN en FCA-04.
- Diseño y diligenciamiento previo de los instrumentos FRAS-01 y BTC-02.
- Obtención de la autorización institucional firmada por el Decano de la Facultad de Ingeniería.
- Instalación base de Snort 3.x y Kali Linux en los nodos del laboratorio. Documentación del ambiente en BTC-02.

Paso 2 — Configuración del IDS y prueba piloto (Semana 3, Sesión S1)

- Configuración de Snort 3.x: activar reglas comunitarias (Snort Community Rules) y crear reglas personalizadas para los 4 tipos de ataque. Registrar N° de reglas en BTC-02.
- Verificación: activar modo promiscuo, ejecutar snort --version, generar hash SHA-256 del archivo snort.conf.
- Prueba piloto con 150 eventos (10% de N): 30 eventos × 5 mini-escenarios. Calcular Kappa de Cohen entre dos investigadores para clasificación VP/FP. $\kappa \geq 0{,}80$ = continuar; $\kappa < 0{,}80$ = revisar criterios de clasificación.

- Ajustar reglas o umbrales si la prueba piloto revela TFP > 20% en alguna categoría.

Paso 3 — Sesiones experimentales (Semanas 4-6, Sesiones S2-S4)

Sesión	Tipo de ataque	Herramienta Kali	N° eventos	Duración	Responsable
S2	Escaneo de puertos TCP/UDP	Nmap 7.x (sV, -sS, -sU flags)	300 eventos	3 horas	Lina Sánchez (ataque)
S3	Fuerza bruta SSH y HTTP	Hydra 9.x (SSH puerto 22, HTTP Basic Auth)	300 eventos	3 horas	Lina Sánchez (ataque)
S4A	Denegación de servicio (DoS)	hping3 (SYN flood, ICMP flood, UDP flood)	300 eventos	1,5 horas	Lina Sánchez (ataque)
S4B	Malware simulado (C2 traffic)	Metasploit Framework 6.x (meterpreter reverso, payloads stageless)	300 eventos	1,5 horas	Lina Sánchez (ataque)

Procedimiento estándar por sesión: (1) Verificar hash snort.conf = hash de S1; (2) Sincronizar NTP en todos los nodos; (3) Iniciar Wireshark en modo captura; (4) Iniciar Snort 3.x en modo IDS; (5) Ejecutar ataque según protocolo; (6) Finalizar captura y exportar alert_fast.txt y archivo .pcap; (7) Diligenciar FRAS-01 con los datos de la sesión; (8) Firmar BTC-02 al cierre.

Paso 4 — Tráfico legítimo de línea base (intercalado con S2-S4)

- 300 eventos de tráfico normal: navegación web, transferencia de archivos, consultas DNS, tráfico SSH legítimo. Propósito: medir TFP en condiciones de tráfico real sin ataques.

Paso 5 — Análisis cualitativo (Semanas 7-8, Sesión S5)

- Aplicación de la LCN-03 (Lista de Cotejo NIST SP 800-94) por dos investigadores de forma independiente.
- Análisis temático de logs según 6 fases de Braun & Clarke (2006): patrones de evasión, tipos de FP más frecuentes, controles NIST incumplidos.

Paso 6 — Integración y elaboración del informe final (Semanas 9-12)

- Integración CUAN → cual: los tipos de ataque con TD% más baja o TFP% más alta guían el análisis cualitativo profundo de los logs.
- Cálculo del IEG, contraste con hipótesis HG, HE1, HE2, HE3.

- Redacción del informe final con secciones: resultados, discusión, conclusiones, recomendaciones.

5.3 Controles Técnicos y Restricciones

Control	Descripción	Momento de aplicación
Integridad de la configuración	Hash SHA-256 del archivo snort.conf verificado al inicio de cada sesión. Cualquier diferencia detiene la sesión.	Inicio de S2, S3, S4A, S4B
Sincronización temporal (NTP)	Todos los nodos sincronizados con servidor NTP local antes de cada sesión. Garantiza precisión de timestamps para cálculo de TMD.	Inicio de cada sesión experimental
Doble revisión VP/FP	Dos investigadores clasifican independientemente las mismas 150 alertas piloto. $\kappa \geq 0{,}80$. En sesiones formales, validación cruzada del 20% de las alertas.	S1 (piloto) y muestreo en S2-S4
Verificación de capturas	Verificar que el archivo .pcap tenga tamaño > 0 KB y contenga el flag FIN en la última captura antes de cerrar Wireshark.	Final de cada sesión experimental
Aislamiento de la red	El segmento 192.168.100.0/24 permanece desconectado de internet durante todas las sesiones experimentales. Se verifica con ping a 8.8.8.8 antes de iniciar.	Antes de S2, S3, S4A, S4B

5.4 Protocolos de Seguridad y Ética Investigativa

El estudio trabaja exclusivamente en el entorno cerrado y aislado del laboratorio de redes de la Universidad EAN. Ningún ataque se ejecuta sobre sistemas externos o de terceros. Todos los ataques son simulados con herramientas de pentesting ético (no se instala código malicioso real). Se cuenta con la autorización institucional firmada de la Facultad de Ingeniería, en cumplimiento de la Ley 1581 de 2012 (Habeas Data), la política de seguridad informática de la Universidad EAN y el Código de Ética APA (2020).

Los archivos de datos brutos (logs, capturas .pcap, FRAS-01) se almacenan en repositorio GitHub privado del equipo con control de acceso y se eliminarán completamente al concluir el proyecto, en cumplimiento del principio de minimización de datos (Ley 1581/2012, Art. 4).

Plan de Contingencia

Contingencia	P	Plan de acción
Falla del nodo IDS	Media	Restaurar snapshot de VM de Snort preconfigurado (≈ 15 min). Repetir sesión en la siguiente semana disponible. Documentar en BTC-02.
Pérdida de log de alertas	Baja	Respaldo automático cada 30 minutos en repositorio GitHub. Recuperar desde última copia. Verificar integridad con SHA-256.
TD = 0% en algún tipo de ataque	Baja	Verificar reglas activas, reiniciar Snort en modo verbose (snort -v), revisar interfaz promiscua. Si persiste, documentar como hallazgo y ajustar reglas.
Laboratorio no disponible	Media	Protocolo alternativo: laboratorio virtual GNS3 + VirtualBox en equipos personales del equipo. Documentar el cambio de entorno en BTC-02 y en la sección de limitaciones del informe.
$\kappa < 0{,}80$ en clasificación VP/FP	Media	Revisar y redefinir criterios de clasificación con el docente supervisor. Repetir el ejercicio de calibración con 30 alertas adicionales hasta alcanzar acuerdo.

6. VALIDACIÓN DE INSTRUMENTOS

6.1 Validez de Contenido por Juicio de Expertos (Lawshe, 1975)

Criterios de selección de expertos

Criterio	Requisito	Justificación
Número mínimo	3 expertos	Con 3 expertos, CVI ≥ 0,80 exige que los 3 califiquen ≥ 3 en la escala 1–4 (Lawshe, 1975)
Nivel académico	Título de maestría o doctorado	Garantiza dominio teórico en el área evaluada
Área de experticia	Ciberseguridad, redes de computadores o IDS/IDPS	Coherencia entre el perfil del experto y el contenido a evaluar
Experiencia práctica	≥ 5 años en ciberseguridad o administración de sistemas	Asegura conocimiento práctico del fenómeno estudiado
Independencia	Sin relación académica o laboral directa con el equipo investigador	Evita sesgo de proximidad en la evaluación

Hoja de evaluación por expertos — 4 dimensiones (Escobar & Cuervo, 2008)

INSTRUCCIONES PARA EL EXPERTO:

Evalúe cada ítem en las 4 dimensiones con la escala: 1=No cumple | 2=Cumple bajo | 3=Cumple aceptable | 4=Cumple excelente

CÁLCULO CVI por ítem (Lawshe, 1975):

CVI = N° expertos que califican ≥ 3 en las 4 dimensiones / N° total de expertos

CVI ≥ 0,80 → Conservar el ítem | 0,60 ≤ CVI < 0,80 → Revisar y modificar | CVI < 0,60 → Eliminar

Ítem	Descripción del ítem	Pertinencia (1-4)	Claridad (1-4)	Suficiencia (1-4)	Relevancia (1-4)	CVI calculado	Observación
T-01	Índice de cobertura de reglas Snort	___	___	___	___	_.__	___
T-02	Verificación modo promiscuo (S/N)	___	___	___	___	_.__	___

Ítem	Descripción del ítem	Pertinencia (1-4)	Claridad (1-4)	Suficiencia (1-4)	Relevancia (1-4)	CVI calculado	Observación
T-03	Hash SHA-256 snort.conf (S/N)	___	___	___	___	_.__	___
T-04	Conteo alertas VP (verdaderos positivos)	___	___	___	___	_.__	___
T-05	Clasificación VP/FP por revisión manual	___	___	___	___	_.__	___
T-06	Timestamps ataque-alerta (TMD en seg)	___	___	___	___	_.__	___
T-07 a T-10	TD% por tipo de ataque (una fila por categoría)	___	___	___	___	_.__	___
T-11	Evaluación controles NIST SP 800-94	___	___	___	___	_.__	___

6.2 Prueba Piloto y Confiabilidad

Aspecto	Detalle técnico
Tamaño del piloto	n = 150 eventos (10% de N = 1.500). Distribución: 30 eventos × 5 mini-escenarios (un por tipo + tráfico legítimo)
Participantes del piloto	NO incluidos en la muestra definitiva. Sesión S1 (semana 3) con condiciones idénticas a S2-S4
Métrica de confiabilidad para clasificación VP/FP	Coeficiente Kappa de Cohen (κ) — confiabilidad interjueces para clasificación dicotómica (Landis & Koch, 1977) $\kappa \geq 0{,}80$ = acuerdo casi perfecto → aceptable $0{,}60 \leq \kappa < 0{,}80$ = acuerdo sustancial → revisar criterios $\kappa < 0{,}60$ → redefinir completamente los criterios de clasificación
¿Por qué no se usa Alfa de Cronbach?	El Alfa de Cronbach (Cronbach, 1951) mide consistencia interna de escalas de ítems de respuesta subjetiva (encuestas, escalas Likert). Los instrumentos FRAS-01 y BTC-02 capturan datos técnicos automatizados o verificaciones objetivas, no respuestas humanas. La métrica apropiada es la confiabilidad interjueces (Kappa) y la estabilidad temporal (test-retest) (Nunnally, 1978).
Test-retest para TMD	Repetir 30 escenarios idénticos con 2 semanas de intervalo

Aspecto	Detalle técnico
	r de Pearson ≥ 0,70 = confiabilidad aceptable (Hernández-Sampieri & Mendoza, 2018) r < 0,70 → revisar precisión del sistema de timestamps
Confiabilidad de LCN-03	Porcentaje de acuerdo entre 2 evaluadores ≥ 85% (DeVellis, 2017) Discrepancias resueltas por el docente supervisor (tercera opinión)

6.3 Tabla de Ajustes Post-Validación

Ítem	Versión original	Observación del experto	CVI	Decisión	Versión ajustada
T-04	Contar alertas en alert_fast.txt que correspondan a ataques ejecutados	[Por completar tras evaluación de expertos]	_.__	[Conservar / Revisar / Eliminar]	[Por completar]
T-05	Clasificar alerta: VP / FP mediante revisión manual del log	[Por completar]	_.__	[Por completar]	[Por completar]
T-11	Evaluar cada control NIST con escala ordinal 0/1/2	[Por completar]	_.__	[Por completar]	[Por completar]

INSTRUCCIÓN: Esta tabla debe completarse después de recibir la evaluación de los 3 expertos seleccionados,

calculando el CVI para cada ítem según la fórmula de Lawshe (1975). Los ítems con CVI < 0,80 deben

revisarse antes de aplicar los instrumentos en las sesiones experimentales formales (S2-S4).

7. PLAN DE ANÁLISIS

7.1 Matriz de Coherencia Analítica (Hair et al., 2019; Field, 2018)

OE	Variable	Escala	Técnica de análisis	Supuestos a verificar	Software
OE1	V. Contextual: tipos de ataques LAN	Nominal + Ordinal	Análisis temático documental (Braun & Clarke, 2006): frecuencia de reporte + clasificación CIA. Estadística descriptiva: frecuencias relativas por categoría	N/A — análisis cualitativo-documental	NVivo 12 / Atlas.ti / Excel
OE2	VI: Índice de cobertura de reglas	Razón (%)	Estadística descriptiva: porcentaje de cobertura. Verificación dicotómica: instalación correcta S/N	N/A — indicador de proceso	Excel / Python (pandas)
OE3	VD: TD%, TFP%, TMD	Razón (%/seg)	1) ANOVA de un factor (4 niveles): comparar TD% entre tipos de ataque (Hair et al., 2019) 2) t-test de una muestra: contrastar TD% vs. umbral HG (75%) 3) Estadística descriptiva: media ± DE, min, max, IC 95% por tipo de ataque 4) Coeficiente de correlación de Pearson: ¿relación entre TD% y TMD?	Normalidad: Shapiro-Wilk (n<50) o Kolmogorov-Smirnov (n≥50) Homocedasticidad: prueba de Levene Independencia: verificada por diseño experimental	SPSS v26 / Python scipy.stats + pandas + matplotlib
OE4	V. Evaluativa: NIST + IEG	Ordinal + Razón	1) IEG = TD%_promedio − TFP% (indicador compuesto) 2) Análisis frecuencial LCN-03: distribución de 25 controles en niveles 0/1/2 3) t-test una muestra: IEG vs. umbral HE3 (70% cumplimiento) 4) Análisis cualitativo: temas emergentes de	Shapiro-Wilk para IEG N/A para análisis cualitativo de logs	SPSS / Python / NVivo

OE	Variable	Escala	Técnica de análisis	Supuestos a verificar	Software
			logs con TD% más baja		
OG	Integración VI+VD	Razón + Ordinal	Narrative integration (Creswell & Plano Clark, 2018): los resultados CUAN (OE3) guían el análisis cual profundo de los tipos de ataque con TD% más baja o TFP% más alta	Verificación de hipótesis HG con t-test y comparación porcentual	SPSS + NVivo + Python (visualización)

7.2 Verificación de Supuestos Estadísticos (Field, 2018)

Supuesto	Prueba estadística	Criterio de decisión	Alternativa no paramétrica si falla
Normalidad de TD% por tipo de ataque	Shapiro-Wilk (n = 300 por grupo, pero el indicador TD% es una proporción; usar Kolmogorov-Smirnov si n > 50)	$p > 0,05$ → distribución normal → ANOVA paramétrico $p \leq 0,05$ → no normal → alternativa no paramétrica	Prueba de Kruskal-Wallis (comparación de 4 grupos independientes)
Homocedasticidad (igualdad de varianzas entre los 4 tipos de ataque)	Prueba de Levene (aplicada sobre los residuos del ANOVA)	$p > 0,05$ → varianzas homogéneas → ANOVA estándar $p \leq 0,05$ → varianzas heterogéneas → alternativa	ANOVA de Welch (robusto a heterocedasticidad) o prueba de Mann-Whitney U para comparaciones por pares
Independencia de las observaciones	Verificación por diseño: cada evento de ataque es generado de forma independiente en sesiones separadas	Garantizada por el diseño cuasiexperimental si los eventos de una sesión no afectan los de otra	Si hay dependencia temporal: ANOVA de medidas repetidas o prueba de Friedman
Normalidad del TMD	Shapiro-Wilk por tipo de ataque (los tiempos de detección suelen tener distribución sesgada a la derecha)	$p > 0,05$ → paramétrico $p \leq 0,05$ → no normal → usar mediana e IQR en vez de media y DE	Mann-Whitney U para comparaciones por pares de TMD entre tipos de ataque

7.3 Análisis Cualitativo — 6 Fases de Braun & Clarke (2006)

APLICACIÓN AL PROYECTO LEB — Componente cualitativo del diseño CUAN → cual:

FASE 1 — FAMILIARIZACIÓN: Lectura repetida de logs Snort de los escenarios con TD% más baja
y de la evaluación LCN-03. Anotaciones iniciales sobre patrones observados.

FASE 2 — CODIFICACIÓN INICIAL: Asignar códigos descriptivos a segmentos de logs.
Ejemplos: [ATAQUE_NO_DETECTADO] [FALSO_POSITIVO_RECURRENTE] [CONTROL_NIST_INCUMPLIDO]
[EVASIÓN_POR_FRAGMENTACIÓN] [REGLA_DEMASIADO_AMPLIA]. Software: Atlas.ti o NVivo.

FASE 3 — BÚSQUEDA DE TEMAS: Agrupar códigos en temas potenciales.
Tema 1: «Limitaciones de detección por tipo de ataque»
Tema 2: «Patrones de falsos positivos y sus causas técnicas»
Tema 3: «Brechas de cumplimiento NIST SP 800-94»

FASE 4 — REVISIÓN DE TEMAS: Verificar coherencia interna de cada tema y su distinción respecto a los otros. Triangular con resultados cuantitativos del OE3.

FASE 5 — DEFINICIÓN Y NOMINACIÓN: Definir el alcance de cada tema y redactar una narrativa analítica (no solo descriptiva) que explique el fenómeno subyacente.

FASE 6 — PRODUCCIÓN DEL INFORME: Integrar temas cualitativos con resultados cuantitativos
en la sección de discusión del informe final. Punto de integración: los indicadores numéricos
del OE3 guían qué patrones se profundizan cualitativamente en el OE4.

7.4 Integración Mixta (Creswell & Plano Clark, 2018)

Momento de integración	Qué se integra	Cómo se integra	Producto esperado
Después de OE3 (Fase 1 CUAN)	TD%, TFP% y TMD calculados por tipo de ataque	Los tipos de ataque con TD% más baja o TFP% más alta se seleccionan como casos para análisis cualitativo profundo de logs (muestreo teórico)	Selección intencional de casos para la Fase 2 cualitativa

Momento de integración	Qué se integra	Cómo se integra	Producto esperado
Durante OE4 (Fase 2 cual)	Análisis de logs cualitativos + evaluación LCN-03	Los temas cualitativos emergentes se contrastan con los indicadores cuantitativos: ¿el tema «reglas demasiado amplias» explica el TFP% alto?	Tabla de integración: indicador cuantitativo ↔ tema cualitativo ↔ control NIST correspondiente
Discusión de resultados	Todos los resultados cuantitativos y cualitativos	Narrative integration (Creswell & Plano Clark, 2018): resultados presentados de forma integrada, verificando cada hipótesis HG, HE1, HE2, HE3	Sección de discusión con hipótesis confirmadas/no confirmadas, temas cualitativos explicativos y recomendaciones de mejora de configuración

MARCO CONTEXTUAL Y CONCEPTUAL

Contexto: Ciberseguridad en Colombia 2024-2026

Durante los primeros once meses de 2024, Colombia registró 36 mil millones de intentos de ciberataques. El Centro de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT) identificó 22.086 vulnerabilidades en ese año, lo que evidencia un volumen inmenso de riesgos potenciales. El Centro Cibernético Policial reportó 59.033 denuncias por delitos informáticos en 2023, aunque la tendencia muestra una leve reducción respecto a 2022, cuando se registraron 65.794 casos. Para el primer semestre de 2026, se prevé la intensificación de ataques dirigidos contra infraestructura crítica, especialmente en sectores como salud, educación, energía y administraciones locales, debido a la persistencia de sistemas heredados y vulnerabilidades sin parches.

Triada CIA y Seguridad de Redes LAN

La ciberseguridad tiene como propósito principal salvaguardar tres principios esenciales conocidos como la triada CIA: Confidencialidad (restringir el acceso no autorizado a la información), Integridad (garantizar que los datos permanezcan sin alteraciones no autorizadas) y Disponibilidad (asegurar el acceso continuo a los sistemas). Para proteger sus infraestructuras, las organizaciones implementan controles como firewalls, sistemas de autenticación, antivirus y herramientas de detección de intrusiones (Whitman & Mattord, 2021). Las redes LAN, al conectar múltiples dispositivos en un espacio geográfico limitado, representan un punto crítico: un intruso con acceso al segmento podría comprometer todos los sistemas conectados.

Sistemas de Detección de Intrusiones (IDS/IPS)

Los IDS analizan el tráfico de red y generan alertas cuando detectan patrones asociados a actividades sospechosas. Los IPS añaden la capacidad de tomar acciones automáticas para bloquear o prevenir ataques (Behl & Behl, 2017). Los IDS se clasifican en basados en red (NIDS) —que monitorean el tráfico del segmento completo— y basados en host (HIDS) —que analizan la actividad de un dispositivo específico— (Stallings & Brown, 2018). Sus métodos de detección son: por firmas (comparación con patrones conocidos) y por anomalías (identificación de desviaciones del comportamiento normal).

Snort 3.x como Herramienta IDS

Snort fue introducido en 1998 por Martin Roesch y desde entonces se ha convertido en un sistema IDS pionero. Con un diseño modular de tres partes —decodificador de paquetes, motor de detección y módulo de salida— Snort puede adaptarse a una variedad de condiciones de red. En 2024, Cisco Talos lanzó SnortML, un nuevo motor de detección basado en aprendizaje automático diseñado para detectar ataques novedosos que encajan en tipos de vulnerabilidades conocidas, abordando el problema de los ataques de día cero. Estudios comparativos recientes muestran que Snort demostró mayor precisión de detección que Suricata en redes de laboratorio, aunque con una tasa de falsos positivos más elevada cuando se usan las reglas por defecto sin ajuste.

Estándar NIST SP 800-94 para evaluación de IDS

El NIST Special Publication 800-94 (Scarfone & Mell, 2007) constituye la guía de referencia internacional para el diseño, implementación, configuración y evaluación de sistemas IDPS. Proporciona orientación práctica para cada una de las cuatro clases de IDPS: basados en red, inalámbricos, de análisis de comportamiento de red y basados en host. Sus criterios de evaluación incluyen: capacidad de detección por firma, generación de alertas en tiempo real, gestión de reglas, cobertura de protocolos, registro de eventos y tasa de falsos positivos aceptable. Estos criterios estructuran la Lista de Cotejo LCN-03 utilizada en el OE4.

MARCO TEÓRICO

Estudios previos sobre efectividad de Snort en entornos de laboratorio

La literatura científica reciente aporta evidencia empírica valiosa para contextualizar los resultados esperados del presente estudio. Islam & Islam (2024) realizaron una evaluación cuantitativa de la efectividad de las reglas Snort ante ataques DoS, fuerza bruta y man-in-the-middle en un entorno de laboratorio controlado con 30 sesiones experimentales y 10 sesiones de línea base, capturando aproximadamente 1,24 millones de paquetes. Su diseño cuantitativo experimental utilizó capturas de paquetes, registros de alertas IDS y eventos de activación de reglas generados durante las sesiones para evaluar el desempeño del IDS.

Robbani et al. (2025) demostraron que Snort detectó todos los ataques simulados en tiempo real en un entorno de laboratorio con escenarios de ping flood, escaneo de puertos y fuerza bruta SSH, concluyendo que la integración de Snort con herramientas de visualización de logs resulta efectiva para la detección y análisis de amenazas en redes.

Respecto a los falsos positivos, investigaciones con la base de datos DARPA 1999 reportaron tasas de FP altas con las reglas por defecto. Sin embargo, el mejor resultado con Snort optimizado alcanzó una tasa de falsos positivos de apenas 8,6% y una tasa de falsos negativos de 2,2% mediante SVM optimizado con algoritmo de luciérnaga. Estos resultados sustentan la hipótesis HE2 del presente estudio (TFP < 15% con reglas personalizadas).

En cuanto al rendimiento en redes de alta velocidad, estudios comparativos entre Snort, Suricata y Zeek muestran que Suricata supera a Snort en redes de alto tráfico gracias a su arquitectura multihilo; sin embargo, para redes LAN de pequeña y mediana escala —como la de laboratorio de este estudio— Snort 3.x ofrece un balance adecuado entre precisión de detección y demanda de recursos computacionales.

Diseño cuasiexperimental en investigación de ciberseguridad

Campbell & Stanley (1966) establecen que el diseño cuasiexperimental —con manipulación de la VI sin aleatorización plena— es metodológicamente apropiado cuando el investigador controla las condiciones experimentales en un entorno cerrado. Este diseño ha sido

ampliamente adoptado en investigaciones de ciberseguridad con IDS (García-Teodoro et al., 2009; Islam & Islam, 2024), donde la aleatorización de los tipos de ataque es técnicamente innecesaria y la validez interna se garantiza mediante el control del entorno de laboratorio.

JUSTIFICACIÓN

La justificación del presente estudio opera en tres dimensiones complementarias.

Desde la perspectiva práctica, el estudio genera evidencia empírica directamente aplicable sobre la capacidad de Snort 3.x —herramienta de costo cero en licenciamiento— para proteger redes LAN institucionales de pequeña escala frente a los cuatro tipos de ataque más frecuentes en Colombia. Los indicadores cuantitativos producidos (TD%, TFP%, TMD, IEG) y las recomendaciones de configuración derivadas del análisis NIST SP 800-94 pueden ser adoptados por otras instituciones educativas sin necesidad de inversión en soluciones propietarias.

Desde la perspectiva académica, el estudio aplica un diseño cuasiexperimental con enfoque mixto explicativo secuencial —metodología rigurosa de nivel de posgrado— al campo de la ciberseguridad práctica, generando una contribución metodológica y técnica al acervo académico en lengua española sobre IDS en contextos latinoamericanos. La triangulación metodológica y de fuentes fortalece la validez interna y externa de los hallazgos.

Desde la perspectiva de la viabilidad, el estudio es factible: los recursos tecnológicos están disponibles en el laboratorio de redes de la Universidad EAN, las herramientas de software (Snort 3.x, Kali Linux, Wireshark, Python) son de código abierto y gratuitas, el equipo investigador cuenta con los conocimientos técnicos necesarios, y el cronograma de 12 semanas es coherente con el calendario académico del primer semestre de 2026.

REFERENCIAS

ACIS — Asociación Colombiana de Ingenieros de Sistemas. (2025, junio). Colombia, el cuarto país con más ciberataques en América Latina: 36.000 millones de intentos en 2024. https://www.acis.org.co/blog/noticias-2/colombia-el-cuarto-pais-con-mas-ciberataques-en-america-latina

Anderson, L. W. & Krathwohl, D. R. (Eds.). (2001). A taxonomy for learning, teaching, and assessing: A revision of Bloom's taxonomy of educational objectives. Longman.

Andress, J. (2019). The basics of information security (2nd ed.). Syngress.

Beale, J., Baker, A. & Caswell, B. (2015). Snort intrusion detection and prevention toolkit. Syngress.

Behl, A. & Behl, K. (2017). Cybersecurity and cyberwar: What everyone needs to know. Springer.

Bernal, C. A. (2016). Metodología de la investigación: Administración, economía, humanidades y ciencias sociales (4.ª ed.). Pearson.

Braun, V. & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Campbell, D. T. & Stanley, J. C. (1966). Experimental and quasi-experimental designs for research. Houghton Mifflin.

Cisco Talos — Snort Team. (2024). SnortML: Open-source machine learning detection engine for Snort 3. Snort Blog. https://blog.snort.org/2024/

Cochran, W. G. (1977). Sampling techniques (3rd ed.). Wiley.

Creswell, J. W. & Creswell, J. D. (2018). Research design: Qualitative, quantitative, and mixed methods approaches (5th ed.). SAGE.

Creswell, J. W. & Plano Clark, V. L. (2018). Designing and conducting mixed methods research (3rd ed.). SAGE.

DeVellis, R. F. (2017). Scale development: Theory and applications (4th ed.). SAGE.

Denzin, N. K. (1978). The research act: A theoretical introduction to sociological methods (2nd ed.). McGraw-Hill.

ERC Colombia. (2024). Colombia: cuarto país con más ciberataques en América Latina — 36.000 millones de intentos en 2024. La República. https://www.larepublica.co/internet-economy/colombia-tuvo-36-000-millones-de-ciberataques-4178202

Escobar, J. & Cuervo, Á. (2008). Validez de contenido y juicio de expertos: Una aproximación a su utilización. Avances en Medición, 6(1), 27–36.

Field, A. (2018). Discovering statistics using IBM SPSS statistics (5th ed.). SAGE.

Flick, U. (2019). An introduction to qualitative research (6th ed.). SAGE.

Gaddam, S. R. & Nandhini, S. R. (2017). An analysis of various Snort-based techniques to detect and prevent intrusions in networks. International Journal of Computer Science Engineering, 5(1), 120–127.

García-Teodoro, P., Díaz-Verdejo, J., Macià-Fernández, G. & Vázquez, E. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. Computers & Security, 28(1–2), 18–28. https://doi.org/10.1016/j.cose.2008.08.003

Hair, J. F., Black, W. C., Babin, B. J. & Anderson, R. E. (2019). Multivariate data analysis (8th ed.). Cengage.

Hernández-Sampieri, R. & Mendoza, C. (2018). Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta. McGraw-Hill.

IBM Security. (2024). Cost of a Data Breach Report 2024. IBM Corporation.

International Organization for Standardization. (2013). ISO/IEC 27001: Information security management systems — Requirements. ISO.

Islam, M. M. & Islam, M. Z. (2024). Quantitative evaluation of Snort IDS rule effectiveness against DDoS, brute-force, and MITM attacks in a controlled lab network. American Journal of Scholarly Research and Innovation, 1(1). https://researchinnovationjournal.com/index.php/AJSRI/article/view/112

Kerlinger, F. N. & Lee, H. B. (2002). Investigación del comportamiento: Métodos de investigación en ciencias sociales (4.ª ed.). McGraw-Hill.

Kim, D. & Solomon, M. (2014). Fundamentals of information systems security (2nd ed.). Jones & Bartlett Learning.

Kizza, J. M. (2020). Guide to computer network security (5th ed.). Springer.

Landis, J. R. & Koch, G. G. (1977). The measurement of observer agreement for categorical data. Biometrics, 33(1), 159–174.

Lawshe, C. H. (1975). A quantitative approach to content validity. Personnel Psychology, 28(4), 563–575.

Ley 1581 de 2012. (2012, octubre 17). Por la cual se dictan disposiciones generales para la protección de datos personales. Congreso de Colombia. Diario Oficial N.° 48.587.

MobileTime Latinoamérica. (2026, abril). Colombia reduce en 48% los ciberataques en 2025, pero aumentan amenazas con IA. https://mobiletime.la/noticias/07/04/2026/colombia-reduce-ciberataques/

Montgomery, D. C. (2017). Design and analysis of experiments (9th ed.). Wiley.

National Institute of Standards and Technology. (2007). Guide to intrusion detection and prevention systems (IDPS) (NIST Special Publication 800-94). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-94

National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity (NIST Cybersecurity Framework v1.1). https://doi.org/10.6028/NIST.CSWP.04162018

Ñaupas, H., Valdivia, M., Palacios, J. & Romero, H. (2019). Metodología de la investigación cuantitativa-cualitativa y redacción de la tesis (5.ª ed.). Ediciones de la U.

Nunnally, J. C. (1978). Psychometric theory (2nd ed.). McGraw-Hill.

Pfleeger, C. P. & Pfleeger, S. L. (2015). Security in computing (5th ed.). Pearson.

Robbani, et al. (2025). Implementation of intrusion detection system using Snort and log visualization using ELK Stack. International Journal of Engineering, Science and Information Technology (IJESTY), 5(1). https://doi.org/10.35746/jtim

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

Sanders, C. (2017). Practical packet analysis: Using Wireshark to solve real-world network problems (3rd ed.). No Starch Press.

Scarfone, K. & Mell, P. (2007). Guide to intrusion detection and prevention systems (IDPS) (NIST SP 800-94). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-94

Sommer, R. & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. Proceedings of the IEEE Symposium on Security and Privacy. https://doi.org/10.1109/SP.2010.25

Stallings, W. (2018). Network security essentials: Applications and standards (6th ed.). Pearson.

Stallings, W. & Brown, L. (2018). Computer security: Principles and practice (4th ed.). Pearson.

Stevens, S. S. (1946). On the theory of scales of measurement. Science, 103(2684), 677–680.

Taylor, S. J. & Bogdan, R. (1987). Introducción a los métodos cualitativos de investigación: La búsqueda de significados. Paidós.

Tripathy, S. S. & Behera, B. (2025). Evaluation of future perspectives on Snort and Wireshark as tools and techniques for intrusion detection system. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5048278

Verizon. (2024). Data breach investigations report 2024. Verizon Communications Inc.

Whitman, M. E. & Mattord, H. J. (2021). Principles of information security (7th ed.). Cengage Learning.

Yin, R. K. (2018). Case study research and applications: Design and methods (6th ed.). SAGE.