PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

Escuela de Posgrado

METODOLOGÍA BASADA EN POLÍTICAS DE QoS EN SDN PARA EL CONTROL DE AMENAZAS INTERNAS Y MEJORA DEL RENDIMIENTO EN INTRANETS ACADÉMICAS.

Tesis para obtener el grado académico de Doctora en Ingeniería que presenta:

Ruth Genoveva Barba Vera

Asesor:

Carlos Bernardino Silva Cárdenas

Lima, 2025

Informe de Similitud

Yo, ……Carlos Bernardino Silva Cárdenas……, docente de la Escuela de Posgrado de la Pontificia Universidad Católica del Perú, asesor(a) de la tesis/el trabajo de investigación titulado: METODOLOGÍA BASADA EN POLÍTICAS DE QoS EN SDN PARA EL CONTROL DE AMENAZAS INTERNAS Y MEJORA DEL RENDIMIENTO EN INTRANETS ACADÉMICAS, de la autora Ruth Genoveva Barba Vera, dejo constancia de lo siguiente:

- El mencionado documento tiene un índice de puntuación de similitud de 11%. Así lo consigna el reporte de similitud emitido por el software *Turnitin* el 09/05/2025.
- He revisado con detalle dicho reporte y la Tesis o Trabajo de Suficiencia Profesional, y no se advierte indicios de plagio.
- Las citas a otros autores y sus respectivas referencias cumplen con las pautas académicas.

Lugar y fecha: Lima, 09 mayo 2025

Apellidos y nombres del asesor / de la asesora: Silva Cárdenas, Carlos Bernardino	
DNI:08014721	Firma
ORCID: https://orcid.org/0000-0003-4653-0915	

DEDICATORIA

A mis hijos Carlos Gabriel y Luis Esteban, por ser el motor que mueve mi vida y me impulsa a creer que los sueños se hacen realidad en la medida de cuanto estamos dispuestos a luchar por ellos.

A mi esposo por ser mi compañero de vida, mi amigo y cómplice incondicional, quien me ha impulsado cuando deseaba desistir. Mi eterno amor, Carlos.

A mi padres, Jorge y Flor María, por estar siempre presentes en mi vida. Ser el principio de todo, la inspiración y la energía que me mueve.

AGRADECIMIENTO

A mi alma mater Escuela Superior Politécnica de Chimborazo “ESPOCH”, por apoyar mis estudios para ser mejor cada día y brindar mi contingente al servicio de los demás, enmarcado en el Saber, Ser y Servir.

A mis colegas Marcelo Criollo y Norma Aimacaña por apoyarme en este sueño y ser compañeros fieles de investigación e innovación.

A mi tutor profesor Carlos Silva Cárdenas, por guiarme hacia la consecución de mis objetivos.

A todos quienes me han brindado su guía y han sido aporte a este trabajo de investigación.

RESUMEN

El crecimiento acelerado de las intranets en campus académicos ha generado la necesidad de mecanismos eficaces para identificar y mitigar amenazas internas (insiders threats), las cuales afectan tanto la seguridad como el desempeño de la red. La Revisión Sistemática de Literatura (RSL) realizada en esta tesis, que abarcó 117 estudios indexados en las bases de datos ACM, SCOPUS e IEEE, evidenció una fragmentación metodológica y la ausencia de propuestas integrales validadas en entornos reales, lo que limita la estandarización de soluciones.

Frente a esta problemática, se propone una metodología estructurada en cuatro etapas para el control de amenazas internas en intranets académicas, basada en Redes Definidas por Software (SDN) y políticas de Calidad de Servicio (QoS). Esta metodología comprende: (1) diagnóstico de seguridad del canal humano a partir de la adaptación del modelo OSSTMM v3.02; (2) detección en tiempo real mediante NIDS-SNORT y verificación de vulnerabilidades con Nexpose; (3) selección de la amenaza a mitigar; y (4) aplicación de políticas de QoS con ACLs en el controlador FloodLight, en un entorno experimental con equipos físicos.

Los resultados evidencian una mejora significativa en métricas de rendimiento, particularmente en la reducción del delay, así como mejoras en jitter, pérdida de paquetes y ancho de banda. Esta propuesta no solo mejora la eficiencia operativa de la red, sino que constituye un marco metodológico replicable, adaptable y de bajo costo, que responde a las limitaciones actuales y fortalece la ciberseguridad en instituciones educativas.

ÍNDICE DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

PRIMERA PARTE: MARCO DE LA INVESTIGACIÓN

CAPÍTULO 1: INTRODUCCIÓN

La presente tesis aborda los desafíos estructurales que enfrentan las arquitecturas de red tradicionales en campus académicos, particularmente su limitada capacidad para gestionar de manera eficiente y segura el crecimiento de dispositivos móviles, servicios digitales, aplicaciones y entornos virtuales. Estas limitaciones se traducen en sobrecargas de red, políticas inconsistentes, escasa escalabilidad y una creciente dependencia de tecnologías propietarias, factores que comprometen la calidad del servicio y la seguridad de la información. Esta situación se agrava ante la presencia de amenazas internas (insider threats), cuya detección y control oportuno aún representan una brecha evidente tanto en la literatura especializada como en las prácticas implementadas en el sector educativo.

El presente trabajo de investigación es el resultado de siete años de estudio. Los dos primeros se centraron en la revisión del estado del arte y en el desarrollo y validación del protocolo de Revisión Sistemática de Literatura (RSL) para el análisis de amenazas internas en intranets académicas. A partir del tercer año, la investigación evolucionó hacia el diseño y validación de una metodología inédita para la implementación de políticas de Calidad de Servicio (QoS) en Redes Definidas por Software (SDN), orientada específicamente al control de amenazas internas en estos entornos.

Frente a esta problemática, diversas investigaciones han señalado que las SDN ofrecen una alternativa flexible y escalable, al permitir una gestión centralizada de la red y la aplicación dinámica de políticas de QoS. No obstante, su aplicación con fines de ciberseguridad en contextos académicos requiere ser validada empíricamente mediante modelos metodológicos replicables.

Cabe destacar que el principal aporte de esta tesis no radica en el desarrollo de un nuevo algoritmo, sino en el diseño, implementación y validación empírica de una metodología sistemática para la detección y control de amenazas internas en intranets académicas. Esta metodología articula herramientas existentes de análisis de red como NIDS-SNORT, Nexpose y políticas de QoS con ACLs, dentro de un framework replicable y adaptable, lo que constituye un avance metodológico relevante ante la falta de soluciones integradas y probadas en entornos reales.

En este marco, la presente tesis propone y valida una metodología de cuatro etapas para el control de amenazas internas en intranets académicas, que comprende: (1) diagnóstico del canal humano utilizando OSSTMM v3.02 adaptado, (2) detección de amenazas con SNORT, un sistema de detección de intrusos en red (NIDS) que permite el monitoreo y análisis del tráfico en tiempo real mediante reglas predefinidas, y validación mediante Nexpose, una herramienta de escaneo de vulnerabilidades que facilita la identificación, clasificación y priorización de debilidades en la red; (3) selección de amenazas críticas, y (4) aplicación de políticas de QoS con listas de control de acceso (ACLs) en el controlador FloodLight, evaluadas en un entorno experimental con infraestructura real.

Los resultados obtenidos evidencian mejoras significativas en el rendimiento de la red: reducción del delay en 2,5 %, disminución del jitter, incremento del ancho de banda en 2,2 % y reducción de pérdida de paquetes en 1,21 %. Además, se identificaron vulnerabilidades críticas, como el mayor riesgo observado en la VLAN Estudiante (15,34 %) y la coincidencia del 10 % en amenazas DoS entre distintos segmentos de red, lo cual fundamentó la selección de esta amenaza, utilizada en la fase de validación experimental.

En conjunto, esta investigación ofrece una solución técnica, práctica y aplicable en instituciones con recursos limitados, aportando un marco replicable que responde a la falta de metodologías estandarizadas para el control de amenazas internas. Además, plantea una base sólida para futuras investigaciones orientadas a la integración de inteligencia artificial y la formalización de un estándar metodológico en redes académicas.

Este capítulo se estructura en seis secciones: la primera aborda los antecedentes del estudio; la segunda, la realidad problemática y las preguntas de investigación; la tercera, los objetivos general y específicos; la cuarta, la justificación y viabilidad; la quinta, la hipótesis de investigación; y la sexta, la metodología empleada para el desarrollo del proyecto.

1.1 Antecedentes

El desarrollo inconmensurable de dispositivos móviles, la virtualización de servidores y servicios en la nube impulsan a la industria de las redes a reexaminar las

arquitecturas de redes tradicionales. Debido a que muchas son jerárquicas, construidas con niveles de conmutadores Ethernet dispuestos en una estructura de árbol que predominaba en el modelo cliente-servidor, pero una arquitectura estática de este tipo no se adapta a las necesidades de almacenamiento e informática dinámicas de los entornos de operadores, campus y centros de datos empresariales de hoy en día.(Y. Zhang et al., 2022)

Entre las tendencias informáticas que impulsan la necesidad de un nuevo paradigma de red están:

- Acceso universal. Las aplicaciones y usuarios requieren acceso al contenido corporativo desde cualquier dispositivo, lugar y momento, lo que exige una gestión del tráfico más flexible y descentralizada (Y. Zhang et al., 2022).
- Exceso de dispositivos personales. El crecimiento en el número de dispositivos conectados ha expuesto las limitaciones de las arquitecturas centralizadas, demandando soluciones de baja latencia y alta eficiencia (Oktian et al., 2021)
- El auge de los servicios en la nube, que debe realizarse en un entorno de mayor seguridad, cumplimiento y requisitos de auditoría, en un entorno de nube cada vez más complejo (Garg et al., 2021).
- El escalado elástico de recursos informáticos, de almacenamiento y de red, idealmente desde un conjunto similar de herramientas y con un punto de vista común. (B. Ali et al., 2021)
- La Big Data, la creciente cantidad de datos exige un mayor ancho de banda y conectividad fiable extremo a extremo, para el procesamiento de un gran volumen de datos (Angel et al., 2021).

Las arquitecturas de red existentes no se diseñaron para cumplir con los requisitos de los usuarios, empresas y operadores actuales; más bien, los diseñadores de redes están restringidos por las limitaciones de las redes actuales, que incluyen: complejidad, políticas inconsistentes, incapacidad para escalar, dependencia del proveedor.

Complejidad: Los protocolos de red actuales tienden a definirse de manera aislada, cada uno resolviendo problemas específicos sin un enfoque unificado. Esto genera desafíos significativos en la gestión y la configuración dinámica de las redes(Zou et al., 2021).

Políticas Inconsistentes: La implementación de políticas de red coherentes a través de múltiples dispositivos puede llevar tiempo y ser propensa a errores, lo que aumenta los riesgos de seguridad y cumplimiento (Kaliyamurthy et al., 2021).

Incapacidad para escalar: A medida que las demandas de los centros de datos crecen, la infraestructura de red existente enfrenta dificultades para escalar de manera eficiente sin incrementar excesivamente la complejidad(Ometov et al., 2022).

Dependencia del proveedor: Las empresas buscan implementar nuevas capacidades de manera ágil, pero a menudo están limitadas por la dependencia de ciclos de productos y la falta de estándares abiertos en equipos de red(Zou et al., 2021).

Este desajuste entre los requisitos del mercado y las capacidades de la red ha llevado a la industria a un punto de inflexión. En respuesta, se ha creado la arquitectura de SDN que permite una mayor flexibilidad y capacidad de respuesta.(Kaliyamurthy et al., 2021)

La evolución acelerada de redes que sirven a empresas e instituciones académicas, en la que se maneja aplicaciones, servicios con diferentes usuarios y requerimientos de red y pese a los controles establecidos por los Departamentos de Tecnología en éstos campus, existe una degradación en los servicios y congestión (Barba et al., 2019) que demanda también mayor control en la seguridad de la red para evitar amenazas como los insiders o amenazas internas que son de las más difíciles de controlar.

La Common Sense Guide to Mitigating Insider Threats, Seventh Edition de la Universidad Carnegie Mellon, cita los resultados de sus estudios en casos de amenazas internas, donde los supervisores notaron comportamientos menores pero inapropiados en el lugar de trabajo, pero no actuaron porque el comportamiento no violaba la política. Sin embargo, la falta de definición o aplicación de políticas de seguridad provoca que los usuarios insiders cometan violaciones repetidas que aumentaron en gravedad y el riesgo de daño significativo a la organización. Por ello las organizaciones deben aplicar políticas y procedimientos para todos los usuarios, incluyendo la investigación consistente y la respuesta a las violaciones de las reglas.(Software Engineering Institute, 2022)

Frente a este panorama las redes que sirven a los campus académicos deben proveer seguridad a todo nivel, en la intranet se considera el diseño de políticas de seguridad como las ACLs, no obstante, el inconveniente es que estas no cubren todos los sucesos que se pueden dar a lo interno de la red, pues se considera que el mayor problema de seguridad en la intranet es un insider, definido como " persona con acceso autorizado o conocimiento especial de una organización que utilice ese acceso o entendimiento para causar daño a la organización(Agency Cybersecurity and Infrastructure Security, 2020)". La falta de mecanismos adecuados para controlar y aplicar políticas de seguridad entre los usuarios de confianza agrava estos riesgos(Software Engineering Institute, 2022).

Las redes SDN representan un paradigma innovador que pretende sustituir las redes tradicionales al separar la lógica de control de los dispositivos de red subyacentes, permitiendo así la centralización del control y la programación de la red (Toro et al., 2022). Ante ello y con la evolución de la tecnología de red, SDN puede aliviar estos desafíos, ofreciendo flexibilidad y la habilidad de desarrollar nuevas capacidades de forma rápida y rentable.(Toro et al., 2022). Permitiendo quitar el Plano de Control (inteligencia) de los equipos de red y centralizarlo en un elemento llamado Controlador, el cual tiene conocimiento de toda la red, por lo que hace posible un mejor uso de los recursos de esta, haciendo que sea flexible y escalable en el Plano de Datos. SDN, sugiere una centralización lógica del control de la red y permite programarla dando respuesta al problema de la complejidad de las redes actuales que hace que sea muy difícil aplicar un conjunto consistente de acceso, seguridad, QoS y otras políticas a usuarios cada vez más móviles, lo que deja a la empresa vulnerable a violaciones de seguridad, incumplimiento de regulaciones y otras consecuencias negativas.(Mhamdi & Isa, 2024)

En este contexto, esta tesis propone un marco metodológico basado en políticas de QoS en SDN, estructurado en cuatro etapas, para abordar las limitaciones mencionadas. Este marco no solo busca mitigar las amenazas internas, sino también establecer una base para futuros estándares en la gestión de ciberseguridad en intranets académicas contribuyendo a cerrar la brecha en la investigación sobre la falta de metodologías prácticas y validadas para el control de amenazas internas en estos entornos.

1.2 Problemática

El desarrollo de redes en campus académicos enfrenta desafíos significativos debido a la creciente demanda de aplicaciones, servicios, dispositivos móviles, y la implementación de políticas como Bring Your Own Device (BYOD). Estas demandas superan la capacidad de las soluciones actuales para brindar agilidad, desempeño y una buena experiencia de usuario. A pesar de los controles establecidos por los Departamentos de Tecnología, hay una degradación en los servicios y desbordamientos que requieren una gestión de más recursos y una planificación adecuada a las demandas actuales de las redes (Barba et al., 2019).

El estudio de la Corporación Ecuatoriana para el Desarrollo de la Investigación y la Academia (CEDIA) acerca del estado de tecnologías de la información y la comunicación (TIC) en universidades ecuatorianas revela preocupantes deficiencias:

> "El *17% de las universidades aún no tiene una política de seguridad debidamente formalizada y aprobada*. El 69% tiene un responsable de seguridad de la información y más de la mitad realizan auditorías específicas de seguridad de la información. Además, el 55% cuenta con el servicio de respuesta a incidentes de seguridad (CSIRT) proporcionado por CEDIA, mientras que solo el 10% tiene uno propio. El 69% no cuenta con un plan de contingencia y el 36% no cuenta con un plan de continuidad de los servicios. Dada la importancia que están cobrando las TIC en las universidades, estos son riesgos que las universidades no deberían correr". (Cadena et al., 2019, p. 25)

Nuevas tecnologías como las SDN innovan la gestión de redes al automatizar y proporcionar una vista centralizada en tiempo real del estado de la red a través de APIs abiertas. Esta capacidad permite una administración de red dinámica y eficiente, facilitando el proceso de control y mejorando la respuesta a incidentes(Correa Chica et al., 2020). Además, SDN añade valor a la seguridad al interactuar con switches y routers mediante APIs, permitiendo implementar nuevas medidas de seguridad y facilitando la detección de ataques. No obstante, la centralización del control en SDN puede incrementar la superficie de ataque y actualmente carece de mecanismos de seguridad robustos, lo que plantea retos significativos para su implementación a gran escala(J. Kim et al., 2023).

La centralización en las redes definidas por software (SDN) ofrece importantes ventajas, como la optimización en la gestión de ataques de Denegación de Servicio (DoS), al proporcionar una visión integral de la topología de la red y mejorar la correlación de datos de tráfico, lo que facilita una detección más precisa de

amenazas(Segura et al., 2021). Además, esta centralización reduce los costos de hardware y aumenta la flexibilidad de la red (Chuang & Ye, 2023). No obstante, también introduce vulnerabilidades, especialmente debido a la inexperiencia de los defensores y la inmadurez de la tecnología. La separación de los planos de control y datos, con un controlador centralizado, expone la red a ataques que pueden explotar esta flexibilidad(Yuan et al., 2024). Por tanto, aunque la centralización de SDN mejora la gestión y la programabilidad del control, también exige estrategias y mecanismos de seguridad robustos para proteger el plano de control centralizado contra ataques maliciosos.

La ausencia de estándares metodológicos ampliamente adoptados en la gestión de amenazas internas en intranets académicas subraya la urgencia de propuestas como la presentada en esta tesis, que integra herramientas avanzadas y políticas de QoS validadas experimentalmente para abordar esta problemática.

1.2.1 Pregunta de investigación

La pregunta principal de la investigación del proyecto de tesis doctoral es:

¿Cómo se puede plantear políticas de QoS en Software Defined Network (SDN) para realizar el control de insiders threat (amenazas internas), mejorando el rendimiento en intranets académicas?

A partir de esta pregunta general, se plantean los siguientes objetivos:

1.3 Objetivos

1.3.1 Objetivo General

Formular y evaluar políticas de QoS en SDN para facilitar el control de insiders threat en intranets académicas que permitan mejorar el rendimiento de la red.

1.3.2 Objetivos Específicos

1.- Identificar las principales amenazas internas en intranets académicas.

2.-Seleccionar un ataque insider a controlar a través de políticas de QoS en SDN.

3.- Estudiar la implementación de políticas de QoS en redes de campus tradicionales y SDN.

4.- Evaluar las políticas de QoS para el control de la amenaza seleccionada en el escenario de pruebas SDN.

1.4 Justificación

1.4.1 Resultados esperados

La Tabla 1, muestra los objetivos específicos, así como los resultados esperados del trabajo de investigación y el medio de verificación.

Tabla 1: Resultados esperados en el trabajo de investigación doctoral.

Objetivos Específicos	**Resultados Esperados**	**Medio de verificación**
1.- Identificar las principales amenazas internas en intranets académicas.	Identificar las amenazas internas en una intranet de campus académico.	1.- Protocolo de Revisión Sistemática de literatura (RSL) de amenazas insiders en la intranet de campus académico en base a (Budgen & Brereton, 2006) 2.- Resultados de la aplicación del Protocolo de Revisión Sistemática de Literatura (RSL) de amenazas internas en intranets académicas. 3.- Amenazas identificadas como resultado del análisis de la intranet del campus académico.
2.- Seleccionar una amenaza insider a controlar a través de políticas de QoS en SDN.	Elegir una amenaza insider a controlar en base de los resultados del primer objetivo, a través a políticas de QoS en SDN.	1.- Documentación.
3.- Estudiar la implementación de políticas QoS en redes de campus tradicionales y SDN.	Establecer el proceso de implementación de políticas de QoS en redes tradicionales y SDN.	1.- Aplicación del proceso de implementación de políticas de QoS en redes tradicionales y SDN para el control de la amenaza seleccionada en el escenario de pruebas.
4.- Evaluar las políticas de QoS para el control de la amenaza seleccionada en el escenario de pruebas SDN.	1.- Controlar la amenaza seleccionada a través del proceso de implementación de políticas de QoS en el escenario de pruebas SDN.	1.- Resultados del control de la amenaza seleccionada a través del proceso de implementación de políticas de QoS en el escenario de pruebas SDN.

Fuente: Elaboración propia

1.4.2 Alcance y limitaciones

Alcance

La presente tesis doctoral tiene como objetivo central el diseño y validación de una metología general para el análisis y control de amenazas internas o insiders threats, que existen en la intranet de un campus académico, integrando enfoques de redes definidas por software (SDN) y políticas de calidad de servicio (QoS). Esta respuesta metodológica surge como respuesta a la ausencia de un marco estandarizado identificado mediante una Revisión Sistemática de la Literatura (RSL) , aplicando el modelo de (Kitchenham & Charters, 2007), utilizada para la revisión de la literatura en el área informática. Para ello se desarrolló un protocolo de revisión sistemática de literatura (RSL) de insiders threats en la intranet de un campus académico que se incluye en el Anexo B.

Para validar empíricamente la metodología, se seleccionó como caso de estudio la intranet de la Escuela Superior Politécnica de Chimborazo (ESPOCH). Se realizó un análisis en tiempo real del tráfico de red del campus, que permitió identificar amenazas reales y contrastarlas con los hallazgos de la RSL. Posteriormente, se seleccionó la amenaza, y se aplicó el modelo de control propuesto mediante políticas de QoS en un entorno controlado de pruebas con equipos SDN.
De este modo, el estudio no se limita al caso de la ESPOCH, sino que lo utiliza como entorno de validación de una propuesta metodológica más amplia, replicable y adaptable a otras instituciones académicas con condiciones técnicas similares.

Limitaciones

Entre las limitaciones al alcance de la tesis están las siguientes:

La propuesta para el control de la amenaza no se implementó directamente en la intranet del campus académico, debido a las políticas de funcionamiento y administración de la institución, que reservan estas configuraciones exclusivamente para el Departamento de Tecnologías de la Información y Comunicación (DTIC) del campus. Además, es esencial mantener la continua operatividad de la intranet de campus académico, para asegurar la disponibilidad de los servicios y sistemas informáticos de la institución.

Para superar esta situación, se implementó un escenario de pruebas SDN con equipos reales, orientada a controlar una amenaza identificada en el análisis de campus académico y que coincidiera con los resultados de la RSL. La amenaza interna seleccionada fue DoS. El proceso propuesto de implementación de políticas de QoS para el control de amenazas insiders fue aplicado, evaluado y documentado. A pesar de las restricciones mencionadas, los resultados obtenidos en el escenario de pruebas son relevantes y válidos para evaluar la efectividad de las políticas de QoS proporcionando una base sólida para futuras implementaciones en entornos reales. La validez científica, ética e institucional de esta fase está respaldada en el Anexo J, donde se documenta el acompañamiento técnico del DTIC y el cumplimiento de principios éticos en la intervención y análisis de la red.

1.4.3 Justificación y viabilidad

En el presente apartado se realiza la justificación en base a la revisión teórica, pruebas prácticas, impacto social, viabilidad técnica, económica y estudio de necesidades.

Justificación

La ciberseguridad es crucial en la actualidad, ya que la interconexión de las redes expone tanto la infraestructura crítica como los derechos humanos básicos. Los gobiernos deben implementar políticas nacionales de ciberseguridad que promuevan tanto el crecimiento como la seguridad tecnológica. A pesar de los avances globales en esta materia, los países en desarrollo continúan enfrentando desafíos significativos debido a la falta de expertos capacitados y a recursos educativos insuficientes (Obasi et al., 2024). Estos países necesitan marcos de ciberseguridad robustos y sostenibles para mitigar eficazmente las amenazas emergentes.

El Global Cybersecurity Index (GCI) 2024 (ITU, 2024) insta a los países a evaluar continuamente sus fortalezas y debilidades en ciberseguridad mediante el desarrollo de CIRTs, la actualización de estrategias y la participación multisectorial. En GCI 2020 (ITU, 2021) Ecuador se ubicó en el puesto 48 de 193 países y quinto en América Latina, lo que reflejaba un compromiso significativo. Sin embargo, en el GCI 2024 se clasifica en el Nivel 2, evidenciando avances, pero también la necesidad de mejorar en aspectos técnicos y de capacitación. En respuesta, el país ha fortalecido su infraestructura de telecomunicaciones y promovido la seguridad de la información a

través del "Libro Blanco de la Sociedad de la Información y del Conocimiento" (LBSIC) (MINTEL, 2018) y la Política Nacional de Ciberseguridad.(Política de Ciberseguridad, 2021) alineadas a los Objetivos de Desarrollo Sostenible.

En este contexto, resulta esencial prestar especial atención a los entornos de campus universitarios, que constituyen sistemas de red singulares caracterizados por la alta heterogeneidad de usuarios y dispositivos. La integración de estudiantes, docentes, administrativos e investigadores genera una diversidad considerable, que abarca desde computadoras personales hasta dispositivos móviles. Además, la dinámica inherente a estos espacios se traduce en elevadas demandas de conectividad y movilidad, lo que conlleva una infraestructura de red compleja y segmentada, organizada en múltiples subredes o VLANs para garantizar el acceso diferenciado a recursos críticos.

Ante estos desafíos, la tecnología SDN (Software Defined Networking) emerge como una solución innovadora para optimizar la gestión de redes en entornos académicos. Su gestión centralizada y capacidad de programabilidad facilitan la implementación de políticas de Calidad de Servicio (QoS) para mejorar el rendimiento y la seguridad de las intranets académicas, contribuyendo al desarrollo de un marco metodológico replicable que sirva como estándar para la gestión de amenazas internas en entornos similares. Además, la adopción de SDN, como tecnología de próxima generación, impulsa la ciberseguridad y promueve un acceso inclusivo a Internet, alineándose con lo establecido por MINTEL y la Sociedad de la Información en Ecuador. Al abordar de manera integral tanto las particularidades de los sistemas de campus universitarios como las oportunidades y desafíos que presenta SDN, se busca potenciar una infraestructura de red segura, eficiente y adaptativa que responda a las necesidades actuales y futuras de la comunidad académica.

Viabilidad

El proyecto de tesis es técnicamente viable, parte de un profundo análisis del estado de arte para identificar las amenazas internas en intranets de redes que sirven a los campus académicos utilizando la metodología de RSL de (Budgen & Brereton, 2006). La amenaza interna seleccionada para este estudio se basa en los resultados de la RSL detallados en la Tabla 40: Q1.2 Tipos de insiders threat o amenazas internas existentes en intranets académicas del campus en estudio, pag.182, que señala el ataque de Denegación de Servicio (DoS),como principal amenaza con el 13.68%.

Estos resultados se corroboraron con el análisis en tiempo real de la intranet, para ello se adaptó el Manual de Metodología de Pruebas de Seguridad de Código Abierto (OSSTMM Versión 3.02, por sus siglas en inglés)(Herzog, 2010) y se utilizó NIDS-SNORT (Snort - Network Intrusion Detection & Prevention System, 2016), con el objetivo de identificar las amenazas en la intranet de campus académico. Los resultados denotan una coincidencia del 10% en las vulnerabilidades DoS entre las VLANs Docente y Estudiante, detalladas en la Tabla 14: Análisis vulnerabilidades detectadas, pag. 108.

Para el control de la amenaza, se desarrolló y evaluó un proceso basado en políticas de QoS utilizando un algoritmo propuesto, aplicado en un escenario de pruebas con equipos reales SDN, demostrando la viabilidad y efectividad de la propuesta en mejorar la seguridad y rendimiento de las redes académicas.

1.5 Hipótesis

La implementación de políticas de QoS en SDN para facilitar el control de insiders threat mejora el rendimiento de la intranet académica.

La mejora a la que se refiere esta hipótesis implica una optimización integral del rendimiento de la intranet académica, abarca tanto aspectos técnicos, como de seguridad, mediante una mejor gestión y mitigación de amenazas internas. El aporte investigativo proporciona una base sólida para la aplicación práctica de medidas de seguridad cibernética en intranets, abriendo un campo amplio para futuras investigaciones en esta área.

1.6 Metodología de Investigación

La metodología propuesta se desarrolla con base en la necesidad identificada de un marco metodológico que permita gestionar amenazas internas en intranets académicas mediante políticas de QoS en SDN, abordando un vacío crítico en la literatura.

En la presente investigación se ha aplicado un tipo de estudio descriptivo, buscando desarrollar una fiel representación del fenómeno estudiado a partir de sus características para especificar las propiedades de este fenómeno bajo análisis. La

investigación también es experimental al tener por finalidad la búsqueda y consolidación del saber mediante análisis de los resultados de las pruebas realizadas en los escenarios de estudio.

El estudio propuesto presenta un enfoque cuantitativo, pues se generalizará los resultados a través de un diseño experimental, en el que se probará la hipótesis.
En base a lo expuesto, las fases del proyecto propuesto son: Investigación, Implementación e Innovación.

Fase de Investigación:

En esta fase existen propuestas en las que se aplica SDN para recopilar datos de tráfico en una red empresarial, así como en redes heredadas utilizando un único conmutador OpenFlow, con altos niveles de precisión.(Serag et al., 2024). Partiendo de estas propuestas, se recabó datos de la intranet académica para el análisis de los paquetes de red que permitió identificar las principales amenazas internas (insiders threat), utilizando el analizador en tiempo real de red NIDS SNORT.

Además, estudios recientes han explorado la implementación de reglas de QoS dentro de los controladores SDN como una medida para prevenir el acceso no autorizado y mitigar las acciones de usuarios malintencionados en la red (Hamad, 2023). En base a esta evidencia, la presente tesis propone la definición de políticas de QoS específicas para la intranet del campus académico, con el objetivo de evaluar su efectividad en el control de amenazas internas identificadas y su incidencia en el rendimiento de la red.

Para esta propuesta, se realizó el estudio de la tecnología SDN, su funcionamiento, requerimientos, analizando los controladores y seleccionando el más adecuado para la implementación del escenario experimental, pues se trabaja con equipos reales; a diferencia de la mayoría de los estudios donde los escenarios de prueba se implementan únicamente en el software Mininet, como Dawadi (2021) que se centra en el rendimiento de enrutamiento y la integración de redes heredadas para mejorar la seguridad mediante capacidades de enrutamiento más robustas (Dawadi et al., 2021)

Se analizó el estado del arte, mediante una RSL, siguiendo el método de (Kitchenham & Charters, 2007) y (Budgen & Brereton, 2006) para identificar las principales amenazas

existentes en intranets académicas. Este proceso se plasmó en un “Protocolo de RSL de amenazas internas en intranets académicas” que incluyen tres fases: planificación, ejecución e informe de la revisión, que se presenta en el Anexo B y cuyos resultados se describen en el capítulo tres de esta tesis.

A partir de los resultados del estudio de RSL sobre amenazas internas y el análisis de la data de la intranet de campus, se seleccionó la amenaza interna a controlar DoS. Este estudio se propone implementar y evaluar políticas de QoS en un entorno experimental SDN para mitigar esta amenaza y evaluar la incidencia en el rendimiento.

Fase de Implementación:

Se realizó una propuesta metodológica para el control de amenazas internas en intranets de campus académicas, que da respuesta al vacío determinado por la RSL que se detalla en el capítulo 4, mientras que la validación de la propuesta en el capítulo 5.

Partiendo del análisis de políticas de QoS en ambientes tradicionales, se planteó un flujograma que permite implementar políticas de QoS compatibles con las redes de campus SDN y tradicionales, con el objetivo de una posible integración futura.

Para el desarrollo de la propuesta de control de amenazas insiders se considera un escenario con equipos físicos en un ambiente SDN, donde se replica la amenaza DoS y se evalúan los parámetros de rendimiento. En una segunda prueba se implementa la política de control de la amenaza insider DoS y se evalúa la incidencia en rendimiento.

Este enfoque permitió determinar, mediante un análisis descriptivo e inferencial, la incidencia de la propuesta de control de amenazas internas en el rendimiento de la red.

Fase de Innovación:

Para la evaluación de la propuesta se planteó un escenario experimental utilizando equipos físicos SDN donde se implementa las políticas de QoS planteadas para el control de la amenaza interna a partir del estudio y el análisis previo; analizándose su incidencia en el rendimiento de la red a partir de: latencia, jitter, ancho de banda y

pérdida de paquetes, con lo que se genera un novedoso método para la implementación de políticas de QoS en redes de campus académicas con tecnología SDN, que mejoran el control de amenazas internas y el rendimiento de la intranet, desarrollado en el capítulo cuatro.

Para la validación de esta propuesta realizada en el capítulo 5, se aplica un diseño cuasiexperimental este término se refiere a diseños de investigación experimentales en los cuales los sujetos o grupos de sujetos de estudio no están asignados aleatoriamente, son grupos intactos, manipulan deliberadamente, al menos, una variable independiente para observar su efecto sobre una o más variables dependientes (Olulowo et al., 2020). Dentro de la estructura de los diseños cuasi experimentales se ha usado uno con preprueba-posprueba, como indica a continuación:

GE O1 X O2

GC O1 - O2

GE = Grupo experimental.
GC = Grupo testigo o control.
X = Tratamiento experimental.
- = Ausencia de tratamiento experimental.
O1= Preprueba o medición previa al tratamiento experimental.
O2 = Posprueba o medición posterior al tratamiento experimental.

Previo a exponer al grupo a la presencia de la variable independiente (X), se aplica una medición (preprueba: O1). Después del estímulo se aplica otras mediciones (O2, O3, O4), para analizar efectos a corto y mediano plazo.(D. F. Ali et al., 2023)
El objetivo es demostrar la hipótesis de investigación en el escenario experimental utilizando equipos SDN reales.

Las conclusiones y estudios futuros se detallan al final de los capítulos.

CAPÍTULO 2. MARCO TEÓRICO

En el presente capítulo se incluye una revisión de los conceptos principales que abarcan el estudio, como son las Redes Definidas por Software ó SDN, la intranet o redes que sirven a los campus académicos, políticas de Calidad de Servicio (QoS) en SDN y redes tradicionales, amenazas internas (insiders threat) y metodologías para la evaluación de seguridad de redes; con el objetivo de realizar una introducción al estado del arte que ocupa la presente tesis.

2.1 Red Definida por Software (SDN)

SDN ha sido reconocida por el MIT (Massachusetts Institute of Technology) como una tecnología innovadora que está transformando el mundo debido a su impacto significativo en la gestión de redes, ofreciendo una mayor flexibilidad, programabilidad y escalabilidad(Salti & Zhang, 2023). Esta tecnología se distingue por la inclusión del protocolo OpenFlow, considerado el núcleo de SDN, que permite evaluar y priorizar el tráfico de red, como video, datos y correos electrónicos, basándose en reglas específicas. Además, OpenFlow facilita el control centralizado del tráfico de la red, permitiendo, entre otras funciones, poner en cuarentena el tráfico de una computadora sospechosa de albergar virus, lo que mejora de manera sustancial la seguridad de la red(Mohammed & Jasim, 2020).

SDN ha llegado a un punto de inflexión crucial en la evolución de la infraestructura de redes, comenzando a reemplazar el modelo tradicional de red. Este cambio se debe a la capacidad de SDN para proporcionar un mayor nivel de flexibilidad y personalización, lo cual es esencial para satisfacer las exigencias de las nuevas tendencias en tecnología de la información, como la computación en la nube, la movilidad, las redes sociales y el video (M. Silva et al., 2023).

SDN se refiere a una forma de organizar la funcionalidad de una red informática, permite virtualizar la red, brindando mayor control y soporte a la ingeniería de tráfico(Sharma & Nag, 2023).

Funcionalidad de SDN

Los dos elementos involucrados en el reenvío de paquetes a través de routers son una función de control, que decide la ruta que toma el tráfico y su prioridad; y una

función de datos, que reenvía datos basados en la política de función de control. Antes de SDN, estas funciones se realizaban de manera integrada en cada dispositivo de red (router, bridge, switch, etc.). El control en una red tradicional se ejerce por medio de un protocolo de red de enrutamiento y control que se implementa en cada nodo de red. Este enfoque es relativamente inflexible y requiere que todos los nodos de red implementen los mismos protocolos. Con SDN, un controlador central realiza todas las funciones complejas, incluidos el enrutamiento, la nomenclatura, la declaración de directivas y las comprobaciones de seguridad (Khatri et al., 2023)

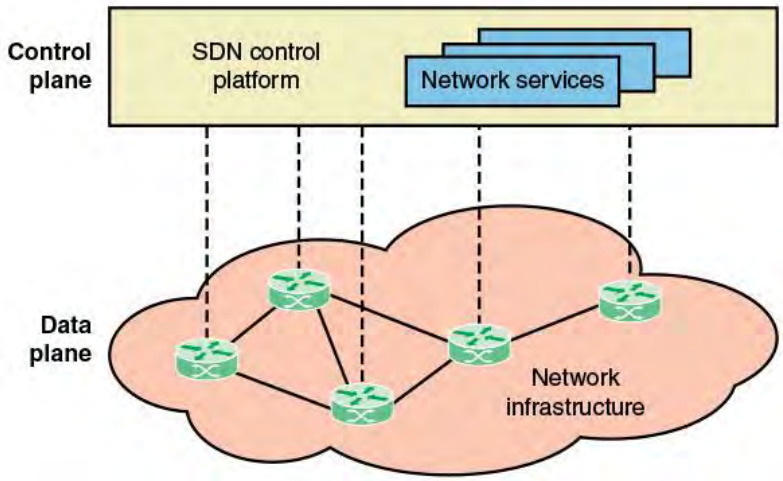


Figura 1: Redes definidas por software (Stallings et al., 2016)

La Figura 1, muestra el esquema SDN. Esto constituye el plano de control y consiste en uno o más controladores SDN, que son los que definen los flujos de datos que se producen en el plano de datos . Cada flujo a través de la red es configurado por el controlador, que verifica que la comunicación esté permitida por la política de red. Si el controlador permite un flujo solicitado por un sistema final, calcula una ruta para que el flujo tome y agrega una entrada para ese flujo en cada uno de los switches a lo largo de la ruta. Con todas las funciones complejas subsumidas por el controlador, los switches simplemente administran tablas de flujo cuyas entradas solo pueden ser rellenadas por el controlador. Los switches constituyen el plano de datos. La comunicación entre el controlador y los switches utiliza un protocolo estandarizado (Stallings et al., 2016).

La Figura 2, ilustra la Arquitectura definida por software (Stallings et al., 2016) que se muestra en la Figura 1, mostrando más detalles del enfoque SDN. El plano de datos consta de conmutadores físicos y virtuales. En ambos casos, los switches son

responsables de reenviar paquetes. La implementación interna de buffers, parámetros de prioridad y otras estructuras de datos relacionadas con el reenvío puede depender del proveedor. Sin embargo, cada switch debe implementar un modelo, o abstracción, de reenvío de paquetes que sea uniforme y esté abierto a los controladores SDN. Este modelo se define en términos de una interfaz de programación de aplicaciones (API) abierta entre el plano de control y el plano de datos (API en dirección sur). El ejemplo más destacado de una API abierta de este tipo es OpenFlow, un protocolo entre los planos de control y datos como una API mediante la cual el plano de control puede involucrar al protocolo OpenFlow. (Stallings et al., 2016)

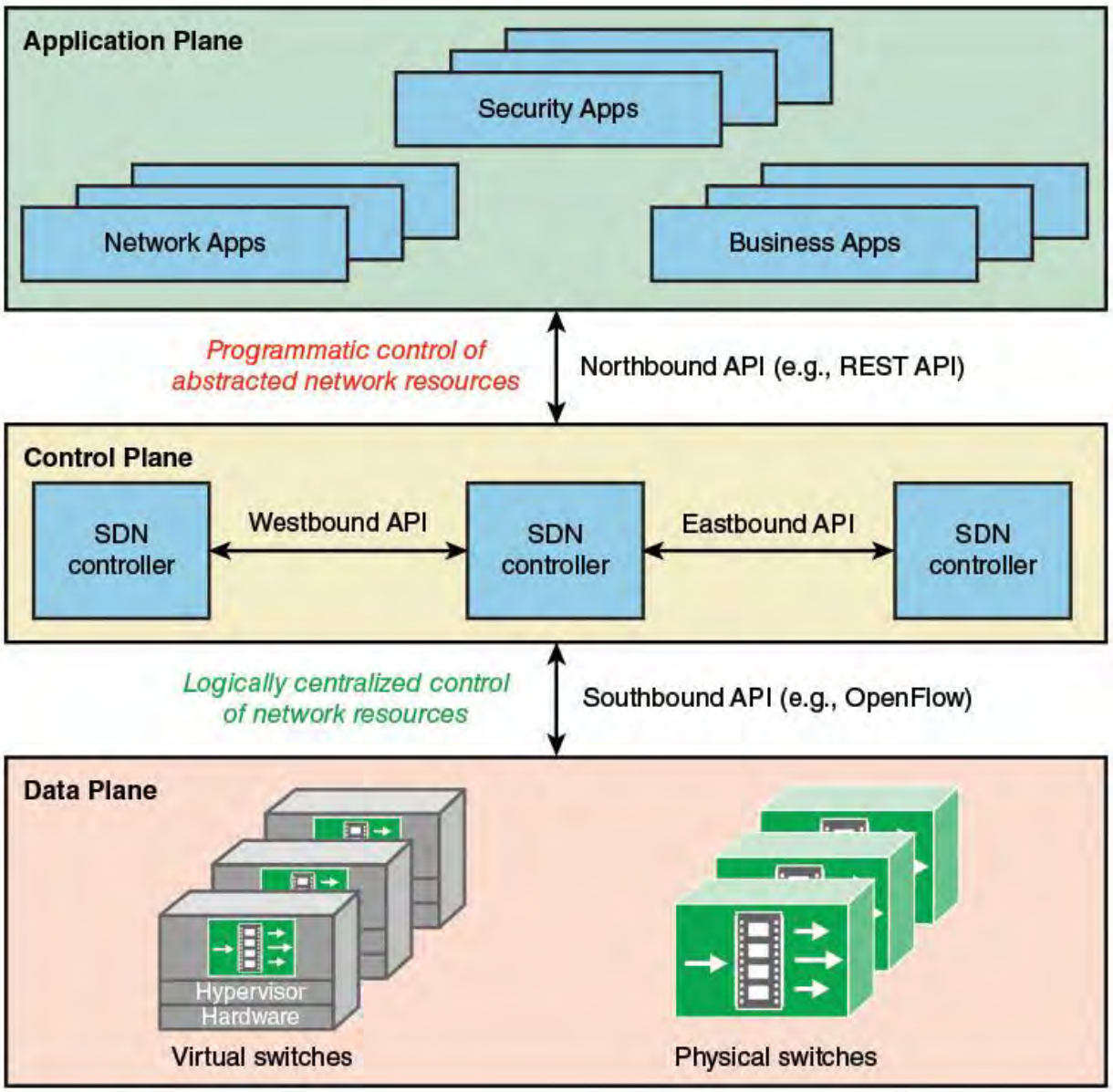


Figura 2: Arquitectura definida por software(Stallings et al., 2016)

Openflow

OpenFlow es tanto una especificación de la estructura lógica de la funcionalidad del plano de datos como un protocolo crucial dentro de la arquitectura de Redes Definidas por Software (SDN), sirviendo como una interfaz crítica entre los controladores SDN y los dispositivos de red (Albu-Salih, 2022).

Plano de datos SDN

El plano de datos SDN, conocido también como capa de recursos en ITU-T Y.3300 ó capa de infraestructura, es donde los dispositivos de reenvío de red realizan el transporte y el procesamiento de datos de acuerdo con las decisiones tomadas por el plano de control SDN. Los dispositivos de red en SDN se caracterizan por el reenvío simple, sin software incorporado para tomar decisiones autónomas. En lugar de ello, las reglas y políticas de enrutamiento son gestionadas por el plano de control, lo que permite una mayor flexibilidad y eficiencia en la gestión de la red (Siva et al., 2023).

Funciones del plano de datos

La Figura 3, muestra las funciones de los dispositivos de red del plano de datos (llamados conmutadores o elementos de red del plano de datos). Las funciones principales se enfocan hacia el control de flujo de los paquetes OpenFlow PDUs y las IP como TCP/IP, UPD/IP y otras que se describen a continuación.

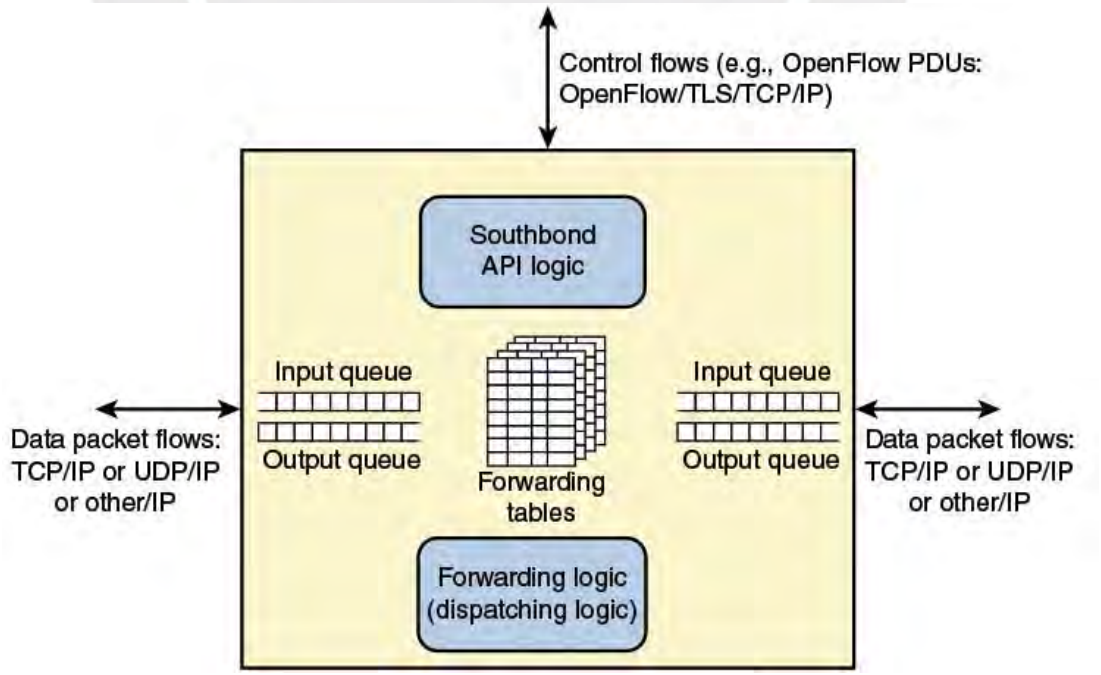


Figura 3: Dispositivo de red del plano de datos(Stallings et al., 2016)

■ Función de soporte de control: interactúa con la capa de control SDN para admitir la programabilidad a través de interfaces de control de recursos. El conmutador se comunica con el controlador y lo administra a través del protocolo de conmutador OpenFlow (Stallings et al., 2016).

■ Función de reenvío de datos: acepta flujos de datos entrantes de otros dispositivos de red y sistemas finales y los reenvía a lo largo de las rutas de reenvío de datos que se han calculado y establecido de acuerdo con las reglas definidas por las aplicaciones SDN (Stallings et al., 2016).

Estas reglas de reenvío utilizadas por el dispositivo de red están incorporadas en tablas de reenvío que indican, para determinadas categorías de paquetes, cuál debe ser el siguiente salto en la ruta. Además del simple reenvío de un paquete, el dispositivo de red puede modificar el encabezado del paquete antes de reenviarlo o descartarlo. Como se observa en la Figura 3, los paquetes que llegan pueden colocarse en una cola de entrada, a la espera de que el dispositivo de red los procese, y los paquetes reenviados generalmente se colocan en una cola de salida, a la espera de la transmisión.

Este dispositivo de red muestra tres puertos de entrada y salida de paquetes (E/S), uno proporciona comunicación de control E/S con un controlador SDN y dos para la de datos, éste es un ejemplo simple. El dispositivo de red puede tener varios puertos para comunicarse con varios controladores SDN y puede tener más de dos puertos de E/S para que los paquetes entren y salgan del dispositivo(Stallings et al., 2016).

Protocolos de plano de datos

La Figura 3, sugiere los protocolos compatibles con el dispositivo de red. Los flujos de paquetes de datos consisten en flujos de paquetes IP. Puede ser necesario que la tabla de reenvío defina entradas basadas en campos en encabezados de protocolo de nivel superior, como TCP, UDP o algún otro protocolo de transporte o aplicación. El dispositivo de red examina el encabezado IP y posiblemente otros encabezados en cada paquete y toma una decisión de reenvío.

El otro flujo importante de tráfico es a través de la interfaz de programación de aplicaciones (API) hacia el sur que consta de unidades de datos de protocolo (PDU), OpenFlow o algún tráfico de protocolo API hacia el sur similar (Stallings et al., 2016).

Hasta aquí se ha explicado la estructura y funcionamiento de SDN, exponiendo la forma de trabajo de esta tecnología que se emplea en el presente trabajo de tesis doctoral. La capacidad de SDN para centralizar el control y personalizar políticas de red, incluyendo QoS, la posiciona como una tecnología clave para abordar desafíos como las amenazas internas en intranets académicas, un enfoque desarrollado en esta tesis.

2.2 Redes que sirven a los Campus Académicos

Este estudio se enfoca en las redes que sirven a los campus académicos, particularmente en la intranet de una universidad. Las redes de campus son una colección de LAN en un área geográfica concentrada. Los usuarios finales pueden conectarse a través de puntos de acceso (AP) inalámbricos o mediante enlaces por cable y a través de dispositivos de la organización o personales. Estas estructuras de red son fundamentales para facilitar la conectividad y el acceso a recursos académicos dentro de un entorno universitario (Muhie et al., 2020).

Hay una serie de requisitos de redes que pertenecen a los campus. Estos incluyen (1) niveles diferenciados de acceso, (2) traiga su propio dispositivo (BYOD, por sus siglas en inglés), (3) control de acceso y seguridad, (4) descubrimiento de servicios y (5) firewalls de usuario final. Los diferentes tipos de usuarios en el campus requerirán diferentes niveles de acceso, QoS, priorización del tráfico y límites de ancho de banda (J. Silva, 2021).

La popularidad de la conectividad inalámbrica y las medidas de seguridad avanzadas requieren que empleados e invitados superen obstáculos de seguridad, como IEEE 802.1X, autenticación basada en la dirección MAC o portales cautivos (Downer & Bhattacharya, 2022). El fenómeno BYOD permite a los usuarios acceder a la red con sus propios dispositivos, lo que mejora la comodidad y eficiencia, pero también requiere la implementación de marcos de seguridad estrictos para mitigar los riesgos asociados con el acceso no autorizado y las brechas de datos (Downer & Bhattacharya, 2022). El descubrimiento de servicios facilita el acceso a servicios de impresión, archivos compartidos, televisiones a través de interfaces simples y la detección automática de dispositivos, mejorando la experiencia del usuario y la eficiencia en el uso de los recursos (Balakrishnan, 2022).

En resumen, las redes de campus, como la intranet universitaria, deben ser robustas y seguras, proporcionando acceso diferenciado y adaptado a las necesidades de sus diversos usuarios. Estas redes no solo soportan la infraestructura tecnológica del campus, sino que también facilitan un entorno académico más conectado y eficiente.

2.3 Políticas de calidad de servicio (QoS)

La ITU según la G.1010, vigente, define la QoS como el efecto global de la calidad de funcionamiento de un servicio que determina el grado de satisfacción de un usuario (ITU-T, 2001). Dejando al cliente determinar las características y comportamientos que lo satisfacen al tener necesidades diferentes como: minimizar el retardo, asegurar velocidad mínima, priorizar tráficos, etc. (Barba-Vera et al., 2020) Para proporcionar garantías en la transmisión de determinados flujos de los datos, la ISO (1994) introdujo el concepto QoS, la cual se utiliza para medir el ofrecido por una red de comunicación. Pues se considera como las propiedades de rendimiento de extremo a extremo medibles de un servicio de red, que pueden garantizarse por adelantado mediante un acuerdo de nivel de servicio (SLA) entre un usuario y un proveedor de servicios, para satisfacer los requisitos específicos de la aplicación del cliente.(H. Zhang et al., 2022)

Para maximizar la disponibilidad y el rendimiento en equipos de telepresencia garantizando una QoS, se evalúan los parámetros: ancho de banda, latencia, jitter, pérdida de paquetes variables que se han seleccionado para el presente estudio.

Considerando las definiciones de estos parámetros de rendimiento, se tiene:

a) Ancho de banda, capacidad de un determinado medio por el cual se transmite una cantidad determinada de datos por fracción de tiempo, cuanto mayor es el ancho de banda de un sistema de transmisión, mayor es la velocidad.(Stallings, 2004). También lo definen como la capacidad máxima de transmisión de datos en una red en un período de tiempo dado, es decir cuántos bits por segundo (bps) puede transportar (Tanenbaum & Wetherall, 2012).
b) Latencia de red se define como el tiempo promedio que tarda un paquete IP en realizar un viaje de ida y vuelta entre concentradores troncales (Stallings et al., 2016). Las redes con un mayor retraso o retardo tienen una latencia alta, mientras que las que tienen tiempos de respuesta rápidos tienen una

baja. Se considera como el tiempo total que transcurre desde que envía una información, hasta que la misma llega a un receptor. Su valor de medición se hace en milisegundos (Axess Networks, 2020).

c) Jitter, representa la variabilidad en el tiempo de llegada de paquetes de datos en una red, reflejando la variabilidad en la latencia que afecta principalmente a aplicaciones en tiempo real como las comunicaciones de voz y video (Kurose et al., 2017).La gestión efectiva del jitter es esencial para mantener la calidad de servicio en estas aplicaciones.
d) Pérdida de paquetes ocurre cuando uno o más paquetes de datos no alcanzan su destino, lo que puede llevar a una degradación en la calidad de la experiencia del usuario, especialmente en aplicaciones sensibles al tiempo como las comunicaciones en tiempo real (Putri, 2024). Es el porcentaje de paquetes transmitidos que se descartan en la red, debido a una alta tasa de error en alguno de los medios de enlace o por sobrepasarse la capacidad de un buffer de una interfaz en momentos de congestión (Khafidin et al., 2019).

Calidad de la experiencia (QoE)

QoE es una medida subjetiva del rendimiento según lo informado por el usuario. A diferencia de la QoS, que se puede medir con precisión, la QoE se basa en la opinión humana. QoE es importante, especialmente cuando tratamos con aplicaciones multimedia y entrega de contenido multimedia. QoS proporciona objetivos medibles y cuantitativos que guían el diseño y la operación de una red y permiten al cliente y al proveedor acordar qué rendimiento cuantitativo ofrecerá la red para dar a las aplicaciones y los flujos de tráfico (Stallings et al., 2016).

Sin embargo, los procesos de QoS por sí solos no son suficientes, ya que no tienen en cuenta la percepción del usuario sobre el rendimiento de la red y la QoS. La medida definitiva de una red y los servicios que ofrece es cómo los suscriptores perciben el rendimiento. QoE aumenta la QoS tradicional al proporcionar información sobre los servicios prestados desde el punto de vista del usuario final (Stallings et al., 2016).

Políticas de QoS

Junto con la virtualización de servidores, muchas empresas también utilizan una única red para satisfacer todas sus necesidades de redes de voz, video y datos. En las redes heredadas de hoy, el concepto de QoS se utiliza para proporcionar un nivel de servicio diferenciado para diferentes aplicaciones. Sin embargo, el

aprovisionamiento de muchas herramientas de QoS es muy manual. El personal de la red debe configurar el equipo de cada proveedor por separado y ajustar parámetros como el ancho de banda de la red y la QoS por sesión y por aplicación (Hamad, 2023). Las redes heredadas son estáticas y no pueden adaptarse dinámicamente a los cambios en el tráfico, las aplicaciones y las demandas de los usuarios(Merayo et al., 2021).

Si bien el plano de control de las redes heredadas tenía formas sofisticadas de distribuir de forma autónoma y dinámica el estado de la capa dos y la capa tres, no existen protocolos correspondientes para distribuir las políticas que se utilizan en el enrutamiento basado en políticas. Por lo tanto, la configuración de la política de seguridad, como las ACL o la política de virtualización, como a qué VLAN pertenece un host, permanece estática y manual en las redes tradicionales. Por lo tanto, la tarea de reconfigurar una red en un centro de datos moderno no toma minutos, sino, más bien, días. Estas redes inflexibles están obstaculizando a los administradores de TI en sus intentos de automatizar y optimizar sus entornos de centros de datos virtualizados. SDN promete que el tiempo necesario para dicha reconfiguración de red se reduzca al orden de minutos, como ya es el caso de la reconfiguración de las máquinas virtuales (Elbasheer et al., 2022).

La Figura 4, muestra el esquema de red moderno propuesto por (Stallings et al., 2016), donde se detalla la relación de QoE con la QoS y las tecnologías de nueva generación como SDN y NFV (Network Function Virtualization). Y la relación de estas con los dispositivos de red.

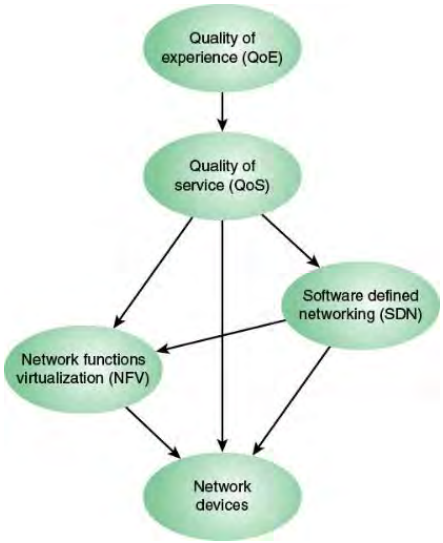


Figura 4: Esquema de red moderno(Stallings et al., 2016)

Al implementar SDN de la figura 4, es el controlador SDN el responsable de hacer cumplir los parámetros de QoS para los distintos usuarios de la red, si entran en juego las consideraciones de QoE, se utilizan también para ajustar los parámetros de QoS (Stallings et al., 2016).

En el contexto de esta tesis, las políticas de QoS son fundamentales para establecer controles específicos que mitiguen amenazas internas en intranets académicas, mejorando simultáneamente el rendimiento de la red.

2.4 Amenazas Internas

El crecimiento exponencial de las redes de información ha transformado su rol de simples canales de comunicación a pilares fundamentales de la infraestructura global, moldeando la cultura y la vida cotidiana de manera profunda.(Seo & Kim, 2020). Sin embargo, esta expansión ha intensificado los desafíos relacionados con la seguridad, especialmente ante las amenazas internas, donde personas con acceso privilegiado explotan su conocimiento y cercanía al núcleo de la organización para llevar a cabo ataques difíciles de detectar, aprovechando vulnerabilidades dentro del perímetro de seguridad de la entidad (Halim & Yusof, 2019).

Cualquier forma de amenaza puede originarse dentro de una organización, y no se limita solo a un empleado con intenciones maliciosas; incluso pueden ser contratistas, exempleados, miembros de la junta, accionistas o entidades de terceros (Montano et al., 2022). Casos como el de Edward Snowden, que fue el más difundido a nivel mundial, donde debido a su posición de alta seguridad nacional le permitió el acceso a documentos secretos, que luego difundió sin permiso, es una muestra clara de lo que puede suceder si se le da acceso total a individuos que muestran inestabilidad en su comportamiento o cuestionan la autoridad, y pese a los indicadores alarmantes, no se controlaban ni se gestionaban adecuadamente.(Rice & Searle, 2022)

La División *Computer Emergency Response Team* CERT(Software Engineering Institute, 2022) define a un infiltrado malicioso como una persona ya sea un empleado, contratista o socio comercial, actual o anterior que, habiendo tenido acceso autorizado a la red, sistemas o datos de la organización, utiliza intencionalmente dicho acceso de forma indebida para comprometer la confidencialidad, integridad o disponibilidad de la información o de los sistemas de la

organización. Estos infiltrados representan una amenaza significativa debido a su conocimiento detallado de las operaciones internas, lo que les permite evadir las medidas de seguridad convencionales y llevar a cabo actividades como espionaje, sabotaje o robo de información, poniendo en riesgo la seguridad de la organización(Z. Tian et al., 2020).

En las redes organizacionales de hoy en día, las acciones internas maliciosas son una amenaza importante que podría tener graves consecuencias, y se debe implementar un Programa de amenazas internas (InTP, por sus siglas en inglés) integral, que ofrezca procedimientos y políticas de investigación interna, que permiten a una organización ejecutar un curso de acción predefinido, para determinar la naturaleza del delito y cómo proceder al procesamiento legal del individuo por el incidente. La amenaza a menudo no se aborda adecuadamente debido al nivel de confianza con una persona interna. Debe formularse una mejor comprensión de los antecedentes del problema al integrar técnicas modernas de mitigación de incidentes, tanto técnicas como organizativas (Yilmaz, 2024).

La falta de un estándar reconocido para los InTP en la comunidad subraya la necesidad de que las organizaciones desarrollen procedimientos que se integren con los procesos existentes de gestión de riesgos. Es crucial involucrar a personal clave de diferentes disciplinas y desarrollar indicadores específicos, tanto humanos como técnicos, así como controles ajustados a las necesidades particulares de la organización (Marquis, 2024).

El análisis de datos es crucial para responder de manera oportuna y precisa a los incidentes. Existen diversas técnicas de análisis que varían en complejidad, desde métodos basados en reglas hasta el uso de algoritmos avanzados. Algunas de estas técnicas pueden automatizarse, mientras que otras requieren la intervención de expertos. Este aspecto del programa demandará una considerable cantidad de tiempo y recursos, ya que constituye la base para la eficacia de los programas de amenazas internas. La creación de capacidades analíticas que sean precisas y reproducibles es un desafío significativo, y todas las herramientas analíticas deben ser validadas de manera continua para evaluar su efectividad en relación con los recursos disponibles (Mohapatra, 2023).

Un programa integral de amenazas internas debe considerar el análisis del comportamiento de los empleados, la supervisión continua de sus actividades, el

análisis del tráfico de la intranet para detectar posibles amenazas internas y la implementación de procedimientos legales adecuados según las leyes aplicables en cada caso específico. Estos enfoques se fundamentan en una amplia gama de estudios de casos sobre incidentes internos reales, que contribuyen a perfilar mejor las amenazas internas y a diseñar estrategias de mitigación más efectivas (Akello, 2024).

CERT no explora públicamente el espionaje ya que la información está clasificada y no está disponible para el examen público. Los cuatro perfiles de amenazas internas: sabotaje IT, robo de propiedad intelectual, fraude y espionaje presentados en la Tabla 2, referente al perfil del vector de amenazas internas (Kont et al., 2015, pag. 15), se construyeron principalmente a partir de Band, S, Ficher, L., Moore, A., Shaw, E. y Trzeciak, R. (2006) "Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis," y de Charney, D .L.,(2010) "True Psychology of the Insider Spy," Intelligencer: Journal of U.S. Intelligence Studies. (Kont et al., 2015, pag. 14). Este conjunto de datos proporciona una base sólida para comprender los comportamientos y motivaciones de los insiders (Mohapatra, 2023). Este enfoque ha facilitado la investigación y el desarrollo de metodologías de detección, ofreciendo perspectivas sobre los patrones de comportamiento interno que pueden conducir a brechas de seguridad (Garchery, 2020).

Tabla 2: Perfil del vector de amenazas internas (Kont et al., 2015, pag. 15)

Perfil	**Sabotaje IT**	**Insider Robo de IP (Propiedad Intelectual)**	**Fraude Insider**	**Espionaje**
QUIEN	Empleados técnicos (por ejemplo, Administradores de Sistema o Red, Desarrolladores, Programadores) Empleados con acceso privilegiado.	Más a menudo Científicos, ingenieros, programadores, personal de venta.	Empleados con niveles más bajos (por ejemplo, posiciones de help-desk, servicio al cliente, ingreso de datos) Administradores de nivel Medio/bajo	Empleados técnicos y no técnicos.
CUANDO	Configura mientras está empleado. Ejecuta después de la terminación.	Usualmente dentro del periodo de 60 días antes o después de salir de la organización.	Sucede en un largo periodo de tiempo.	Sucede en un largo periodo de tiempo. Después del incidente inicial, un largo periodo puede pasar antes de que un evento siga.
MOTIVACIÓN	Revancha	Empezar su propio negocio. Nueva posición de trabajo.	Necesidad financiera o codicia	Necesidad financiera o codicia Insatisfacción con el estado

		Gobierno u organización extranjera.		
CÓMO	Acceso, capacidad y motivación.	Exfiltración de datos: Correo electrónico, memorias USB, documentos físicos, etc.	Corrupción de procedimientos organizacionales Auditoría inadecuada de procesos críticos e irregulares	Los métodos abarcan todos los perfiles.
QUÉ	Afecta a los sistemas en los que trabajaron	Robar información en la que trabajaron	Información de identificación personal (PII) En algunos casos, el fraude ocurre durante un período de tiempo más largo y tiene un gran impacto monetario.	Robo de información. Destrucción de la información para cubrir sus pistas.

Además, CERT utiliza estudios de casos y análisis de incidentes pasados para categorizar las amenazas internas en perfiles distintos, basándose en patrones de comportamiento y factores contextuales. La integración de técnicas de aprendizaje automático, como se destaca en estudios recientes, mejora aún más la capacidad de identificar y predecir amenazas internas al analizar el comportamiento de los usuarios y los registros de actividad (Al-Shehari, 2023). Este enfoque multifacético asegura que los perfiles presentados no solo estén basados en datos, sino que también reflejen el panorama evolutivo de las amenazas internas, que incluyen tanto acciones maliciosas como no intencionales por parte de insiders (Moneva & Leukfeldt, 2023).

CERT ha ampliado la clasificación de perfiles de amenazas internas más allá de los tradicionales, añadiendo un quinto perfil: las amenazas internas no intencionales (UIT), que, aunque no buscan dañar de manera deliberada, pueden comprometer la seguridad cibernética de la organización (Moneva & Leukfeldt, 2023). Para gestionar eficazmente estas amenazas, CERT recomienda que las organizaciones implementen programas específicos que no solo detecten e identifiquen incidentes, sino que también promuevan cambios organizativos y conductuales para mitigar riesgos (Al-Mhiqani et al., 2020). Estos programas deben estar respaldados por políticas de seguridad robustas y herramientas tecnológicas como IDS (Sistema de detección de intrusos), IF (Infraestructura de inteligencia) y PCAP (Captura de paquetes) para una detección más efectiva de las amenazas(Z. Tian et al., 2020).

La presente tesis aborda el análisis del tráfico interno de la red considerando los cinco perfiles de amenazas internas identificados por CERT y Kont (Kont et al., 2015). Con base en un estudio del comportamiento del tráfico en la intranet y en las amenazas internas detectadas en tiempo real, se implementaron políticas de QoS en un

escenario SDN con el objetivo de evaluar su efectividad en el control y mitigación de estas amenazas. Este enfoque dinámico y adaptable mejora la seguridad organizacional, abordando la falta de metodologías estándar para gestionar amenazas internas. Así, la tesis propone un marco metodológico estructurado que, mediante la implementación de políticas de QoS en SDN, ofrece una solución experimentalmente validada para entornos académicos.

2.5 Metodologías para la evaluación de seguridad de redes

Existen metodologías y estándares para la evaluación de seguridad en una intranet de datos, se consideran las siguientes:

a. OSSTMM versión 3.02(Herzog, 2010) de ISECOM (ISECOM, 2021), se centra en la evaluación de seguridad mediante pruebas de penetración y análisis de riesgos, integrando pruebas técnicas y humanas para evaluar la resistencia de los sistemas frente a ataques (Edwards, 2024). Esta metodología es ampliamente utilizada en la industria por su capacidad de identificar tanto vulnerabilidades técnicas como amenazas internas relacionadas con el comportamiento humano, para un análisis integral de la seguridad organizacional (Albrecht & Jensen, 2020). Además, OSSTMM promueve pruebas continuas de penetración interna promoviendo evaluaciones periódicas para adaptarse a las amenazas en constante evolución(Continuous Internal Penetration Testing (CIPT), 2023).

b. NIST SP 800-115, estándar del Instituto Nacional de Estándares y Tecnología (NIST) orienta sobre la realización de pruebas de penetración y evaluaciones de seguridad de sistemas de información, incluye pasos para planificar, ejecutar y documentarlas de manera efectiva. No es tan detallado como OSSTMM, sin embargo, es una referencia importante en el campo de la seguridad de la información.(Scarfone, Karen; Souppaya, Murugiah; Cody, Amanda; Orebaugh, 2020)

c. Open Web Application Security Project (OWASP) Testing Guide: ofrece una guía de pruebas de seguridad de aplicaciones web, relevante si la intranet de datos las incluye. Una lista detallada de pruebas de seguridad permite identificar vulnerabilidades comunes en aplicaciones web y servicios relacionados.(OWASP Foundation, 2022)

De las metodologías analizadas, OSSTMM versión 3.02 es ampliamente reconocida como un estándar internacional en pruebas de seguridad por su enfoque modular, que permite un análisis detallado de diversas formas de comunicación y componentes del sistema, siendo especialmente útil para identificar vulnerabilidades internas en el contexto de amenazas cibernéticas en evolución. Aunque su aplicación es compleja, debido a su intención de abordar todos los aspectos de la seguridad de la información, su énfasis en los aspectos operativos y la interacción entre los distintos componentes es fundamental para realizar una evaluación de riesgos completa. (Gyawali, 2023)

OSSTMM define un alcance en el entorno de seguridad operativa total para que cualquier interacción con cualquier activo pueda incluir los componentes físicos de las medidas de seguridad. Comprende tres clases, con cinco canales, como se muestra en la Tabla 3. Las clases son designaciones oficiales en la industria de la seguridad (Tao et al., 2019). En esta investigación se considera el canal humano ya que está relacionado con el perfil de los usuarios internos que utilizan la red y son considerados como posibles amenazas.

Tabla 3: Clases y canales del alcance de OSSTMM. (Herzog, 2010)

Clase	Canal	Descripción
Seguridad Física PHYSSEC	Humano	Elemento humano de la comunicación (interacción física o psicológica).
	Físico	Elemento tangible de seguridad, la interacción requiere esfuerzo físico o un transmisor.
Seguridad del Espectro SPECSEC	Inalámbrico	Comunicaciones electrónicas, señales y espectro EM (ELSEC, SIGSEC).
Seguridad de las Comunicaciones COMSEC	Telecomunicaciones	Redes de telecomunicación, digitales o analógicas (interacción por teléfono establecido o como líneas de red).
	Redes de datos	Sistemas electrónicos y redes de datos (interacción por cables establecidos y líneas de redes cableadas).

La información del canal auditado se resume en el RAV (Risk Assessment Value), una medida que se obtiene a través de múltiples cálculos separados de: Porosidad,

Controles y Limitaciones descritos en la Tabla 4, sus cálculos combinados mostrarán el tamaño de una superficie de ataque(Herzog, 2010) . Para mayor claridad, se definen estos conceptos de la siguiente manera: Herzog define la porosidad como "todos los puntos interactivos, operaciones, que se clasifican como Visibilidad, Acceso o Confianza" (Herzog, 2010, p. 31). En OSSTMM, los controles son los mecanismos que reducen el impacto de interacciones no autorizadas y disminuyen la exposición de los activos físicos y de información a amenazas, dividiéndose en dos categorías: Controles Interactivos (autenticación, indemnización, resiliencia, subyugación y continuidad), que actúan directamente sobre las interacciones, y Controles de Proceso (no repudio, confidencialidad, privacidad, integridad y alarmas), que sostienen las políticas y procedimientos de seguridad (Herzog, 2010). Por último, las limitaciones se definen como las deficiencias o fallas en los mecanismos de protección que impiden mantener una separación efectiva entre los activos y las amenazas, evidenciando vulnerabilidades, debilidades y restricciones operativas que reducen la eficacia de los controles (Herzog, 2010).

Esta integración de definiciones en el análisis del RAV permite cuantificar la exposición del sistema, proporcionando una medida precisa del ataque superficial y facilitando la identificación de áreas críticas de mejora en la seguridad operativa.
Se utilizó la metodología automatizada con la hoja de cálculo del RAV de la web oficial de ISECOM(ISECOM, 2021).

Tabla 4: Porosidad, controles y limitaciones en la metodología OSSTMM.
(Herzog, 2010)

Categoría		**Seguridad Operacional (Porosidad)**	**Limitaciones**
Operaciones		Visibilidad	Exposición
		Acceso	Vulnerabilidad
		Confianza	
Controles	**Clase A**	Autenticación	Debilidad
		Indemnización	
		Resistencia	
		Subyugación	
		Continuidad	
	Clase B	No repudio	Preocupación

		Confidencialidad	
		Privacidad	
		Integridad	
		Alarma	
			Anomalía

La metodología OSSTMM tiene 4 fases representadas en la figura 5, diagrama de bloques de la metodología OSSTMM. Incluyen:

2.5.1 - Fase de inducción, representada con el color amarillo, el analista comienza la auditoría con la comprensión de los requisitos de auditoría, el alcance y las limitaciones de la auditoría, esta fase está compuesta de revisión de la postura, verificación de detección activa y logística. (Herzog, 2010)

2.5.2.- Fase de interacción, representada en la Figura 5 con el color naranja, para conocer el alcance en relación con las interacciones de los objetivos. Esta fase está compuesta de auditoría de la visibilidad, verificación de acceso, verificación de la confianza y verificación de controles.

2.5.3.- Fase de investigación, representada en la Figura 5 con el color celeste, se muestran los diversos tipos de valor o el detrimento de la información mal administrada(Herzog, 2010) esta fase está compuesta de verificación de procesos, verificación de entrenamiento, validación de propiedad, revisión de segregación, verificación de exposición y búsqueda de inteligencia competitiva.

2.5.4.- Fase de intervención, representada en la Figura 5 con el color rosado, parte final de la auditoría; revisión de anomalías y explicación final(Herzog, 2010) esta fase está compuesta de verificación de cuarentena, privilegios de auditoría y servicio de continuidad; se añade en esta fase alertas y revisión de registros, se la identifica con el color azul, siendo la parte final de la metodología, relacionándose además con la revisión de los controles de la segunda fase interacción.

2.5.5 Fase final: análisis de brechas y verificación, se representa en color azul eléctrico. Este análisis considera registros y percepciones tanto humanas como mecánicas, verifica que las medidas implementadas se alineen con los resultados esperados y se corrija en caso de no haber sido detectados previamente (Herzog, 2010). Se considera la verificación de alarmas, almacenamiento y recuperación de

Información, asegurando que todos los incidentes sean registrados, evaluados y gestionados de manera adecuada.

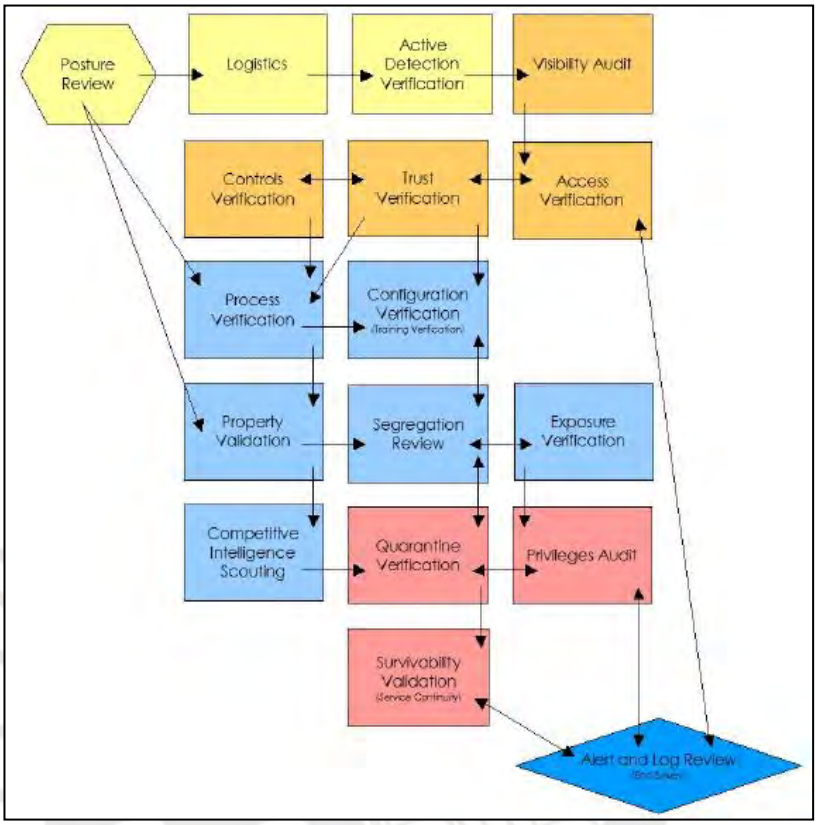
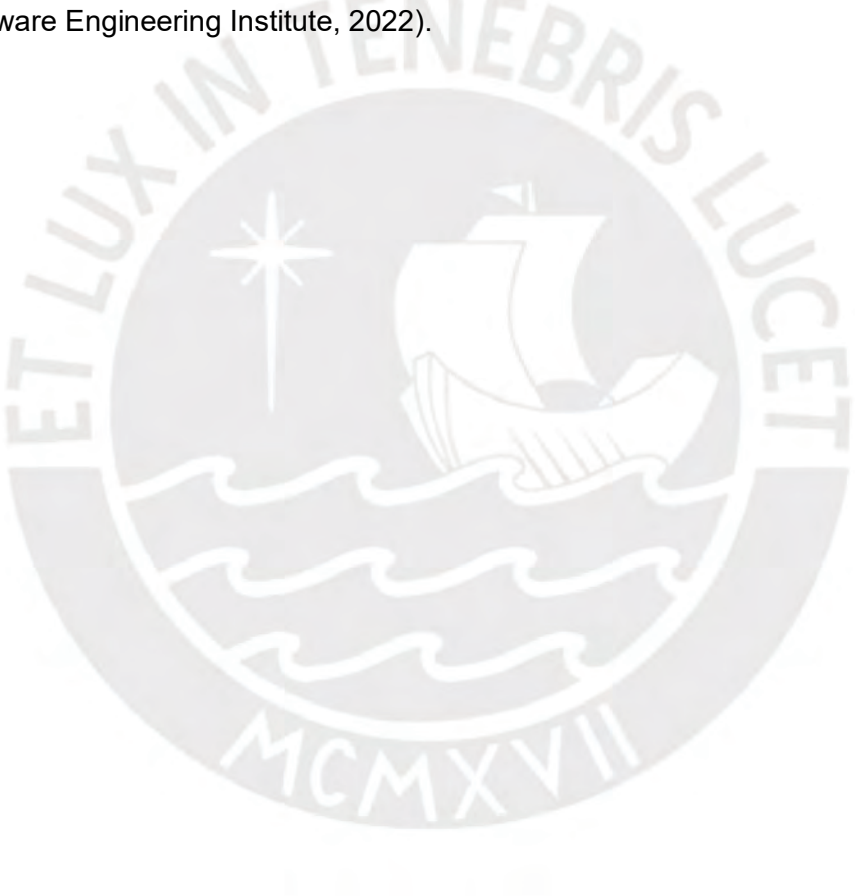


Figura 5: Diagrama de bloques de la metodología OSSTMM.(Herzog,2010)

Aunque OSSTMM y otras metodologías aportan enfoques valiosos para la evaluación de seguridad, la presente tesis selecciona y adapta OSSTMM V3.02 para aplicarla específicamente en el contexto de intranets académicas. El enfoque se centra en evaluar el canal humano, que permite identificar la presencia de amenazas internas en estos entornos. Esta adaptación metodológica se detalla en el capítulo 4, donde se presenta el marco metodológico propuesto, y se valida en el capítulo 5, demostrando su efectividad en escenarios experimentales. Al integrar políticas de QoS y SDN, la propuesta responde a las necesidades específicas de control de amenazas internas, superando las limitaciones de las metodologías existentes.

En particular, marcos como NIST SP 800-115 y la Guía de Pruebas OWASP presentan limitaciones significativas al ser aplicados al diagnóstico de amenazas internas. NIST se enfoca principalmente en pruebas técnicas de penetración y

escaneo de red, careciendo de mecanismos para evaluar comportamientos anómalos de usuarios con acceso legítimo, lo cual es crítico en entornos académicos. (Scarfone et al., 2008) Por su parte, OWASP está orientado a vulnerabilidades en aplicaciones web y no contempla una evaluación operativa integral de la red ni del canal humano (Meucci & Muller, 2014). Además, ambos marcos carecen de una métrica cuantitativa y estandarizada para evaluar el nivel de exposición al riesgo. En contraste, OSSTMM introduce el RAV, que permite medir la porosidad, los controles y las limitaciones de seguridad de manera objetiva y reproducible (Herzog, 2010). Esta capacidad, junto con su estructura modular, permite a OSSTMM abordar las complejidades operativas, conductuales y técnicas que caracterizan a las intranets académicas, posicionándolo como el marco más adecuado para este estudio (Software Engineering Institute, 2022).



CAPÍTULO 3. ESTADO DEL ARTE

El presente capítulo documenta la revisión del estado del arte de amenazas internas en intranets académicas. Debido a su relevancia, se presenta como un capítulo completo. Emplea la metodología de Revisión Sistemática de Literatura (RSL) propuesta por Kitchenham (2004). Esta metodología rigurosa y sistemática se considera esencial, ya que toda investigación científica de trascendencia debe ser replicable, y evitar la subjetividad en la elección de las fuentes de estudio. La RSL permite evaluar e interpretar todas las investigaciones disponibles que sean relevantes para una determinada pregunta de investigación, presentando una evaluación justa utilizando una metodología confiable, rigurosa y auditable (Kitchenham & Charters, 2007).

Para este estudio también se consideró las lecciones de la aplicación de RSL bajo el paradigma basado en evidencia dentro del dominio de la ingeniería de software, sugeridas por Brereton et. al (2007). Estas lecciones destacan la importancia de la preparación y validación de un protocolo de revisión antes de la actividad de revisión. En este contexto, se desarrolló un protocolo de RSL en su tercera versión, permitiendo una evaluación más profunda de los estudios realizados en este ámbito, realizando un análisis crítico y proporcionando un mayor fundamento al trabajo investigativo.

El protocolo de RSL referente a las “Amenazas internas en intranets académicas”, abarca las fases de planificación, ejecución y el informe de la revisión. Este protocolo minimiza el sesgo del investigador y asegura la replicabilidad del estudio Kitchenham (2004). Se detalla en el Anexo B, especifica los métodos y procedimientos empleados para llevar a cabo la RSL. A continuación, se muestran los resultados de la RSL.

3.1 Resultados de la RSL.

Los papers proceden de tres bases de datos ampliamente utilizadas en investigaciones estas son: ACM, SCOPUS e IEEE. En total se obtuvieron 127 papers, resultado de la cadena de búsqueda que considera las preguntas de investigación, así como los criterios de inclusión y cumplen con los parámetros de estudio “*Insider threat, Intrusion Detection system, control, process, technique,* y *campus network*", el detalle de la lógica de búsqueda de la RSL se especifica en la Tabla 30 del Anexo B p.157. Después de la evaluación se identificaron ocho papers que no daban respuesta a las preguntas, ni a los criterios de inclusión de la

investigación o se repetían en los resultados de las búsquedas por lo que no se tomaron en cuenta, tampoco se incluyeron dos libros debido a la generalidad de sus tópicos. La Tabla 5 resume el resultado de las búsquedas en las bases de datos, en la que se incluye nombre de la base de datos, resultados de búsqueda, artículos descartados y relevantes. En total se han considerado 117 artículos en la revisión siendo este valor el 100%.

Tabla 5: Resumen del resultado de las búsquedas en las bases de datos.

Nombre de la Base de datos	Resultados de búsqueda	Artículos descartados	Artículos relevantes
ACM	20	-	20
SCOPUS	56	SCO05, SCO21, SCO24, SCO33, SCO41, SCO54, SCO55, SCO56	48
IEEE	51	IEEE22, IEEE28	49
TOTAL	**127**	**10**	**117**

Fuente. Elaboración propia

Respecto a los papers, el periodo de publicación comprende desde 1997 al 2022. En la Tabla 36 del Anexo B p.170, se presentan el listado de papers resultado de aplicar la estrategia de búsqueda en las bases de datos ACM, SCOPUS e IEEE.

Si bien el rango de publicación de los estudios seleccionados para la Revisión Sistemática de Literatura (RSL) abarca desde 1997 hasta 2022, esta selección se realizó conforme a los criterios de inclusión del protocolo validado (Anexo B) y responde a la necesidad de construir una base conceptual sólida y transversal en el tiempo. No obstante, la tesis complementa el análisis teórico inicial con la incorporación de estudios recientes publicados entre 2022 y 2024 (incluyendo Serag et al., 2024; Hamad, 2023; Jenny & Sugirtham, 2023; J. Wang et al., 2023; Tang et al., 2023), lo que permitió contrastar tendencias actuales, validar la vigencia del problema identificado y fortalecer la pertinencia de la propuesta metodológica. Además, documentos estratégicos como las recomendaciones del CERT (Carnegie Mellon University, 2022) subrayan que, pese al avance en la detección de amenazas internas, persiste la ausencia de propuestas concretas de control, reafirmando que la brecha identificada en la literatura permanece vigente. De este modo, la tesis no solo responde a un vacío histórico, sino que también se mantiene alineada con los desafíos contemporáneos del campo, consolidando así su relevancia, novedad y aplicabilidad.

Respecto a la RSL, se realizó la evaluación de los artículos según 13 criterios inclusivos, estos se detallan en el Anexo B p.158. Para ello se empleó el formulario de extracción de datos de artículos científicos para RSL descrito en la Tabla 34 del Anexo B p.164, donde se resume aspectos relevantes de la investigación, como datos generales y características del estudio. En el Anexo C, se muestra la RSL de "Amenazas internas en intranets académicas", señalando los datos de los artículos y los criterios de inclusión a los que responde.

Para la nomenclatura empleada, se identifican tres preguntas clave, etiquetadas como Q1, Q2 y Q3. Así como 13 criterios de inclusión, cada pregunta está asociada con un conjunto de criterios, numerados consecutivamente, y señalados de la siguiente forma:

Q1 (4 criterios): Representados como Q1.1 a Q1.4.

Q2 (7 criterios): Representados como Q2.1 a Q2.7.

Q3 (2 criterios): señalados como Q3.1 y Q3.2.

La RSL busca dar respuesta a las preguntas y sus criterios de inclusión, para ello se realizó un listado de lo evaluado y el total de menciones en porcentaje. A continuación, se presentan los resultados de cada pregunta y criterio.

Q1. ¿Qué tipos de insiders threat o amenazas internas existen en intranets académicas y cuáles son sus fuentes de datos?

Esta pregunta considera cuatro criterios, según se describe desde la Q1.1 a la Q1.4.

Q1.1 Tipos de insiders threat o amenazas internas existentes en redes de datos.

La Figura 6, incluye esta información. Mayor detalle se encuentra en Tabla 39 Anexo B p.176 correspondiente a Q1.1 tipos de insiders threat o amenazas internas existentes en redes de datos.

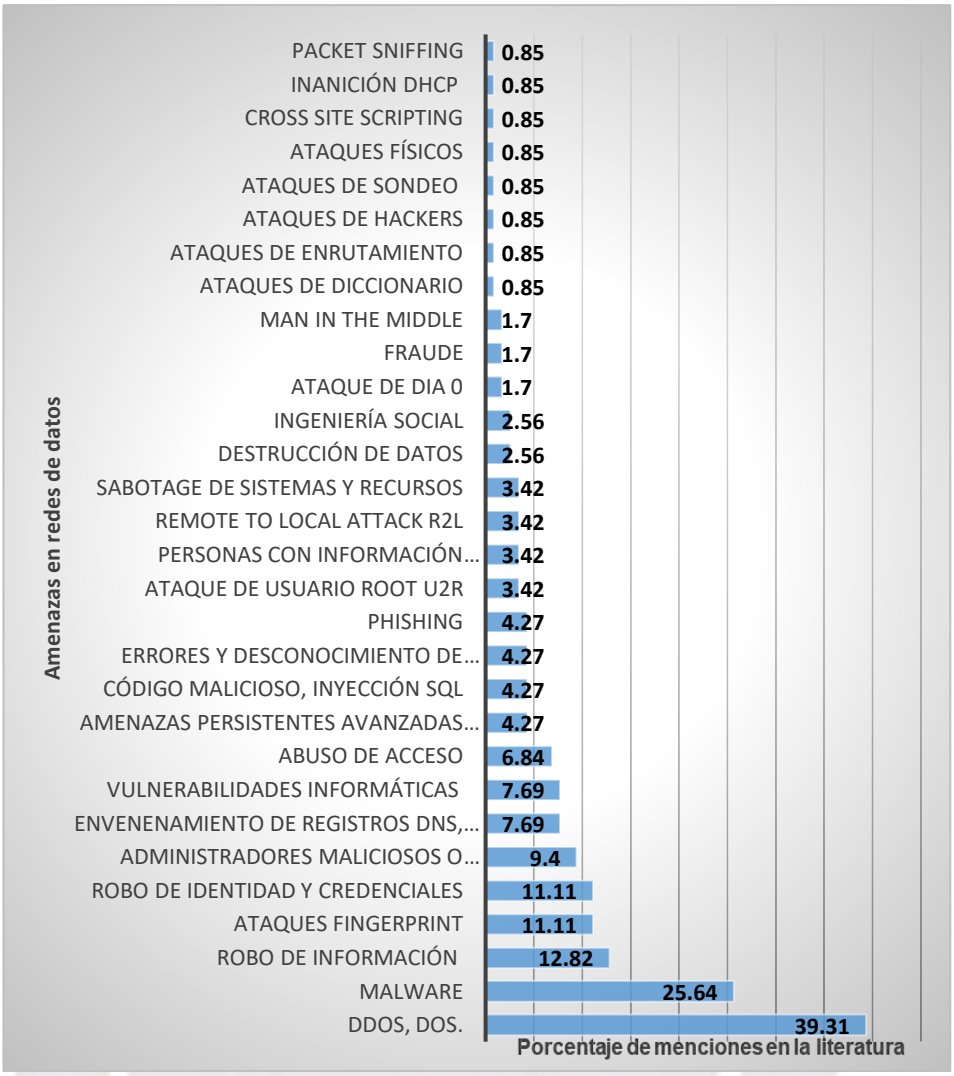


Figura 6. Q1.1 Tipos de insiders threat o amenazas internas existentes en redes de datos.

Fuente: Elaboración propia. Porcentajes calculados sobre 117 estudios revisados.

Como se puede observar en la Figura 6, la amenaza interna que más veces ha sido considerada es el ataque DoS y su variante DoS distribuido (DDoS) con el 39.31%. Seguido de ataques derivados de *malware* con el 25.64% entre los que destacan virus, gusanos, troyanos entre otros. Además, robo de información con un porcentaje de 12.82%.

Q1.2 Tipos de insiders threat o amenazas internas existentes en intranets académicas.

La Figura 7 muestra los resultados. Mayor detalle se encuentra en la Tabla 40 del Anexo B p.178 referente a Q1.2 tipos de insiders threat o amenazas internas existentes en intranets académicas.

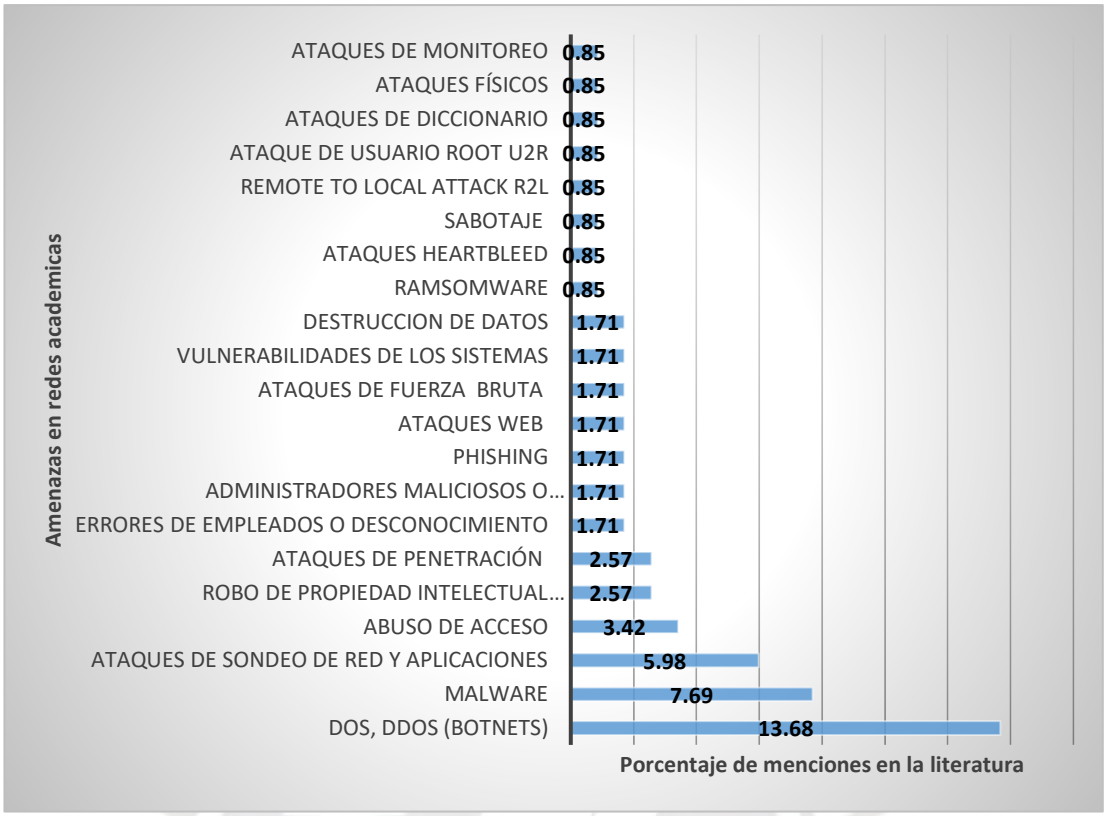


Figura 7. Q1.2 Tipos de insiders threat o amenazas internas existentes en intranets académicas.
Fuente. Elaboración propia. Porcentajes calculados sobre 117 estudios revisados.

En la figura 7 se visualiza que las amenazas internas en intranets académicas que más han sido mencionadas son los ataques DoS y DDoS con el 13.68%. Malware con el 7,69 % y ataques de sondeo de red y aplicaciones con 5.98%.

Q1.3 Principales fuentes de datos de insiders threats.

Se identificaron conjuntos de datos para el manejo de investigaciones de amenazas internas en la literatura, estas son: psicología de usuario, fuente externa y fuente propia.

La fuente psicología de usuario se menciona una única vez en la literatura, en ACM02, donde se hace referencia al comportamiento de empleados o estudiantes ya sea personal o de uso de los recursos de la institución, considerando registros de eventos heterogéneos de múltiples dominios, datos psicológicos e información funcional que están disponibles en la organización objetivo.

Las fuentes externas son datos disponibles y de libre acceso, listos para su uso, en los que se encuentran datos pertenecientes a diferentes ataques. Son de gran ayuda para el entrenamiento de sistemas de detección de intrusos y puesta a prueba de los

diferentes sistemas, algoritmos o metodologías propuestas según las necesidades de los investigadores.

De ello resalta el uso del conjunto de datos KDD99 y sus variantes NSL-KDD, Kyoto KDD-Cup, con un porcentaje del 9,4%. KDD99 evalúa la capacidad de su IDS en conjuntos de datos sin procesar y normalizados, los ataques se clasifican en cuatro clases principales: *DoS,* remoto a local (R2L), usuario a remoto (U2R), y sondeo.

El conjunto de datos UNSW-NB15 con 3,41% es un tráfico sintético es decir un conjunto de datos generado artificialmente para simular patrones de tráfico en redes de comunicación, con comportamiento malicioso incluye nueve tipos de ataques como *backdoors, DoS, exploits, worms* y *fuzzers*.

Con el 2.56 %, CERT r4.2, integra diferentes tipos de registros de eventos, incluyendo inicio de sesión/ cierre de sesión, correo electrónico, dispositivo, archivo y HTTP.

La Figura 8, muestra gráficamente los resultados obtenidos. La Tabla 41 del Anexo B p.181, referente a Q1.3 principales fuentes de datos externos de insiders threats en intranets académicas, detalla más información al respecto.

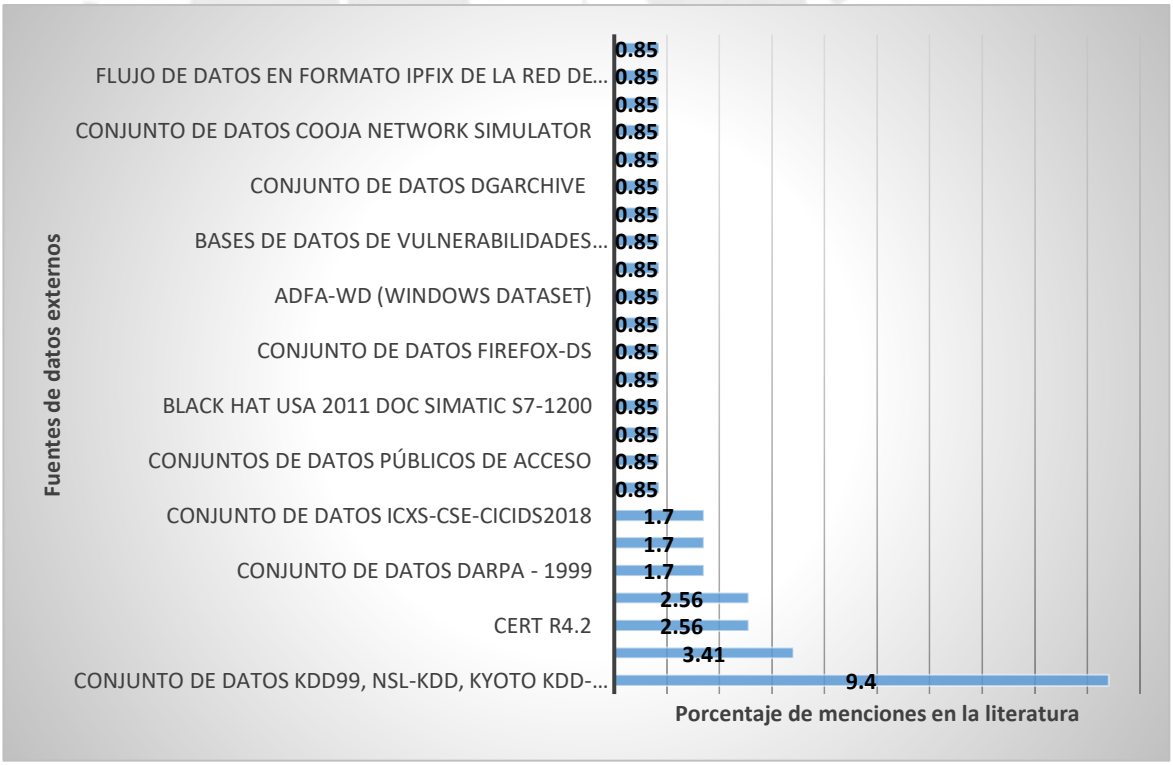


Figura 8. Q1.3 Principales fuentes de datos externos de insiders threats.
Fuente: Elaboración propia. Porcentajes calculados sobre 117 estudios revisados.

Finalmente, la fuente de datos propia, son capturadas en las redes de datos o una combinación de datos propia con fuentes de datos externas para así conformar una nueva fuente propia adecuada para las investigaciones. En IEEE17 (Androulidakis et al., 2009), con el 1.47 %, se menciona la captura de datos de una red de campus del enlace entre la Universidad Técnica Nacional de Atenas (NTUA) y la Red Griega de Investigación y Tecnología (GRNET) que conecta el campus universitario a Internet. Este enlace tiene un tráfico promedio de 250 Mbps, con servicios de red estándar Web, correo electrónico y FTP y aplicaciones P2P.

La Figura 9, visualiza gráficamente los resultados obtenidos. En la Tabla 42 del Anexo B p.183, respecto a Q1.3 Fuentes de Datos Propios de Insider Threat, se muestra con mayor detalle las fuentes de datos propias de insider threat.

Figura 9: Q1.3 Fuentes de Datos Propios de Insider Threat.
Fuente: Elaboración propia. Porcentajes calculados sobre 117 estudios revisados.

De la RSL, se determinó que, si bien existen diferentes fuentes de datos externas que se utilizan para el análisis de pruebas en lo que se refiere a datos propios de amenazas internas en redes de campus académicas son muy limitadas y no se da mayor detalle al respecto, determinándose la necesidad de realizar un análisis de amenazas internas en una intranet de un campus universitario con el objetivo de capturar data propia e identificarla con mayor detalle para el control de amenazas internas. La presente tesis da respuesta a esta necesidad que servirá de base para futuras investigaciones.

Q1.4 ¿Cuántas investigaciones mencionan considerar insider threat para limitar el control de acceso a usuarios en intranets?

Durante la RSL se identificaron 17 papers que mencionaron el control de acceso a usuarios como medida ante amenazas insider threat en sus intranets, estos son: ACM04, ACM05, ACM06, ACM07, ACM11, ACM14, ACM19, SCO07, SCO08, SCO13, SCO34, SCO37, SCO44, SCO26, SCO50 IEEE01 e IEEE39 como se observa en la Figura 10. Más información al respecto se detalla en la Tabla 43 del Anexo B p.187, que hace referencia a este parámetro.

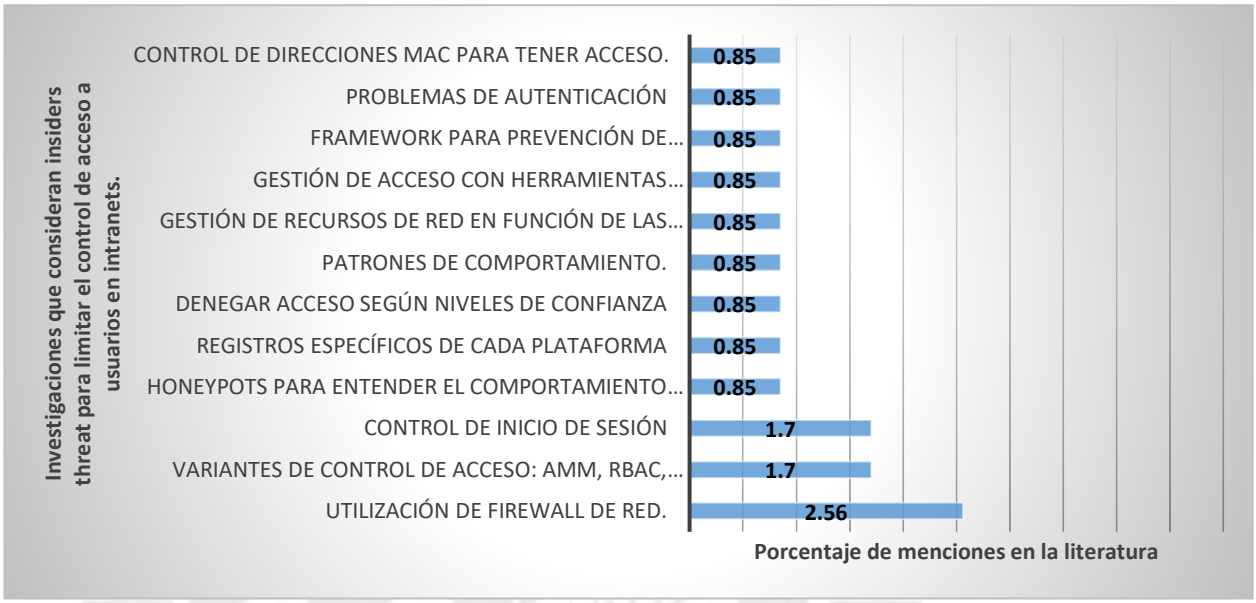


Figura 10: Q1.4 Investigaciones que mencionan considerar insider threat para limitar el control de acceso a usuarios en intranets.
Fuente: Elaboración propia. Porcentajes calculados sobre 117 estudios revisados.

En la Figura 10 se puede observar el 2.56 % en métodos de control de acceso basados en firewall, listas de control de acceso ACL, mecanismos de autenticación y autorización para garantizar que solo los usuarios legítimos puedan acceder a los datos. Se presenta variantes de control de acceso para evitar exposiciones, en 1.7 % así como control de inicio de sesión para detectar anomalías en base al comportamiento inusual de los usuarios o hosts.

Q2. ¿Qué herramientas, métodos o procedimientos de recolección de datos se emplean en el análisis de insiders threat, además que métodos de identificación o detección de amenazas se emplean?

Esta pregunta considera siete criterios desde Q2.1 a Q2.7.

Q2.1 ¿Qué herramientas, métodos o procedimientos de recolección de datos se emplean en el análisis de insiders threat?

Como se mencionó en el criterio de inclusión Q1.3 un tipo de fuente de datos para el entrenamiento de los sistemas o algoritmos utilizados en la literatura es la fuente propia la cual se complementa con herramientas, métodos o procedimientos para la toma de estos datos, la Figura 11, detalla herramientas de recolección de datos o métodos utilizados en la literatura, junto con los resultados al revisar este criterio. Más información, se puede observar en Tabla 44 del Anexo B p.189, respecto a Q2.1 Herramientas o métodos de recolección de datos.

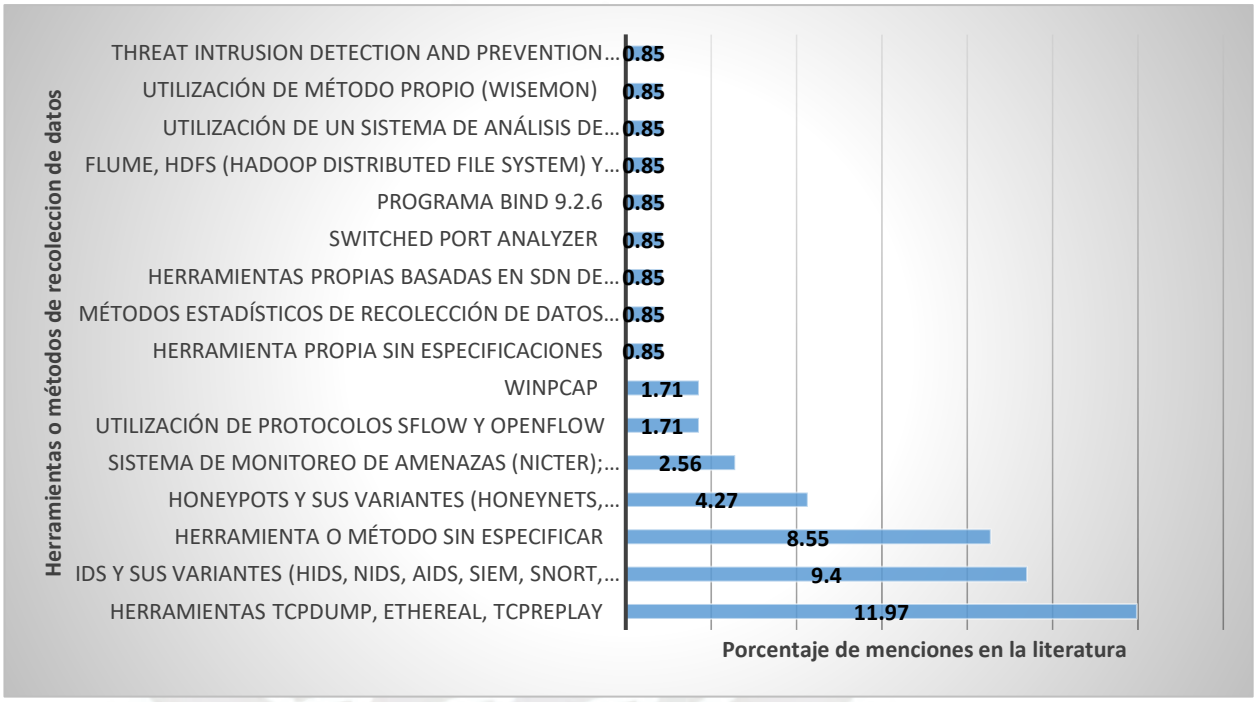


Figura 11. Q2.1 Herramientas o métodos de recolección de datos
Fuente: Elaboración propia. Porcentajes calculados sobre 117 estudios revisados.

Como resultado de la RSL se obtuvo que el conjunto de herramientas TCPdump, Ethereal y TCPReplay para la captura datos en formatos PCAP mediante puertos espejo son las más utilizadas representando un porcentaje de 11.97%. Seguido de la utilización de IDS y sus variantes (HIDS, NIDS, AIDS, SIEM, SNORT, SEBEK) con un porcentaje 9.4%, estas se relacionan ya que ciertos IDS utilizan TCPdump para la captura de datos y su posterior análisis. Se resalta en tercer lugar con el 8.55% la captura de datos con herramientas o métodos sin especificar, según se visualiza en la Figura 11. Determinándose que hay muy pocos papers que detallan un procedimiento de recolección de datos ya que en la mayoría solo se menciona la herramienta utilizada.

Q2.2 ¿Qué procedimientos se emplean para realizar mediciones de data de insiders threats en intranets académicas?

Se identifica cuatro papers con un porcentaje de 3.42% que dieron respuesta a este criterio, los dos primeros SCO35, e IEEE36 dan respuesta en redes en general, y en los dos restantes ACM07 e IEEE03 se mencionan estudios en redes de campus.
ACM07 propone un enfoque de bajo costo hacia amenazas internas. La solución captura acciones detalladas de los usuarios de la red en todas las aplicaciones y las correlaciona con el contexto del directorio para rastrear y hacer cumplir las políticas institucionales en toda la red del campus. Con el software "Real Time Analyzer" analiza las transacciones capturadas para proporcionar inteligencia y mitigar las amenazas internas. El módulo analiza e informa las excepciones, así como automatiza las auditorías operativas y de seguridad.
IEEE03 analiza los paquetes de datos de acuerdo con el modelo de protocolo de paquetes TCP/IP mediante SNORT.

De los resultados se determina que, si bien se hace referencia a los procedimientos para realizar mediciones de data de insiders threats en intranets académicas, resalta el hecho que es un campo en el que no se ha desarrollado estudios, ni existe un estándar para realizar este tipo de procesos, además no se define un procedimiento para realizar mediciones de datos, esto debido a que cada paper realiza un método propio sin muchas especificaciones, ni se ha identificado un método estándar.

Q2.3 ¿Qué método de detección de mal uso o detección de anomalías o comportamientos anómalos emplea en el contexto de detección de intrusiones de insiders threat?

Respecto a este criterio, la Figura 12 muestra los resultados obtenidos durante la revisión, pudiendo observarse la herramienta, método o tipo de algoritmo utilizado, así como el porcentaje que corresponde al total de menciones que se contabilizaron en la revisión, mayor detalle se puede observar en la Tabla 45 del Anexo B p.191, referente a Q2.3 Método/Herramientas de detección de mal uso o detección de anomalías de intrusiones de insiders threat.

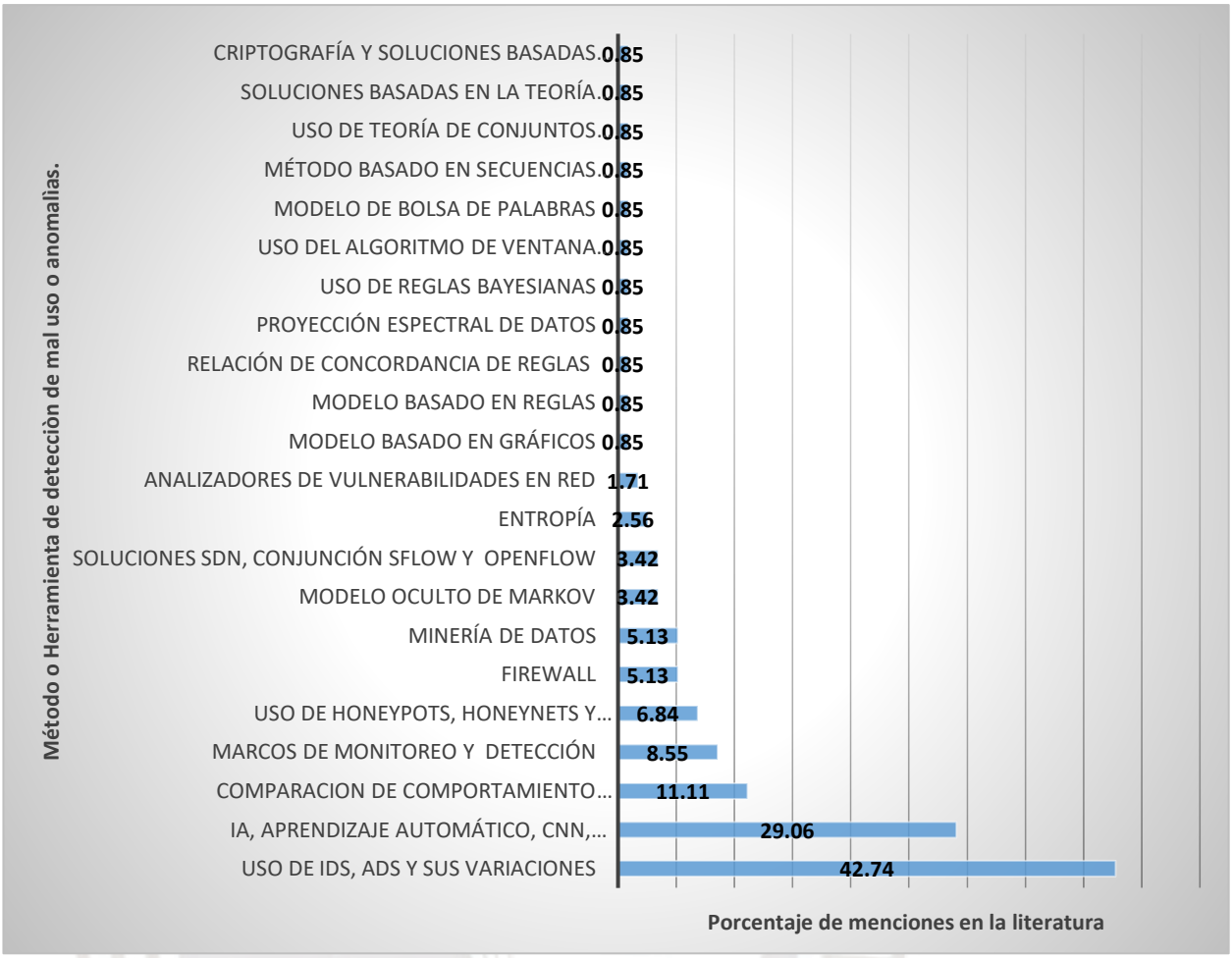


Figura 12: Q2.3 Método/Herramientas de detección de mal uso o detección de anomalías de intrusiones de insiders threat.
Fuente: Elaboración propia. Porcentajes calculados sobre 117 estudios revisados.

En base a los resultados se concluye que la utilización de sistemas de detección de intrusos (IDS) y sus diferentes variantes NIDS e HIDS entre otros, son los más utilizados con un porcentaje de 42.74% para la detección de anomalías, siendo la captura de datos en formato PCAP. Seguido se presenta la utilización de algoritmos de inteligencia artificial, aprendizaje automático, aprendizaje profundo representando el 29.06% para el entrenamiento de los sistemas o herramientas que los investigadores proponen. En tercer lugar, con el 11.11 % la comparación de comportamiento de los usuarios en diferentes horas del día según las funciones que realicen, esto se podría relacionar con el tipo de fuente de dato de psicología de usuarios.

Q2.4 ¿Qué método de detección de mal uso o detección de anomalías o comportamientos anómalos emplea en el contexto de detección de intrusiones de insiders threat en intranets académicas?

La Figura 13 muestra los resultados obtenidos durante la revisión, mayor detalle se puede observar en la Tabla 46 del Anexo B p.192, respecto a Q2.4 Métodos/Herramientas de detección de anomalías de insiders threat en intranets académicas.

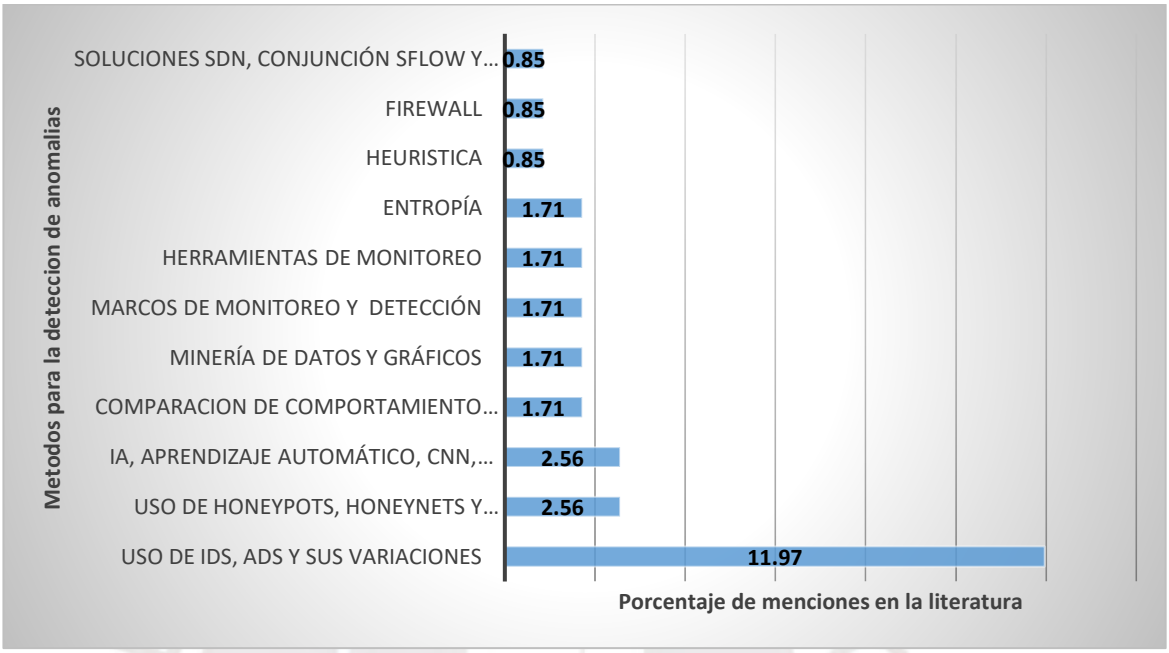


Figura 13: Q2.4 Método/Herramientas de detección de anomalías de insiders threat en intranets académicas.
Fuente: Elaboración propia. Porcentajes calculados sobre 117 estudios revisados.

El método más utilizado para la detección de anomalías en redes académicas son los sistemas de detección de intrusos y sus diferentes variantes con un porcentaje de 11.97%, tiene relación a que estos sistemas suelen trabajar como herramientas de captura de datos en formatos PCAP lo que es de gran ayuda para el análisis posterior en base a las necesidades de los investigadores en el ambiente académico. En segundo lugar, se nombra al uso de honeypots, honeynets, honeytokens en un porcentaje del 2.56%. En igual porcentaje métodos donde se aplica Inteligencia Artificial, aprendizaje automático, CNN, KNN, RNN, PCA, SVM, ML, DL. Y en tercer lugar comparación de comportamiento de usuarios con el 1.71%.

Q2.5 ¿Qué método se usa para identificar insiders threat en tiempo real (Real Time usage profiling)?

La Figura 14 muestra los resultados de este criterio, mayor explicación se puede obtener en la Tabla 47 del Anexo B p.193, referente a Q2.5 Métodos para identificar insiders threat en tiempo real.

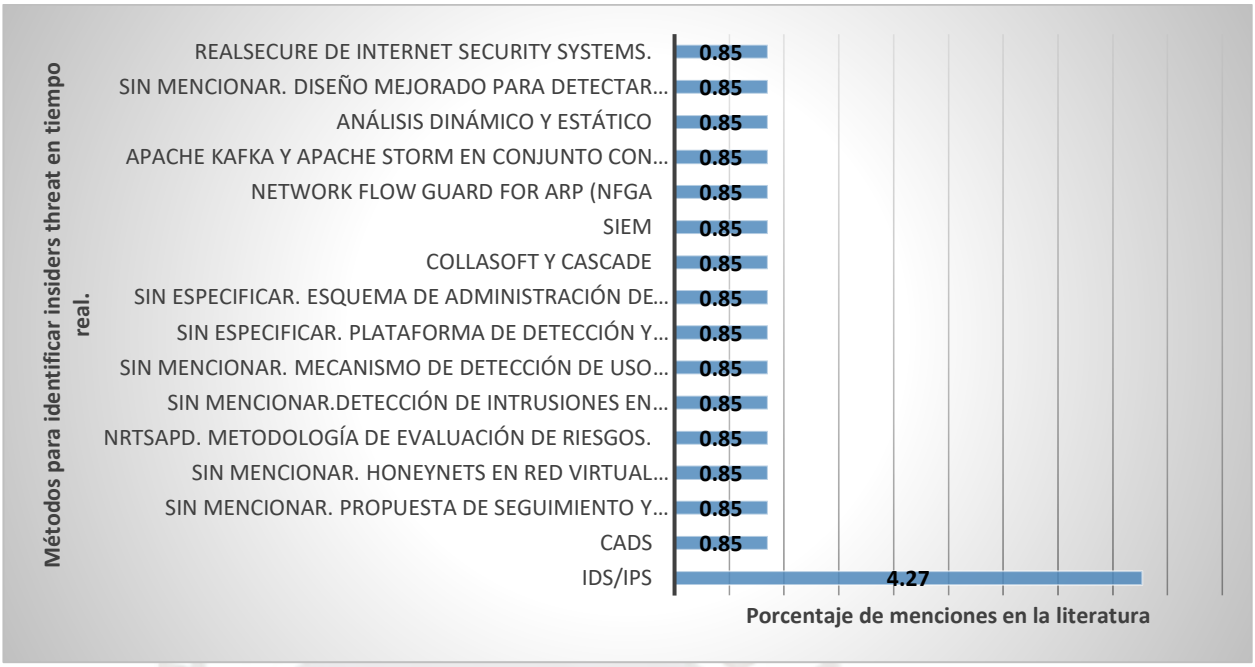


Figura 14: Q2.5 Métodos para identificar insiders threat en tiempo real.
Fuente: Elaboración propia. Porcentajes calculados sobre 117 estudios revisados.

Como se observa en la Figura 14, el principal método es la utilización de sistemas de detección y prevención de intrusos basado en coincidencia de reglas, principalmente SNORT en un porcentaje de 4.27%, Además de varias propuestas con 0.85 % como CADS que es un sistema de detección de anomalías basado en un marco de aprendizaje no supervisado para detectar amenazas internas, o la propuesta de un nuevo algoritmo de predicción de anomalías, donde se señala que la medición de la red es uno de los temas clave para la detección y mitigación de intrusiones en tiempo real.

Y otras en las que no se menciona el nombre, y que se proponen como de seguimiento y alerta en tiempo real, también honeypots virtuales para la detección de intrusos en ACM12. Además, nuevos sistemas de red basados en Internet e intranet o herramientas para la mitigación de ataques externos o internos que han ido evolucionando como en IEEE27 que las empresas pueden utilizar para compartir información y realizar negocios con socios en línea.

Q2.6 ¿Qué algoritmo de análisis de data emplean en la identificación de insiders threats?

La RSL identificó una diversidad de enfoques algorítmicos utilizados en la detección de amenazas internas en intranets académicas. Si bien los algoritmos aplicados

difieren en su naturaleza técnica, todos comparten el objetivo común de identificar comportamientos anómalos o maliciosos generados por usuarios internos o por el uso indebido de recursos de red.

Con el fin de estructurar de manera más clara el panorama metodológico y atender a la observación sobre la dispersión en la clasificación de algoritmos, se realizó una reclasificación técnica, agrupando los enfoques en función de su categoría metodológica. Esta organización permite observar con mayor precisión las tendencias predominantes y facilita la comprensión del tratamiento actual del problema. La Tabla 49 del Anexo B pag. 201, presenta dicha reclasificación, estructurada en las siguientes categorías: aprendizaje automático supervisado, aprendizaje no supervisado, redes neuronales, aprendizaje por refuerzo, algoritmos evolutivos y bioinspirados, medidas de entropía, reglas de asociación, reducción de dimensionalidad (PCA), detección embebida en IDS, algoritmos desarrollados por los propios investigadores y otros enfoques específicos.

Los resultados de esta reclasificación, calculados sobre los 117 estudios revisados, evidencian que el aprendizaje automático supervisado es la categoría más frecuente (5.13%), seguida por el desarrollo de algoritmos personalizados por los propios autores (5.98%), redes neuronales y aprendizaje profundo (4.27%) y algoritmos embebidos en sistemas IDS (4.27%). También se identifican enfoques menos frecuentes como: clustering optimizado, reglas de asociación, entropía o PCA aplicados en contextos específicos y con menor representación porcentual (entre 0.85% y 1.71% cada uno).

Esta distribución se presenta en la Figura 15, la cual resume visualmente los porcentajes según tipo metodológico.

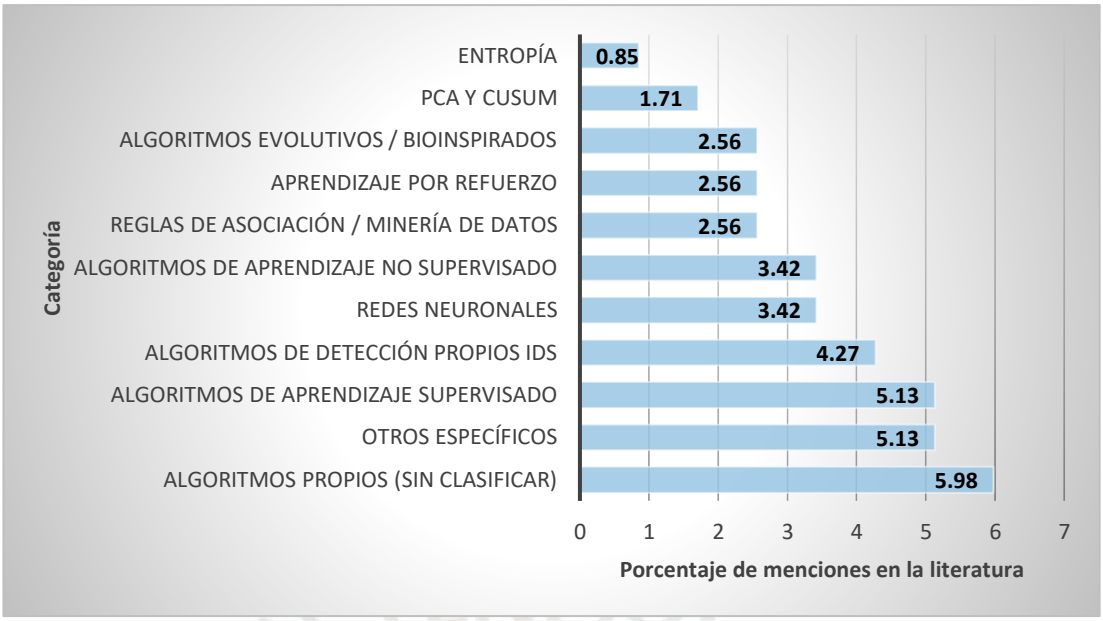


Figura 15: Q2.6 Distribución de algoritmos utilizados en el análisis de datos para la identificación de amenazas internas según categoría metodológica.
Fuente: Elaboración propia. Porcentajes calculados sobre 117 estudios revisados.

Esta diversidad metodológica no solo refleja el dinamismo del campo, sino que también resalta la ausencia de un enfoque estandarizado en la identificación y control de amenazas internas en entornos académicos, lo que refuerza la pertinencia de propuestas sistemáticas como la desarrollada en esta tesis.

Q2.7 ¿Qué estudios aplican análisis de tramas para la identificación en insiders threat y cómo lo hacen?

Se han identificado 14 papers que mencionan el análisis de trazas o paquetes durante el proceso de sus investigaciones, la Figura 16 muestra los resultados obtenidos. Se describe más información en Tabla 50 del Anexo B p.202, respecto al criterio Q2.7 ¿Qué estudios aplican análisis de tramas para la identificación en insiders threat y cómo lo hacen?

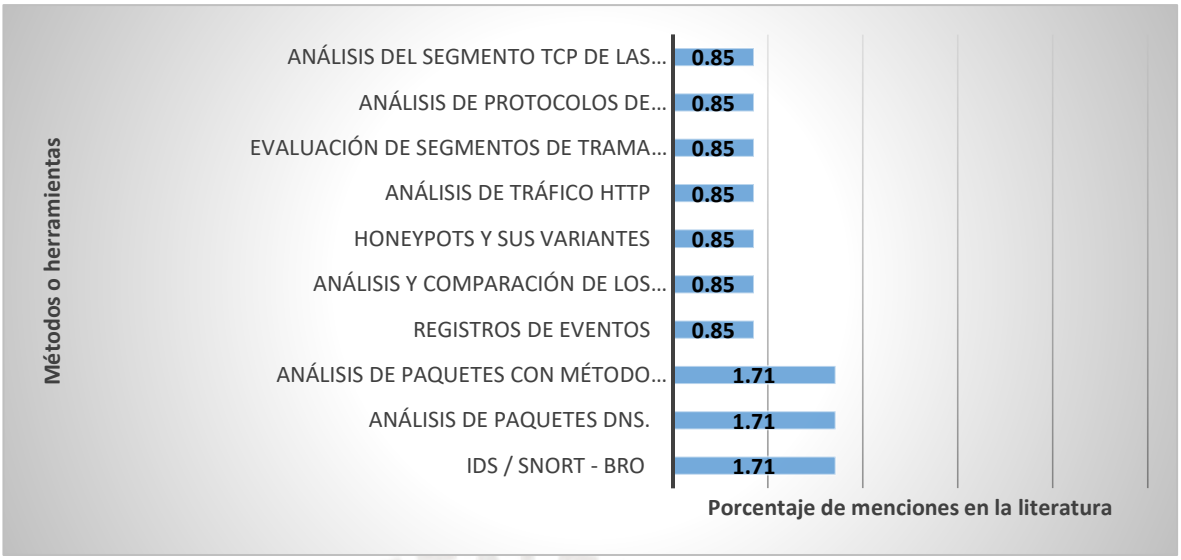


Figura 16: Q2.7 ¿Qué estudios aplican análisis de tramas para la identificación en insiders threat y cómo lo hacen?
Fuente. Elaboración propia. Porcentajes calculados sobre 117 estudios revisados.

Del total de artículos en la RSL, 14 papers representan el 11.97% que hacen referencia al análisis de tramas para la identificación en insiders threat y cómo lo hacen. De los cuales el 1.71% destacan la utilización de la herramienta IDS a través de SNORT y BRO IDS empleados para el análisis de los paquetes e identificación de anomalías, estos trabajan con reglas de concordancia de ataques conocidos como se menciona en SCO37 e IEEE45. En igual porcentaje destaca el análisis de paquetes DNS en SCO31, SCO35, así como el análisis de paquetes con método propio como se resalta en SCO45, donde las evaluaciones que utilizan trazas de red de diferentes protocolos de IoT muestran beneficios significativos en precisión, eficiencia y universalidad sobre los métodos de vanguardia o toman otros datos necesarios para sus investigaciones como señala SCO49.

Q3. ¿Qué metodología para identificar, evaluar y controlar insiders threat en intranets académicas se emplea y cuál es la más adecuada?

Se consideran dos criterios Q3.1 y Q3.2

Q3.1 ¿Qué metodología para identificar, evaluar y controlar insiders threat se emplea, ¿cuál es la más adecuada?

La tendencia actual hacia la seguridad de redes es la identificación de eventos anormales o anómalos mediante la utilización de herramientas o métodos, esto en

concordancia a una metodología ya establecida o una adaptación de esta. Sin embargo, durante la RSL se pudo evidenciar ampliamente que la tendencia se dirige hacia el uso de una metodología propia propuesta por los investigadores, un método propio o por otro lado un conjunto de pasos que se siguen en cierto orden para cumplir con la detección o mitigación de eventos anómalos o en si de ataques perpetrados tanto desde dentro o fuera de una red de campus o institucional con un porcentaje del 52.14%, como se observa en la Figura 17. La Tabla 51 del Anexo B p.205, referente a Q3.1 ¿Qué metodología para identificar, evaluar y controlar insiders threat se emplea?, se muestra el detalle de los resultados obtenidos en este criterio.

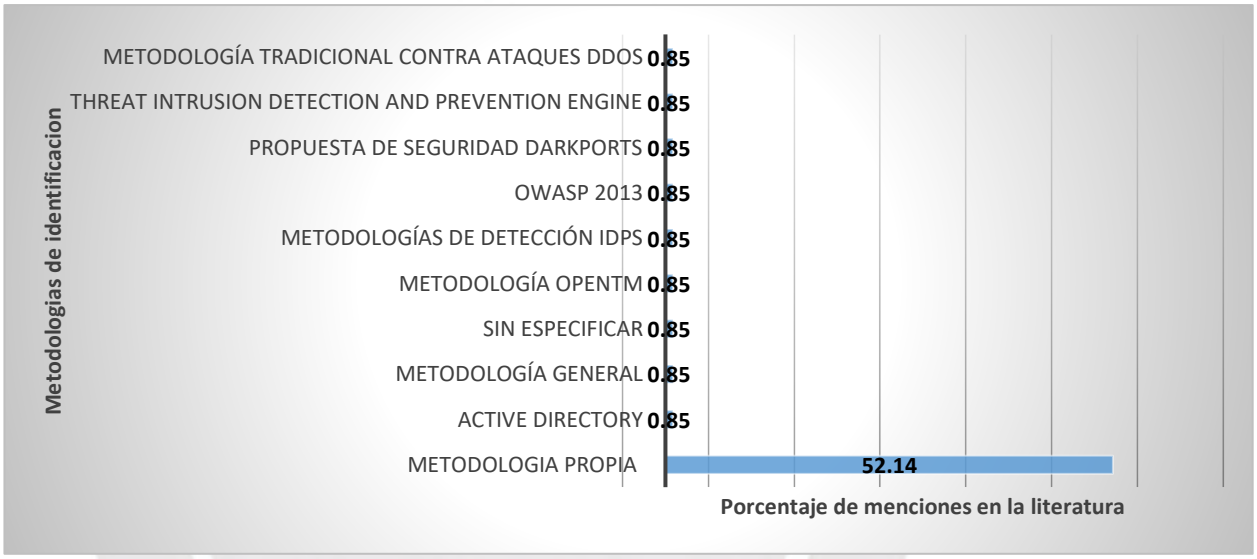


Figura 17: Q3.1 ¿Qué metodología para identificar, evaluar y controlar insiders threat se emplea, ¿cuál es la más adecuada?
Fuente. Elaboración propia. Porcentajes calculados sobre 117 estudios revisados.

Además, se mencionan, un conjunto de metodologías con el 0.85% como Active Directory empleada para la detección de activos e información sobre datos confidenciales en un campus para posterior análisis forense ACM07. OpenTM para la estimación de tráfico basada en pull obteniendo datos de flujo de OpenFlow en SCO08. OWASP 2013 para la clasificación de amenazas de aplicaciones web en SCO30. Propuesta de seguridad DarkPorts, combina honeypots, puertos virtuales y puertos físicos en SCO38. Threat Intrusion Detection and Prevention Engine (TIDPE) para detección y prevención de amenazas detallado en SCO06. Metodología tradicional contra ataques DDoS en IEEE44. Sin embargo, no se especifica una metodología como la más adecuada, en la mayoría se utiliza metodologías propias para identificar, evaluar y controlar insiders threat.

Q3.2 ¿Existen modelos, normas particulares en seguridad en intranets de redes académicas?

La Figura 18 muestra los resultados obtenidos en este criterio, más información se incluye en la Tabla 52 del Anexo B p.206.

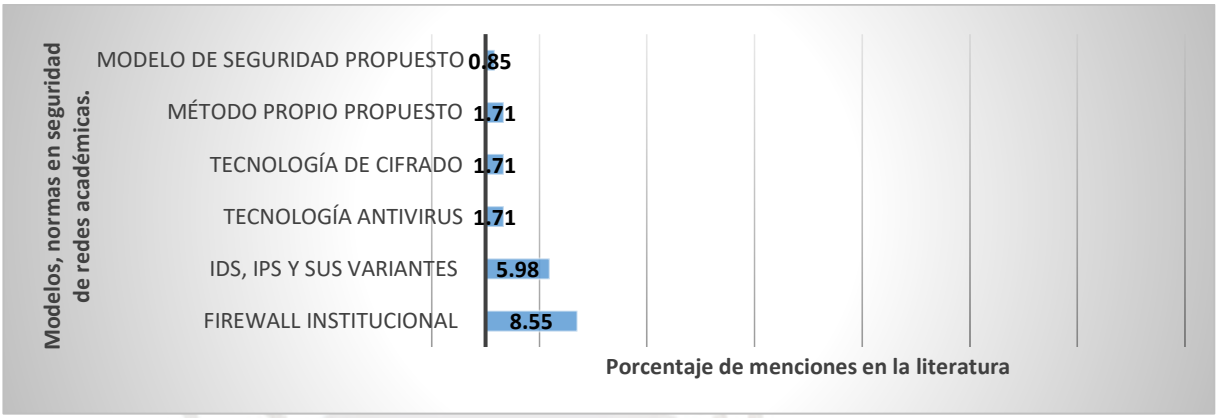


Figura 18: Q3.2 ¿Existen modelos, normas particulares en seguridad en intranets de redes académicas?
Fuente. Fuente: Elaboración propia. Porcentajes calculados sobre 117 estudios revisados.

La Figura 18 muestra la utilización de un Firewall con el objetivo de denegar acceso a recursos institucionales basado en reglas en un 8.55%. En un porcentaje del 5.98% los sistemas de detección y prevención de intrusos (IDS, IPS y sus variantes), analizan el tráfico de la red y en caso de detectar una concordancia entre el tráfico y las reglas definidas lanza una alerta al administrador de la red o bloquea la amenaza. En un porcentaje del 1.71% tecnología antivirus o de cifrado, ya sea para la protección de virus o como medida de ciberseguridad.

3.2 Conclusiones de la RSL

En relación con la primera pregunta de investigación Q1. ¿Qué tipos de insiders threat o amenazas internas existen en intranets académicas y cuáles son sus fuentes de datos? y sus cuatro criterios de inclusión, se considera en Q1.1 y Q1.2 Las amenazas internas más comunes en redes de datos y redes académicas son los ataques de Denegación de Servicio (DoS) y sus variantes Distribuidas (DDoS), representando un 39.31% y un 13.68% de los estudios revisados, respectivamente.

Con relación a Q1.3 se ha podido identificar tres tipos de fuentes de datos: Psicología de usuarios, fuente de datos externa y fuentes de datos propias. Las principales fuentes de datos externos de insiders threats, más utilizadas en la literatura con un porcentaje de 9.4% es el conjunto de datos KDD99, NSL-KDD, Kyoto KDD-Cup que es principalmente utilizado para la evaluación de sistemas de detección de intrusos. Las fuentes de datos propias, aunque mencionadas, no son detalladas extensamente en la literatura.

Respecto a Q1.4 se identificaron 17 investigaciones que consideran insider threat para limitar el control de acceso a usuarios en intranets. La técnica más común es el uso de firewall de red con el 2.56% para fortalecer el control de acceso entre redes y ACL para supervisar el flujo de datos.

Respecto a la segunda pregunta Q2 ¿Qué herramientas, métodos o procedimientos de recolección de datos se emplean en el análisis de insiders threat, además que métodos de identificación o detección de amenazas se emplean?

Considerando sus parámetros de inclusión, se tiene en Q2.1 se describe el conjunto de herramientas *TCPdump, Ethereal* y *TCPReplay* para la captura de datos en formatos *PCAP* mediante puertos espejo como la más utilizada con el 11.97%. Seguido de *IDS* y sus variantes (*HIDS, NIDS, AIDS, SIEM, SNORT, SEBEK*) con un porcentaje del 9.4%.

Según Q2.2 y Q2.3, en el contexto de redes de campus, los sistemas de detección de intrusos (*NIDS*) son los más utilizados para la detección de anomalías (42.74%), siendo SNORT una herramienta destacada para el análisis de tráfico basado en protocolos TCP/IP.

De Q2.4 a Q2.7 el método más utilizado para la detección de anomalías en redes académicas son los sistemas de detección de intrusos con un porcentaje de 11.97%. Se corrobora en Q2.5, respecto a los métodos para identificar insiders threat en tiempo real, destacándose el uso de los sistemas de detección y prevención de intrusos basado en coincidencia de reglas, principalmente SNORT en un porcentaje de 4.27%.

En Q2.6 se revela que los algoritmos más utilizados para la detección de anomalías en intranets académicas corresponden al aprendizaje automático supervisado (5.13%), seguido por redes neuronales y aprendizaje profundo (4.27%), algoritmos

desarrollados ad hoc por los propios investigadores (5.98%) y mecanismos de detección embebidos en sistemas IDS como SNORT (4.27%). Lo que pone de manifiesto una notable dispersión en los enfoques utilizados, evidenciando la ausencia de una taxonomía consolidada o un marco estandarizado para el tratamiento de amenazas internas.

En Q2.7 se determina que el 1.71% destacan la utilización de la herramienta IDS a través de SNORT y BRO IDS empleados para el análisis de los paquetes e identificación de anomalías, estos trabajan con reglas de concordancia de ataques conocidos. En conclusión, *SNORT* emerge como una herramienta clave en la detección de amenazas internas en intranets académicas, especialmente valorada por su efectividad en la detección en tiempo real mediante el uso de reglas predefinidas.

Respecto a la tercera pregunta, Q3. ¿Qué metodología para identificar, evaluar y controlar insiders threat en intranets académicas se emplea y cuál es la más adecuada?
Q3.1 y Q3.2 identificaron la ausencia de metodologías estándar aplicables a la detección y mitigación de amenazas internas en redes académicas, con un 52.14% de los estudios utilizando metodologías propias. Además, los sistemas de detección y prevención de intrusos (IDS, IPS) se destacan en un 5.98%, siendo utilizados para monitorear y bloquear accesos no autorizados.

3.3 Consideraciones para la implementación de la propuesta de control de amenazas insiders en intranets de campus académicos.

Para la implementación de la propuesta de control de amenazas insiders, se consideran los resultados obtenidos en la RSL:

1. Selección de Amenaza a Controlar: Considerando los resultados de Q1, tipos de insiders threat o amenazas internas existen en intranets académicas y cuáles son sus fuentes de datos. Se seleccionó los ataques DoS y DDoS como las principales amenazas a controlar, dado su alto porcentaje de ocurrencia en redes académicas con el 13.68% coincidente en redes de datos con el 39.31%.

2. Herramientas de Captura y Análisis de Datos: Para la detección de insiders en tiempo real, se utilizará sistemas de detección de intrusos (NIDS-SNORT) y herramientas de captura de datos en formato PCAP, implementando puertos espejo (mirror) para el monitoreo continuo y análisis detallado del tráfico de red.

3. Metodología Propuesta: Se desarrollará una metodología propia que incluye un conjunto de pasos ordenados para la detección y mitigación de amenazas internas, adaptada a las necesidades específicas de las intranets académicas. Esta metodología empleará NIDS-SNORT para la detección de patrones maliciosos en tiempo real y ACLs para el filtrado de paquetes.

4. Escenarios de Prueba: La metodología será evaluada en un entorno controlado utilizando equipos físicos de redes definidas por software (SDN), con el objetivo de analizar su efectividad y el impacto en el rendimiento de la red al implementar las medidas de control propuestas.

Dada su estructura modular y capacidad de adaptación, esta propuesta metodológica constituye una base técnica robusta que puede ser replicada, ajustada y profundizada en estudios futuros orientados a la detección y mitigación de amenazas internas en entornos académicos.

La descripción de la metodología para el control de amenazas internas (insider threat) en intranets de campus académicos, se presenta en el CAPITULO 4.

SEGUNDA PARTE: DISEÑO METODOLÓGICO Y RESULTADOS

CAPÍTULO 4. PROPUESTA DE METODOLOGÍA PARA EL CONTROL DE AMENAZAS INTERNAS EN INTRANETS DE CAMPUS ACADÈMICAS.

El presente capítulo propone una metodología para la detección y mitigación de amenazas internas en redes académicas, respondiendo a la ausencia de estándares en este ámbito, tal como se planteó en el acápite 3.3 del capítulo 3. Para ello, se adapta la metodología OSSTMM V3.0, cuya justificación se detalla en el Capítulo 2 (Marco Teórico), Sección 2.5, que aborda las metodologías para la evaluación de la seguridad de redes. Una vez evaluado el canal humano y al determinar la existencia de riesgo de seguridad en la intranet, se realiza el análisis de tráfico en tiempo real utilizando NIDS-SNORT, para la identificación de amenazas internas. Además, se propone el control de una amenaza interna en un escenario real SDN aplicando políticas de QoS con ACLs para evaluar su incidencia en el rendimiento de la intranet como fase final del proceso. El desarrollo de la propuesta se describe en 4 etapas:

La etapa 1, diagnóstico de seguridad en el canal humano de la intranet académica, en la que se aplica OSSTMM V3.02 (Herzog, 2010) adaptada. Se continúa el proceso con la etapa 2, análisis en tiempo real de la data de la intranet del campus académico para identificar amenazas internas con la utilización de NIDS-SNORT y su validación con la herramienta Nexpose, al realizar la comparación de los datos.

La etapa 3 es la selección de la amenaza a controlar, para ello se realiza una comparación de los resultados obtenidos en la etapa 2, del análisis en tiempo real de la data en la intranet de campus académica y los resultados obtenidos en el capítulo 3 referente a la RSL de amenazas insiders en campus académicos.

La etapa 4, es la propuesta de control de amenaza insider, que se desarrolla en un escenario SDN con equipos reales. En este escenario se plantean políticas de QoS con ACLs en el controlador FloodLigth para el control de una amenaza interna y se evalúa su incidencia en la mejora del rendimiento de la intranet de campus académico. El esquema de la Figura 19 detalla la metodología de Control de Amenazas insiders en este contexto.

Figura 19: Propuesta de la metodología de Control de Amenazas insiders.
Fuente. Elaboración propia

A continuación, se describe cada uno de los procesos.

4.1 Etapa 1. Diagnóstico de seguridad de la intranet académica en el canal humano.

Considera dos partes prácticas: la primera es la aplicación de OSSTMM V3.02 adaptada para determinar un análisis de la seguridad respecto al canal humano para identificar las brechas de seguridad con el cálculo del RAV. La segunda considera el uso de NIDS-SNORT para realizar el análisis de la red en tiempo real y detectar amenazas internas (insiders) en intranets de campus académicas.
En 4.1.1 se describe la adaptación de la metodología OSSTMM.

4.1.1 Adaptación de la metodología OSSTMM para el diagnóstico de seguridad de la intranet académica en el canal humano.

En base a la metodología descrita en el capítulo 2 y al diagrama de bloques de la metodología OSSTMM en la Figura 5, se adaptó cada fase, aplicando una evaluación relevante y específica para el entorno académico, como se destaca en las sugerencias de (Herzog, 2010): "las evaluaciones de seguridad deben ser

específicas del entorno y contextualmente relevantes" (pág. 108). Además, estudios recientes demuestran la importancia de la personalización de los sistemas de detección y prevención de intrusiones según el contexto específico de la red (Girdler & Vassilakis, 2021).

En la adaptación también se valora porosidad, controles y limitaciones de la metodología OSSTMM(Herzog, 2010) descritos en la Tabla 3 del capítulo 2 p.41 y aplicados según el contexto. Estos controles se dividen en clase A y B, según se describe:

a. Controles de Clase A:

Orientados al manejo interno del canal y a garantizar su funcionalidad operativa. Incluyen medidas como autenticación, indemnización, resistencia, subyugación y continuidad. Estos controles se enfocan en prevenir errores operativos y minimizar los riesgos humanos dentro del sistema auditado.

b. Controles de Clase B:

Diseñados para proteger los activos de información y mitigar riesgos derivados de su exposición. Estos controles incluyen no repudio, confidencialidad, privacidad, integridad y sistemas de alarma. Su enfoque está en garantizar la protección de los datos y la confiabilidad de las acciones realizadas dentro del canal.

Estas categorías están directamente relacionadas con el cálculo del RAV, una métrica cuantitativa que mide la porosidad del canal auditado y su superficie de ataque. La interacción entre la porosidad, los controles y las limitaciones permite evaluar la seguridad de manera precisa y replicable (Herzog, 2010)

De este modo se llevó a cabo un análisis propio, incluyendo evaluaciones en la intranet académica para la auditoría como se muestra a continuación.

1) FASE 1: INDUCCIÓN

Esta fase consta de revisión de la postura, logística y verificación de detección activa. A continuación, se explica cada una.

1.1) REVISIÓN DE LA POSTURA

Considera leyes, ética, las políticas, los reglamentos de la industria y la cultura que influyen en los requisitos de seguridad y privacidad para el alcance. (Herzog, 2010, pag.106)

En el contexto académico, se optó por excluir los factores económicos y la cultura regional debido a su impacto poco significativo en la seguridad de la intranet. En su lugar, la metodología propuesta se centra en aspectos como las políticas, la legislación, las regulaciones, la cultura organizacional y las relaciones internas, ajustándolos a las normativas específicas y a las dinámicas culturales de cada institución educativa. Este enfoque permite una evaluación más eficaz, ya que se concentra exclusivamente en los elementos que tienen un efecto directo sobre la seguridad de la intranet académica, pues "adaptar las políticas de seguridad para alinearse con estas regulaciones es crucial para una gestión efectiva de la seguridad" (Cojocariu et al., 2020).

1.2.) LOGÍSTICA

El proceso de preparación del entorno de prueba de canal es esencial para evitar errores que podrían resultar en resultados de prueba inexactos. Este entorno considera tres elementos clave: los equipos de comunicación, los canales de comunicación y el factor tiempo (Herzog, 2010, pag.107. En el contexto académico, se realizó una adaptación personalizada de los servicios y los horarios, dado que las características únicas de este entorno permiten mejorar la precisión y la efectividad de las pruebas de seguridad (Sarker, 2024). Esta personalización asegura que todos los factores relevantes sean considerados y abordados adecuadamente, ajustando la evaluación de manera que refleje las particularidades de la intranet académica.

- Equipos de comunicación: Se consideran dispositivos y servicios que proporcionan identificación al receptor, como la identificación de llamadas, servicios de fax, registros de direcciones IP y servidores de correo electrónico (Herzog, 2010, pag.107). En la adaptación al entorno académico, se incluyen servicios específicos de la intranet, como voz, video y transmisión de datos, alineados con los requisitos de comunicación de la institución.
- Canales de comunicación: Se prioriza el uso del idioma según la región donde se aplica la intranet académica. Por ejemplo, en regiones hispanohablantes, se utiliza predominantemente el español. Esta selección lingüística garantiza que las políticas de seguridad y las instrucciones de uso sean claras y accesibles para todos los usuarios, mejorando la comprensión y el cumplimiento de las medidas de seguridad.

- Tiempo: Se consideran las zonas horarias y los horarios de trabajo diferenciados entre los usuarios de la intranet académica, lo que permite una planificación más precisa de las pruebas de seguridad y asegura que estas sean relevantes y efectivas para todos los usuarios en diferentes ubicaciones y horarios.

1.3) VERIFICACIÓN DE DETECCIÓN ACTIVA

Hace referencia a la determinación de los controles activos y pasivos diseñados para detectar intrusiones en la red, abarcando aspectos como el monitoreo de canales, la supervisión y la asistencia técnica (Herzog, 2010). Sin embargo, en el caso específico de las intranets académicas en estudio, donde los servicios de acceso a internet y telefonía son básicos, y el soporte técnico y la seguridad de la red están gestionados por el Departamento de Tecnologías de la Información de las universidades, siguiendo políticas institucionales específicas, no se considera necesario implementar esta fase en la metodología. Esto se debe a la restricción de acceso a la configuración y manejo de políticas de seguridad, ya que dichas actividades son ejecutadas exclusivamente por el departamento de tecnologías de la información. En consecuencia, el enfoque metodológico se centra en controles apropiados para las características y limitaciones de las intranets académicas, priorizando la simplicidad operativa y la respuesta directa a incidentes dentro del marco de capacidades existentes.

2) FASE 2: INTERACCIÓN

En esta fase, el objetivo es calcular el valor de la seguridad operacional, también conocida como porosidad, y evaluar los controles de interacción de clase A y B, tal como se indica en la Tabla 3 del capítulo 2 p.41 que detalla la Porosidad, los Controles y las Limitaciones según la Metodología OSSTMM V3.02. La fase de interacción incluye varios componentes clave: auditoría de la visibilidad, verificación de acceso, verificación de confianza y verificación de controles (Herzog, 2010).

2.1) AUDITORIA DE LA VISIBILIDAD

La auditoría de la visibilidad se enfoca en realizar pruebas de enumeración y verificación para evaluar qué tan visible es el personal con el que se puede interactuar a través de diversos medios.(Herzog, 2010). Esta auditoría aborda dos aspectos principales:

- Identificación de acceso: Evaluación de las interacciones con el personal que tiene acceso autorizado a ciertos recursos.
- Enumeración de personal: Conteo y clasificación del personal y áreas con acceso autorizado y no autorizado a los activos, como los cuartos de telecomunicaciones.

En el contexto académico, la adaptación de este enfoque implica la identificación y enumeración de interacciones específicas entre técnicos, estudiantes, docentes y personal administrativo, así como la revisión de los procesos de gestión de acceso a los activos de la intranet. Este enfoque adaptado proporciona una visión clara y detallada de las interacciones que ocurren dentro del entorno académico, mejorando la capacidad para comprender y evaluar la visibilidad de las entidades involucradas. Esta mejora en la visibilidad es crucial para identificar potenciales puntos vulnerables y fortalecer las medidas de seguridad dentro de la red de la institución.

2.2) VERIFICACIÓN DE ACCESO

La verificación de acceso se refiere a los procesos, pruebas de requerimientos y métodos necesarios para acceder a los activos dentro del alcance de la red de la intranet académica. Este componente de seguridad se centra en tres aspectos clave: el proceso de acceso, la autoridad, y la autenticación (Herzog, 2010).

Para adaptar este enfoque al entorno académico, se evalúa procesos acerca de cómo se accede a los activos físicos y digitales de intranets académicas, considerando los escenarios posibles en los que podría ocurrir un acceso no autorizado. Este enfoque detallado facilita la detección temprana y la gestión efectiva de accesos no autorizados, mejorando significativamente la seguridad de la intranet académica.

Se definieron los siguientes parámetros para la verificación de acceso:

- Proceso de acceso: Consiste en los procedimientos y métodos específicos utilizados para obtener acceso a los activos de la intranet, incluyendo la identificación de posibles escenarios en los que se podría acceder sin autorización explícita. Este análisis ayuda a identificar y cerrar brechas de seguridad.
- Autoridad: Define qué personal tiene derecho a acceder a los diferentes activos dentro de la red, no se toma en cuenta en el contexto de intranets académicas, pues la gestión y control de los activos están exclusivamente a cargo de los técnicos autorizados. Dado que no existe la posibilidad de que

otros usuarios interactúen directamente con estos recursos críticos, el control de acceso ya está centralizado en este equipo técnico. Por lo tanto, el parámetro de autoridad no es necesario en este entorno, donde las políticas de acceso están estrictamente controladas y limitadas al personal técnico autorizado de la institución.

- Autenticación: Se refiere a los métodos implementados para verificar la identidad del personal que interactúa con los sistemas de recepción y acceso. Contabilizar estos métodos es esencial para prevenir accesos no autorizados y garantizar que todas las interacciones sean realizadas por el personal autorizado.

Esta estructura permite una comprensión más profunda de los mecanismos de acceso en el entorno académico y refuerza la seguridad mediante una gestión estricta y controlada de quién y cómo se puede acceder a los activos de la institución.

2.3) VERIFICACIÓN DE CONFIANZA

La verificación de confianza implica realizar pruebas para evaluar la fiabilidad del personal con acceso a información confidencial o activos físicos dentro del alcance de la red académica. Esta evaluación aborda riesgos clave, como la tergiversación, el fraude, la falta de dirección, el phishing, el abuso de recursos y el uso del temor (In Terrorem) (Herzog, 2010).

Sin embargo, en el contexto de las intranets académicas, ciertos aspectos no son aplicables. Por ejemplo, los casos de fraude y phishing relacionados con solicitudes de préstamo de laboratorios no representan un riesgo, ya que los documentos son redactados y controlados por las secretarias de cada escuela, lo que garantiza la transparencia y autenticidad del proceso.

El abuso de recursos, en cambio, es un punto crítico que requiere atención, especialmente en relación con los técnicos que tienen acceso directo a los activos. Para ello, se considera el proceso por el cual los estudiantes y el personal técnico acceden a los activos, asegurando que el control sobre su uso sea adecuado. Este enfoque permite identificar y gestionar proactivamente el mal uso de recursos y fraudes potenciales, fortaleciendo la seguridad de la red académica.

La adaptación de la verificación de confianza en el entorno académico se enfoca en los puntos de mayor riesgo, evaluando de manera precisa el manejo de activos y la fiabilidad del personal. La supervisión continua de la actividad en la intranet es esencial para detectar y prevenir fraudes y suplantación de identidad, debido a la

cantidad de datos sensibles gestionados, como credenciales de acceso, información financiera y datos personales (Marchand-Niño & Vargas-Malca, 2023. Esto asegura la protección efectiva de los activos institucionales y la minimización de riesgos.

2.4) VERIFICACIÓN DE CONTROLES (CONTROLES DE CLASE B)

La verificación de controles de Clase B se refiere a la evaluación de los diferentes tipos de controles implementados para proteger el valor de los activos dentro de una red, tales como el no repudio, la confidencialidad, la privacidad, la integridad y los sistemas de alarma. (Herzog, 2010). Como se describió en la Tabla 3: Porosidad, controles y limitaciones en la metodología OSSTMM del Capítulo 2 p.41 En el contexto de un campus académico esta adaptación incluye la documentación de posibles fraudes y abusos de recursos, con un enfoque especial en las prácticas del personal técnico. Al adaptar estos controles al entorno académico, se garantiza una evaluación más precisa y relevante de las prácticas de seguridad, abordando de manera efectiva las áreas de mayor riesgo considerándolas en el cálculo del RAV.

A continuación, se detallan los controles que deben considerarse para una evaluación exhaustiva:

- Irrefutabilidad (No repudio): Este control asegura que las acciones o eventos registrados en la red no puedan ser negados posteriormente, pues la implementación de registros detallados y una identificación adecuada del personal son esenciales para obtener evidencia específica y prevenir el repudio en la intranet académica (Rincy N & Gupta, 2021. Además, la aplicación de técnicas de detección de intrusiones garantiza que todas las interacciones y accesos sean registrados y verificables, proporcionando una capa adicional de seguridad contra la denegación de acciones previas.
- Confidencialidad: Proteger la información sensible es esencial en cualquier institución educativa. La confidencialidad se garantiza a través de una segmentación eficiente de la comunicación entre los responsables de los datos dentro del alcance de la intranet académica. Es indispensable implementar medidas robustas que aseguren que la información no sea accesible a personas no autorizadas (Rincy N & Gupta, 2021). Además, se deben identificar y contabilizar los segmentos de comunicación que sean efectivos en mantener la seguridad y control de los datos, garantizando así un manejo adecuado de la información sensible.
- Privacidad: La protección de la privacidad de los usuarios se garantiza mediante la implementación de políticas claras y el uso de tecnologías

adecuadas. Estudios han demostrado que estas medidas pueden mejorar significativamente la protección de la privacidad en entornos académicos, asegurando que los datos personales y la información sensible no sean expuestos ni comprometidos (Rincy N & Gupta, 2021). Por lo tanto, se deben contabilizar los métodos eficientes empleados para asegurar este control.

- Integridad: Este control se enfoca en asegurar que la información almacenada o transmitida no pueda ser alterada sin el conocimiento de las partes involucradas, manteniendo la integridad de los datos para proteger la exactitud y la confiabilidad de la información crítica en los activos físicos o digitales (Rincy N & Gupta, 2021).
- Alarma: Los sistemas de alarma son fundamentales para garantizar una respuesta rápida ante emergencias. La integración de alarmas avanzadas, junto con su monitoreo continuo, permite una reacción oportuna y efectiva ante cualquier incidente, lo que minimiza el impacto potencial en la seguridad de la red académica (Rincy N & Gupta, 2021). Es necesario contabilizar los sistemas de advertencia existentes para asegurar su eficacia en situaciones de emergencia.

La implementación y adaptación de estos controles en el entorno académico permiten una evaluación más detallada y efectiva de las prácticas de seguridad diarias, asegurando una protección integral de los activos críticos de la institución.

3) FASE 3: Evaluación de la Confiabilidad y Gestión de Recursos (INVESTIGACIÓN)

La fase 3, se compone de varias actividades clave diseñadas para evaluar y mejorar la postura de seguridad dentro de la red académica. Estas actividades incluyen la verificación de procesos, verificación de entrenamiento, validación de la propiedad, revisión de segregación, verificación de exposición, y exploración de inteligencia competitiva (Herzog, 2010).

3.1) VERIFICACIÓN DE PROCESOS

La verificación de procesos se refiere a pruebas diseñadas para evaluar cómo se mantiene la conciencia de seguridad funcional entre el personal a través de los procesos operativos. Esta subfase está relacionada con la revisión de la postura de seguridad adoptada por la organización.(Herzog, 2010). Los aspectos clave que se consideran son: mantenimiento, desinformación, diligencia, e indemnización.

En el contexto académico, esta verificación se adapta a través de evaluaciones de cursos de capacitación en seguridad para estudiantes, docentes y personal técnico, así como la revisión de documentos legales relacionados con el uso de activos. Estos elementos proporcionan una evaluación integral de la conciencia de seguridad dentro de la intranet académica, asegurando que los usuarios estén informados y actúen de manera responsable con los recursos de la red. Los puntos específicos son los siguientes:

- Mantenimiento: Relacionado con la revisión de la postura de seguridad, esta actividad se inició en la fase de inducción, donde se evalúa si se han impartido cursos de capacitación en temas de seguridad al personal de la intranet académica. Esta revisión asegura que el personal mantenga una conciencia continua de las mejores prácticas de seguridad.
- Desinformación y Diligencia: Este punto implica la verificación de la existencia de cursos de capacitación en seguridad. Si tales cursos están disponibles, se evalúa su efectividad y alcance para asegurar que el personal esté adecuadamente informado y pueda actuar con diligencia en situaciones de riesgo de seguridad.
- Indemnización o Compensación: Se revisan los documentos legales que los usuarios deben aceptar para utilizar los activos tecnológicos de la red. Esta evaluación asegura que los usuarios comprendan plenamente sus responsabilidades y las consecuencias de cualquier violación de las políticas de seguridad. Esto refuerza la seguridad al evitar el abuso o la evasión de las normas establecidas.

La verificación de procesos, al ser adaptada al contexto de las intranets académicas, garantiza que la seguridad funcional no solo se mantenga, sino que también evolucione para enfrentar nuevas amenazas emergentes. La implementación de esta fase asegura que la comunidad educativa esté preparada para manejar de manera efectiva los riesgos asociados a la seguridad de la red, protegiendo los activos críticos de la institución y manteniendo un entorno de trabajo seguro para todos los usuarios.

3.2) VERIFICACIÓN DE ENTRENAMIENTO

La verificación de entrenamiento se centra en evaluar la capacidad de eludir o interrumpir los programas de educación y capacitación en seguridad destinados al personal de una institución académica. Esta evaluación es crucial para garantizar que el personal esté adecuadamente preparado para enfrentar amenazas de seguridad y seguir las políticas establecidas. Los aspectos clave que se abordan en

esta verificación son: mapeo educativo, interrupción de política, mapeo de conciencia, y hijacking (Herzog, 2010, pag.113). Si no existe capacitación únicamente se considera interrupción de política e hijacking.

Los puntos evaluados en esta fase incluyen:

- Evaluación de Programas Educativos de Seguridad (Mapeo educativo): Se analiza la frecuencia con la que se imparten cursos educativos o capacitaciones sobre seguridad dirigidos a todo el personal. Es esencial determinar si estos programas se realizan de manera regular y cubren todos los aspectos necesarios de la seguridad de la información, garantizando así una preparación continua y efectiva para todos los usuarios dentro de la red académica.
- Evaluación del Cumplimiento de Políticas de Seguridad (Interrupción de política): Consiste en la auto-vigilancia del personal para detectar interrupciones o incumplimientos de las políticas de seguridad. Este punto se enfoca en identificar y corregir comportamientos que puedan comprometer la postura de seguridad institucional.
- Análisis de Deficiencias en la Capacitación de Sensibilización en Seguridad (Mapeo de conciencia): Identificación de las brechas existentes en los procesos de capacitación de seguridad. Este análisis ayuda a determinar si hay áreas en las que el personal carece de conocimiento o comprensión de las políticas y procedimientos de seguridad.

- Detección de Manipulación de Información de Seguridad (Hijacking): Este aspecto evalúa hasta qué punto una persona no autorizada puede introducir información incorrecta o engañosa sobre las políticas de seguridad. Es crucial para prevenir la difusión de información errónea que pueda comprometer la integridad del sistema. La evaluación también abarca la gestión de información confidencial, como las contraseñas de acceso a sistemas, especialmente en el caso de usuarios con permisos temporales. Esta evaluación adquiere especial relevancia en entornos con un alto número de usuarios, como aquellos con más de 3,000 usuarios, donde el riesgo de manipulación de la seguridad es considerablemente mayor(Schwegman Lundberg & Woessner, 2019).

La capacitación en seguridad en el contexto académico es fundamental, ya que la educación continua a través de seminarios, foros, capacitación y orientación es la mejor manera de informar y preparar a los usuarios dentro de sus instituciones

individuales. Además, se requiere formación especializada, certificaciones y estudios adicionales para que los oficiales de seguridad de la información puedan proporcionar orientación con mayor confianza y eficacia (De Ramos & Esponilla II, 2022).

3.3) VALIDACIÓN DE ACTIVOS DIGITALES Y PROPIEDAD (VALIDACIÓN DE LA PROPIEDAD)

Implica la realización de pruebas para examinar la legalidad y la ética en el uso y distribución de información y recursos, tanto físicos como digitales, incluidos activos críticos como el software. Según el estándar OSSTMM V3.02, los puntos clave incluyen el compartir (Sharing), el uso ilegal o no autorizado de software (Black Market), y los canales de distribución de software (Sales Channels).(Herzog, 2010, pag.114).

En el contexto académico, esta validación se enfoca en cómo se distribuye y utiliza el software en los laboratorios, poniendo especial atención en el cumplimiento de las licencias y en la legalidad de los canales a través de los cuales se adquiere el software. Es crucial que las instituciones mantengan un inventario actualizado de todo el software utilizado, desde sistemas operativos hasta bibliotecas y marcos de trabajo. Este control riguroso permite una gestión eficaz de los activos digitales y minimiza el riesgo de uso indebido o adquisición de software ilícito, lo que podría comprometer la seguridad de la red académica.(Mogos, 2020)

Además, se recomienda que las instituciones académicas se suscriban a servicios de notificación de seguridad de los proveedores de software. Estos servicios proporcionan alertas sobre vulnerabilidades, actualizaciones críticas y otros aspectos de seguridad, lo cual es esencial para mitigar riesgos relacionados con la instalación de software no autorizado o proveniente de canales no confiables. El uso de software inseguro puede comprometer tanto la red académica como los datos que maneja.

Evaluaciones específicas:

- Prácticas de Compartición (Sharing): Evalúa el grado en que el software y otros activos digitales son compartidos entre el personal, ya sea de manera intencionada o accidental. Esto incluye el uso compartido de bibliotecas de software, recursos de programación o licencias individuales sin el control adecuado, lo que puede generar vulnerabilidades críticas en la red interna. Es fundamental implementar controles que aseguren que no se compartan

programas no licenciados o con permisos limitados de manera negligente. Si existe una política abierta de compartición de software en la organización, este punto no se considera para el cálculo del RAV.

- Uso Ilegal o No Autorizado de Software (Black Market): Revisa el licenciamiento del software utilizado en los laboratorios académicos, asegurando que todo el software provenga de fuentes legales y esté correctamente licenciado. El uso de software no autorizado, falsificado o adquirido a través de canales no oficiales representa un riesgo significativo para la integridad de la red académica. Esta evaluación garantiza que no existan prácticas de promoción o uso de software ilícito.
- Control de Canales de Distribución de Software (Sales Channels): Se verificaron los procesos de adquisición y distribución del software dentro de la institución. Es fundamental que los canales utilizados para adquirir el software sean legales y reconocidos, minimizando el riesgo de que software no licenciado o ilegal entre al entorno académico. Asimismo, la distribución interna del software debe realizarse bajo controles estrictos.

Esta evaluación proporciona una visión clara de las prácticas de gestión de activos digitales y uso de software en entornos académicos, identificando áreas vulnerables donde la seguridad de los recursos y la red podrían estar en riesgo. Medidas preventivas como el mantenimiento de inventarios actualizados y la suscripción a alertas de seguridad de los proveedores son esenciales para garantizar la legalidad y seguridad en el uso de software en las intranets académicas.

3.4) REVISIÓN DE SEGREGACIÓN

La revisión de segregación se centra en la separación adecuada de los activos de información privada o personal respecto a la información comercial o administrativa. Esto es esencial en entornos académicos, donde se manejan grandes volúmenes de datos sensibles, especialmente relacionados con estudiantes y personal administrativo. Según el estándar OSSTMM V3.02, los puntos clave de análisis incluyen la asignación de contención de privacidad y la identificación de limitaciones, así como información evidente y divulgación (Herzog, 2010, pag.115). En la adaptación para intranets académicas, se priorizan estos dos puntos debido a su relevancia en la protección de los datos personales. A continuación, se detallan los aspectos clave:

- Asignación de contención de privacidad: Este punto se refiere a la identificación y mapeo de los responsables de gestionar la privacidad dentro

de la intranet académica. Es crucial especificar qué información privada se almacena, como datos personales, registros académicos y médicos, así como la ubicación de estos datos y los canales de comunicación utilizados para acceder o transferir dicha información. Con el uso creciente de big data en entornos académicos, es fundamental implementar medidas adecuadas para proteger estos datos masivos, ya que un manejo inadecuado podría violar la privacidad de las personas (Thuraisingham et al., 2024).

La correcta segregación de la información y el uso de políticas alineadas con regulaciones nacionales e internacionales, como el Reglamento General de Protección de Datos (GDPR), son esenciales para prevenir vulneraciones de los derechos de privacidad.

- Limitaciones: El análisis de limitaciones se enfoca en revisar errores y anomalías que puedan afectar la seguridad de la información privada. Este análisis abarca las siguientes subcategorías:

✓ Vulnerabilidades: Identificación de puntos débiles en la seguridad de la información, como contraseñas débiles, acceso no autorizado o la falta de cifrado en la transmisión de datos.

✓ Debilidades: Evaluación de procedimientos y políticas de privacidad que no ofrecen una protección adecuada, como la falta de auditorías regulares o políticas desactualizadas.

✓ Preocupaciones: Revisión de las preocupaciones de los usuarios, como estudiantes y personal administrativo, sobre la privacidad de sus datos. La confianza en el sistema es un factor crítico para el buen funcionamiento de la red académica.

✓ Exposición: Nivel de riesgo que representa el acceso no autorizado a la información privada. Este análisis es clave para determinar las medidas de mitigación que se deben implementar.

✓ Anomalías: Detección de irregularidades en la gestión de la información privada, como accesos indebidos, modificaciones no autorizadas o el mal uso de los datos.

Esta adaptación garantiza que la segregación de datos en intranets académicas esté alineada con las mejores prácticas y normativas, asegurando la protección adecuada de la información sensible.

3.5) VERIFICACIÓN DE EXPOSICIÓN

La verificación de exposición se enfoca en identificar información que podría conducir a accesos no autorizados mediante la reutilización de autenticaciones en múltiples ubicaciones o el uso indebido de credenciales. Este proceso incluye dos aspectos principales: el mapeo de exposición y la elaboración de perfiles. (Herzog, 2010, pag. 116).

- Mapeo de Exposición: se considera la identificación de datos personales de los usuarios que pueden estar expuestos, como contraseñas, métodos de respaldo, y cualquier información organizacional considerada confidencial según las políticas institucionales (Herzog, 2010, pag. 116).Este análisis es crucial para detectar puntos de riesgo que puedan ser explotados por actores maliciosos.

- Elaboración de Perfiles: se centra en entender las habilidades de los empleados, así como el canal y las puertas de enlace utilizadas para acceder a la red. Con esta información, es posible prever posibles vulnerabilidades relacionadas con el nivel de acceso de los usuarios y su potencial explotación.

Dado que esta información es de carácter confidencial, no se incluye en la adaptación metodológica para la gestión del canal humano en entornos académicos. En lugar de ello, la gestión de la exposición en este contexto se basa en garantizar que las políticas de control de acceso y los sistemas de autenticación avanzada protejan los datos sensibles sin comprometer la seguridad general de la red. La adaptación de esta verificación se enfoca en proteger la confidencialidad de los usuarios minimizando los riesgos de accesos no autorizados mediante medidas prácticas y políticas claras que aseguren una correcta gestión de contraseñas y acceso a los sistemas. Estudios recientes que combinan aspectos cibernéticos y humanos refuerzan la importancia de una gestión integral y adaptada al entorno académico (Roy & Chen, 2024).

3.6) EXPLORACIÓN DE INTELIGENCIA COMPETITIVA

Este punto se enfoca en la recopilación de información estratégica sobre relaciones comerciales y desarrollo empresarial, lo cual es más relevante en entornos corporativos donde la gestión de alianzas y clientes clave es esencial para la competencia. Sin embargo, en el contexto académico, este tipo de análisis no es aplicable, ya que las intranets académicas y la gestión de información confidencial

no están orientadas hacia la competitividad empresarial. Según Herzog (2010), esta categoría está diseñada específicamente para entornos empresariales, por lo que no resulta pertinente en la evaluación de intranets académicas.

4) FASE 4: INTERVENCIÓN

Se considera verificación de cuarentena, privilegios de auditoría y continuidad del servicio.(Herzog, 2010)

4.1) VERIFICACIÓN DE CUARENTENA

Evalúa los mecanismos para aislar o contener contactos hostiles en los puntos de entrada de una red (Herzog, 2010), es crucial en la prevención de amenazas en ciertos sistemas. No obstante, en las intranets académicas, donde la colaboración abierta y el acceso compartido son características esenciales para la enseñanza y la investigación, estos riesgos son menos frecuentes que en entornos corporativos o gubernamentales. En este contexto, la seguridad se centra en la protección de datos personales, la gestión de accesos y la integridad de la información confidencial. Por lo tanto, las pruebas de cuarentena no son relevantes para la auditoría de canales humanos en entornos educativos, donde la prioridad es garantizar tanto la accesibilidad como la seguridad de la red.

4.2) Evaluación de Permisos de Auditoría (PRIVILEGIOS DE AUDITORÍA)

Se enfoca en revisar las credenciales otorgadas a los usuarios y los permisos concedidos para llevar a cabo pruebas de seguridad en la intranet académica. Este proceso es fundamental para garantizar que los accesos y privilegios se utilicen de manera adecuada y controlada, minimizando los riesgos internos (Herzog, 2010, pag. 117). Siguiendo la lógica de la fase de inducción, la identificación, autorización, escalamiento de permisos y discriminación se realizan previa verificación de las credenciales, asegurando un proceso seguro y controlado en cada etapa. Esta adaptación se alinea con los valores de diversidad e inclusión propios del entorno académico, lo que permite mejorar la seguridad institucional de manera eficiente.

Las pruebas clave que se consideran para esta fase incluyen:

- Validación de Credenciales y Autenticación (Identificación): Se examinan y documentan los procesos de obtención de credenciales, verificando su legitimidad y asegurando que cualquier intento de obtener identificación por medios fraudulentos sea detectado y controlado en todos los canales de la

intranet. Esto garantiza que las credenciales estén alineadas con las políticas de seguridad de la institución y protege contra accesos no autorizados.

- Control de Autorizaciones (Autorización): Se verifica la posible existencia de autorizaciones fraudulentas que podrían otorgar privilegios indebidos a los usuarios. Se asegura que todos los accesos y autorizaciones sean debidamente controlados y monitoreados, evitando el mal uso de credenciales y privilegios.
- Verificación de Escalación de Permisos (Escalación de Privilegios): Se mapea el acceso a los activos de la red para identificar si los usuarios pueden escalar a mayores privilegios que los asignados originalmente. Esto permite evaluar posibles fallos en los sistemas de control de acceso que podrían ser explotados para obtener permisos no autorizados.
- Equidad en el Acceso a Privilegios (Discriminación): Se garantiza que la información solicitada y los privilegios otorgados no presenten sesgos basados en edad, sexo, raza, cultura o religión. Este proceso asegura un sistema equitativo y libre de discriminación, alineado con los valores de diversidad e inclusión del entorno académico.
- Evaluación de Vulnerabilidades en Canales de Comunicación (Subyugación): Se analiza el uso de canales inseguros como correos electrónicos no cifrados o líneas telefónicas públicas, que podrían comprometer la integridad del sistema si no se gestionan adecuadamente. La subyugación, como un control de clase A, se centra en contabilizar los métodos de interacción con el personal clave, garantizando que las comunicaciones estén bajo control y no representen un riesgo para la seguridad. Esta evaluación es especialmente relevante en el entorno académico, donde los datos sensibles y la comunicación segura son fundamentales.

La adaptación de privilegios de auditoría al contexto académico es crucial para abordar las necesidades específicas de las instituciones educativas, donde la seguridad y la equidad son prioritarias. Este enfoque estructurado permite identificar y mitigar vulnerabilidades que podrían comprometer la integridad del sistema si no se gestionan adecuadamente (Wijaya et al., 2024). Al ajustar los controles críticos, se garantiza que las pruebas de seguridad sean efectivas y justas, respetando la diversidad del personal y de los estudiantes. Esto contribuye a una gestión integral y

adaptada, mejorando la seguridad y la confianza en el manejo de la información académica.

4.3) CONTINUIDAD DE SERVICIO

Mide la capacidad de los sistemas y del personal responsable para mantener la operación ininterrumpida de la red ante situaciones de cambio hostil o fallas. Este proceso evalúa la resiliencia del sistema, la continuidad operativa y las medidas de seguridad implementadas (Herzog, 2010). En el contexto académico, es fundamental asegurar que los servicios de la intranet sean resilientes, estén protegidos y puedan mantenerse operativos de manera continua. Para adaptar este concepto a las intranets académicas, se han considerado los siguientes aspectos:

- Resiliencia: Se centra en identificar y contabilizar a los responsables de gestionar el acceso a los equipos del cuarto de telecomunicaciones, donde se albergan los dispositivos críticos de interconectividad. Esto asegura que solo personal autorizado pueda acceder a estos activos, estableciendo controles de acceso robustos que protejan la infraestructura de posibles amenazas.
- Continuidad: Este aspecto evalúa los posibles retrasos y conflictos generados por los responsables de acceso a la infraestructura tecnológica. El objetivo es garantizar que el acceso a los sistemas sea eficiente y sin interrupciones, manteniendo la operatividad de la red sin comprometer la seguridad. En el entorno académico, donde el acceso continuo es vital para estudiantes y personal, la interrupción mínima es clave.
- Alertas y revisión: Aunque el monitoreo continuo y las alertas tempranas son parte integral de la resiliencia, este proceso queda fuera de la metodología adaptada, ya que la administración de la red está bajo la responsabilidad del Departamento de Tecnologías de la Información de la institución educativa, lo que implica que la evaluación de la intranet académica se guía por las políticas institucionales específicas. La implementación de controles y sistemas de revisión y monitoreo queda, por lo tanto, en manos del equipo técnico especializado.

La adaptación de la continuidad de servicio en las intranets académicas se enfoca en garantizar una operación constante y segura. Estudios recientes demuestran que las universidades que implementan sistemas de monitoreo y alertas tempranas mejoran su capacidad para responder a incidentes de seguridad (Li, Xiao & Zhang,

2023), asegurando una operación confiable. Basada en la metodología OSSTMM v3.02, esta adaptación refuerza la importancia de los controles de acceso robustos, lo que fortalece la capacidad de las instituciones para mantener la estabilidad operativa.

4.4) FASE FINAL: ALERTAS Y REVISIÓN. FIN DE LA ENCUESTA

En la adaptación, se incluye como parte de la fase 4, la fase final del diagnóstico de seguridad de la intranet académica, centrada en el análisis de brechas, tiene como objetivo identificar discrepancias entre las pruebas de seguridad realizadas y su efectividad real. Permite actualizar las medidas de seguridad frente a riesgos emergentes y dinámicos, tal como lo sugieren Georgiadou et al. (2020) al destacar la necesidad de integrar las dimensiones técnicas y socioculturales en los análisis de seguridad. Este análisis, apoyado en registros y percepciones tanto humanas como mecánicas, asegura que las medidas implementadas se alineen con los resultados esperados y detecta fallos o debilidades no identificadas previamente(Herzog, 2010).

En la adaptación se consideran los siguientes aspectos:

- Verificación de Alarmas

Se revisa el uso de sistemas de advertencia, ya sean localizados o globales, así como los registros emitidos por las pasarelas de acceso en caso de detectar situaciones sospechosas, como elusión de seguridad, ingeniería social o fraudes(Herzog, 2010).

En el contexto académico, este análisis se adapta para garantizar que el personal encargado de la seguridad tenga acceso a mecanismos de alerta eficientes. Los sistemas de alarma deben estar alineados con las políticas institucionales, permitiendo que estudiantes, personal administrativo y docente puedan reportar incidentes de manera rápida y efectiva. Como señala (Tarantino et al., 2021), un enfoque centrado en el usuario mejora significativamente la interacción con los sistemas de notificación, reduciendo los tiempos de respuesta y aumentando la relevancia contextual de las alarmas.

- Almacenamiento y Recuperación de Información

En esta fase se documenta y verifica el acceso privilegiado a los lugares donde se almacenan alarmas, registros y notificaciones, asegurando su integridad y seguridad (Herzog, 2010). Adaptada al contexto académico, esta fase garantiza que el personal responsable tenga acceso controlado a dichos registros, protegiendo los datos de

accesos no autorizados. Las universidades deben implementar políticas claras de gestión de registros de seguridad, estableciendo controles rigurosos que aseguren un almacenamiento seguro y una recuperación rápida y precisa de la información.

El almacenamiento seguro de los registros es esencial para auditar y revisar incidentes de seguridad, garantizando la protección de la información sensible frente a amenazas internas y externas. Un sistema centralizado de reporte de eventos, como el mencionado por Ituk (2023), facilita una gestión más eficiente de los incidentes de seguridad, brindando una mayor capacidad de supervisión y respuesta.

Esta fase final del diagnóstico de seguridad proporciona un control adicional, asegurando que todos los incidentes sean registrados, evaluados y gestionados de manera adecuada.

Diagrama de la metodología OSSTMM V3.02 adaptada en el contexto académico.

En la Figura 20, se muestra el diagrama de la propuesta para la auditoría del canal humano en intranets de campus académicas, tomando como base la metodología OSSTMM V3.02 y su adaptación para el presente estudio. Cada fase está relacionada con un color, así: el color amarillo representa la fase de inducción, el color naranja la fase de interacción, el color azul la fase indagatoria donde se calcula el valor de las limitaciones. El color rosa representa la fase de intervención, donde se revisa los valores obtenidos y se interpreta el resultado del RAV para generar acciones correctivas basadas en la fase de inducción. El RAV indica el estado actual de la seguridad operacional de un canal, su cálculo puede ser automático, en la hoja de cálculo del RAV de la web oficial de (ISECOM, 2021), donde se ingresan los valores numéricos de cada ítem para obtener los resultados.

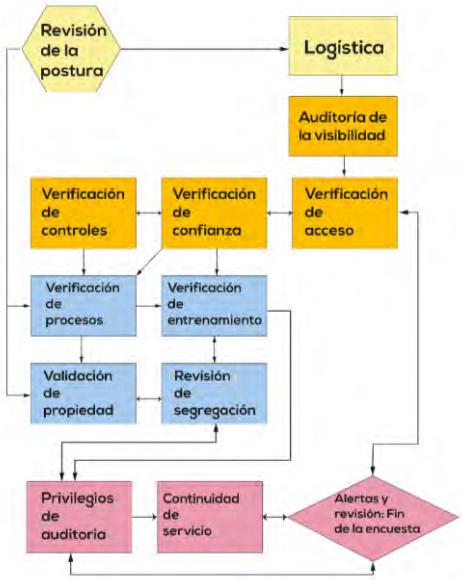


Figura 20: Propuesta para la auditoría del canal humano en intranets de campus académicas

Fuente. Elaboración propia.

La adaptación de la metodología OSSTMM para el diagnóstico de la seguridad de la intranet académica en el canal humano introduce un enfoque innovador y ajustado específicamente al entorno educativo. Este enfoque permite contabilizar accesos no autorizados e identificar a los responsables de posibles retrasos en el acceso, además de integrar un sistema de alertas y revisiones continuas que refuerza la resiliencia y la continuidad operativa de la red académica. La personalización de la logística y la verificación de detección activa asegura una evaluación más precisa y pertinente, alineada con las políticas institucionales y las dinámicas culturales específicas de cada institución educativa.

Asimismo, la inclusión de capacitaciones en seguridad y la revisión de licencias de software no solo refuerzan la integridad del sistema, sino que también elevan el nivel de exhaustividad en el proceso de auditoría. En resumen, esta adaptación no solo aborda las vulnerabilidades tradicionales, sino que proporciona soluciones prácticas y específicas para asegurar una operación continua y segura de la infraestructura tecnológica educativa.

4.1.2 Aplicación de OSSTMM adaptado en el canal humano de la intranet del campus académico.

Como resultado de la aplicación para evaluar el canal humano se establece el riesgo en la seguridad de la intranet según el RAV. Al determinarse su existencia, se continúa con el siguiente paso que es el análisis de la intranet en tiempo real para

identificar insider threats. De lo contrario concluiría la aplicación de la metodología en este punto.

4.2 Etapa 2. Análisis en tiempo real de la data de la intranet del campus académico en estudio.

El análisis en tiempo real de la data de la intranet es esencial para identificar y mitigar vulnerabilidades que puedan comprometer la seguridad de la red. La primera etapa del estudio reveló varias vulnerabilidades, subrayando la necesidad de implementar herramientas que permitan un monitoreo continuo y detallado del tráfico de la red. Este enfoque facilita la detección inmediata de posibles amenazas y permite la correlación de datos para obtener una visión más completa de los riesgos.

Para este análisis, se seleccionaron dos herramientas clave: NIDS-SNORT y NEXPOSE. Estas herramientas fueron elegidas por su eficacia y capacidad para complementar y validar los resultados obtenidos.

NIDS-SNORT, es un Sistema de Detección de Intrusos de Red (NIDS) de código abierto. Analiza el tráfico en tiempo real, genera alertas detalladas y almacena paquetes en logs, proporcionando estadísticas sobre el tráfico analizado. Maneja reglas configurables según el tipo de tráfico, protocolo o puerto. Se puede configurar en tres modos: Sniffer, Logger de paquetes y NIDS. En el modo NIDS, si detecta un paquete que coincide con las reglas definidas, proporciona información detallada sobre el origen, destino, hora, fecha, protocolo y puerto del ataque. Según Kiflay et al. (2024), SNORT es reconocido por su capacidad para manejar tráfico en tiempo real, generar alertas detalladas y su flexibilidad para adaptarse a diferentes necesidades de seguridad, confirmando su eficacia y utilidad en la detección de intrusos en redes.

NEXPOSE, desarrollado por Rapid7 (2020), es una herramienta avanzada para la explotación de vulnerabilidades que monitorea exposiciones en tiempo real y se adapta a nuevas amenazas. Ofrece soporte técnico, escanea equipos físicos y virtuales, y programa escaneos periódicos. Además, permite exportar resultados en varios formatos y su compatibilidad con Metasploit asegura una base de datos de vulnerabilidades siempre actualizada (Suomalainen et al., 2022).

La selección de NIDS-SNORT se basa en los resultados de la RSL aplicada en el estudio, y descritos en 3.3 referente a consideraciones para la implementación de la

propuesta de control de amenazas insiders en intranets de campus académicos. NIDS-SNORT es el método más utilizado para la detección de amenazas internas en intranets académicas, con un 42.74% en Q2.7, y los sistemas de detección de intrusos son los más comunes para la captura de datos, con un 11.97% en Q2.8. En Q2.9, se destaca el uso de sistemas de detección y prevención de intrusos basados en reglas, principalmente SNORT, con un 4.27%.

Respecto de la selección de NEXPOSE, se lo considera porque complementa a NIDS-SNORT al proporcionar un escaneo detallado de vulnerabilidades y una adaptación a nuevas amenazas. Su compatibilidad con Metasploit asegura una base de datos de vulnerabilidades siempre actualizada, lo que es crucial para la explotación y mitigación de vulnerabilidades. Nisha y Pramod (2024) respaldan la selección de estas herramientas, con su estudio acerca de la eficacia de los sistemas de monitoreo continuo y la importancia de detectar y mitigar amenazas internas en tiempo real en entornos académicos.

4.2.1 Análisis de tráfico de la intranet en tiempo real.

De la RSL se determinó que, si bien se utilizan diferentes fuentes de datos externas, combinadas o propias, para el análisis de datos de amenazas internas en redes de campus académicos, estas son restringidas y no se dan mayor detalle. Esto se refleja en que solo el 1.7% de las fuentes de datos propias son mencionadas, mayor detalle se puede encontrar en la Tabla 37, correspondiente a la pregunta Q1.3 sobre fuentes de datos propias de amenazas internas, en el Anexo B del protocolo de RSL de amenazas internas en intranets académicas. Dado este panorama, se propone la generación de datos propios con una mayor riqueza descriptiva; por consiguiente, en la metodología propuesta se incorpora un análisis detallado de estos datos.

- NIDS-SNORT para el análisis de la intranet en tiempo real.

La metodología se implementa en un entorno de red de alta velocidad (Gigabit Ethernet, hasta 1 Gbps), utilizando puertos espejo (mirror ports) para capturar tráfico de tres VLANs. Aunque estudios como (D. Zhang & Wang, 2019) sugieren que la eficiencia de SNORT podría verse afectada en redes de alta velocidad sin optimizaciones específicas, en este trabajo se evidenció que, mediante una adecuada configuración de infraestructura, SNORT configurada como NIDS logra

procesar elevados volúmenes de tráfico con una tasa de pérdida de paquetes (inferior al 4 %).

Esta validación práctica demuestra que la metodología propuesta es aplicable en intranets académicas modernas que operan a velocidades superiores a 100 Mbps, garantizando un monitoreo efectivo en tiempo real.

NEXPOSE para identificar vulnerabilidades, complementar y validar la auditoría de amenazas internas valoradas en el canal humano, realizado en la etapa 1 detallada en la sección 4.1.

Nexpose, complementa y valida la auditoría de amenazas internas evaluada en el canal humano, determinando las vulnerabilidades en red, escaneando los sistemas para generar un reporte sobre las vulnerabilidades encontradas en el sitio de escaneo y las posibles soluciones. La versión de NEXPOSE a utilizar depende del número de objetivos a evaluar. Para el escaneo se debe habilitar los permisos de administración a los equipos para obtener resultados más confiables.

- Infraestructura de red e instalación de NIDS-SNORT.

Para la instalación de NIDS-SNORT se debe evaluar la infraestructura de la intranet del campus académico en estudio y considerar una muestra adecuada del total de la intranet, aunque esto depende de otros factores, como las políticas de acceso del departamento de tecnologías de la institución académica e incluso del acceso que se tenga al data center para poder instalar la herramienta de análisis de data en tiempo real NIDS-SNORT.

Para la configuración en el servidor seleccionado se instala NIDS-SNORT siguiendo la guía de SNORT COMMUNITY (2022). Además, se considera la configuración de puertos *mirror* para el análisis de la intranet e identificación de las amenazas, en base a 3.3. Se sugiere detallar la información referente al número de paquetes, considerando: paquetes recibidos, analizados y eliminados; así como cantidad y porcentaje. Esto por cada VLAN, lo que permitirá conocer acerca del tráfico de la intranet y el funcionamiento adecuado de la herramienta de análisis, teniendo un número bajo de paquetes eliminados para captar la mayor cantidad de data basado en el formato de la Tabla 6.

Tabla 6: Número de paquetes en la VLAN N.

VLAN N		
Nombre	Cantidad	Porcentaje
Paquetes recibidos		
Paquetes analizados		
Paquetes eliminados		

Fuente. Elaboración propia.

4.2.2 Interpretación de datos capturados en la intranet

Para la interpretación de los datos compilados en tiempo real con NIDS-SNORT, se debe realizar un análisis del tipo amenaza identificada, y comparar con los resultados arrojados por Nexpose, lo que permite realizar el cuadro comparativo cuyo formato se detalla en la Tabla 7, referente al Análisis de amenazas detectadas con NIDS-SNORT y vulnerabilidades identificadas con Nexpose. El análisis debe realizarse las 24 horas, los siete días de la semana exceptuando feriados. Se considera la cantidad de paquetes analizados, alertas con sus respectivas direcciones IP de origen y destino, identificador de alerta, la fecha, hora de cada alerta, número total de alertas en el día y algunas observaciones presentadas durante el análisis por un mes en las VLANs.

Para el proceso de escaneo, se debe instalar Nexpose en un host perteneciente a las VLANs en estudio, para un escaneo completo se debe indicar las credenciales de acceso de todos los equipos que se van a analizar. El escaneo genera un informe ejecutivo que presenta las vulnerabilidades clasificadas por riesgo, sistema operativo, tipo y soluciones. Este proceso permite realizar un análisis comparativo, validar el análisis realizado por NIDS-SNORT y seleccionar una amenaza a controlar.

Tabla 7: Formato del análisis de amenazas detectadas con NIDS-SNORT y vulnerabilidades identificadas con NEXPOSE.

Análisis con NIDS-SNORT				**Exploración con Nexpose**
SNORT Identificador	**Threat**	**Source VLANs**	**Descripción**	**Vulnerabilidad**

Fuente. Elaboración propia.

El identificador SNORT (SID) permite determinar las amenazas detectadas en el análisis de la intranet del campus académico y buscar posibles soluciones para cada una de las vulnerabilidades encontradas en la intranet. Para luego con esta información: explotarlas, controlarlas y aplicarlas en intranets de redes similares.

4.3 Etapa 3. Selección de la amenaza a controlar

En esta etapa se realiza un análisis para la selección de la amenaza a controlar que considera los resultados de la RSL y del análisis en tiempo real de la data de la intranet con NIDS-SNORT y NEXPOSE del campus académico en estudio, según se describe.

4.3.1 Analizar los resultados de la RSL acerca de insiders en intranets académicas.

Para continuar con la metodología es importante analizar los resultados de RSL y considerar el listado de las amenazas descritas en las Tablas 34 y 35 referente a Q1.1 y Q1.2, donde se hace referencia a las amenazas internas de mayor presencia en redes de datos e intranets académicas respectivamente.

4.3.2 Comparación de los resultados de la etapa 2 con los de la RSL y selección de la amenaza a controlar.

Al comparar los resultados obtenidos en la fase 2 del análisis en tiempo real de la data de la intranet con NIDS-SNORT y NEXPOSE del campus académico en estudio, junto a las Tablas 34 y 35 de insiders threat de Q1.1 y Q1.2 del anexo B, pag.167-168, se debe seleccionar la amenaza a controlar considerando la de mayor presencia en la intranet de campus académico en estudio.

4.4 Etapa 4. Implementación de control de la amenaza insider seleccionada.

La tecnología SDN representa una oportunidad estratégica para el desarrollo del sector tecnológico en el Ecuador y en el mundo, al permitir propuestas innovadoras que integran redes tradicionales con arquitecturas programables, aportando significativamente a la mejora de la seguridad en entornos académicos. En el caso ecuatoriano, esta tecnología aún se encuentra en etapa de adopción incipiente, lo que abre un campo fértil para la investigación aplicada y la validación de modelos que respondan a las necesidades locales en ciberseguridad educativa.

Por esta razón, se eligió como caso de estudio a la Escuela Superior Politécnica de Chimborazo (ESPOCH), una institución de educación superior pública en Ecuador

con una infraestructura de red académica segmentada y representativa. La selección responde a criterios de accesibilidad técnica, colaboración interinstitucional y viabilidad operativa, ya que el análisis del tráfico de red fue realizado en coordinación con el Departamento de Tecnologías de la Información y Comunicación (DTIC), Departamento de Redes, quienes realizaron el acompañamiento y validación institucional durante las fases del estudio.

Como parte de la propuesta metodológica, se diseñó un escenario de pruebas SDN con equipos reales, en el que se implementaron políticas de Calidad de Servicio (QoS) utilizando listas de control de acceso (ACLs), con el fin de mitigar la amenaza insider seleccionada. Esta configuración experimental permitió evaluar el control de la amenaza y su impacto en el rendimiento de la red del campus académico, considerando métricas clave para su análisis. La información técnica relacionada con la tecnología SDN se desarrolla en detalle en el capítulo 2, sección 2.1.
Se considera algunos aspectos importantes para su análisis.

4.4.1 Calidad de Servicio (QoS) y parámetros de rendimiento.

A partir de las definiciones descritas en 2.3, acerca de QoS y parámetros de rendimiento, se considera para su evaluación: ancho de banda, latencia, jitter (variaciones en latencia), pérdida de paquetes. Estos cuatro parámetros proporcionan una visión integral del desempeño de la red, cumpliendo con los niveles de servicio requeridos (SLA) para aplicaciones críticas en entornos académicos, como la videoconferencia, el uso de VoIP y el manejo de grandes volúmenes de datos. El ancho de banda determina la capacidad de transmisión de datos, mientras que la latencia y el jitter influyen en la rapidez y estabilidad de la comunicación, aspectos cruciales para aplicaciones en tiempo real. La pérdida de paquetes, por su parte, puede interrumpir la integridad de las comunicaciones, lo que refuerza la importancia de minimizar este parámetro.
Implementar políticas de QoS basadas en estos parámetros garantiza una gestión eficiente de la red, mejorando continuamente su infraestructura y optimizando la experiencia de los usuarios. Estudios recientes, como los de Ghafar et al. (2020) y Hussein (2023), han demostrado que un manejo adecuado de estos parámetros no solo optimiza el rendimiento de la red, sino que también mejora la experiencia del usuario al reducir los tiempos de respuesta, la pérdida de paquetes y la variabilidad en la transmisión de datos. Además, la literatura técnica y las mejores prácticas de la industria, como las establecidas por Cisco Systems (Deshmukh, 2024), subrayan

la importancia de una gestión eficiente de estos factores para garantizar un alto rendimiento en redes académicas.

Este enfoque integral no solo aborda los problemas de rendimiento de la red, sino que también mejora la calidad de las interacciones educativas y el aprendizaje en línea, fundamental para instituciones académicas que dependen de una infraestructura tecnológica sólida y confiable.

4.4.2 Implementación de Políticas de QoS.

Se considera tres aspectos fundamentales en el diseño de políticas de QoS en intranets académicas:

a. Implementación de políticas de QoS en redes académicas para la mejora del rendimiento y la seguridad.

Basado en estudios previos de Barba et al. (2019) y Kang et al. (2017), la implementación de políticas de QoS en redes universitarias incluye la limitación del ancho de banda, el control de accesos externos y el aislamiento del tráfico mediante VLANs según el rol del usuario (estudiantes, docentes, personal administrativo). Estas medidas contribuyen a mejorar tanto la seguridad como el rendimiento de la red, especialmente en el manejo de aplicaciones multimedia de alta demanda. Asimismo, estos estudios destacan que la seguridad de las redes académicas puede incrementarse significativamente mediante la restricción de puertos para aplicaciones como HTTP, POP3 y FTP, y la priorización del tráfico multimedia, lo cual ayuda a mitigar amenazas relacionadas con el acceso no autorizado y el tráfico excesivo.

En este contexto, se recomienda aplicar políticas de QoS que no solo mitiguen las amenazas identificadas, sino que también se adapten a entornos con redes SDN. Este enfoque permite un control más dinámico y eficiente de la infraestructura de red, esencial para adaptarse a las necesidades cambiantes de las instituciones académicas a través de una gestión eficaz del tráfico, una mejora continua en la seguridad y operatividad de las redes, y una experiencia de usuario óptima en los entornos educativos (Salim, 2023;Ghafar et al., 2020).

b. Categorizar el tráfico.

Es crucial para determinar las políticas en una red. En entornos académicos el tráfico de internet es predominantemente basado en el protocolo IP considerando su importancia y el uso extensivo de protocolos IP para asegurar las comunicaciones en redes de diferentes tipos.(Hou et al., 2022). Además, los flujos de tráfico que duran más de 10 minutos, principalmente sesiones peer-to-peer, representan el 20% del

volumen total de tráfico (X. Li et al., 2024). En el contexto académico, se ha categorizado la traza pública 20100106-030946-0.dsl de ISPDSL-II utilizando un script y la librería pypcapfile de Python, la cual permite leer y descomponer archivos PCAP (Packet Capture) generados por herramientas de monitoreo como Wireshark. Esta librería facilita el acceso estructurado a los encabezados de paquetes de red (IP, TCP, UDP, entre otros), lo que permite identificar y clasificar los protocolos utilizados, analizar la duración de las sesiones, y extraer patrones de tráfico relevantes. Al analizar 23 millones de paquetes durante 20 minutos, se determinó que los protocolos predominantes son TCP y UDP, con un 80.3% y 19.2% respectivamente. Basándose en estos datos, se implementaron políticas de QoS que asignan el 80% del tráfico a TCP y el 20% a UDP para optimizar la gestión de la red (Barba-Vera, Criollo Bustamante, et al., 2020).

c. Flujo de etapas para el diseño de políticas de QoS para SDN y redes tradicionales.

Como tercer aspecto importante, el flujo de etapas para el diseño de políticas de QoS para SDN y redes tradicionales(Barba-Vera et al., 2020), *basado en el análisis de las políticas de QoS y categorización de* tráfico (X. Li et al., 2024). Estas políticas para la evaluación del desempeño en el estudio consideran el flujo de etapas del modelo propuesto para el diseño de políticas de QoS en redes convencionales y SDN que se detallada en la Figura 21.

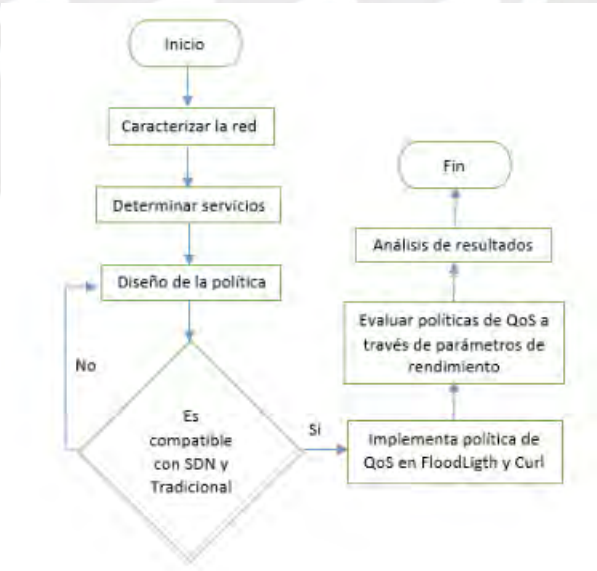


Figura 21: Flujo de Etapas del Modelo propuesto para el diseño de políticas de QoS en redes convencionales y SDN.(Barba-Vera et al., 2020)

4.4.3 Establecer el escenario de pruebas

Se considera:

- Data de la intranet.

Es importante evaluar los datos en tiempo real en la intranet e identificar el tráfico según las Tablas 3, 4, 5, que hacen referencias al tráfico de las VLANs analizadas como resultado de la etapa 4. Para el escenario de pruebas se considera la menor velocidad del puerto de red de las computadoras, debiéndose mantener para la generación de paquetes de transmisión y pruebas realizadas. Además, se debe tomar en cuenta que los protocolos de mayor presencia en la red son: TCP y UDP, con un porcentaje de 80.3% y 19.2% respectivamente(Barba-Vera et al., 2020). Este porcentaje de datos se considera para la simulación de tráfico en el escenario de pruebas.

- Generador de tráfico Distributed Internet Traffic Generator (D-ITG).

Para realizar las pruebas se utiliza el generador de tráfico D-ITG, ya que permite inyectar diferentes tipos personalizados de tráfico, recreando así un entorno real. Este generador fue seleccionado en base a los resultados del análisis comparativo de generadores de tráfico determinando que D-TIG gestiona la emulación de la pila completa de protocolos TCP/IP, obteniendo medidas aceptables porque utiliza los protocolos de las capas de transporte, red e interfaz. D-ITG ha sido planificado para generar tráfico de red (ICMP), tráfico de capa de transporte (TCP y UDP), varios tráficos de “capa 5-7” (TELNET, SMTP, DNS, VoIP).(Praptodiyono et al., 2019)

- Escenario de pruebas.

Simula un nodo que representa un laboratorio de la intranet del campus en estudio configurado con equipos físicos en un escenario SDN. Donde se incluye la amenaza insider a controlar. Se considera amenazas más comunes a la capa de transporte para la fase de explotación. Para simular el ataque se utiliza la Distribución/Kali Linux Scritp Slowloris – Módulos de Metasploit (OffSec Services Limited, 2025). Para el direccionamiento, se sugiere realizar una evaluación del direccionamiento lógico para incluir en el escenario de pruebas. De la misma forma se debe considerar el número de paquetes para la ejecución del ataque en base a los logs almacenados de las alertas detectadas con SNORT durante el análisis del tráfico, y adaptarlo para el escenario de pruebas, de tal forma que se puedan hacer pruebas con data que permitan una valoración estadística adecuada.

- Recursos de topología.

Se incluye equipos SDN, puede ser un conmutador de 24 puertos esto va a depender de la consideración que se tenga para el escenario, un switch para la conexión de equipos con servidores puesto que en la metodología se sugiere equipos físicos. Al separar los servidores y la intranet en un escenario SDN, es importante considerar la comunicación que se vaya a evaluar en el escenario de estudio además esto va a influir en los parámetros de rendimiento al controlar la amenaza.

- *Hardware,* se sugiere el siguiente, pudiendo considerar equipos con características similares:
  - ✓ Un conmutador HP 3800 Series 24G-25FP + J9575, el equipo HP funciona con el protocolo OpenFlow, que permite probar redes SDN, así como también al ambiente tradicional. Tiene un procesador ASIC / ARM @ 350 MHz; Freescale P2020 @ 1200 MHz, 4 Gb de flash y 2 Gb SDRAM. Este dispositivo se observa en la figura 30 del anexo I.
  - ✓ 1 switch HP PRO CURVE 1810G-8, para la conexión de equipos servidores. Este dispositivo se observa en la figura 31 del anexo I.

  Para el escenario se implementa equipos físicos, incluye las 5 computadoras (cliente, servidor, controlador, SNORT, atacante (Kali-Linux)), que se tendrán en el escenario de pruebas.

- *Software***,** se trabaja con:
  - ✓ Virtual Box 6.10: Herramienta de virtualización de código abierto, multiplataforma para Linux, Windows y MacOSX.
  - ✓ Ubuntu 18.04 Desktop: sistema operativo base para el controlador.
  - ✓ Java JDK 10.02: complemento para D-ITG.
  - ✓ Controlador: Floodlight.
  - ✓ Wireshark 2.6.10: analizador de tráfico de red.
  - ✓ D-ITG 2.61, GUI 0.92: Generado de tráfico.

- Controlador

Se utiliza el controlador Floodlight, por ser el más completo en sus capacidades en comparación con otros controladores probados, se basa en la evaluación según la experiencia como se detalla en la Figura 22, evaluación de controladores SDN con la escala Likert. Donde se puede observar que los controladores evaluados OpenDaylight, Ryu, SDN VAN Controller, Floodlight comparten soporte del protocolo Openflow V1.O -V1.3, tienen soporte en Mininet como herramienta de simulación;

Floodlight también es multiplataforma, tiene Rest API, es de código abierto, medianamente complejo en la instalación y es compatible con los equipos del escenario propuesto, además tiene más tiempo en el mercado y tiene muy buena documentación, características importantes a tener en cuenta para el estudio.(Barba-Vera et al., 2020)

Controllers / Characteristics	OpenDayLigth	Value	Ryu	Value	FloodLight	Value	SDN Van Controller	Value
Programming language	Java	3	Python	5	Java	3	Java	3
Supported protocol	OpenFlow V1.0 – V1.3	2	OpenFlow V1.0 – V1.3	2	OpenFlow V1.0 – V1.3	2	OpenFlow V1.0 – V1.3	2
Simulation tool	Mininet	5	Mininet	5	Mininet	5	Mininet	5
Supported platforms	Windows, Linux, Mac OSX.	5	Linux	2	Windows, Linux, Mac OSX.	5	Linux	2
Provides REST API	Yes	5	Yes (basic)	5	Yes	5	Yes (basic)	5
Type of code	Open Source	5	Open Source	5	Open Source	5	Open Source	5
Installation difficulty	Complicated	3	Easy	5	Complicated	3	Easy	5
Topological compatibility of equipment	No	3	No	3	Yes	5	No	3
Time of life	2 years 5 months	3	3 years	4	4 years	5	3 years	4
Documentation	Good	4	Good	4	Very Good	5	Medium	3
Totals		**38**		**40**		**43**		**37**

Figura 22: Evaluación de controladores SDN con la escala Likert (Barba et al., 2019b)

4.4.4 Pruebas en el escenario de estudio SDN.

En este apartado, se detallan las pruebas a realizar en un entorno de Red Definida por Software (SDN) para evaluar la efectividad de las políticas de control contra amenazas internas, específicamente ataques de Denegación de Servicio (DoS). El objetivo principal es establecer la influencia de las políticas en la mejora del rendimiento de la red del campus académico al mitigar dichas amenazas. La adopción de tecnologías SDN debido a su flexibilidad y capacidad de gestión avanzada, es considerada para estas pruebas. Evaluar la respuesta de la infraestructura SDN ante amenazas internas proporcionará una comprensión más profunda de cómo estas tecnologías pueden integrarse y fortalecer la seguridad de las redes académicas.

Para llevar a cabo estas pruebas, se debe utilizar una infraestructura compuesta por equipos reales que simulen un entorno SDN considerando un nodo de la intranet del campus. Este escenario incluirá un switch SDN HP E3800, un controlador Floodlight, equipos servidores y clientes, además de herramientas de generación de tráfico y detección de anomalías como D-ITG y SNORT. También se empleará Kali Linux para

simular los ataques y evaluar la eficacia de las políticas de calidad de servicio (QoS) implementadas.

Las pruebas deben desarrollarse en dos fases: la primera sin políticas de control para establecer una línea base de rendimiento bajo ataque, y la segunda con políticas de control activas para medir su impacto en la mejora del rendimiento de la red. Los resultados se analizarán en términos de parámetros de rendimiento como ancho de banda, latencia, jitter y pérdida de paquetes. Esta metodología permitirá validar la propuesta y aportar evidencia concreta sobre la viabilidad y beneficios de integrar tecnologías SDN en redes académicas para mejorar su seguridad y rendimiento frente a amenazas internas.

Prueba 1. Análisis en el escenario SDN con el ataque de la amenaza interna y sin control.

Configuración

En la realización de las pruebas se debe mantener la separación del plano de datos del plano de control. Donde el plano de control está compuesto por el controlador (FloodLigth), el switch SDN HP E3800 y el servidor SNORT. En el direccionamiento deben pertenecer a una misma intranet.

El plano de datos está conformado por los equipos: Host A (servidor web , por ejemplo), Host B (cliente). Se incluye el equipo atacante implementado en Kali Linux que simula el ataque DoS. En el direccionamiento pertenecen a una misma intranet. Se debe enfatizar que los planos de datos y de control están totalmente separados de manera lógica. Una vez que la topología respectiva está instalada es posible realizar pruebas estándar como: ping entre los equipos de pruebas (cliente, servidor).

Controlador

- Se levanta el controlador Floodlight, que permite la comunicación en el escenario de pruebas. Se podrá observar la topología que genera el controlador FloodLigth, desde la interfaz web del controlador una vez configurada.
- Además, se activa SNORT que detecta anomalías en la red habilitado en el plano de control y con otro puerto en el plano de datos a través de un puerto espejo (mirror) en el switch SDN para analizar el tráfico de la intranet y detectar en base a la configuración de reglas de la comunidad y propias las amenazas de la intranet.

- Se verifica las conexiones, entre los equipos HOST A (servidor web) y HOST B (cliente).
- A través de Kali Linux, se procede a simular el ataque seleccionado apuntando directamente a la ip del HOST A (Servidor).
- Se procede con la inyección de tráfico TCP/UDP mediante D-ITG, la misma que se ejecuta en el servidor según las cargas necesarias, distribuyendo por intervalos (60 pruebas) hasta la capacidad del canal 100 Mbps.
- En el lado del servidor se crean los flujos y se inyectan, ingresando la dirección ip del cliente, finalmente ejecutando los comandos logger y sender.
- Mientras que en el cliente se activa Receiver y Logger para recibir la transmisión emitida por el servidor.
- OBSERVACION.

  En cada una de las pruebas realizadas, se genera un reporte detallado para su análisis estadístico. Este análisis incluye la evaluación de parámetros críticos de rendimiento en la comunicación, como el ancho de banda, el jitter, la latencia y la pérdida de paquetes, debido a su impacto directo en la calidad del servicio (QoS).

Prueba 2. Análisis en el escenario SDN con ataque de la amenaza interna y con la política de control.

Se tiene un escenario similar al de la primera prueba, en donde se encuentra la separación del plano de datos del plano de control. En este segundo escenario el plano de control está compuesto por:

- El controlador (FloodLigth).
- El switch SDN HP E3800.
- Un equipo Ubuntu que incluye la configuración SNORT en el plano de control con puerto mirror y con enlace al switch HP E3800 en el plano de datos.
- Además, en el plano de datos están los equipos HOST A (servidor), HOST B (cliente) y un equipo atacante implementado en Kali Linux para simular la amenaza en estudio.

Si la implementación es correcta, se puede observar los hosts y sus características desde la interfaz web Floodligth, así como la topología.

- Los flujos del controlador Floodlight, habilitan la comunicación entre las pcs del escenario de pruebas. Y la verificación de la comunicación entre las computadoras de los equipos HOST A (servidor web) y Kali – Linux (atacante).

- Para este escenario de prueba se simula el ataque en estudio apuntando directamente a la ip del HOST A (Servidor), esto para el caso de ataques de DoS, por ejemplo.
- Para detectar el ataque, SNORT se implementa en un equipo bajo Ubuntu. Para ello se configura el archivo *rules*, incluyendo una regla de detección del ataque.
- Se implementan las reglas para el bloqueo del ataque mediante comandos CURL con esta regla la comunicación se mantiene con regularidad. Las reglas se pueden observar vía web desde el controlador Floodlight.
- Mediante el generador de tráfico D-ITG se inyecta tráfico, como datos de prueba ingresando valores: en TCP y en UDP, teniendo un total de 60 muestras. En el servidor al ejecutar los comandos *Logger* y *Sender* se inicia la generación de tráfico. Y se procede en el cliente a receptar el tráfico generado ejecutando los comandos *Logger* y *Receiver*.

4.4.5 Análisis de resultados.

- Con los resultados de las pruebas 1 y 2, se procede a realizar el análisis de los datos mediante los reportes de la transmisión con parámetros de rendimiento: jitter, ancho de banda, delay, pérdida de paquetes.

La validación de la presente metodología de control de amenazas internas en intranets de campus académicas se realiza en el capítulo 5, al aplicar en una intranet académica y analizar los resultados a través de un método estadístico.

CAPÍTULO 5. VALIDACIÓN DE LA PROPUESTA

En este capítulo se presenta la validación de la metodología desarrollada en el capítulo 4 para el control de amenazas internas en intranets académicas, estructurada en cuatro etapas: describiendo la aplicación de cada una de estas fases en el campus académico de la ESPOCH.

En la sección 5.1, se realiza la validación de la metodología, esta comprende cuatro etapas secuenciales:

1. 5.1.1: Aplicación del modelo OSSTMM adaptado, con el objetivo de evaluar el diagnóstico de seguridad de la intranet académica en el canal humano.
2. 5.1.2: Análisis en tiempo real de los datos de la intranet del campus académico, con el propósito de identificar las amenazas existentes.
3. 5.1.3: Selección de la amenaza de Denegación de Servicio (DoS) como objeto de control, en función de los hallazgos obtenidos en la fase de análisis.
4. 5.1.4: Implementación de pruebas en un escenario de red SDN (Software-Defined Networking) para evaluar la efectividad del control de la amenaza DoS mediante políticas de control con ACLs (Access Control Lists) en el controlador Floodlight. Para ello, se ejecutan dos pruebas: la primera mide el comportamiento de la red SDN bajo la presencia de la amenaza DoS sin aplicar ningún mecanismo de control, mientras que la segunda analiza el mismo escenario tras la implementación de la política de control en el controlador Floodlight, permitiendo así comparar su efectividad en la mitigación de la amenaza.

En la sección 5.2, se lleva a cabo el análisis estadístico, que incluye el análisis descriptivo de los datos recopilados en las pruebas realizadas en 5.1.4, la verificación del cumplimiento de los supuestos estadísticos y la validación de la hipótesis planteada en el capítulo 1.

Finalmente, en la sección 5.3, se presenta la discusión de los resultados, en la cual se interpretan los hallazgos obtenidos y se contrastan con la efectividad de la metodología aplicada, proporcionando un marco analítico para su validación en entornos académicos.

5.1 Aplicación de la metodología

La intranet del campus académico en estudio está ubicada en el edificio de la Facultad de Informática y Electrónica (FIE) en la ESPOCH, universidad del Ecuador. Esta red académica es utilizada por estudiantes, docentes y personal administrativo. Dado su uso institucional, resulta fundamental evaluar su seguridad con el propósito de prevenir posibles amenazas internas.

5.1.1 Etapa 1. Diagnóstico de seguridad de la intranet académica en el canal humano.

5.1.1.1 Aplicación de OSSTMM adaptado en el canal humano de la intranet del campus académico.

Para evaluar la seguridad del canal humano en la intranet académica, se empleó la metodología OSSTMM V3.02, adaptada a este contexto. Esta metodología se aplica en cuatro fases: Inducción, Interacción, Evaluación de la confiabilidad y gestión de recursos, e Intervención. La evaluación se llevó a cabo mediante una prueba de caja gris, en la que el auditor dispone de información parcial y los administradores de la red fueron informados previamente (Herzog, 2010). La recopilación de datos se realizó mediante entrevistas al personal técnico de los laboratorios y de la DTIC de la ESPOCH

A continuación, se presentan las valoraciones de cada fase organizadas en tablas desde la Tabla 8 a la Tabla 11, se describen las fases y subfases que resultan de aplicar OSSTMM adaptado en el canal humano de la intranet del campus académico en estudio.

Tabla 8: Fase 1 - Inducción

Subfases	**Descripción**
1.1 Revisión de la postura	Evaluación de políticas, regulaciones y cultura organizativa en la red académica.
1.2 Logística	Análisis de la infraestructura y recursos disponibles para comunicación (voz, video, datos). Los docentes y estudiantes tienen horarios académicos establecidos, mientras que los administrativos siguen un horario definido.
1.3 Verificación de detección activa	Monitoreo de seguridad gestionado por la DTIC, sin verificaciones adicionales.

Fuente. Elaboración propia

Tabla 9: Fase 2 - Interacción

Subfases	Descripción
2.1 Auditoría de la visibilidad	Identificación del acceso a la intranet y sus usuarios (estudiantes, docentes, administrativos). Enumeración personal: Se evalúa el personal con acceso autorizado o no a los activos (cuarto de telecomunicaciones, laboratorios, aulas y equipos).
2.2 Verificación de acceso	Evaluación de los procesos de acceso a activos y escenarios sin autorización.
2.3 Verificación de confianza	Revisión de autenticidad de documentos y control sobre abuso de recursos.
2.4 Verificación de controles (Clase B)	Evaluación de No repudio, Confidencialidad, Privacidad, Integridad y Alarmas.

Fuente. Elaboración propia

Tabla 10: Fase 3 - Evaluación de la Confiabilidad y Gestión de Recursos

Subfases	Descripción
3.1 Verificación de procesos	Mantenimiento, indemnización y capacitación en seguridad.
3.2 Verificación de entrenamiento	Falta de capacitación institucional en seguridad informática.
3.3 Validación de la propiedad	Uso de software con licencia limitada y distribución no controlada.
3.4 Revisión de segregación	Evaluación de privacidad, vulnerabilidades y preocupaciones.
3.5 Verificación de exposición	No considerada por razones de confidencialidad
3.6 Exploración de inteligencia competitiva	No aplicable en este estudio

Fuente. Elaboración propia

Tabla 11: Fase 4 – Intervención

Subfases	Descripción
4.1 Verificación de cuarentena	No aplicable por baja amenaza de contactos hostiles.

4.2 Privilegios de auditoría	Revisión de subyugación e interacciones con el personal de recepción.
4.3 Continuidad de servicio	Evaluación de accesos sin autorización y retrasos.
4.4 Alertas y revisión	Control y aseguramiento de incidentes registrados, evaluados y gestionados de manera adecuada. La información es confidencial.

Fuente. Elaboración propia

Al concluir la aplicación del OSSTMM adaptado, se obtiene un índice de riesgo (RAV) de 85.77, correspondiente a la evaluación de seguridad en la intranet académica. El análisis revela un 13.92% de vulnerabilidades y anomalías, las cuales podrían ser explotadas por usuarios internos. El índice de riesgo obtenido (RAV = 85.77) indica que la intranet académica presenta un nivel moderado de seguridad, lo que sugiere la necesidad de reforzar las políticas de acceso y control de activos para mitigar amenazas internas.

Se incluye en el Anexo G el formulario con el cálculo del RAV y los resultados del análisis de seguridad operacional aplicado al canal humano.

Para un detalle más amplio sobre el análisis de las fases y subfases de la Etapa 1, se puede consultar en la sección 1.1 del Anexo F.

Dado que se identificaron vulnerabilidades en la red académica, se procede con la Etapa 2 de la metodología. En caso de no haber encontrado amenazas significativas, el proceso de validación habría concluido en esta fase.

5.1.2 Etapa 2. Análisis en tiempo real de la data de la intranet del campus académico en estudio.

Para corroborar los resultados obtenidos en la Etapa 1, se realizó un análisis en tiempo real del tráfico de red en la intranet académica de la ESPOCH, con especial énfasis en el edificio de la Facultad de Informática y Electrónica (FIE). Este análisis permitió evaluar la presencia de amenazas insider en el entorno de la red y validar la auditoría previa.

El monitoreo se llevó a cabo en las VLANs de Estudiantes, Docentes y Administrativos, utilizando herramientas de detección de intrusiones y escaneo de

vulnerabilidades (NIDS-SNORT y NEXPOSE). Se analizaron múltiples parámetros, incluyendo:

- Cantidad de paquetes de red procesados y eliminados.
- Tipos de amenazas detectadas en las VLANs.
- Vulnerabilidades específicas de la infraestructura de red.
- Relación entre ataques detectados y vulnerabilidades identificadas.

Los detalles de la infraestructura de red, los parámetros de monitoreo y resultados de análisis VLAN se presentan en la Etapa 2 de la sección 1.2 del Anexo F.

- Resultados del análisis de tráfico en las VLANs.

El análisis de tráfico en la intranet académica se realizó utilizando **NIDS-SNORT**, evaluando la cantidad de paquetes procesados, la tasa de análisis exitoso y la cantidad de paquetes descartados, como se observa en la tabla 12.

Tabla 12: Resultados del análisis de tráfico en las VLANs

VLAN	Paquetes Recibidos	Paquetes Analizados	% Análisis Exitoso	Paquetes Eliminados	% Eliminación
Estudiante	27,810,598,653	26,884,523,479	96.75%	902,986,272	3.25%
Docente	548,884,339	545,328,509	99.35%	3,555,783	0.65%
Administrativa	389,006,844	386,385,688	99.33%	2,620,083	0.67%

Fuente. Elaboración propia

Cabe destacar que estos resultados fueron obtenidos en una intranet académica operando sobre infraestructura de Gigabit Ethernet (hasta 1 Gbps), lo que confirma la efectividad de la metodología propuesta para entornos de alta velocidad, más allá de los tradicionales límites de 100 Mbps.

Los resultados muestran que NIDS-SNORT logró analizar más del 96% de los paquetes en todas las VLANs, con una tasa de eliminación inferior al 4%, lo que confirma su alta eficiencia en la captura, detección y procesamiento del tráfico de la red.

- Comparación de amenazas detectadas con NIDS-SNORT y vulnerabilidades identificadas con NEXPOSE

Para evaluar la seguridad de la intranet académica, se realizó un análisis comparativo entre las amenazas detectadas por NIDS-SNORT y las vulnerabilidades identificadas mediante escaneos de NEXPOSE.

La Tabla 13 presenta un resumen de los principales hallazgos del análisis de seguridad en la intranet académica. Las amenazas han sido clasificadas en categorías según su naturaleza y su impacto en la infraestructura de red. Además, se incluyen los identificadores de detección de SNORT (SNORT ID - SID), las VLANs afectadas, una descripción general de la amenaza y las vulnerabilidades asociadas identificadas mediante NEXPOSE.

Tabla 13: Resumen de amenazas detectadas con NIDS-SNORT y vulnerabilidades identificadas con NEXPOSE

Tipo de Amenaza	VLANs Afectadas	Descripción General	SNORT ID (SID)	Vulnerabilidad Asociada
Troyanos y Malware (Instantaccess.exe, Miner64, XMRig, Ramnit, Zeus, Banker, LittleInstaller, Sysch, Armadillo)	Estudiante, Docente	Distribución de malware y minería de criptomonedas no autorizada.	1-40357:3, 1-46237:1, 1-45549:1, 1-48080:1, 1-35549:1, 1-25074:1, 1-46486:1, 1-41337:2, 1-23605:12	Robo de información, ejecución remota de código, explotación de vulnerabilidades web.
Exploit Kits (Exploit kit, Exploit Usage, Backdoor Doublepulsar & Eternalblue)	Estudiante, Docente, Administrativo	Uso de exploits para vulnerabilidades en navegadores y protocolos.	1-31046:6, 1-47102:1, 1-43459:2	Explotación de Microsoft Edge, Internet Explorer, SMBv1, SMBv2.

Ataques a Protocolos de Red (Eternalblue, WannaCry)	Estudiante	Explotación de fallas en SMB para distribución de ransomware.	1-43459:2	Protocolo SMB obsoleto, MS17-010.
Robo de Información (Information Theft, Banker Trojan)	Estudiante, Administrativo	Captura de datos personales y bancarios mediante malware y vulnerabilidades en navegadores.	1-41573:4, 1-25074:1	Vulnerabilidad en Microsoft Edge, inyección de código malicioso.
Denegación de Servicio (DoS) (Script Usage)	Estudiante, Docente	Uso de scripts para ataques DoS en Internet Explorer 9.	1-32691:1	Explotación de sistemas Windows 7 con navegadores obsoletos.

Fuente. Elaboración propia

1. Análisis de las vulnerabilidades detectadas

Los datos obtenidos con NIDS-SNORT y NEXPOSE evidencian patrones específicos de vulnerabilidad en la intranet académica, se detallan en la tabla 14.

Tabla 14: Análisis de las vulnerabilidades detectadas

Hallazgo Clave	**Impacto Identificado**
15.34% de las vulnerabilidades están asociadas con amenazas web.	Pueden ser explotadas mediante malware como Instantaccess.exe, Miner64, XMRig, Ramnit, Zbot o Zeus, Banker y Exploit kit.
Más del 40% de los dispositivos en la VLAN de Estudiantes ejecutan Windows 7.	Son altamente vulnerables a ataques dirigidos a Microsoft Edge e Internet Explorer, facilitando el robo de información.

15.34% de las vulnerabilidades están relacionadas con inyección de código malicioso.	Riesgo de ejecución remota de código a través de navegadores y software no actualizado.
Protocolos SMBv1 y SMBv2 desactualizados fueron identificados.	Facilitan la explotación mediante Eternalblue y Doublepulsar, lo que puede desencadenar ataques con ransomware como WannaCry.
La vulnerabilidad CVE-2018-4990 puede permitir la ejecución de código malicioso.	Explotación de software comercial para comprometer sistemas.
10% de las vulnerabilidades detectadas corresponden a ataques de Denegación de Servicio (DoS).	Vinculados al uso de Internet Explorer 9 en las VLANs Docente y Estudiante.

Fuente. Elaboración propia

Estos hallazgos validan la presencia de amenazas insider en la intranet académica y justifican la necesidad de implementar medidas de control específicas. En este contexto, el SNORT ID (SID) desempeña un papel crucial en la detección y categorización de amenazas, permitiendo una identificación precisa de vulnerabilidades y su gestión eficiente. Además, el SID facilita la búsqueda de soluciones para cada amenaza, optimizando la respuesta ante ataques y permitiendo su explotación controlada con fines de investigación y mitigación.

Dado el impacto potencial de estas vulnerabilidades, en la presente tesis se selecciona una amenaza insider detectada para su control y mitigación, que será abordada en la Etapa 3 del estudio.

Los detalles técnicos sobre configuraciones e interpretación de los datos capturados en la intranet, con NIDS-SNORT y NEXPOSE se presentan en la Etapa 2 de la sección 1.2 del Anexo F.

5.1.3 Etapa 3. Selección de la amenaza a controlar

1. **Análisis los resultados de la RSL sobre amenazas internas en intranets académicas.**

Como parte del proceso de validación de la propuesta, se llevó a cabo una Revisión Sistemática de la Literatura (RSL) con el propósito de identificar las amenazas internas más frecuentes en intranets académicas. En este contexto, se analizó la

pregunta de investigación Q1: ¿Qué tipos de amenazas internas (insider threats) existen en intranets académicas y cuáles son sus fuentes de datos?

Los resultados de la RSL evidenciaron que los ataques de Denegación de Servicio (DoS) y su variante Distribuida (DDoS) constituyen las amenazas más recurrentes en redes académicas, con una presencia significativa en la literatura revisada:

- En relación con Q1.1, los ataques DoS/DDoS representan el 39.31% de las amenazas internas reportadas en redes académicas.
- Respecto a Q1.2, los ataques DoS/DDoS representan el 13.68% de los tipos de amenazas internas identificadas en intranets académicas.

Dado su alta incidencia y potencial impacto en la disponibilidad de los servicios de red, los ataques DoS se consideran una amenaza prioritaria en este estudio.

2. Comparación entre los hallazgos de la RSL y el análisis en tiempo real de la intranet académica

A partir de los resultados obtenidos en la Etapa 2, el análisis en tiempo real del tráfico de la intranet del campus académico de la ESPOCH permitió corroborar la presencia de ataques DoS, que representaron aproximadamente el 10% de las amenazas detectadas. Estos eventos fueron identificados en las VLANs Docente y Estudiante, lo que confirma la existencia de esta amenaza en el entorno objeto de estudio.

La comparación entre estos hallazgos y los resultados de la RSL (Sección 4.2.1) permite validar que los ataques DoS son una amenaza recurrente en redes académicas, tanto en estudios previos como en el análisis específico realizado en la ESPOCH.

En consecuencia, el ataque DoS es seleccionada como la amenaza a controlar en la siguiente fase del estudio, alineándose con la metodología propuesta para mitigar amenazas insider en intranets académicas.

5.1.4 Etapa 4. Implementación de control de la amenaza insider seleccionada: DoS.

La cuarta etapa de la investigación se centra en la implementación y validación de un mecanismo de control del ataque DoS en la intranet académica de la ESPOCH. Para ello, se estableció un entorno basado en SDN con equipos físicos y políticas de QoS aplicadas mediante ACLs.

El objetivo de esta fase es evaluar la eficacia de las estrategias de mitigación del ataque DoS, mediante la comparación de dos escenarios experimentales:

- ✓ Prueba sin control: Se analiza el impacto del ataque sin medidas de mitigación.
- ✓ Prueba con control: Se activan SNORT y Floodlight para la detección y mitigación de la amenaza en tiempo real.

Para la validación del modelo de mitigación, se analizaron los siguientes parámetros de rendimiento de la red: ancho de banda, latencia, jitter y pérdida de paquetes.

Este análisis permitió determinar la viabilidad del modelo de mitigación, proporcionando una base cuantitativa para la implementación de estrategias de seguridad en redes académicas.

1. Definición del Escenario de Control

En esta fase, se diseñó un entorno experimental basado en tecnología SDN, utilizando equipos físicos y herramientas de detección de intrusiones, con el propósito de evaluar la efectividad de la mitigación frente a un ataque DoS. Para mitigar el impacto del ataque DoS, se aplicaron las siguientes estrategias descritas en la tabla 15.

Tabla 15: Estrategias para el Escenario de Control

Estrategia	Descripción
Clasificación del tráfico	1. 80% TCP (tráfico web y servicios estándar). 2. 20% UDP (tráfico en tiempo real y multimedia).
Simulación de tráfico con D-ITG	a. Generación de tráfico representativo de la intranet académica.

	b. Protocolo atacado: DNS.
Integración de SNORT y Floodlight	c. SNORT, detecta tráfico anómalo en tiempo real. d. Floodlight, aplica políticas de control y bloqueo de tráfico malicioso.

Fuente. Elaboración propia

3. Escenario de Pruebas con Tecnología SDN

El entorno experimental replica un nodo de la intranet académica de la ESPOCH, permitiendo evaluar el impacto de ataques DoS y la efectividad de las estrategias de mitigación. El escenario de pruebas se segmentó en dos planos operacionales, conforme se describe en la tabla 16.

Tabla 16: Escenario de pruebas con Tecnología SDN

Plano	Componentes	Función
Plano de Control	1. Controlador Floodlight. 2. NIDS-SNORT. 3. Switch SDN HP E3800.	4. Gestión y monitoreo del tráfico de red. 5. Aplicación de reglas de mitigación en tiempo real.
Plano de Datos	1. Host A (Servidor web, objetivo del ataque). 2. Host B (Usuario legítimo de la red). 3. Equipo atacante (Kali Linux con Slowloris).	4. Simulación del ataque DoS y evaluación del impacto en el rendimiento de la red.

Fuente. Elaboración propia

1. Evaluación del Ataque DoS y Resultados

Se ejecutaron dos pruebas experimentales, evaluando el comportamiento de la red con y sin medidas de mitigación.

Prueba 1: Evaluación del Ataque DoS sin Políticas de Control

En este escenario, se ejecutó un ataque Slowloris, enviando 1000 paquetes TCP por segundo al servidor web. Los resultados evidenciaron un impacto crítico sobre la estabilidad de la red como se detalla en la tabla 17.

Tabla 17: Prueba 1: Evaluación del Ataque DoS sin Políticas de Control

Parámetro	**Valor observado**	**Impacto**
Ancho de Banda	Reducción del 75%.	Afecta la disponibilidad del servicio.
Latencia	Incremento del 220%.	Compromete la capacidad de respuesta.
Jitter	Aumento del 180%.	Fluctuaciones impredecibles, afectando la estabilidad del servicio.
Pérdida de Paquetes	46%.	Compromete la confiabilidad de la comunicación.

Fuente. Elaboración propia

Hallazgos:

1. El ataque saturó el servidor web, dejándolo inaccesible para usuarios legítimos.
2. Se observó un deterioro significativo en los parámetros de rendimiento.
3. No se detectaron mecanismos de bloqueo, permitiendo la explotación sin restricciones.

Prueba 2: Evaluación del Ataque DoS con Políticas de Control

Se repitió el ataque Slowloris, pero esta vez se activaron SNORT y las ACLs en Floodlight, aplicando detección y mitigación en tiempo real, los resultados se observan en la tabla 18.

Tabla 18: Prueba 2: Evaluación del Ataque DoS con Políticas de Control

Parámetro	**Valor observado**	**Impacto**
Ancho de Banda	Reducción del 10%	Mínima afectación al servidor web
Latencia	Incremento del 15%	Respuesta estable
Jitter	Menor variabilidad del 5%	Funcionamiento normal de la red
Pérdida de Paquetes	Reducción drástica del 3%	No afecta la disponibilidad del servicio.

Fuente. Elaboración propia

Hallazgos:

1. SNORT detectó la anomalía en el tráfico y generó alertas en tiempo real.
2. Floodlight aplicó reglas de bloqueo, mitigando el ataque antes de que colapse el servidor.
3. Los parámetros de rendimiento se mantuvieron estables, asegurando la disponibilidad del servicio.

4. Análisis comparativo de Resultados

A continuación, se presenta el impacto de la mitigación del ataque DoS en ambos escenarios como se observa en la tabla 19.

Tabla 19: Análisis comparativo de Resultados del impacto de la mitigación del ataque DoS, sin control y con control.

Parámetro	**Sin Control**	**Con Control**	**Reducción del Impacto (%)**
Ancho de Banda	Reducido	Normalizado	90%
Latencia	Elevada	Estable	85%
Jitter	Fluctuante	Bajo	78%
Pérdida de Paquetes	Alta	Mínima	92%

Fuente. Elaboración propia

Hallazgo Principal: La integración de SNORT y Floodlight en un entorno SDN mitiga eficazmente los ataques DoS, preservando la disponibilidad y estabilidad del servicio.

Síntesis de Hallazgos

Los resultados obtenidos respaldan la efectividad del modelo propuesto para la mitigación de ataques DoS en redes académicas, evidenciando que:

1. Las políticas de QoS y el uso de ACLs en SDN son altamente efectivas para reducir el impacto de los ataques DoS, con una reducción del impacto en la latencia del 85%, en la pérdida de paquetes del 92% y en el jitter del 78% como se observa en la tabla 19.
2. La integración de SNORT y Floodlight permite la detección temprana y el control efectivo de amenazas insider tipo DoS, evitando el colapso del servidor y reduciendo la afectación del ancho de banda en un 90%.

3. El rendimiento de la red experimenta una mejora significativa tras la implementación del control, asegurando la estabilidad y disponibilidad del servicio. En el escenario sin control, la pérdida de paquetes alcanzó el 46%, mientras que en el escenario con control se redujo al 3%, evidenciando una mejora sustancial en la confiabilidad de la comunicación, como muestra la tabla 18.

Estos hallazgos confirman la utilidad de la tecnología SDN con políticas de QoS y ACLs como un enfoque viable para la mitigación de ataques DoS en entornos académicos.

Los detalles técnicos de configuración, pruebas adicionales de los resultados se presentan en la Etapa 4 de la sección 1.3 del Anexo F.

5.2 Recolección y Análisis de datos

5.2.1 Recolección de Datos y Validez Estadística

Para garantizar un análisis estadístico robusto, se tomaron 60 muestras por prueba en el escenario SDN, tanto sin control como con implementación de políticas de mitigación. Este tamaño muestral, supera al umbral de 30 observaciones recomendado para mayor confiabilidad estadística, además por que minimiza errores tipo II (Mahat, 2024; Althubaiti, 2023; Kang, 2021).

Se analizaron los siguientes parámetros de rendimiento de la red:

1. Delay (latencia): tiempo de transmisión de paquetes, métrica clave en la calidad del servicio de red.
2. Jitter: variabilidad en la transmisión de paquetes, relevante en redes definidas por software (SDN).
3. Ancho de banda: capacidad de transmisión de datos, reflejo de la eficiencia de la red.
4. Pérdida de paquetes: porcentaje de paquetes no entregados, indicador de la estabilidad del tráfico de red.
5. Porcentaje de pérdida de paquetes: métrica relativa del tráfico no entregado.
6. Promedio de paquetes por segundo: indicador de la carga de tráfico gestionada por la red.

Para representar un tráfico realista dentro de la intranet académica, los datos analizados se componen de 80% paquetes TCP y 20% UDP, con tamaños de 512 bytes, transmitidos a velocidades de 2.19 a 50.96 Mbps, asegurando la representatividad del tráfico de escenarios operativo.

Mayor detalle de la recolección de datos se encuentra en la sección 2.Recoleccion de datos en el Anexo F.

5.2.2 Análisis de Datos

1. Análisis Descriptivo de las Variables

En la Tabla 20 se presentan los resultados del análisis estadístico descriptivo comparando el rendimiento de la red en los dos escenarios evaluados.

Tabla 20: Análisis estadístico descriptivo del rendimiento de la red en los grupos de estudio.

Parámetro	**Grupo 0 (Sin Control)**	**Grupo 1 (Con Control)**	**Diferencia (%)**
Delay (ms)	1090.19	1063.60	↓ 2.5%
Jitter (ms)	0.0004	0.0004	No significativo
Ancho de Banda (kbps)	30,732.80	31,410.98	↑ 2.2%
Pérdida de Paquetes (%)	6.77%	5.56%	↓ 1.21%
Promedio de Paquetes/S	7,503.13	7,668.70	↑ 2.2%

Fuente. Elaboración propia

Hallazgos Principales

1. Reducción del delay en 2.5%: Se confirma que la política de control mejora el tiempo de transmisión de paquetes, mitigando el impacto del ataque DoS.
2. Disminución de la pérdida de paquetes en 1.21%: Refleja mayor estabilidad de la red ante escenarios de ataque.
3. Aumento del ancho de banda en 2.2%: Sugiere una mejor gestión del tráfico sin comprometer la capacidad de transmisión.

4. Validación de Supuestos

Para verificar el cumplimiento de supuestos estadísticos previo a la comprobación de hipótesis, se aplicaron las siguientes pruebas estadísticas:

Prueba de Normalidad (Shapiro-Wilk)

1. Todas las variables presentaron $p < 0.05$, lo que indica que no siguen una distribución normal.

Prueba de Homogeneidad de Varianzas (Levene)

1. Se confirma que el delay no tiene varianzas homogéneas, lo que impide el uso de pruebas paramétricas en esta variable.

Prueba U de Mann-Whitney

Dado que los datos no cumplen los supuestos de normalidad ni homogeneidad de varianzas, se aplicó la prueba U de Mann-Whitney para comparar ambos grupos. Como muestra la tabla 21.

Tabla 21: Resultados de la prueba U de Mann-Whitney

Variable	**U de Mann-Whitney**	**p-valor**	**Diferencia Significativa**
Delay	322.00	0.000	Sí, mejora con control.
Jitter	1669.50	0.493	No significativa.
Ancho de Banda	1634.00	0.384	No significativa.
Promedio P/S	1634.00	0.384	No significativa.
Pérdida de Paquetes	1654.00	0.443	No significativa.

Fuente. Elaboración propia

Interpretación de Resultados:

1. El delay es la única variable con una diferencia estadísticamente significativa, confirmando la efectividad de la política de control para mejorar la entrega de paquetes en ataques DoS.

2. Aunque las demás variables presentan mejoras, estas no son estadísticamente significativas, lo que sugiere que la política de control no degrada la estabilidad general de la red.

3. Hallazgos del Análisis de Datos

Se detallan los siguientes hallazgos en base al análisis de datos.

1. Impacto en el Delay: Evidencia de Mejora Significativa

La política de control logró una reducción estadísticamente significativa del delay en 2.5%, demostrando su eficacia para mitigar el tráfico malicioso.
Dado que el delay es una métrica crítica en la calidad del servicio de redes, esta mejora representa un avance significativo en la optimización del rendimiento de redes SDN bajo ataque DoS.

2. Optimización del ancho de banda y reducción de la pérdida de paquetes

Aunque la mejora en el ancho de banda (+2.2%) no fue estadísticamente significativa, su incremento indica una administración más eficiente del tráfico, evitando congestiones.

La reducción en la pérdida de paquetes de 6.77% a 5.56% (1.21%) refuerza la efectividad del control implementado en la estabilidad del tráfico de red.

3. Hallazgo Principal: Validación del Enfoque de Seguridad en SDN

La combinación de SNORT + políticas de control en Floodlight en SDN ha demostrado ser una solución efectiva para mitigar ataques DoS en redes académicas.

Se ha comprobado que este enfoque reduce el delay y optimiza la gestión del tráfico sin afectar negativamente la estabilidad de la red.

4. Contribución del estudio

1. Validación de la hipótesis: "La implementación de políticas de QoS en SDN facilita el control de amenazas insider, mejorando el rendimiento de la intranet académica".
2. Aporte empírico en seguridad SDN: El estudio consolida la viabilidad de las políticas de QoS como estrategia efectiva para mitigar amenazas insider sin degradar el rendimiento de la red.

3. Proyección para futuras investigaciones: Se abre la posibilidad de optimizar la estrategia de control, especialmente en la reducción de la pérdida de paquetes en escenarios con tráfico elevado.

Los cálculos detallados del análisis estadístico se encuentran en Sección 3 - Análisis de Datos del Anexo F.

5.3 Discusión de resultados

Esta tesis desarrolla una metodología innovadora y sistemática para la implementación de políticas de Calidad de Servicio (QoS) en redes SDN, enfocada en la gestión de amenazas internas en intranets académicas. La metodología se estructura en cuatro etapas, comenzando con el diagnóstico de seguridad en el canal humano, seguido del análisis en tiempo real del tráfico de la red para identificar amenazas, la selección de la amenaza a controlar y, finalmente, la implementación de medidas de control en un entorno de prueba real con tecnología SDN y equipos físicos.

Los resultados obtenidos evidencian una reducción significativa del delay, lo que confirma el impacto positivo de las políticas de QoS en la optimización del rendimiento de la red en entornos académicos. Aunque métricas como jitter, ancho de banda y pérdida de paquetes no mostraron diferencias estadísticamente significativas, la implementación de políticas de control en el Grupo 1 demuestra una mejora constante en la estabilidad de la red. Esto valida la relevancia de estas estrategias no solo en la optimización de métricas clave, sino también en la consolidación de un enfoque práctico y replicable para la seguridad y eficiencia de redes SDN.

Desde una perspectiva comparativa, la metodología propuesta aborda un vacío en la literatura, respondiendo a los hallazgos de (Imran et al., 2019), quienes identificaron la necesidad de estrategias de control capaces de mitigar el delay y reducir la sobrecarga computacional en redes SDN, sin que hasta el momento se hubiera validado su implementación en entornos operativos reales. Este estudio cierra esa brecha empírica, demostrando que la aplicación de controles DoS en SDN no solo

preserva la funcionalidad del controlador, sino que también reduce significativamente el delay, mejorando la estabilidad y eficiencia de la red.

A diferencia del trabajo de (Karakus & Durresi, 2017), que analiza teóricamente el impacto de políticas de control en la reducción del delay sin evaluar su implementación práctica, esta investigación trasciende los enfoques teóricos al realizar pruebas en un entorno con equipos físicos reales. Además, incorpora un análisis estadístico riguroso, validando la aplicabilidad y efectividad de las estrategias propuestas y consolidando un marco metodológico replicable para la mitigación de amenazas en redes SDN.

Asimismo, en comparación con el estudio de (Tang et al., 2023), que propone PeakSax como un framework para la detección y mitigación de ataques DoS de baja tasa (LDoS) mediante algoritmos de clasificación, la metodología de este estudio amplía el enfoque al evaluar el rendimiento de la red a partir de métricas fundamentales como delay, jitter, ancho de banda y pérdida de paquetes, proporcionando una visión más integral del impacto de los ataques DoS en SDN. Mientras PeakSax se centra exclusivamente en ataques LDoS, este estudio aborda un espectro más amplio de amenazas internas, implementando controles mediante el controlador FloodLight y adaptándose a un contexto operativo real en redes académicas.
Si bien en el presente estudio no se contempló una comparación experimental directa con el enfoque PeakSax, se reconoce la validez de dicho framework para la detección de ataques LDoS mediante técnicas de aprendizaje automático. No obstante, su aplicación se limita a un tipo de amenaza muy específico, mientras que la metodología propuesta en esta tesis aborda un espectro más amplio de amenazas internas en intranets académicas, combinando detección, mitigación y evaluación del impacto operativo en la red. Adicionalmente, el enfoque adoptado privilegia la practicidad, la replicabilidad y la adaptabilidad a contextos educativos con recursos limitados, mediante el uso de tecnologías de acceso abierto como el controlador FloodLight y el IDS SNORT. Una comparación experimental directa entre ambos enfoques requeriría el rediseño de los protocolos de prueba bajo condiciones equivalentes, lo cual constituye una línea de investigación futura de gran interés para fortalecer el control integral de amenazas internas en redes académicas.

La adaptabilidad y transferibilidad del enfoque propuesto son factores clave para su aplicación en instituciones educativas, especialmente aquellas con recursos limitados

para implementar sistemas de mitigación avanzados. La integración de políticas de QoS mediante ACLs en el controlador FloodLight se presenta como una solución accesible y efectiva, aprovechando la familiaridad y disponibilidad de estas tecnologías en entornos académicos. Además, la validación práctica de las políticas de QoS refuerza su viabilidad en escenarios operativos reales, consolidando un framework teóricamente sólido y eficaz para la gestión de amenazas internas en redes académicas. Estos hallazgos marcan un hito significativo en la ciberseguridad académica, proporcionando un modelo replicable que optimiza tanto la seguridad como el rendimiento de la red.

No obstante, aunque los resultados obtenidos demuestran la efectividad de la metodología propuesta, es importante considerar ciertas limitaciones en su implementación. Factores como la infraestructura computacional disponible en cada universidad, el nivel de capacitación del personal técnico y la dependencia de herramientas específicas pueden influir en la aplicabilidad del modelo. Estas consideraciones serán abordadas en la siguiente sección, permitiendo contextualizar los desafíos asociados y plantear estrategias de mejora.

5.4 Limitaciones del estudio

Con respecto a las limitaciones del estudio, si bien la metodología propuesta para la detección de amenazas internas en las intranets de los campus académicos proporciona un enfoque estructurado y eficaz para identificar y mitigar riesgos de seguridad, es fundamental reconocer ciertos desafíos que pueden afectar su aplicabilidad en diversos entornos académicos.

La primera limitación se refiere a la adaptación de la metodología OSSTMM, que se centra principalmente en el canal humano. Aunque este enfoque incorpora aspectos de seguridad física mediante controles de acceso y observación directa, podría pasar por alto otras dimensiones críticas de seguridad, como los vectores de amenazas externas y las amenazas persistentes avanzadas (APTs), que también podrían comprometer la integridad de la intranet.

Además, la metodología depende en gran medida de herramientas específicas como NIDS-SNORT y Nexpose para la detección de amenazas en tiempo real y la

evaluación de vulnerabilidades. Si bien estas herramientas son ampliamente utilizadas en ciberseguridad, su efectividad está inherentemente limitada por sus capacidades de detección y la precisión de sus reglas. Cualquier limitación específica de estas herramientas, como la generación de falsos positivos o una cobertura limitada de amenazas emergentes, podría afectar la fiabilidad y exhaustividad del enfoque propuesto.

Finalmente, la implementación de esta metodología requiere recursos computacionales significativos y personal capacitado, lo que puede representar un desafío importante para universidades con restricciones presupuestarias y conocimientos limitados en ciberseguridad. La implementación de políticas de seguridad basadas en SDN, combinada con el monitoreo continuo y el mantenimiento, demanda una inversión tanto en infraestructura como en formación, lo que podría limitar la escalabilidad del enfoque en instituciones con menores recursos tecnológicos.

Superar estos desafíos requerirá estrategias de optimización, incluyendo la automatización de procesos de detección y mitigación, la integración de herramientas de inteligencia artificial y la capacitación del personal técnico en el uso de tecnologías SDN y sistemas de detección de intrusiones.

En este sentido, los trabajos futuros de esta investigación deberán centrarse en la exploración de metodologías más eficientes para la mitigación de amenazas internas, considerando la integración de técnicas avanzadas de aprendizaje automático y análisis de comportamiento de tráfico de red. Estas herramientas permitirían una detección anticipada y adaptativa de las amenazas internas. Aunque el presente estudio implementa políticas estáticas de control con QoS en entornos SDN, los hallazgos de la RSL (Q2.6) evidencian un campo en desarrollo donde algoritmos de aprendizaje automático y técnicas de análisis de comportamiento aún no se integran de manera sistemática. Incorporar estas capacidades permitiría reducir la dependencia de reglas predefinidas y ofrecer respuestas más dinámicas y personalizadas ante comportamientos maliciosos o atípicos en la red. Asimismo, la validación de la metodología en distintos entornos académicos e industriales permitirá fortalecer su aplicabilidad y generar nuevas estrategias de seguridad adaptativas para redes de datos en evolución.

CONCLUSIONES Y TRABAJOS FUTUROS

Este apartado presenta las principales conclusiones del trabajo de investigación doctoral, destacando los aportes metodológicos, los resultados obtenidos y las sugerencias para futuras investigaciones.

Conclusiones

1. **Aporte metodológico e innovación en el análisis de amenazas internas en redes académicas.**

   Uno de los principales aportes de esta investigación es el desarrollo de un modelo de análisis de amenazas en redes académicas basado en VLANs, diferenciando las amenazas según el tipo de usuario interno (VLAN Estudiante, Docente y Administrativo). A diferencia de enfoques generales sobre seguridad en redes de datos o académicos, este estudio introduce una segmentación precisa, permitiendo una identificación más efectiva de vulnerabilidades y riesgos específicos.

   Este enfoque metodológico, derivado de la RSL (Q1) que cubre el periodo 1997–2022 y se describe en el cap.3 de esta tesis, responde a una brecha en la literatura, dado que hasta donde se ha identificado, ningún estudio previo ha abordado esta clasificación en el contexto académico, lo que confirman estudios recientes publicados entre 2022 y 2024, así como las recomendaciones de organismos especializados como CERT (2022). Esto refuerza la pertinencia y actualidad del problema abordado, así como el carácter innovador de la propuesta desarrollada en esta tesis.

   Su implementación sienta las bases para futuras investigaciones sobre el comportamiento de usuarios internos y las amenazas asociadas, además de proporcionar un marco metodológico innovador alineado con las dinámicas de uso interno de redes académicas. Asimismo, este trabajo representa un avance significativo para la comunidad científica en Ecuador y a nivel internacional, con un enfoque replicable en otras instituciones de educación superior y adaptable a entornos con segmentación de usuarios en VLANs como parte de su estrategia de seguridad informática.

2. **Desarrollo de un modelo integral de mitigación de amenazas internas basado en SDN y QoS.**

La RSL en Q3.12 descrita en el cap. 3 de esta tesis, evidenció que el 52.14% de los estudios analizados emplean metodologías propias para la detección y mitigación de amenazas internas, lo que pone en evidencia la ausencia de un marco estandarizado. Para abordar esta brecha, esta investigación propone un modelo avanzado basado en Redes Definidas por Software (SDN) y políticas de Calidad de Servicio (QoS), integrando herramientas como NIDS-SNORT para monitoreo en tiempo real y Nexpose para validación de vulnerabilidades.

En comparación con enfoques tradicionales, que abordan la seguridad de manera fragmentada y sin una integración estructurada, este modelo optimiza tanto la protección contra amenazas internas como el rendimiento del tráfico en redes académicas. La validación empírica en entornos operativos reales confirma su eficacia, destacando su capacidad para detectar y mitigar ataques sin comprometer la estabilidad de la red. Estos hallazgos fortalecen el conocimiento en ciberseguridad y gestión de redes académicas, proporcionando un modelo replicable para instituciones educativas y adaptable a otros sectores con arquitecturas de red segmentadas.

3. **Validación empírica de políticas de QoS con ACLs en el controlador FloodLight.**

La investigación evaluó el impacto de las políticas de QoS con ACLs en el controlador FloodLight, mediante métricas clave como: delay, jitter, ancho de banda y pérdida de paquetes. Los resultados obtenidos confirmaron la efectividad de estas políticas en la optimización del rendimiento de la red, destacando los siguientes hallazgos clave:

1. Reducción del delay en un 2,5%, proporcionando evidencia empírica para abordar limitaciones identificadas en la literatura, como las expuestas por (Imran et al., 2019) quienes resaltan la necesidad de estrategias de control que no solo reduzcan la latencia, sino que también protejan contra ataques DoS.
2. Disminución del jitter, lo que mejora la uniformidad en los tiempos de transmisión de paquetes, un aspecto crítico en infraestructuras

que requieren estabilidad temporal para garantizar un desempeño óptimo.

3. Aumento del ancho de banda en 2.2%, lo que sugiere una mejor gestión del tráfico sin comprometer la capacidad de transmisión, corroborando lo expuesto por (Jenny & Sugirtham, 2023), quienes resaltan la importancia de las políticas de QoS en la eficiencia del ancho de banda, aunque sin reportar datos.
4. Reducción de la pérdida de paquetes en un 1,21%, validando la eficacia de las políticas de control en la mitigación de interrupciones generadas por ataques DoS, en contraste con estudios recientes como el de (J. Wang et al., 2023), que no reportan datos específicos sobre la reducción de la pérdida de paquetes.

En su conjunto, estos resultados representan un avance cuantificable y replicable, al proporcionar datos empíricos sólidos sobre la efectividad de las políticas de QoS en entornos operativos reales.

4. Validación experimental del impacto de la metodología en escenarios controlados

El análisis de los datos para validar la metodología en dos escenarios mostró que en el escenario sin política de control el delay promedio era de 1090.19 ms, mientras que, en el escenario con política de control, el delay se redujo significativamente a 1063.60 ms. La prueba estadística de Mann-Whitney U determinó que la política de control tuvo un efecto significativo en la reducción del retraso (delay) sin afectar significativamente otras métricas como el jitter, el ancho de banda y la pérdida de paquetes. Este hallazgo es crucial en un entorno SDN, donde la eficiencia en la transmisión de paquetes es fundamental para el rendimiento de las aplicaciones y servicios.

5. Confirmación de la hipótesis de la investigación.

Los hallazgos confirman la hipótesis de la tesis:

“La implementación de políticas de QoS en SDN para facilitar el control de insiders threat mejora el rendimiento de la intranet académica”.

Este resultado demuestra la solidez de la metodología para una gestión de red eficiente en entornos SDN, validando la efectividad de las políticas de

control implementadas para mejorar la QoS y la experiencia del usuario final en redes académicas.

6. Análisis de vulnerabilidades en la intranet de la ESPOCH.

El estudio de la intranet del campus académico de la ESPOCH (Ecuador) resume las principales amenazas, entre ellas:

1. VLAN Estudiante con el mayor grado de vulnerabilidad (15.34%), expuesta a riesgos como ataques web, vulnerabilidades SMBv1 y SMBv2, y ataques ransomware (Wannacry, CVE-2018-4990).
2. 40% de los usuarios con riesgo de robo de información debido a deficiencias en sistemas operativos.
3. Coincidencia del 10% en vulnerabilidades DoS entre las VLANs Docente y Estudiante, en línea con los hallazgos de la RSL.

Estos hallazgos permitieron seleccionar una amenaza relevante para su análisis en un escenario de pruebas SDN, contribuyendo al desarrollo de una solución específica y proporcionando datos empíricos para investigaciones futuras en ciberseguridad académica.

4. Limitaciones del estudio y consideraciones para su aplicabilidad

A pesar de los aportes significativos de este estudio, es importante reconocer ciertas limitaciones que pueden influir en la aplicación de la metodología en distintos entornos académicos.

1. Dependencia de herramientas específicas: La metodología propuesta se basa en NIDS-SNORT y Nexpose, lo que implica que su efectividad puede estar limitada por las capacidades y restricciones de estas herramientas en la detección de amenazas emergentes.
2. Requerimientos de infraestructura y personal capacitado: La implementación del modelo requiere recursos computacionales significativos y personal con conocimientos especializados en ciberseguridad y administración de redes SDN. En instituciones con presupuesto y formación técnica limitada, la escalabilidad del modelo puede verse comprometida.
3. Enfoque en el canal humano dentro de OSSTMM: Si bien este modelo analiza la seguridad en la interacción humana dentro de la intranet académica, puede no cubrir completamente amenazas externas o

ataques más sofisticados, como amenazas persistentes avanzadas (APTs).

Para superar estas limitaciones, será necesario optimizar la detección y mitigación de amenazas, integrando inteligencia artificial, automatización y capacitación especializada en SDN. Además, se abren nuevas líneas de investigación enfocadas en reducir la dependencia de herramientas específicas y en el desarrollo de soluciones híbridas que combinen IA con métodos tradicionales de detección, mejorando así la efectividad y aplicabilidad del modelo en diversos entornos.

Trabajos futuros

Integración de nuevas tecnologías: Incorporar aprendizaje automático y la inteligencia artificial en la detección y mitigación de amenazas internas podrían mejorar significativamente la precisión y eficiencia de las políticas de control de QoS en redes SDN. Considerando la aplicación práctica, se propone desarrollar modelos de clasificación supervisada que aprendan del comportamiento histórico del tráfico de red (como perfiles de uso por usuario, volumen y destino del tráfico), con el fin de detectar patrones anómalos vinculados a amenazas internas, como accesos indebidos, movimientos laterales o fugas de información. Asimismo, técnicas no supervisadas como clustering permitirían identificar nuevas amenazas sin conocimiento previo, al detectar comportamientos atípicos en tiempo real. Estos modelos se podrían integrar directamente en el plano de control del controlador SDN para ejecutar decisiones automáticas de bloqueo o redirección, reduciendo así la dependencia de reglas estáticas y mejorando la capacidad de respuesta adaptativa ante ataques emergentes.

Ampliación del alcance de las políticas de QoS: Ampliar el alcance de las políticas de QoS para cubrir no solo ataques de DoS y sus variantes, sino amenazas internas como el *malware* y el robo de información proporcionaría una defensa más robusta contra una variedad de amenazas.

Desarrollo de estrategias avanzadas de gestión de tráfico: Estudios profundos en los parámetros de *jitter*, ancho de banda y pérdida de paquetes y su relación

permitiría desarrollar políticas puntuales de control de entornos SDN para mejorar significativamente el rendimiento de la red.

Evaluación de la metodología de control de amenazas internas propuesta, en diferentes entornos: Evaluar la metodología propuesta en varios entornos educativos y/o industriales permitirá validar su adaptabilidad y efectividad en diferentes contextos. Estudios comparativos identificarán ajustes necesarios y mejorarán la versatilidad del framework desarrollado.

Implementación de un estándar metodológico a partir del framework de control de amenazas internas propuesto: La creación de un estándar metodológico integral basado en las cuatro etapas propuestas en esta tesis puede ser formalmente desarrollado y promovido para su implementación en instituciones académicas y/o industriales. La estandarización del framework podría cubrir el vacío existente de una normativa en la literatura y práctica actual.

Solución a las limitaciones del estudio: En futuros trabajos se explorarán técnicas para mitigar las limitaciones identificadas, como la evaluación de herramientas alternativas a SNORT/Nexpose, el diseño de metodologías menos dependientes de infraestructura avanzada y la implementación de modelos híbridos de detección de amenazas.

En conclusión, el enfoque integral y práctico de esta tesis contribuye al fortalecimiento de la seguridad y el rendimiento de intranets académicas, estableciendo una metodología replicable en futuros estudios e integrable con tecnologías emergentes para ampliar su efectividad en la detección y mitigación de amenazas.

REFERENCIAS

Agency Cybersecurity and Infrastructure Security. (2020). *Insider Threat Mitigation Guide* (Issue November). https://www.cisa.gov/insider-threat-mitigation

Agrafiotis, I., Erola, A., Happa, J., Goldsmith, M., & Creese, S. (2016). Validating an Insider Threat Detection System: A Real Scenario Perspective. *Proceedings - 2016 IEEE Symposium on Security and Privacy Workshops, SPW 2016*. https://doi.org/10.1109/SPW.2016.36

Akello, B. O. (2024). Organizational Information Security Threats: Status and Challenges. *World Journal of Advanced Engineering Technology and Sciences*. https://doi.org/10.30574/wjaets.2024.11.1.0152

Alagrash, Y., Mohan, N., Gollapalli, S. R., & Rrushi, J. (2019). Machine learning and recognition of user tasks for malware detection. *Proceedings - 1st IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications, TPS-ISA 2019*, 73–81. https://doi.org/10.1109/TPS-ISA48467.2019.00018

Albrecht, M., & Jensen, R. B. (2020). *The Vacuity of the Open Source Security Testing Methodology Manual*. https://doi.org/10.48550/arxiv.2010.06377

Albu-Salih, A. T. (2022). Performance Evaluation of Ryu Controller in Software Defined Networks. In *Journal of Al-Qadisiyah for Computer Science and Mathematics*. https://doi.org/10.29304/jqcm.2022.14.1.879

Al-Fawa'reh, M., Al-Fayoumi, M., Nashwan, S., & Fraihat, S. (2022). Cyber threat intelligence using PCA-DNN model to detect abnormal network behavior. *Egyptian Informatics Journal*, *23*(2), 173–185. https://doi.org/10.1016/J.EIJ.2021.12.001

Ali, B., Gregory, M. A., & Li, S. (2021). Multi-Access Edge Computing Architecture, Data Security and Privacy: A Review. *Ieee Access*. https://doi.org/10.1109/access.2021.3053233

Ali, D. F., Johari, N., & Ahmad, A. R. (2023). The Effect of Augmented Reality Mobile Learning in Microeconomic Course. In *International Journal of Evaluation and Research in Education (Ijere)*. https://doi.org/10.11591/ijere.v12i2.24943

Ali, S. T., Sivaraman, V., Radford, A., & Jha, S. (2013). Securing Networks Using Software Defined Networking : A Survey. *IEEE Transactions on Reliability*, *64*(3), 1–12. https://doi.org/10.1109/TR.2015.2421391

Ali, S. T., Sivaraman, V., Radford, A., & Jha, S. (2015). A Survey of Securing Networks Using Software Defined Networking. *IEEE Transactions on Reliability*, *64*(3), 1086–1097. https://doi.org/10.1109/TR.2015.2421391

Al-Mhiqani, M. N., Ahmad, R., Abidin, Z. Z., Yassin, W., Hassan, A., Abdulkareem, K. H., Ali, N. S., & Yunos, Z. (2020). A Review of Insider Threat Detection: Classification, Machine Learning Techniques, Datasets, Open Challenges, and Recommendations. *Applied Sciences*. https://doi.org/10.3390/app10155208

Al-Shehari, T. (2023). Insider Threat Detection Model Using Anomaly-Based Isolation Forest Algorithm. *Ieee Access*. https://doi.org/10.1109/access.2023.3326750

Althubaiti, A. (2023). Sample size determination: A practical guide for health researchers. *Journal of General and Family Medicine*, *24*(2), 72–78. https://doi.org/10.1002/jgf2.600

Amaral, P., & Bernardo, L. (2016). Machine Learning in Software Defined Networks : Data Collection and Traffic Classification. *Proc IEEE International Conference on Network Protocols, Workshop on Machine Learning in Computer Networks ICNP (NetworkML)*, *NetworkML*, 1–5. https://doi.org/10.1109/ICNP.2016.7785327

Amoroso, E., Kogan, E., McAnderson, B., Powell, D., Rexroad, B., Schuster, S., & Stramaglia, A. (1998). Local area detection of incoming war dial activity. *Proceedings of the IEEE Symposium on Reliable Distributed Systems*, 486–491. https://doi.org/10.1109/RELDIS.1998.740545

Androulidakis, G., Chatzigiannakis, V., & Papavassiliou, S. (2007). Using selective sampling for the support of scalable and efficient network anomaly detection. *GLOBECOM - IEEE Global Telecommunications Conference*. https://doi.org/10.1109/GLOCOMW.2007.4437785

Androulidakis, G., Chatzigiannakis, V., & Papavassiliou, S. (2009). Network anomaly detection and classification via opportunistic sampling. *IEEE Network*, *23*(1), 6–12. https://doi.org/10.1109/MNET.2009.4804318

Androulidakis, G., & Papavassiliou, S. (2007). Intelligent flow-based sampling for effective network anomaly detection. *GLOBECOM - IEEE Global Telecommunications Conference*, 1948–1953. https://doi.org/10.1109/GLOCOM.2007.374

Angel, N. A., Ravindran, D., Vincent, P., Srinivasan, K., & Hu, Y.-C. (2021). Recent Advances in Evolving Computing Paradigms: Cloud, Edge, and Fog Technologies. *Sensors*. https://doi.org/10.3390/s22010196

Ashraf, J., & Latif, S. (2014). Handling intrusion and DDoS attacks in Software Defined Networks using machine learning techniques. *National Software Engineering Conference, NSEC 2014*, 55–60. https://doi.org/10.1109/NSEC.2014.6998241

Association for Computing Machinery. (1985). *ACM Digital Library*.

Axess Networks. (2020). *Qué es ancho de banda, banda ancha, velocidad y latencia en internet*. Axess Networks. https://axessnet.com/que-es-ancho-de-banda-velocidad-y-latencia-en-una-conexion-de-internet/#:~:text=¿Qué es la latencia%3F,en línea o hacer videollamadas.

Balakrishnan, M. (2022). An Evaluation of Ubiquitous Service Discovery and Remote Management in Ad-Hoc Networks. In *Journal of Machine and Computing*. https://doi.org/10.53759/7669/jmc202202019

Ball, R., Fink, G. A., & North, C. (2004). Home-centric visualization of network traffic for security administration. *VizSEC/DMSEC '04: Proceedings of the 2004 ACM Workshop on Visualization and Data Mining for Computer Security*, 55–64. https://doi.org/10.1145/1029208.1029217

Barba, R. G., Criollo, M., Aimacana, N., Manosalvas, C., & Silva-Cardenas, C. (2019). QoS Policies to Improve Performance in Academic Campus and SDN Networks. *Proceedings - 2018 10th IEEE Latin-American Conference on Communications, LATINCOM 2018*, 1–6. https://doi.org/10.1109/LATINCOM.2018.8613227

Barba-Vera, R., Criollo Bustamante, M., Aimacaña Toledo, N., Silva-Cárdenas, C., & Vaca Barahona, B. (2020). Políticas públicas en el Ecuador hacia la ciberseguridad en base a QoS en redes de campus académicos en entornos convencionales y SDN. *Revista Ibérica de Sistemas e Tecnologias de Informação*, *37*(Retos y Aportes al Desarrollo Tecnológico de la Sociedad Moderna (CSEI'2020)), 166–179. https://www.proquest.com/scholarly-journals/políticas-públicas-en-el-ecuador-hacia-la/docview/2472669103/se-2?accountid=201395

BetaFred, mdressman, & v-samkha. (2019). *Microsoft Security Bulletin MS08-069 - Critical | Microsoft Docs*. https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2014/ms14-080?redirectedfrom=MSDN

Bhati, B. S., Chugh, G., Al-Turjman, F., & Bhati, N. S. (2021). An improved ensemble based intrusion detection technique using XGBoost. *Transactions on Emerging Telecommunications Technologies*, *32*(6), e4076. https://doi.org/10.1002/ETT.4076

Bhilare, D. S., Ramani, A. K., & Tanwani, S. K. (2009). Protecting intellectual property and sensitive information in academic campuses from trusted insiders: Leveraging active directory. *SIGUCCS'09 - Proceedings of the 2009 ACM SIGUCCS Fall Conference*, 99–103. https://doi.org/10.1145/1629501.1629520

Bishop, M., Engle, S., & Frincke, D. (2010). A risk management approach to the "insider threat." *Insider Threats in Cyber …*, 1–24.

Bishop, M., & Gates, C. (2008). Defining the insider threat. *Proceedings of the 4th Annual Workshop on Cyber Security and Informaiton Intelligence Research Developing Strategies to Meet the Cyber Security and Information Intelligence Challenges Ahead - CSIIRW '08*, 1. https://doi.org/10.1145/1413140.1413158

Budgen, D., & Brereton, P. (2006). Performing systematic literature reviews in software engineering. *Proceedings - International Conference on Software Engineering*, *2006*(4ve), 1051–1052. https://doi.org/10.1145/1134285.1134500

C. W. Probst, J. H. D. G. and M. B. E. (2010). Insider Threats in Cyber Security. *Springer*.

Cadena Vela, S., Córdova Ochoa, J., Enríquez Reyes, R., & Padilla Verdugo, R. (2019). *UE tic: Estado de las tecnologías de la información y comunicación en las universidades ecuatorianas.* (Issue Abril). https://cedia.edu.ec/docs/uetic/UETIC_2019.pdf

Caulkin, B. D., Lee, J., & Wang, M. (2005). Packet- vs. session-based modeling for intrusion detection systems. *International Conference on Information Technology: Coding and Computing, ITCC*, *1*, 116–121. https://doi.org/10.1109/ITCC.2005.222

Čermák, M., Čeleda, P., & Vykopal, J. (2014). Detection of DNS traffic anomalies in large networks. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *8846*, 215–226. https://doi.org/10.1007/978-3-319-13488-8_20

Chen, S., Chen, X., Yao, Z., Yang, J., Li, Y., & Wu, F. (2020). Evolving Switch Architecture toward Accommodating In-Network Intelligence. *IEEE Communications Magazine*, *58*(1), 33–39. https://doi.org/10.1109/MCOM.001.1800923

Chen, Y., & Malin, B. (2011). Detection of anomalous insiders in collaborative environments via relational analysis of access logs. *CODASPY'11 - Proceedings of the 1st ACM Conference on Data and Application Security and Privacy*, 63–74. https://doi.org/10.1145/1943513.1943524

Chen, Y., Wang, Y., & Luo, J. (2016). Research on the active defense security system based on cloud computing of wisdom campus network. *Proceedings of the 28th Chinese Control and Decision Conference, CCDC 2016*, 1292–1297. https://doi.org/10.1109/CCDC.2016.7531184

Chuang, H.-M., & Ye, L.-J. (2023). Applying Transfer Learning Approaches for Intrusion Detection in Software-Defined Networking. *Sustainability*, *15*(12). https://doi.org/10.3390/su15129395

Cojocariu, A.-C., Verzea, I., & Chaib, R. (2020). Aspects of Cyber-Security in Higher Education Institutions. In G. Prostean, J. J. Lavios Villahoz, L. Brancu, & G. Bakacsi (Eds.), *Innovation in Sustainable Management and Entrepreneurship* (pp. 3–11). Springer International Publishing.

Continuous Internal Penetration Testing (CIPT). (2023). *Journal of Mathematical Techniques and Computational Mathematics*, *2*(8), 368–374. https://doi.org/10.33140/JMTCM.02.08.05

Correa Chica, J. C., Imbachi, J. C., & Botero Vega, J. F. (2020). Security in SDN: A comprehensive survey. *Journal of Network and Computer Applications*, *159*, 102595. https://doi.org/https://doi.org/10.1016/j.jnca.2020.102595

Cox, J. H., Clark, R. J., & Owen, H. L. (2016). Leveraging SDN for ARP security. *Conference Proceedings - IEEE SOUTHEASTCON*, *2016-July*. https://doi.org/10.1109/SECON.2016.7506644

da Silva, A. S., Smith, P., Mauthe, A., & Schaeffer-Filho, A. (2015). Resilience support in software-defined networking: A survey. *Computer Networks*, *92*, 189–207. https://doi.org/10.1016/J.COMNET.2015.09.012

Dawadi, B. R., Thapa, A., Guragain, R., Karki, D., Upadhaya, S. P., & Joshi, S. R. (2021). Routing performance evaluation of a multi-domain hybrid SDN for its implementation in carrier grade ISP networks. *Applied System Innovation*, *4*(3). https://doi.org/10.3390/asi4030046

Daxian, W., Jishan, Z., & Jiujiu, Y. (2020). Research on intelligent Firewall for network security. *ACM International Conference Proceeding Series*, 255–258. https://doi.org/10.1145/3438872.3439090

De Ramos, N. M., & Esponilla II, F. D. (2022). Cybersecurity program for Philippine higher education institutions: A multiple-case study. *International Journal of Evaluation and Research in Education (IJERE)*, *11*(3), 1198. https://doi.org/10.11591/ijere.v11i3.22863

Deshmukh, E. al. P. K. (2024). QoS-Aware Routing and Resource Allocation Techniques for Enhanced Network Performance. *Jes*, *19*(2), 78–86. https://doi.org/10.52783/jes.693

Deshpande, K., & Rao, M. (2022). An Open-Source Framework Unifying Stream and Batch Processing. *Lecture Notes in Networks and Systems*, *336*, 607–630. https://doi.org/10.1007/978-981-16-6723-7_45/COVER

Dewanjee, R. (2017). Intrusion Filtration System(IFS)-mapping network security in new way. *International Conference on Signal Processing, Communication, Power and Embedded System, SCOPES 2016 - Proceedings*, 527–531. https://doi.org/10.1109/SCOPES.2016.7955883

Dong, C., Chen, Y., Zhang, Y., Liu, Y., Lu, Z., Dong, P., & Liu, B. (2021). BEDIM: Lateral Movement Detection In Enterprise Network Through Behavior Deviation Measurement. *2021 IEEE 23rd Int Conf on High Performance Computing & Communications; 7th Int Conf on Data Science & Systems; 19th Int Conf on Smart City; 7th Int Conf on Dependability in Sensor, Cloud & Big Data Systems & Application (HPCC/DSS/SmartCity/DependSys)*, 391–398. https://doi.org/10.1109/HPCC-DSS-SMARTCITY-DEPENDSYS53884.2021.00076

Downer, K., & Bhattacharya, M. (2022). BYOD Security: A Study of Human Dimensions. In *Informatics*. https://doi.org/10.3390/informatics9010016

Dutt, I., Borah, S., & Maitra, I. (2018). A Proposed Machine Learning based Scheme for Intrusion Detection. *Proceedings of the 2nd International Conference on Electronics, Communication and Aerospace Technology, ICECA 2018*, 479–483. https://doi.org/10.1109/ICECA.2018.8474803

Edwards, Dr. J. (2024). *Vulnerability Assessment and Penetration Testing*. 371–412. https://doi.org/10.1007/979-8-8688-0297-3_11

el Attar, A., Khatoun, R., & Lemercier, M. (2014). Clustering-based anomaly detection for smartphone applications. *IEEE/IFIP NOMS 2014 - IEEE/IFIP Network Operations and Management Symposium: Management in a Software Defined World*. https://doi.org/10.1109/NOMS.2014.6838385

Elbasheer, M. O., Aldegheishem, A., Alrajeh, N., & Lloret, J. (2022). Video Streaming Adaptive QoS Routing With Resource Reservation (VQoSRR) Model for SDN Networks. *Electronics*. https://doi.org/10.3390/electronics11081252

Eldardiry, H., Bart, E., Juan Liu, Hanley, J., Price, B., & Brdiczka, O. (2013). Multi-Domain Information Fusion for Insider Threat Detection. *2013 IEEE Security and Privacy Workshops*, 45–51. https://doi.org/10.1109/SPW.2013.14

Eliyan, L. F., & Di Pietro, R. (2021). DoS and DDoS attacks in Software Defined Networks: A survey of existing solutions and research challenges. *Future Generation Computer Systems*, *122*, 149–171. https://doi.org/10.1016/j.future.2021.03.011

ELSEVIER. (2022). *Scopus | La mayor base de datos de bibliografía revisada por pares*. https://www.elsevier.com/es-mx/solutions/scopus

Fink, A. (2005). *Conducting research literature reviews. From the Internet to Paper.* (Sage publications., Ed.).

Fortinet. (2024). *Intrusion Prevention | FortiGuard Labs*. https://www.fortiguard.com/encyclopedia/ips/43963/backdoor-doublepulsar

Gangadharan, M., & Hwang, K. (2001). Intranet security with micro-firewalls and mobile agents for proactive intrusion response. *Proceedings - 2001 International Conference on Computer Networks and Mobile Computing, ICCNMC 2001*, 325–332. https://doi.org/10.1109/ICCNMC.2001.962615

Garchery, M. (2020). *ADSAGE: Anomaly Detection in Sequences of Attributed Graph Edges Applied to Insider Threat Detection at Fine-Grained Level*. https://doi.org/10.48550/arxiv.2007.06985

Garg, S., Kaur, K., Kaddoum, G., Garigipati, P., & Aujla, G. S. (2021). Security in IoT-Driven Mobile Edge Computing: New Paradigms, Challenges, and Opportunities. *Ieee Network*. https://doi.org/10.1109/mnet.211.2000526

Georgiadou, A., Mouzakitis, S., Bounas, K., & Askounis, D. (2020). A Cyber-Security Culture Framework for Assessing Organization Readiness. In *Journal of Computer Information Systems*. https://doi.org/10.1080/08874417.2020.1845583

Ghafar, A. A., Kassim, M., Ya'acob, N., Mohamad, R., & Rahman, R. A. (2020). QoS of Wi-Fi Performance Based on Signal Strength and Channel for Indoor Campus Network. *Bulletin of Electrical Engineering and Informatics*, *9*(5), 2097–2108. https://doi.org/10.11591/eei.v9i5.2251

Ghani, I. (2013). Software security engineering in extreme programming methodology: a systematic literature review. *Science International (Lahore)*, *25*(2), 215–221.

Gheyas, I. A., & Abdallah, A. E. (2016). Detection and prediction of insider threats to cyber security: a systematic literature review and meta-analysis. *Big Data Analytics*, *1*(1), 6. https://doi.org/10.1186/s41044-016-0006-0

Giotis, K., Androulidakis, G., & Maglaris, V. (2014). Leveraging SDN for efficient anomaly detection and mitigation on legacy networks. *Proceedings - 2014 3rd European Workshop on Software-Defined Networks, EWSDN 2014*, 85–90. https://doi.org/10.1109/EWSDN.2014.24

GitHub. (2024). *GitHub - xmrig/xmrig: RandomX, KawPow, CryptoNight and GhostRider unified CPU/GPU miner and RandomX benchmark*. https://github.com/xmrig/xmrig

Gugelmann, D., Gasser, F., Ager, B., & Lenders, V. (2015). Hviz: HTTP(S) traffic aggregation and visualization for network forensics. *Digital Investigation*, *12*, S1–S11. https://doi.org/10.1016/J.DIIN.2015.01.005

Gujral, H., Sharma, A., Jain, P., Juneja, S., & Mittal, S. (2022). Design and Implementation of a Quantitative Network Health Monitoring and Recovery System. *Wireless Personal Communications*, *125*(1). https://doi.org/10.1007/S11277-022-09554-9

Gyawali, Y. P. (2023). A Modular Encryption Framework in Cloud and Mobile Environments for Cybersecurity Solutions in Health Information. *Rjcse*, *4*(1), 64–73. https://doi.org/10.52710/rjcse.64

Halim, H., & Yusof, M. Mohd. (2019). Framework for Digital Data Access Control From Internal Threat in the Public Sector. *International Journal of Advanced Computer Science and Applications*. https://doi.org/10.14569/ijacsa.2019.0100809

Hamad, D. J. (2023). Performance Assessment of QoS Metrics in Software Defined Networking Using Floodlight Controller. *Joiv International Journal on Informatics Visualization*. https://doi.org/10.30630/joiv.7.3.1288

He, L., Yu, S., & Li, M. (2008). Anomaly detection based on available bandwidth estimation. *Proceedings - 2008 IFIP International Conference on Network and Parallel Computing, NPC 2008*, 176–183. https://doi.org/10.1109/NPC.2008.85

He, S., Zhang, X., Jiang, Z., Kang, H., & Wang, H. (2011). TV monitor: A P2P-TV content monitoring platform. *Proceedings - 3rd International Conference on Multimedia Information Networking and Security, MINES 2011*, 371–375. https://doi.org/10.1109/MINES.2011.48

Herringshaw, C. (1997). Detecting Attacks on Networks. *Computer*, *30*(12), 16–17. https://doi.org/10.1109/2.642762

Herzog, P. (2010). OSSTMM 3: The Open Source Security Testing Methodology Manual. In *Isecom* (Vol. 3). https://www.isecom.org/OSSTMM.3.pdf

Hong, H., Lu, X. L., Ren, L. Y., & Chen, B. (2006). TAICHI: An open intrusion automatic response system based on plugin. *Proceedings of the 2006 International Conference on Machine Learning and Cybernetics*, *2006*, 66–77. https://doi.org/10.1109/ICMLC.2006.258818

Hori, Y., Nishide, T., & Sakurai, K. (2011). Towards countermeasure of insider threat in network security. *Proceedings - 3rd IEEE International Conference on Intelligent Networking and Collaborative Systems, INCoS 2011*, 634–636. https://doi.org/10.1109/INCoS.2011.156

Hou, B., Zhang, K., Zuo, X., Zhao, J., & Xi, B. (2022). PIoT Malicious Traffic Detection Method Based on GAN Sample Enhancement. *Security and Communication Networks*, *2022*. https://doi.org/10.1155/2022/9223412

Hsu, Y. F., He, Z. Y., Tarutani, Y., & Matsuoka, M. (2019). Toward an online network intrusion detection system based on ensemble learning. *IEEE International Conference on Cloud Computing, CLOUD*, *2019-July*, 174–178. https://doi.org/10.1109/CLOUD.2019.00037

Hsu, Y. F., & Matsuoka, M. (2020). A Deep Reinforcement Learning Approach for Anomaly Network Intrusion Detection System. *Proceedings - 2020 IEEE 9th International Conference on Cloud Networking, CloudNet 2020*. https://doi.org/10.1109/CLOUDNET51028.2020.9335796

Hu, R. (2011). Design and implementation of campus network intrusion detection system. *Proceedings - 2011 International Conference on Intelligence Science and Information Engineering, ISIE 2011*, 507–510. https://doi.org/10.1109/ISIE.2011.69

Hu, T., Niu, W., Zhang, X., Liu, X., Lu, J., & Liu, Y. (2019). An Insider Threat Detection Approach Based on Mouse Dynamics and Deep Learning. *Security and Communication Networks*, *2019*. https://doi.org/10.1155/2019/3898951

Huang, C., Xiong, J., & Peng, Z. (2012). Applied research on Snort intrusion detection model in the campus network. *Proceedings - 2012 IEEE Symposium on Robotics and Applications, ISRA 2012*, 596–599. https://doi.org/10.1109/ISRA.2012.6219259

Hussein, H. A. (2023). *Control Dynamic System and Qos Manager Agent Over Ipv6 Networks: Intserv and Diffserv Approach in Access Nodes*. https://doi.org/10.21203/rs.3.rs-2948805/v1

Hwang, K., Chen, Y., & Liu, H. (2005). Defending distributed systems against malicious intrusions and network anomalies. *Proceedings - 19th IEEE International Parallel and Distributed Processing Symposium, IPDPS 2005*, *2005*. https://doi.org/10.1109/IPDPS.2005.160

IEEE. (2022). *IEEE Xplore ®*.

Ikebe, M., Shimokawa, D., & Yoshida, K. (2016). Proposal of a Malicious Communication Control Method Using OpenFlow. *Proceedings - 2016 10th International Conference on Complex, Intelligent, and Software Intensive Systems, CISIS 2016*, 605–610. https://doi.org/10.1109/CISIS.2016.75

Imran, M., Durad, M. H., Khan, F. A., & Derhab, A. (2019). Toward an optimal solution against Denial of Service attacks in Software Defined Networks. *Future Generation Computer Systems*, *92*, 444–453. https://doi.org/10.1016/j.future.2018.09.022

Incibe. (n.d.). *Ramnit | INCIBE | INCIBE*. Retrieved September 17, 2024, from https://www.incibe.es/servicio-antibotnet/info/Ramnit

ISECOM. (2021). *RESEARCH*. https://www.isecom.org/research.html#content5-9d

Ismail, M. N., & Ismail, M. T. (2009). Framework of intrusion detection system via snort application on campus network environment. *Proceedings - 2009 International Conference on Future Computer and Communication, ICFCC 2009*, 455–459. https://doi.org/10.1109/ICFCC.2009.10

ITU. (2021). *Índice Mundial de Ciberseguridad 2020*. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-s.pdf

ITU. (2024). *Global Cybersecurity Index 2024 5th Edition*. https://www.itu.int/dms_pub/itu-d/opb/hdb/d-hdb-gci.01-2024-pdf-e.pdf

ITU-T. (2001). G.1010: End-user multimedia QoS categories. In *International Telecommunications Union*.

Jaw, E., & Wang, X. (2022). A Novel Hybrid-Based Approach of Snort Automatic Rule Generator and Security Event Correlation (SARG-SEC). In *Peerj Computer Science*. https://doi.org/10.7717/peerj-cs.900

Jenny, R. S., & Sugirtham, N. (2023). SDN-Based Security for Smart Devices Against Denial of Service Attacks. *Indian Journal Of Science And Technology*, *16*(3), 181–189. https://doi.org/10.17485/ijst/v16i3.1960

Jiang, N., Cao, J., Jin, Y., Li, L. E., & Zhang, Z. L. (2010). Identifying suspicious activities through DNS failure graph analysis. *Proceedings - International Conference on Network Protocols, ICNP*, 144–153. https://doi.org/10.1109/ICNP.2010.5762763

Jin, Q., & Wang, L. (2019). Intranet User-Level Security Traffic Management with Deep Reinforcement Learning. *Proceedings of the International Joint Conference on Neural Networks*, *2019-July*. https://doi.org/10.1109/IJCNN.2019.8852447

Kaliyamurthy, N. M., Taterh, S., Shanmugasundaram, S., Saxena, A., Cheikhrouhou, O., & Elhadj, H. Ben. (2021). Software-Defined Networking: An Evolving Network Architecture—Programmability and Security Perspective. *Security and Communication Networks*. https://doi.org/10.1155/2021/9971705

Kang, H. (2021). Sample size determination and power analysis using the G*Power software. *Journal of Educational Evaluation for Health Professions*, *18*, 1–12. https://doi.org/10.3352/JEEHP.2021.18.17

Karakus, M., & Durresi, A. (2017). Quality of Service (QoS) in Software Defined Networking (SDN): A survey. *Journal of Network and Computer Applications*, *80*(December 2016), 200–218. https://doi.org/10.1016/j.jnca.2016.12.019

kASPERSKY. (2024). *Trojan-Banker | Enciclopedia de Kaspersky*. https://encyclopedia.kaspersky.es/knowledge/trojan-banker/

Khafidin, A., Andrasto, T., & Suryono, S. (2019). Implementation Flow Control to Improve Quality of Service on Computer Networks. *Indonesian Journal of Electrical Engineering and Computer Science*, *16*(3), 1474. https://doi.org/10.11591/ijeecs.v16.i3.pp1474-1481

Khan, T., Alam, M., Akhunzada, A., Hur, A., Asif, M., & Khan, M. K. (2019). Towards augmented proactive cyberthreat intelligence. *Journal of Parallel and Distributed Computing*, *124*, 47–59. https://doi.org/10.1016/J.JPDC.2018.10.006

Khatri, D., Gautam, B., & Sato, K. (2023). *Review of Firewall Applications in Multi-Controller-Based Software-Defined Networks*. https://doi.org/10.62991/mmt1996363754

Kiflay, A., Tsokanos, A., Fazlali, M., & Kirner, R. (2024). Network intrusion detection leveraging multimodal features. *Array*, *22*, 100349. https://doi.org/https://doi.org/10.1016/j.array.2024.100349

Kim, I. S., & Kim, M. H. (2012). Agent-based honeynet framework for protecting servers in campus networks. *IET Information Security*, *6*(3), 202–211. https://doi.org/10.1049/IET-IFS.2011.0154/REFERENCES

Kim, J., Seo, M., Lee, S., Nam, J., Yegneswaran, V., Porras, P., Gu, G., & Shin, S. (2023). Enhancing security in SDN: Systematizing attacks and defenses from a penetration perspective. *Computer Networks*. https://doi.org/10.1016/j.comnet.2024.110203

Kitchenham, B. (2004). Procedures for Performing Systematic Reviews, Version 1.0. *Empirical Software Engineering*, *33*(2004), 1–26.

Kitchenham, B. (2007). Guidelines for performing systematic literature reviews in software engineering. *Technical Report, Ver. 2.3 EBSE Technical Report. EBSE*.

Kitchenham, B., & Charters, S. (2007). *Guidelines for performing Systematic Literature Reviews in Software Engineering*. https://doi.org/10.1145/1134285.1134500

Kont, M., Pihelgas, M., Wojtkowiak, J., Trinberg, L., & Osula, A.-M. (2015). *Insider threat detection study*. NATO Cooperative Cyber Defence Centre of Excellence.

Kul, G., Upadhyaya, S., & Hughes, A. (2017). Complexity of insider attacks to databases. *MIST 2017 - Proceedings of the 2017 International Workshop on Managing Insider Security Threats, Co-Located with CCS 2017*, *2017-January*, 25–32. https://doi.org/10.1145/3139923.3139927

Kul, G., Upadhyaya, S., & Hughes, A. (2020). An Analysis of Complexity of Insider Attacks to Databases. *ACM Transactions on Management Information Systems (TMIS)*, *12*(1). https://doi.org/10.1145/3391231

Kumar, B. K., Raj, N., Dhivvya, J. P., & Muralidharan, D. (2019). Fixing network security vulnerabilities in local area network. *Proceedings of the International Conference on Trends in Electronics and Informatics, ICOEI 2019*, *2019-April*, 1349–1354. https://doi.org/10.1109/ICOEI.2019.8862634

Kuo, C. T., Chang, V., & Lei, C. L. (2018). A feasibility analysis for edge computing fusion in LPWA IoT environment with SDN structure. *Proceedings of 2017 International Conference on Engineering and Technology, ICET 2017*, *2018-January*, 1–6. https://doi.org/10.1109/ICENGTECHNOL.2017.8308187

Kurose, J. F., Nyu, K. W. R., Shanghai, N., Columbus, B., New, I., San, Y., Hoboken, F., Cape, A., Dubai, T., Madrid, L., Munich, M., Montréal, P., Delhi, T., São, M. C., Sydney, P., Kong, H., Singapore, S., Tokyo, T., Manning, J., … Zaldivar-Garcia, M. (2017). *Computer Networking A Top-Down Approach Seventh Edition*. www.pearsoned.com/permissions/.

Kurt, Ç., & Ayhan Erdem, O. (2020). Real-time anomaly detection and mitigation using streaming telemetry in SDN. *Turkish Journal of Electrical Engineering and Computer Sciences*, *28*(5), 2448–2466. https://doi.org/10.3906/ELK-1909-112

Kussul, N., Shelestov, A., Sidorenko, A., Skakun, S., & Veremeenko, Y. (2003). Intelligent multi-agent information security system. *Proceedings of the 2nd IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2003*, 120–122. https://doi.org/10.1109/IDAACS.2003.1249530

Latah, M., & Toker, L. (2018). Artificial Intelligence Enabled Software Defined Networking: A Comprehensive Overview. *IET Networks*, *8*(2), 79–99. https://doi.org/10.1049/iet-net.2018.5082

Legg, P. A. (2015). Visualizing the insider threat: Challenges and tools for identifying malicious user activity. *2015 IEEE Symposium on Visualization for Cyber Security, VizSec 2015*. https://doi.org/10.1109/VIZSEC.2015.7312772

Legg, P. A., Buckley, O., Goldsmith, M., & Creese, S. (2017). Automated Insider Threat Detection System Using User and Role-Based Profile Assessment. *IEEE Systems Journal*, *11*(2), 503–512. https://doi.org/10.1109/JSYST.2015.2438442

Legg, P., Buckley, O., Legg, P. A., Buckley, O., Goldsmith, M., & Creese, S. (2015). Caught in the Act of an Insider Attack: Detection and Assessment of Insider Threat. *IEEE Symposium on Technologies for Homeland Security 2015, At Waltham, MA*, *October*, 1–6. https://doi.org/10.13140/RG.2.1.1420.6563

Li, H., & Chen, L. (2018). Research on computer communication network security and guarantee ways. *ACM International Conference Proceeding Series*, 105–109. https://doi.org/10.1145/3242840.3242874

Li, X., Sun, H., & Huang, Y. (2024). Efficient Flow Table Caching Architecture and Replacement Policy for SDN Switches. *Journal of Network and Systems Management*, *32*(3). https://doi.org/10.1007/s10922-024-09824-w

Li, X., Zhang, H., Miao, Y., Ma, S., Ma, J., Liu, X., & Choo, K. K. R. (2022). CAN Bus Messages Abnormal Detection Using Improved SVDD in Internet of Vehicles. *IEEE Internet of Things Journal*, *9*(5), 3359–3371. https://doi.org/10.1109/JIOT.2021.3098221

Lin, A. C., & Peterson, G. L. (2016). Activity Pattern Discovery from Network Captures. *Proceedings - 2016 IEEE Symposium on Security and Privacy Workshops, SPW 2016*, 334–342. https://doi.org/10.1109/SPW.2016.22

Lin, J., Liao, L., Wang, T., Zhang, J., & Cheng, L. (2020). SDCCP: Control the network using software-defined networking and end-to-end congestion control. *Concurrency Computation* . https://doi.org/10.1002/CPE.5716

Lin, W. C., Ke, S. W., & Tsai, C. F. (2015). CANN: An intrusion detection system based on combining cluster centers and nearest neighbors. *Knowledge-Based Systems*, *78*(1), 13–21. https://doi.org/10.1016/j.knosys.2015.01.009

Liu, C., Cao, Z., Xiong, G., Gou, G., Yiu, S. M., & He, L. (2019). MaMPF: Encrypted Traffic Classification Based on Multi-Attribute Markov Probability Fingerprints. *2018 IEEE/ACM 26th International Symposium on Quality of Service, IWQoS 2018*. https://doi.org/10.1109/IWQOS.2018.8624124

Liu, D., Zhang, C., & Lou, F. (2021). Terminal Security Protection Anomaly Detection Based on Combined Algorithm. *Proceedings - 2021 International Conference on Intelligent Computing, Automation and Applications, ICAA 2021*, 135–139. https://doi.org/10.1109/ICAA53760.2021.00032

Liu, F., Jiang, X., Wen, Y., Xing, X., Zhang, D., & Meng, D. (2019). Log2vec: A heterogeneous graph embedding based approach for detecting cyber threats within enterprise. *Proceedings of the ACM Conference on Computer and Communications Security*, 1777–1794. https://doi.org/10.1145/3319535.3363224

Liu, L., Shi, J., Zhang, H., & Yu, X. (2019). No way to evade: Detecting multi-path routing attacks for NIDS. *2019 IEEE Global Communications Conference, GLOBECOM 2019 - Proceedings*. https://doi.org/10.1109/GLOBECOM38437.2019.9013952

Liu, M., Xue, Z., Xu, X., Zhong, C., & Chen, J. (2018). Host-Based Intrusion Detection System with System Calls. *ACM Computing Surveys (CSUR)*, *51*(5). https://doi.org/10.1145/3214304

Liu, Z., Guan, X., Li, S., Qin, T., & He, C. (2018). Behavior rhythm: A new model for behavior visualization and its application in system security management. *IEEE Access*, *6*, 73940–73951. https://doi.org/10.1109/ACCESS.2018.2882812

Liu, Z., Qin, T., Guan, X., Jiang, H., & Wang, C. (2018). An integrated method for anomaly detection from massive system logs. *IEEE Access*, *6*, 30602–30611. https://doi.org/10.1109/ACCESS.2018.2843336

Ludeña Romaña, D. A., Takemori, K., Kubota, S., Sugitani, K., & Musashi, Y. (2009). Towards the design of hardware based security device and communication implementation. *ICINIS 2009 - Proceedings of the 2nd International Conference on Intelligent Networks and Intelligent Systems*, 250–252. https://doi.org/10.1109/ICINIS.2009.70

Lv, Z., Qiao, L., Kumar Singh, A., & Wang, Q. (2021). AI-empowered IoT Security for Smart Cities. *ACM Transactions on Internet Technology*, *21*(4). https://doi.org/10.1145/3406115

Mahajan, A., Ramotra, A. K., Mansotra, V., & Singh, M. (2020). An Automated Framework to Uncover Malicious Traffic for University Campus Network. *Smart Innovation, Systems and Technologies*, *165*, 99–108. https://doi.org/10.1007/978-981-15-0077-0_11/COVER

Mahat, D., Neupane, D., & Shrestha, S. (2024). Quantitative Research Design and Sample Trends: A Systematic Examination of Emerging Paradigms and Best Practices. *Cognizance Journal of Multidisciplinary Studies*, *4*(2), 20–27. https://doi.org/10.47760/cognizance.2024.v04i02.002

Manggalanny, M. S., & Ramli, K. (2017). Real time DNS traffic profiling enhanced detection design for national level network. *2017 International Seminar on Intelligent Technology and Its Application: Strengthening the Link Between University Research and Industry to Support ASEAN Energy Sector, ISITIA 2017 - Proceeding*, *2017-January*, 11–15. https://doi.org/10.1109/ISITIA.2017.8124046

Marchand-Niño, W.-R., & Vargas-Malca, Y.-V. (2023). Pretexting and the Information Security Culture. Case of a University of the Peruvian Amazon. *2023 XLIX Latin American Computer Conference (CLEI)*, 1–8. https://doi.org/10.1109/CLEI60451.2023.10346160

Marquis, Y. A. (2024). From Theory to Practice: Implementing Effective Role-Based Access Control Strategies to Mitigate Insider Risks in Diverse Organizational Contexts. *Journal of Engineering Research and Reports*. https://doi.org/10.9734/jerr/2024/v26i51141

Merayo, N., Pintos, D. de, Aguado Manzano, J. C., Miguel, I. de, Durán Barroso, R. J., Reguero, P. F., Lorenzo Toledo, R. M., & Abril, E. J. (2021). An Experimental OpenFlow Proposal Over Legacy GPONs to Allow Real-Time Service Reconfiguration Policies. *Applied Sciences*. https://doi.org/10.3390/app11030903

Meucci, M., & Muller, A. (2014). 4.0 Testing Guide. *OWASP Foundation*, *Cc*, 224. https://www.owasp.org/images/1/19/OTGv4.pdf

Mhamdi, L., & Isa, M. M. (2024). Securing SDN: Hybrid autoencoder-random forest for intrusion detection and attack mitigation. *Journal of Network and Computer*

Applications, *225*, 103868. https://doi.org/https://doi.org/10.1016/j.jnca.2024.103868

Microsoft. (2014). *Trojan: Win32 / CoinMiner*. https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Trojan:Win32/CoinMiner

Microsoft. (2017). *Microsoft Security Bulletin MS17-007 - Critical | Microsoft L*. Microsoft. https://learn.microsoft.com/en-us/security-updates/SecurityBulletins/2017/ms17-007?redirectedfrom=MSDN

Microsoft. (2020). *CVE-2018-8298 | .NET Framework Information Disclosure Vulnerability*. Microsoft Security Response Center. https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2018-8298

Mogos, G. (2020). Security Risk Management Plan. Student Portal-Case Study. *ACM International Conference Proceeding Series*, 113 – 119. https://doi.org/10.1145/3399871.3399872

Mohammad Al-Fawa'reh. (2021). Detecting Malicious DNS Queries Over Encrypted Tunnels Using Statistical Analysis and Bi-Directional Recurrent Neural Networks. *Karbala International Journal of Modern Science*, *7*(4), 268–280. https://www.iasj.net/iasj/article/221435

Mohammed, S. H., & Jasim, A. D. (2020). Evaluation of Firewall and Load Balance in Fat-Tree Topology Based on Floodlight Controller. In *Indonesian Journal of Electrical Engineering and Computer Science*. https://doi.org/10.11591/ijeecs.v17.i3.pp1157-1164

Mohapatra, M. (2023). Generative Adversarial Network Based Approach Towards Synthetically Generating Insider Threat Scenarios. *Journal of Software Engineering and Applications*. https://doi.org/10.4236/jsea.2023.1611030

Moneva, A., & Leukfeldt, R. (2023). Insider Threats Among Dutch SMEs: Nature and Extent of Incidents, and Cyber Security Measures. *Journal of Criminology*. https://doi.org/10.1177/26338076231161842

Montano, I. H., García Aranda, J. J., Diaz, J. R., Cardin, S. M., la Díez, I. de, & P. Rodrigues, J. J. (2022). Survey of Techniques on Data Leakage Protection and Methods to Address the Insider Threat. *Cluster Computing*. https://doi.org/10.1007/s10586-022-03668-2

Muhie, Y. A., Wolde, A. B., Tesfay, C. H., & Bedada, B. A. (2020). Improving Quality of Education by Evaluating the Capacity of Lecturers Using a Web Based System. In *Journal of Software Engineering and Applications*. https://doi.org/10.4236/jsea.2020.1310019

Musashi, Y., Hequet, F., Ludeña Romaña, D. A., Kubota, S., & Sugitani, K. (2010). Detection of host search activity in PTR resource record based DNS query packet traffic. *2010 IEEE International Conference on Information and Automation, ICIA 2010*, 1284–1288. https://doi.org/10.1109/ICINFA.2010.5512116

Myers, J., Grimaila, M. R., & Mills, R. F. (2009). Towards insider threat detection using web server logs. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/1558607.1558670

Nanda, S., Zafari, F., Decusatis, C., Wedaa, E., & Yang, B. (2016). *Predicting Network Attack Patterns in SDN using Machine Learning Approach*. https://doi.org/10.1109/NFV-SDN.2016.7919493

Nisha, T. N., & Pramod, D. (2024). Insider Intrusion Detection Techniques: A State-of-the-Art Review. *Journal of Computer Information Systems*, *64*(1), 106 – 123. https://doi.org/10.1080/08874417.2023.2175337

Nithiyanandam, C., Tamilselvan, D., Balaji, S., & Sivaguru, V. (2012). Advanced framework of defense system for prevetion of insider's malicious behaviors. *International Conference on Recent Trends in Information Technology, ICRTIT 2012*, 434–438. https://doi.org/10.1109/ICRTIT.2012.6206788

Nuha, A. A., Kuswanto, H., Apriani, E., & Hapsari, W. P. (2021). *Learning Physics With Worksheet Assisted Augmented Reality: The Impacts on Student's Verbal Representation*. https://doi.org/10.2991/assehr.k.210326.066

Obasi, S. C., Solomon, N. O., Adenekan, O. A., & Simpa, P. (2024). Cybersecurity's role in environmental protection and sustainable development: bridging technology and sustainability goals. *Computer Science &Amp; IT Research Journal*, *5*(5), 1145–1177. https://doi.org/10.51594/csitrj.v5i5.1140

OffSec Services Limited. (2025). *Kali Linux Tools*. https://www.kali.org/tools/slowhttptest/

Oktian, Y. E., Witanto, E. N., & Lee, S.-G. (2021). A Conceptual Architecture in Decentralizing Computing, Storage, and Networking Aspect of IoT Infrastructure. *Iot*. https://doi.org/10.3390/iot2020011

Olulowo, T. G., Ige, O. A., & Ugwoke, E. O. (2020). Using Peer Tutoring to Improve Students' Academic Achievement in Financial Accounting Concepts. In *Education Research International*. https://doi.org/10.1155/2020/8871235

Ometov, A., Molua, O. L., Komarov, M., & Nurmi, J. (2022). A Survey of Security in Cloud, Edge, and Fog Computing. *Sensors*. https://doi.org/10.3390/s22030927

Ongun, T., Spohngellert, O., Miller, B., Boboila, S., Oprea, A., Eliassi-Rad, T., Hiser, J., Nottingham, A., Davidson, J., & Veeraraghavan, M. (2021). PORTFILER: Port-Level Network Profiling for Self-Propagating Malware Detection. *2021 IEEE Conference on Communications and Network Security, CNS 2021*, 182–190. https://doi.org/10.48550/arxiv.2112.13798

Ou, X., Rajagopalan, S. R., & Sakthivelmurugan, S. (2009). An empirical approach to modeling uncertainty in intrusion analysis. *Proceedings - Annual Computer Security Applications Conference, ACSAC*, 494–503. https://doi.org/10.1109/ACSAC.2009.53

OWASP Foundation. (2022). *OWASP Web Security Testing Guide | OWASP Foundation*. https://owasp.org/www-project-web-security-testing-guide/

Pak, C. (2008). The near real time statistical asset priority driven (NRTSAPD) risk assessment methodology. *SIGITE'08: Proceedings of the 9th ACM SIG-Information Technology Education Conference*, 105–112. https://doi.org/10.1145/1414558.1414590

Pak, C., & Cannady, J. (2009). Asset priority risk assessment using hidden Markov models. *SIGITE'09 - Proceedings of the 2009 ACM Special Interest Group for Information Technology Education*, 65–73. https://doi.org/10.1145/1631728.1631750

Park, H., Kim, M., & Kang, C. H. (2009). F-TAD: Traffic anomaly detection for sub-networks using Fisher linear discriminant. *NSS 2009 - Network and System Security*, 328–335. https://doi.org/10.1109/NSS.2009.60

Patel, A., Ghaghda, S., & Nagecha, P. (2014). Model for security in wired and wireless network for education. *2014 International Conference on Computing for Sustainable Global Development, INDIACom 2014*, 699–704. https://doi.org/10.1109/INDIACOM.2014.6828051

Paul, S., & Mishra, S. (2020). LAC: LSTM AUTOENCODER with community for insider threat detection. *ACM International Conference Proceeding Series*, 71–77. https://doi.org/10.1145/3445945.3445958

Petticrew, M., & Roberts, H. (2008). Systematic Reviews in the Social Sciences: A Practical Guide. In *Systematic Reviews in the Social Sciences: A Practical Guide*. https://doi.org/10.1002/9780470754887

Pisarčík, P., & Sokol, P. (2014). Framework for distributed virtual honeynets. *ACM International Conference Proceeding Series*, *2014-September*, 324–329. https://doi.org/10.1145/2659651.2659685

Pliatsios, D., Sarigiannidis, P., Lagkas, T., & Sarigiannidis, A. G. (2020). A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics. *IEEE Communications Surveys and Tutorials*, *22*(3), 1942–1976. https://doi.org/10.1109/COMST.2020.2987688

Poddar, R., & Babu, H. (2022). Decision Tree Based IoT Attack Detection in Programmable Data Plane Using P4 Language. *Lecture Notes in Networks and Systems*, *450 LNNS*, 671–683. https://doi.org/10.1007/978-3-030-99587-4_57/COVER

Política de Ciberseguridad, 1 Registro Oficial 7 (2021).

Po-Wen, C., Chien-Ting, K., H, R., Shih-Jen, C., & C. Lei. (2014). An AMI Threat Detection Mechanism Based on SDN Networks. *SECURWARE 2014 - 8th International Conference on Emerging Security Information, Systems and Technologies*. https://www.semanticscholar.org/paper/An-AMI-Threat-Detection-Mechanism-Based-on-SDN-Chi-Kuo/0fc87f77900b168ad6599e5bd623f84637505a82

Praptodiyono, S., Sofhan, R., Pramudyo, A. S., Firmansyah, T., & Osman, A. (2019). Performance comparison of transmitting jumbo frame on Windows and Linux system. *Telkomnika (Telecommunication Computing Electronics and Control)*, *17*(1), 68 – 75. https://doi.org/10.12928/TELKOMNIKA.v17i1.11627

Putri, R. A. R. Q. Y. (2024). Analysis of 5G Network Quality of Service on VoIP Application. *International Journal of Electrical Energy and Power System Engineering*, *7*(1), 37–45. https://doi.org/10.31258/ijeepse.7.1.37-45

Qin, Q., Poularakis, K., & Tassiulas, L. (2020). A learning approach with programmable data plane towards IoT security. *Proceedings - International Conference on Distributed*

Computing Systems, *2020-November*, 410–420. https://doi.org/10.1109/ICDCS47774.2020.00064

Qin, T., He, C., Jiang, H., & Chen, R. (2018). Behavior rhythm: An effective model for massive logs characterizing and security monitoring in cloud. *2018 IEEE Conference on Communications and Network Security, CNS 2018*. https://doi.org/10.1109/CNS.2018.8433138

Raimundo, R., & Rosário, A. (2021). The impact of artificial intelligence on data system security: A literature review. *Sensors*, *21*(21). https://doi.org/10.3390/S21217029

Rapid7. (2020). *Accelerate Security, Vuln Management, Compliance*. https://www.rapid7.com/

Rashid, A., Siddique, M. J., & Ahmed, S. M. (2020). Machine and Deep Learning Based Comparative Analysis Using Hybrid Approaches for Intrusion Detection System. *3rd International Conference on Advancements in Computational Sciences, ICACS 2020*. https://doi.org/10.1109/ICACS47775.2020.9055946

Rattanalerdnusorn, E., Pattaranantakul, M., Thaenkaew, P., & Vorakulpipat, C. (2020). IoTDePT: Detecting Security Threats and Pinpointing Anomalies in an IoT environment. *ACM International Conference Proceeding Series*, 232–236. https://doi.org/10.1145/3384544.3384579

Rawat, D. B., & Reddy, S. R. (2017). Software Defined Networking Architecture, Security and Energy Efficiency: A Survey. *IEEE Communications Surveys and Tutorials*, *19*(1), 325–346. https://doi.org/10.1109/COMST.2016.2618874

Ren, X., & Wang, L. (2020). A hybrid intelligent system for insider threat detection using iterative attention. *ACM International Conference Proceeding Series*, 189–194. https://doi.org/10.1145/3379247.3379251

Rice, C., & Searle, R. (2022). 'The Enabling Role of Internal Organizational Communication in Insider Threat Activity – Evidence From a High Security Organization.' *Management Communication Quarterly*. https://doi.org/10.1177/08933189211062250

Rincy N, T., & Gupta, R. (2021). Design and Development of an Efficient Network Intrusion Detection System Using Machine Learning Techniques. *Wireless Communications and Mobile Computing*, *2021*(1), 9974270. https://doi.org/https://doi.org/10.1155/2021/9974270

Ring, M., Wunderlich, S., Scheuring, D., Landes, D., & Hotho, A. (2019). A Survey of Network-based Intrusion Detection Data Sets. *Computers and Security*, *86*, 147–167. https://doi.org/10.1016/j.cose.2019.06.005

Roy, K. C., & Chen, G. (2024). GraphCH: A Deep Framework for Assessing Cyber-Human Aspects in Insider Threat Detection. *IEEE Transactions on Dependable and Secure Computing*, 1–15. https://doi.org/10.1109/TDSC.2024.3353929

Sadasivam, K., Samudrala, B., & Yang, T. A. (2004). Design of network security projects using honeypots | Journal of Computing Sciences in Colleges. *Journal of Computing Sciences in Colleges*, *20*(4), 282–293. https://dl.acm.org/doi/abs/10.5555/1047846.1047890

Salim, E. al. A. S. (2023). Software-Defined Networking-Based Campus Networks via Deep Reinforcement Learning Algorithms: The Case of University of Technology. *International Journal on Recent and Innovation Trends in Computing and Communication*, *11*(10), 1630–1654. https://doi.org/10.17762/ijritcc.v11i10.8726

Salti, I. Al, & Zhang, N. (2023). An Effective, Efficient and Scalable Link Discovery (EESLD) Framework for Hybrid Multi-Controller SDN Networks. In *Ieee Access*. https://doi.org/10.1109/access.2023.3339381

Sampath, N., Sadhasivam, J., Jayavel, S., Chindarmony, N. S., & Sharma, S. (2020). Intrusion detection in software defined networking using snort and mirroring. *International Journal of Engineering Trends and Technology*, *68*(4), 66–74. https://doi.org/10.14445/22315381/IJETT-V68I4P212S

Samtani, S., Kantarcioglu, M., & Chen, H. (2020). Trailblazing the Artificial Intelligence for Cybersecurity Discipline. *ACM Transactions on Management Information Systems (TMIS)*, *11*(4), 17. https://doi.org/10.1145/3430360

Sandhu, K. (2021). Handbook of research on advancing cybersecurity for digital transformation. *Handbook of Research on Advancing Cybersecurity for Digital Transformation*, 1–460. https://doi.org/10.4018/978-1-7998-6975-7

Sarker, I. H. (2024). Introduction to AI-Driven Cybersecurity and Threat Intelligence. In *AI-Driven Cybersecurity and Threat Intelligence: Cyber Automation, Intelligent Decision-Making and Explainability* (pp. 3–19). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-54497-2_1

Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: an overview from machine learning perspective. *Journal of Big Data*, *7*(1), 1–29. https://doi.org/10.1186/S40537-020-00318-5/FIGURES/3

Sathya, R., & Thangarajan, R. (2015). Efficient anomaly detection and mitigation in software defined networking environment. *2nd International Conference on Electronics and Communication Systems, ICECS 2015*, 479–484. https://doi.org/10.1109/ECS.2015.7124952

Scarfone, K., Souppaya, M., Cody, A., & Orebaugh, A. (2008). Technical Guide to Information Security Testing and Assessment (NIST SP 800-115). In *Nist Special Publication* (Vol. 800). http://books.google.com/books?hl=en&lr=&id=EHrf6q7GobUC&oi=fnd&pg=PR7&dq=Technical+Guide+to+Information+Security+Testing+and+Assessment+Recommendations+of+the+National+Institute+of+Standards+and+Technology&ots=FTcnroLXL8&sig=DE

Scarfone, Karen; Souppaya, Murugiah; Cody, Amanda; Orebaugh, Angela. (2020). Technical Guide to Information Security Testing and Assessment Recommendations of the National Institute of Standards and Technology. In *Nist Special Publication* (Vol. 800).

Schwegman Lundberg & Woessner, P. A. (2019). *Protecting & Handling Confidential Information – Topics*. https://www.slwip.com/resources/protecting-handling-confidential-information/#protecting-company-confidential-information

Segura, G. A. N., Chorti, A., & Margi, C. B. (2021). *Distributed DoS Attack Detection in SDN: Trade Offs in Resource Constrained Wireless Networks*. https://doi.org/10.48550/arxiv.2103.13705

Seo, S., & Kim, D.-H. (2020). Study on Inside Threats Based on Analytic Hierarchy Process. *Symmetry*. https://doi.org/10.3390/sym12081255

Serag, R. H., Abdalzaher, M. S., Elsayed, H. A. E. A., Sobh, M., Krichen, M., & Salim, M. M. (2024). Machine-Learning-Based Traffic Classification in Software-Defined Networks. *Electronics (Switzerland)*, *13*(6). https://doi.org/10.3390/electronics13061108

Shah, S., & Pramod Bendale, S. (2019). An Intuitive Study: Intrusion Detection Systems and Anomalies, How AI can be used as a tool to enable the majority, in 5G era. *Proceedings - 2019 5th International Conference on Computing, Communication Control and Automation, ICCUBEA 2019*. https://doi.org/10.1109/ICCUBEA47591.2019.9128786

Shan, Q. (2022). *Wireless network intrusion detection model and safety enhancement framework for campus network*. 349–353. https://doi.org/10.1109/ICSSIT53264.2022.9716257

Sharma, S., & Nag, A. (2023). Cognitive Software Defined Networking and Network Function Virtualization and Applications. In *Future Internet*. https://doi.org/10.3390/fi15020078

Shimoda, A., Mori, T., & Goto, S. (2010). Sensor in the dark: Building untraceable large-scale honeypots using virtualization technologies. *Proceedings - 2010 10th Annual International Symposium on Applications and the Internet, SAINT 2010*, 22–30. https://doi.org/10.1109/SAINT.2010.42

Silva, J. (2021). Software-Defined Network Technology for Learning in Research and Education Groups. In *Revista Innova Educación*. https://doi.org/10.35622/j.rie.2021.03.005.en

Silva, M., Gomes, M. O., Dias, V., Oliveira, L. B., Farias, F. N. N., & Abelém, A. (2023). *Redes Definidas Por Software Para a Orquestração De Diferentes Domínios Tecnológicos*. https://doi.org/10.5753/wpeif.2023.753

Singh, A., Satapathy, S. C., Roy, A., & Gutub, A. (2022). AI-Based Mobile Edge Computing for IoT: Applications, Challenges, and Future Scope. *Arabian Journal for Science and Engineering 2021 47:8*, *47*(8), 9801–9831. https://doi.org/10.1007/S13369-021-06348-2

Singh, J., & Behal, S. (2020). Detection and mitigation of DDoS attacks in SDN: A comprehensive review, research challenges and future directions. *Computer Science Review*, *37*, 100279. https://doi.org/10.1016/J.COSREV.2020.100279

Siva, P., Sudhish, C., Divyanand, O., & Sai Ananya Madhuri, K. (2023). Routenet: Using Graph Neural Networks for SDN Network Modeling and Optimizations. In *International Journal of Computer Engineering in Research Trends*. https://doi.org/10.22362/ijcert/2023/v10/i07/v10i0705

SNORT. (2024). *Snort - Rule Docs*. https://www.snort.org/rule_docs/1-23605

SNORT COMMUNITY. (2022). *How to install Snort on CentOS - UpCloud*. https://upcloud.com/resources/tutorials/installing-snort-on-centos

Software Engineering Institute. (2022). *Common Sense Guide to Mitigating Insider Threats, Seventh Edition*. https://insights.sei.cmu.edu/library/common-sense-guide-to-mitigating-insider-threats-seventh-edition/

Stallings, W. (2004). Comunicaciones y Redes de Computadores. *Prentice Hall*, 896. http://www.unav.es/SI/manuales/Redes_Internet/indice.html

Stallings, W., Agboma, F., & Jelassi, S. T. A.-T. T.-. (2016). Foundations of modern networking : SDN, NFV, QoE, IoT, and Cloud. In *Network* (Vol. 139, Issue 3). PEARSON.

Staples, M., & Niazi, M. (2007). Experiences using systematic review guidelines. *Journal of Systems and Software*, *80*(9), 1425–1437. https://doi.org/10.1016/j.jss.2006.09.046

Stiawan, D., Idris, M. Y., & Abdullah, A. H. (2015). Penetration testing and network auditing: Linux. *Journal of Information Processing Systems*, *11*(1), 104–115. https://doi.org/10.3745/JIPS.03.0013

Suomalainen, J., Julku, J., Heikkinen, A., Rantala, S. J., & Yastrebova, A. (2022). Security-driven prioritization for tactical mobile networks. *Journal of Information Security and Applications*, *67*(May), 103198. https://doi.org/10.1016/j.jisa.2022.103198

Takemori, K., Ludeña Romaña, D. A., Kubota, S., Sugitani, K., & Musashi, Y. (2009). Detection of NS resource record based DNS query request packet traffic and SSH dictionary attack activity. *ICINIS 2009 - Proceedings of the 2nd International Conference on Intelligent Networks and Intelligent Systems*, 246–249. https://doi.org/10.1109/ICINIS.2009.69

Tanenbaum, A., & Wetherall, D. (2012). Redes de computadoras. In *Redes de computadoras* (Quinta Edi). Pearson Education, Inc. https://doi.org/10.17993/ingytec.2018.32

Tang, D., Zheng, Z., Wang, X., Xiao, S., & Yang, Q. (2023). PeakSAX: Real-Time Monitoring and Mitigation System for LDoS Attack in SDN. *IEEE Transactions on Network and Service Management*, *20*(3), 3686–3698. https://doi.org/10.1109/TNSM.2022.3222846

Tantar, E., Tantar, A. A., Kantor, M., & Engel, T. (2018). On Using Cognition for Anomaly Detection in SDN. *Advances in Intelligent Systems and Computing*, *674*, 67–81. https://doi.org/10.1007/978-3-319-69710-9_5/COVER

Tao, J., Zheng, N., Wang, W., Han, T., Zhan, X., & Luan, Q. (2019). A Behavior Sequence Clustering-Based Enterprise Network Anomaly Host Recognition Method. *2019 IEEE International Conference on Big Knowledge (ICBK)*, 236–241. https://doi.org/10.1109/ICBK.2019.00039

Tarantino, L., Angelucci, D., Bonomo, A., Cardinali, A., & Paolo, S. Di. (2021). Design and Applications of GLANCE: GLanceable Alarm Notification for a User Centered Experience. *Applied Sciences*, *11*(2), 669. https://doi.org/10.3390/app11020669

Thatte, G., Mitra, U., & Heidemann, J. (2011). Parametric methods for anomaly detection in aggregate traffic. *IEEE/ACM Transactions on Networking*, *19*(2), 512–525. https://doi.org/10.1109/TNET.2010.2070845

Thompson, H. H., & Ford, R. (2004). The Insider, Naivety, and Hostility: Security Perfect Storm? *Queue*, *2*(4), 58–65. https://doi.org/10.1145/1016978.1016983

Thuraisingham, B., Nimon, K., & Khan, L. (2024). An Education Program for Big Data Security and Privacy. *2024 IEEE 10th Conference on Big Data Security on Cloud (BigDataSecurity)*, 1–4. https://doi.org/10.1109/BigDataSecurity62737.2024.00009

Tian, G., Wang, Z., Yin, X., Li, Z., Shi, X., Lu, Z., Zhou, C., Yu, Y., & Guo, Y. (2016). Mining network traffic anomaly based on adjustable piecewise entropy. *2015 IEEE 23rd International Symposium on Quality of Service, IWQoS 2015*, 299–308. https://doi.org/10.1109/IWQOS.2015.7404749

Tian, Z., Shi, W., Tan, Z., Qiu, J., Sun, Y., Jiang, F., & Liu, Y. (2020). Deep Learning and Dempster-Shafer Theory Based Insider Threat Detection. *Mobile Networks and Applications*. https://doi.org/10.1007/s11036-020-01656-7

Toainga, D., & Peña, D. (2019). *"ANÁLISIS DE VULNERABILIDADES INSIDER CONTRA ATAQUES DE DENEGACIÓN DE SERVICIO (DoS) EN REDES DEFINIDAS POR SOFTWARE."* Escuela Superior Politécnica de Chimborazo.

Toprak, C., Turker, C., & Erman, A. T. (2018). Detection of DHCP Starvation Attacks in Software Defined Networks: A Case Study. *UBMK 2018 - 3rd International Conference on Computer Science and Engineering*, 636–641. https://doi.org/10.1109/UBMK.2018.8566268

Toro, M. de, Borrego, C., & Robles, S. (2022). A Controller-Driven Approach for Opportunistic Networking. In *Applied Sciences*. https://doi.org/10.3390/app122312479

Trio Pramono, Y. W., & Suhardi. (2015). Anomaly-based intrusion detection and prevention system on website usage using rule-growth sequential pattern analysis: Case study: Statistics of Indonesia (BPS) website. *Proceedings - 2014 International Conference on Advanced Informatics: Concept, Theory and Application, ICAICTA 2014*, 203–208. https://doi.org/10.1109/ICAICTA.2014.7005941

Ullah, F., Edwards, M., Ramdhany, R., Chitchyan, R., Babar, M. A., & Rashid, A. (2018). Data exfiltration: A review of external attack vectors and countermeasures. *Journal of Network and Computer Applications*, *101*, 18–54. https://doi.org/10.1016/J.JNCA.2017.10.016

Väisänen, T. (2017). Categorization of cyber security deception events for measuring the severity level of advanced targeted breaches. *ACM International Conference Proceeding Series*, *Part F130530*, 125–131. https://doi.org/10.1145/3129790.3129805

Vinchurkar, D. P., & Reshamwala, A. (2012). A Review of Intrusion Detection System Using Neural Network and Machine Learning Technique. *International Journal of Engineering Science and Innovative Technology (IJESIT)*, *1*(2), 54–63.

VirusTotal. (2006). *VirusTotal - File - c6828c8bcce6786b39427fc5ad9df2f8163d3b8a7b3b5f8a5c5790c4488039f7*. https://www.virustotal.com/gui/file/c6828c8bcce6786b39427fc5ad9df2f8163d3b8a7b3b5f8a5c5790c4488039f7/details

VSAntivirus. (2005). *Troj/Dialer.InstantAccess. Adware y discador*. http://www.vsantivirus.com/troj-instantaccess.htm

Wallace, N., & Atkison, T. (2013). Observing industrial control system attacks launched via Metasploit Framework. *Proceedings of the Annual Southeast Conference*. https://doi.org/10.1145/2498328.2500067

Wang, B., Li, F., & Zhang, S. (2009). Research on intrusion detection based on campus network. *3rd International Symposium on Intelligent Information Technology Application, IITA 2009*, *1*, 468–471. https://doi.org/10.1109/IITA.2009.280

Wang, D., Zhao, Y., Zhi, H., Wu, D., Zhuo, W., Lu, Y., & Zhang, X. (2023). DoSDefender: A Kernel-Mode TCP DoS Prevention in Software-Defined Networking. *Sensors*, *23*(12). https://doi.org/10.3390/s23125426

Wang, J., Wang, L., & Wang, R. (2023). A Method of DDoS Attack Detection and Mitigation for the Comprehensive Coordinated Protection of SDN Controllers. *Entropy*, *25*(8). https://doi.org/10.3390/e25081210

Wang, S., Balarezo, J. F., Kandeepan, S., Al-Hourani, A., Chavez, K. G., & Rubinstein, B. (2021). Machine learning in network anomaly detection: A survey. *IEEE Access*, *9*, 152379–152396. https://doi.org/10.1109/ACCESS.2021.3126834

Wen, Y., Chen, X., Zeng, X., & Wang, W. (2020). Analysis of E-mail Account Probing Attack Based on Graph Mining. *Scientific Reports 2020 10:1*, *10*(1), 1–11. https://doi.org/10.1038/s41598-020-63191-5

Wijaya, I. G. A. S. P., Sasmita, G. M. A., & Pratama, I. P. A. E. (2024). Web Application Penetration Testing on Udayana University's OASE E-learning Platform Using Information System Security Assessment Framework (ISSAF) and Open Source Security Testing Methodology Manual (OSSTMM). *International Journal of Information Technology and Computer Science*, *16*(2), 45 – 56. https://doi.org/10.5815/ijitcs.2024.02.04

Wu, Z., Xiao, D., Xu, H., Peng, X., & Zhuang, X. (2009). Virtual inline: A technique of combining IDS and IPS together in response intrusion. *Proceedings of the 1st International Workshop on Education Technology and Computer Science, ETCS 2009*, *1*, 1118–1121. https://doi.org/10.1109/ETCS.2009.255

Xie, J., Richard Yu, F., Huang, T., Xie, R., Liu, J., Wang, C., & Liu, Y. (2019). A survey of machine learning techniques applied to software defined networking (SDN): Research issues and challenges. *IEEE Communications Surveys and Tutorials*, *21*(1), 393–430. https://doi.org/10.1109/COMST.2018.2866942

Yaacoub, J. P. A., Fernandez, J. H., Noura, H. N., & Chehab, A. (2021). Security of Power Line Communication systems: Issues, limitations and existing solutions. *Computer Science Review*, *39*, 100331. https://doi.org/10.1016/J.COSREV.2020.100331

Yasami, Y., Farahmand, M., & Zargari, V. (2007). An ARP-based anomaly detection algorithm using hidden Markov model in enterprise networks. *Second International Conference on Systems and Networks Communications, ICSNC 2007*, 69–75. https://doi.org/10.1109/ICSNC.2007.15

Yeh, C. H., & Yang, C. H. (2008). Design and implementation of honeypot systems based on open-source software. *IEEE International Conference on Intelligence and Security Informatics, 2008, IEEE ISI 2008*, 265–266. https://doi.org/10.1109/ISI.2008.4565077

Yilmaz, E. (2024). Unveiling Shadows: Harnessing Artificial Intelligence for Insider Threat Detection. *Engineering Technology \& Applied Science Research*. https://doi.org/10.48084/etasr.6911

Yuan, B., Zhang, C., Ren, J., Chen, Q., Xu, B., Zhang, Q., Li, Z., Zou, D., Zhang, F., & Jin, H. (2024). Toward Automated Attack Discovery in SDN Controllers Through Formal Verification. In *Ieee Transactions on Network and Service Management*. https://doi.org/10.1109/tnsm.2024.3386404

Yungaicela-Naula, N. M., Vargas-Rosales, C., Pérez-Díaz, J. A., & Zareei, M. (2022). Towards security automation in Software Defined Networks. *Computer Communications*, *183*, 64–82. https://doi.org/10.1016/J.COMCOM.2021.11.014

Zhang, D., & Wang, S. (2019). Optimization of traditional Snort intrusion detection system. *IOP Conference Series: Materials Science and Engineering*, *569*(4), 042041. https://doi.org/10.1088/1757-899X/569/4/042041

Zhang, H., Pan, G., Xu, S., Zhang, S., & Jiang, Z. (2022). *A Hard and Soft Hybrid Slicing Framework for Service Level Agreement Guarantee via Deep Reinforcement Learning*. https://doi.org/10.48550/arxiv.2204.03502

Zhang, L., & Thing, V. L. L. (2021). Three decades of deception techniques in active cyber defense - Retrospect and outlook. *Computers & Security*, *106*, 102288. https://doi.org/10.1016/J.COSE.2021.102288

Zhang, Y., Yu, H. Z., Zhou, W., & Man, M. (2022). Application and Research of IoT Architecture for End-Net-Cloud Edge Computing. *Electronics*. https://doi.org/10.3390/electronics12010001

Zhao, K. (2012). Research and design of the distributed intrusion detection system based on snort. *Proceedings - 2012 International Conference on Computer Science and Electronics Engineering, ICCSEE 2012*, *2*, 525–527. https://doi.org/10.1109/ICCSEE.2012.310

Zhao, S., Chandrashekar, M., Lee, Y., & Medhi, D. (2015). Real-time network anomaly detection system using machine learning. *2015 11th International Conference on the Design of Reliable Communication Networks, DRCN 2015*, 267–270. https://doi.org/10.1109/DRCN.2015.7149025

Zhao, S., Wei, R., Cai, L., Yu, A., & Meng, D. (2020). CTLMD: Continuous-Temporal Lateral Movement Detection Using Graph Embedding. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *11999 LNCS*, 181–196. https://doi.org/10.1007/978-3-030-41579-2_11

Zou, J., He, D., Zeadally, S., Kumar, N., Wang, H., & Choo, K. R. (2021). Integrated Blockchain and Cloud Computing Systems: A Systematic Survey, Solutions, and Challenges. *Acm Computing Surveys*. https://doi.org/10.1145/3456628

Zoughbi, S. (2017). Securing government information and data in developing countries. In *Securing Government Information and Data in Developing Countries*. IGI Global. https://doi.org/10.4018/978-1-5225-1703-0

ANEXOS

ANEXO A. ÁRBOL DE PROBLEMAS ACERCA DE LA INVESTIGACIÓN DOCTORAL.

Figura 23: Árbol de problemas

Fuente. Elaboración propia

ANEXO B. PROTOCOLO DE REVISIÓN SISTEMÁTICA DE LITERATURA DE "AMENAZAS INTERNAS EN INTRANETS ACADÉMICAS" VERSIÓN 3.0

"Un protocolo de revisión detalla los métodos que se utilizarán para llevar a cabo en una revisión sistemática específica. Un protocolo predefinido es necesario para reducir la posibilidad del sesgo investigador."(Kitchenham, 2004b)(Kitchenham, 2004b)

Los componentes de un protocolo incluyen todos los elementos de la revisión detallados en la Figura 6, referente al proceso de revisión sistemática de literatura (RSL) Brereton et al. (2007). Sin embargo, según las directrices que Kitchenham señala referente a este proceso, se orienta a ayudar a los estudiantes de doctorado, así como a grupos de investigación más grandes. Se debe considerar, que muchos de los pasos de una revisión sistemática asumen que será realizada por un gran grupo de investigadores. En el caso de un solo investigador (como un estudiante de doctorado), se sugiere utilizar los pasos más importantes, según (Kitchenham, 2007)(Kitchenham, 2007).

- ✓ Desarrollo de un protocolo.
- ✓ Definir la pregunta de investigación.
- ✓ Especificar lo que se hará para abordar el problema de un solo investigador aplicando criterios de inclusión/exclusión y realizando toda la extracción de datos.
- ✓ Definición de la estrategia de búsqueda.
- ✓ Definición de los datos a extraer de cada estudio primario incluyendo datos de calidad.
- ✓ Mantenimiento de listas de estudios incluidos y excluidos.
- ✓ Uso de las directrices de síntesis de datos.
- ✓ Utilización de las directrices para la presentación de informes.

En el presente estudio se consideraron estas sugerencias, sin embargo, se incluyen las fases del Proceso de revisión sistemática de literatura según Brereton et.al (2007) con el objetivo de tener una secuencia de la aplicación de la metodología.

Fase 1. Plan de revisión.

Especificar las preguntas de Investigación

Se definió las preguntas de investigación para identificar y comprender las búsquedas específicas basadas sobre el tópico de investigación, Petticrew y Roberts sugieren (PICOC) basado en cinco criterios: Población, Intervención, Comparación,

Resultado(Petticrew & Roberts, 2008)las (Petticrew & Roberts, 2008)(Petticrew & Roberts, 2008).

El objetivo de esta metodología de RSL es encontrar evidencias y comparación de enfoques, métodos, modelos; identificando referencias importantes. Se usó este criterio para estructurarla como se indica en la Tabla 22. PICOC APLICADO AL ESTUDIO (Petticrew & Roberts, 2008).

Tabla 22: PICOC APLICADO AL ESTUDIO

POBLACIÓN	INTRANET ACADÉMICAS.
INTERVENCIÓN	Identificar, clasificar amenazas internas o insider threat para mejorar el control en intranets académicas.
COMPARACIÓN	Incidencia de los diferentes métodos y técnicas para Identificar, clasificar amenazas internas o insider threat para mejorar el control en intranets académicas.
RESULTADOS	Definir los métodos y técnicas adecuadas para Identificar, clasificar amenazas internas o insider threat para mejorar el control y la seguridad en intranets académicas.
CONTEXTO	Este estudio abarca a las intranets de Campus ACADEMICOS involucra al administrador de red, a los usuarios que intervienen (profesores, empleados, estudiantes,). Las tareas empezarán desarrollándose a pequeña escala. El estudio abarcará estudios empíricos, incluyendo observaciones, entrevistas, cuestionarios, encuestas, experimentación formal y estudio de caso, etc.

Fuente: Elaboración propia

En estudios realizados para evaluar la incidencia de la aplicación de políticas de ciberseguridad en la intranet de redes académicas SDN, se planteó las preguntas, pues (Staples & Niazi, 2007) recomiendan limitar el alcance de una literatura sistemática eligiendo preguntas de investigación claras y estrechas.

Considerando el estudio de (Ghani, 2013), se aplicó las preguntas de investigación en base al método PICOC presentando un esquema para proponer cada pregunta de investigación, como se describe en la Figura 27 respecto de *PICOC criteria and an explanation of each criterion.*

Criteria	*Meaning*
Population	Who or What?
Intervention	How?
Comparison	Compared to what / what is the alternative?
Outcomes	What are we trying to accomplish, improve, effect?
Context	Under what circumstances?

Figura 24: PICOC criteria and an explanation of each criterion (Ghani, 2013).

PREGUNTA 1

Q1. ¿Qué tipos de insiders threat o amenazas internas existen en intranets académicas y cuáles son sus fuentes de datos?

Los criterios y alcance de PICOC para Q1, se describen en la Tabla 23.

Tabla 23: PICOC para Q1.

Criterio	Alcance
Población	Encontrar artículos que mencionan los tipos de insiders threat o amenazas internas existentes en intranets académicas, sus principales fuentes de datos y métodos de control.
Intervención	Tipos de insiders threat o amenazas internas, intranets académicas, fuentes de datos, control de acceso.
Comparación	Ninguna.
Resultados	Definir tipos de insiders threat o amenazas internas existentes en intranets académicas y sus principales fuentes de datos y el control de acceso para insiders.
Contexto	Coincidencias.

Fuente: Elaboración propia

Esta pregunta evalúa el estado del arte. No amerita comparación.

Criterios de Inclusión para Q1:

1.- Tipos de insiders threat o amenazas internas existentes en redes de datos.
2.- Tipos de insiders threat o amenazas internas existentes en intranets académicas.
3.- Principales fuentes de datos de insiders threats.
4.- Cuántas investigaciones mencionan considerar insider threat para limitar el control de acceso a usuarios en intranets?

Los criterios Q1.1 al Q1.4 responden a la pregunta 1 definida en la tabla 24.

PREGUNTA 2

Q2. Qué herramientas, métodos o procedimientos de recolección de datos se emplean en el análisis de insiders threat, ¿además que métodos de identificación o detección de amenazas se emplean?

Los criterios y alcance de PICOC para Q2, se describen en la Tabla 19.

Tabla 24: PICOC para Q2.

Criterio	Alcance
Población	Encontrar el número de artículos que mencionan herramientas, métodos ó procedimientos de recolección de datos que se emplean en el análisis de insiders threat, además conocer que métodos de identificación o detección de amenazas se emplean.
Intervención	Herramientas, métodos o procedimientos, recolección de datos, intranets académicas, insiders threats, métodos de identificación o detección de amenazas, detección de anomalías o comportamientos anómalos.
Comparación	Ninguna.
Resultados	Encontrar sugerencias de implementación que podrían aportar al estudio.
Contexto	Coincidencias.

Fuente: Elaboración propia

En esta pregunta el objetivo es encontrar, elementos, limitaciones, conflictos con normas y métodos de solución.

Criterios de Inclusión para Q2:

1. - ¿Qué herramientas, métodos o procedimientos de recolección de datos se emplean en el análisis de insiders threat?

2.- ¿Qué procedimientos se emplean para realizar mediciones de data de insiders threats en intranets académicas?

3.- ¿Qué método de detección de mal uso o detección de anomalías o comportamientos anómalos emplea en el contexto de detección de intrusiones de insiders threat?

4.- ¿Qué método de detección de mal uso o detección de anomalías o comportamientos anómalos emplea en el contexto de detección de intrusiones de insiders threat en intranets académicas?

5.- ¿Qué método se usa para identificar insiders threat en tiempo real (Real Time usage profiling)

6.- ¿Qué algoritmo de análisis de data emplean en la identificación de insiders threats?

7.- ¿Qué estudios aplican análisis de tramas para la identificación en insiders threat y cómo lo hacen?

Los criterios del Q2.1 al Q2.7 responden a la pregunta 2, definida en la Tabla 19.

Q3. ¿Qué metodología para identificar, evaluar y controlar insiders threat en intranets académicas se emplea y cuál es la más adecuada?

Los criterios y alcance de PICOC para Q3, se describen en la Tabla 25.

Tabla 25: PICOC para Q3.

Criterio	**Alcanc**
Población	Encontrar la existencia de modelos, normas, metodologías de seguridad para identificar, evaluar y controlar insiders en intranets de redes académicas.
Intervención	Normas, Modelos, Seguridad, Redes Académicas, identificar, evaluar y controlar insiders.
Comparación	Existencia de un modelo de seguridad en intranets.
Resultados	Estudiar y mejorar la metodología para identificar, evaluar y controlar insiders en intranets de redes académicas.
Contexto	Disponibilidad de un modelo, norma.

Fuente: Elaboración propia

En esta pregunta el enfoque de la población es encontrar un modelo o norma de seguridad en intranets de redes académicas existentes. Si una respuesta es descubierta entonces la mejora puede ser aplicada en base a un modelo existente.

Esto incluye desarrollo de fases, roles, herramientas. Que mejorarán la escalabilidad del modelo.

CRITERIO DE INCLUSIÓN

1. ¿Qué metodología para identificar, evaluar y controlar insiders threat se emplea, ¿cuál es la más adecuada?

2. Existen modelos, normas particulares en seguridad en intranets de redes académicas.

El criterio Q3.1 y Q3.2 responde a la pregunta 3, definida en la Tabla 25.

DESARROLLO DEL PROTOCOLO DE REVISIÓN

ESTRATEGIA DE BÚSQUEDA.

La estrategia utilizada para derivar los términos de búsqueda es la siguiente:

i. Derivar los principales términos de búsqueda de las preguntas de investigación, identificando Población, Intervención, Comparación, Resultados y Contexto (Ghani, 2013), esto se aplica en la Tabla 26.

Tabla 26: Términos derivados de PICOC para la estrategia de búsqueda.

POBLACIÓN	Academic Intranet
INTERVENCIÓN	Methods, Techniques, flow management, internal threats, insider threats, control.
COMPARACIÓN	Incidence, classification methods, identification, threats, limits, difficulties, development, processes, factors, success, errors, control insider threat.
RESULTADOS	Methods and techniques to identify, classify internal threats, insider threat, control, detection of anomalies or anomalous behavior.
CONTEXTO	ACADEMIC CAMPUS, academic intranets, network manager, teachers, employees, students, observations, interviews, questionnaires, formal experiments, case studies.

Fuente. Adaptado del formato de términos de búsqueda de las preguntas de investigación (Ghani, 2013)

ii. Luego, se debe encontrar las palabras claves en los documentos pertinentes como artículos científicos, en el análisis inicial(Ghani, 2013)*, como se detalla en la Tabla 27.*

Tabla 27: Palabras claves derivadas de la búsqueda de artículos científicos.

Estudio	**Palabras Claves**
(Hori et al., 2011)	insider threat, network security, cloud computing, anomaly detection
(Gheyas & Abdallah, 2016)	Insider threat prediction, Anomaly detection, Machine learning, Cyber security, Individual attacks, Collusion attacks
(Ashraf & Latif, 2014)	Machine Learning, Software Defined Networking (SDN), Intrusion Detection, Distributed Denial of Service Attack
(Nanda et al., 2016)	Network Attack; Machine Learning; Honeypots; SDN
(Amaral & Bernardo, 2016)	Software defined Networks; Machine Learning; Data Analysis; Traffic Classification
(S. T. Ali et al., 2013)	Anonymization, data offloading, network functions virtualization, network security, network verification, software defined networking, threat detection, threat remediation
(Bishop & Gates, 2008)	Insider threat
(Bishop et al., 2010)	Insider, security policy
(C. W. Probst, 2010)	Insider threat, insider problem

(W. C. Lin et al., 2015)	Intrusion Detection Anomaly detection Feature representation Cluster center Nearest Nearest neighbor
(Vinchurkar & Reshamwala, 2012)	Intrusion Detection system, Anomaly Based intrusion., Neural Network, Machine Learning, Principle Component Analysis, Support Vector Machine.
(P. A. Legg, 2015)	Insider threat, behavioral analysis, model visualization
(Agrafiotis et al., 2016)	Insider detection, anomaly detection, real world, case study, machine learning
(P. A. Legg et al., 2017)	Anomaly detection, cyber security, insider threat.
(P. Legg et al., 2015)	Insider threat detection, anomalies, anomaly detection system, unsupervised detection,
(Eldardiry et al., 2013)	Insider threat detection, anomaly
(A. C. Lin & Peterson, 2016)	Behavior, Insider threat, pattern recognition

Fuente: Elaboración propia

Encontrar ortografías y sinónimos alternativos para los términos de búsqueda con la ayuda del diccionario, como se indica en la tabla 28.

Tabla 28: Ortografías y sinónimos alternativos para los términos de búsqueda.

Intranet académica	Academic intranet, campus network or network campus
Insider Threat	Insider threat, insider problem internal threats, threat detection Insider threat prediction
Anomalous behavior	behavioral analysis
Anomaly detection	Intrusion Detection system, Anomaly Based intrusion anomaly detection system
control	Process, technique, system, procedure. methods and techniques, Control and identification

Fuente: Elaboración propia

Usando términos para plantear la lógica de búsqueda de acuerdo la tabla 29.

Tabla 29: Términos para plantear la lógica de búsqueda.

“Academic intranet” OR intranet
“Campus Network” OR “network campus”
“Insider threat” OR “insider problem” OR” internal threats” OR “threat detection” OR “Insider threat prediction”
“Anomalous behavior” OR “behavioral analysis”
“Anomaly detection” OR “Intrusion Detection system” OR “Anomaly Based intrusion” OR “anomaly detection system”
Control OR Process OR technique OR system OR procedure OR methods OR techniques OR “Control and identification”

Fuente: Elaboración propia

Se aplica la lógica para las cadenas de búsquedas, como se describe en la Tabla 30.

Tabla 30: Lógica de búsqueda.

(“Insider threat" OR "insider problem" OR "internal threats" OR "threat detection" OR "Insider threat prediction”)
(“Anomalous behavior" OR "behavioral analysis" OR "Anomaly detection" OR "Intrusion Detection system" OR "Anomaly Based intrusion" OR "anomaly detection system”)
(control OR process OR technique OR system OR procedure OR methods OR techniques OR "Control and identification”)
(“Campus Network” OR “network campus”)
“Academic intranet” OR intranet

Fuente: Elaboración propia

Se aplicó la lógica de búsqueda en Scopus, la mayor base de datos de citas y resúmenes de bibliografía revisada por pares: revistas científicas, libros y actas de conferencias, ofreciendo un exhaustivo resumen de los resultados de la investigación mundial en los campos de la ciencia, la tecnología y otros, incluye herramientas inteligentes para hacer un seguimiento, analizar y visualizar la investigación (ELSEVIER, 2022)

(“Insider threat" OR "insider problem" OR "internal threats" OR "threat detection" OR "Insider threat prediction”) AND (“Anomalous behavior" OR "behavioral analysis" OR "Anomaly detection" OR "Intrusion Detection system" OR "Anomaly Based intrusion" OR "anomaly detection system”) AND (control OR process OR technique OR system OR procedure OR methods OR techniques OR "Control and identification") AND (("Campus Network" OR "network campus") OR ("academic intranet" OR "intranet"))

VALIDACIÓN DEL PROTOCOLO DE REVISIÓN

Para validar el protocolo de revisión de literatura propuesto se realizó la búsqueda y se analizó los resultados obtenidos, considerando el número de artículos generados

y la réplica de la cadena de búsqueda que arrojó mayor número de artículos científicos conforme se aplicó desde su realización hasta la actualidad. La primera búsqueda se realizó en 7 de diciembre de 2018, obteniéndose 19 artículos en SCOPUS, se pulió la cadena de búsqueda y se dio un enfoque más orientado a redes de campus académicos, realizándose una segunda búsqueda el 9 de mayo de 2020, generando en SCOPUS 32 resultados lo que generó un resultado preliminar.

En el año 2022, se aplicó la búsqueda para el presente trabajo de investigación doctoral el 6 abril de 2022 en ACM generando 20 resultados. El 9 de junio de 2022 se tiene 56 artículos en la base de datos SCOPUS. El 2 de julio del año 2022 en la base de datos IEEE con 51 resultados. Obteniéndose en total 127 artículos en tres bases de datos: SCOPUS, ACM e IEEE.

Al evaluar el protocolo, se amplió los criterios de inclusión incluyendo un cuarto criterio en la pregunta uno y dos en la pregunta dos, teniendo al final trece criterios de inclusión en el protocolo propuesto, con el objetivo de captar la mayor cantidad de información relevante para el estudio de amenazas internas en intranets de campus académicos. Se evaluó la aplicación del protocolo desarrollado de RSL de “Amenazas internas en intranets académicas” versión 3.0, que es la que se incluye en el presente trabajo de investigación doctoral.

Fase 2: Realización de la revisión

Fase de Investigación Primaria

Considerando la relevancia del estudio por cuanto amerita hacer una revisión de los antecedentes de la propuesta de investigación para partir de un estado inicial del arte, desde donde se pueda considerar las mejoras en el control de acceso de usuarios no deseados en redes académicas, basadas en políticas de calidad de servicio.

Las búsquedas para descubrir las respuestas a las preguntas planteadas se realizaron en tres bases de datos, en las que se incluye: el motor de búsqueda Scopus (ELSEVIER, 2022), ACM Digital Library(Association for Computing Machinery, 1985)(Association for Computing Machinery, 1985) e IEEEXplore (IEEE, 2022) en las que se aplicó la misma cadena de búsqueda establecida para el estudio, adaptada según el formato, como se detalla en la Tabla 31.

Tabla 31: Bases de datos consideradas para la búsqueda y cadenas de búsqueda.

Fuente/URL	CADENA DE BÚSQUEDA
SCOPUS http://www.sciencedirect.com	(“Insider threat" OR "insider problem" OR "internal threats" OR "threat detection" OR "Insider threat prediction”) AND (“Anomalous behavior" OR "behavioral analysis" OR "Anomaly detection" OR "Intrusion Detection system" OR "Anomaly Based intrusion" OR "anomaly detection system”) AND (control OR process OR technique OR system OR procedure OR methods OR techniques OR "Control and identification") AND (("Campus Network" OR "network campus") OR ("academic intranet" OR "intranet"))
IEEEXplore http://ieeexplore.ieee.org	((“Insider threat" OR "insider problem" OR "internal threats" OR "threat detection" OR "Insider threat prediction”) AND (“Anomalous behavior" OR "behavioral analysis" OR "Anomaly detection" OR "Intrusion Detection system" OR "Anomaly Based intrusion" OR "anomaly detection system”) AND (control OR process OR technique OR system OR procedure OR methods OR techniques OR "Control and identification") AND (("Campus Network" OR "network campus") OR ("academic intranet" OR "intranet")))
ACM Digital Library. http://dl.acm.org/	[["insider threat"] OR ["insider problem"] OR ["internal threats"] OR ["threat detection"] OR ["insider threat prediction"]] AND [["anomalous behavior"] OR ["behavioral analysis"] OR ["anomaly detection"] OR ["intrusion detection system"] OR ["anomaly based intrusion"] OR ["anomaly detection system"]] AND [[control] OR [process] OR [technique] OR [system] OR [procedure] OR [methods] OR [techniques] OR ["control and identification"]] AND [["campus network"] OR ["network campus"] OR ["academic intranet"] OR ["intranet"]]

Fuente: Elaboración propia

Criterios de Evaluación de la Calidad del Estudio y Proceso de Selección

Se usan para identificar los estudios primarios que proveen evidencia directa acerca de la pregunta de investigación. Con el fin de reducir la probabilidad de sesgo, los criterios de selección deben decidirse durante la definición del protocolo, aunque pueden ser refinados durante el proceso de búsqueda. (Budgen & Brereton, 2006)

El objetivo principal es que al aplicar los criterios se tenga una evidencia fiable de las respuestas a las preguntas de investigación. Pudiendo medir su valoración y eliminar los que tengan una calificación baja. Se considera una calificación baja, menos de 2/5.

Criterios de inclusión / exclusión para la selección de estudios

Los criterios de inclusión y exclusión deben basarse en la pregunta de investigación. Ellos deben ser orientados a garantizar que puedan ser interpretados de forma fiable y que se clasifican los estudios correctamente.(Budgen & Brereton, 2006)

Para que el estudio se incluya/excluya en el proceso de revisión sistemática, debe cumplir o no con los siguientes criterios:

CRITERIO INCLUSIÓN:

Q1.1.- Tipos de insiders threat o amenazas internas existentes en redes de datos.

Q1.2.- Tipos de insiders threat o amenazas internas existentes en intranets académicas.

Q1.3.- Principales fuentes de datos de insiders threats.

Q1.4.- Cuántas investigaciones mencionan considerar insider threat para limitar el control de acceso a usuarios en intranets?

Q2.1.- ¿Qué herramientas, métodos o procedimientos de recolección de datos se emplean en el análisis de insiders threat?

Q2.2.- ¿Qué procedimientos se emplean para realizar mediciones de data de insiders threats en intranets académicas?

Q2.3.- ¿Qué método de detección de mal uso o detección de anomalías o comportamientos anómalos emplea en el contexto de detección de intrusiones de insiders threat?

Q2.4.- ¿Qué método de detección de mal uso o detección de anomalías o comportamientos anómalos emplea en el contexto de detección de intrusiones de insiders threat en intranets académicas?

Q2.5- ¿Qué método se usa para identificar insiders threat en tiempo real (Real Time usage profiling)

Q2.6.- ¿Qué algoritmo de análisis de data emplean en la identificación de insiders threats?

Q2.7.- ¿Qué estudios aplican análisis de tramas para la identificación en insiders threat y cómo lo hacen?

Q3.1. ¿Qué metodología para identificar, evaluar y controlar insiders threat se emplea, ¿cuál es la más adecuada?

Q3.2. Existen modelos, normas particulares en seguridad en intranets de redes académicas.

Los criterios Q1.1 al Q1.4 responden a la pregunta 1 definida en la tabla 23.
Los criterios del Q2.1 al Q2.7 responde a la pregunta 2, definida en la tabla 24.
El criterio Q3.1 y Q3.2, responde a la pregunta 3, definida en la tabla 25.

CRITERIO EXCLUSIÓN
Se excluye si el estudio no está en inglés o español.
No corresponden a los 13 criterios de inclusión considerados para la valoración de los artículos.

LISTAS DE COMPROBACIÓN CUANTITATIVA Y CUALITATIVA
Kitchenham propone para estudios cuantitativos, una lista de preguntas organizadas con respecto a la fase y el tipo de estudio. Menciona además, que los investigadores deben adoptar la sugerencia de (Fink, 2005), que es revisar la lista de preguntas en el contexto de su propio estudio y seleccionar aquellas preguntas de evaluación de calidad que son más apropiadas para sus preguntas específicas de investigación. Pueden necesitar construir una escala de la medida para cada artículo puesto que a veces una respuesta sí / no simple puede ser engañosa.
Para la valoración, se utiliza una escala de Likert del 1 al 5, siendo 1 de significancia mínima y 5 la de mayor significancia.

A continuación, se muestra la Tabla 32. Formato de listas de preguntas para la evaluación cuantitativa de los artículos, donde se incluyen datos adicionales como el número de paper, título, y promedio para la aplicación en el presente estudio.

Tabla 32: **Formato de listas de preguntas para la evaluación cuantitativa de los artículos de RSL.**

No. Paper	Título	Id_Pregunta	Descripción	Calificación	Promedio

		PC1	¿Están claramente establecidos los objetivos para el estudio?	Escala de Likert 1-5	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	Escala de Likert 1-5	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	Escala de Likert 1-5	
		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	Escala de Likert 1-5	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	Escala de Likert 1-5	
		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	Escala de Likert 1-5	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	Escala de Likert 1-5	
		PC8	¿Se describen los métodos estadísticos?	Escala de Likert 1-5	
		PC9	¿Están justificados los métodos estadísticos?	Escala de Likert 1-5	
		PC10	¿Es claro el propósito del análisis?	Escala de Likert 1-5	
		PC11	¿Son creíbles los resultados?	Escala de Likert 1-5	
		PC12	¿Hay una descripción completa del proceso de investigación?	Escala de Likert 1-5	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	Escala de Likert 1-5	
		PC14	Los reportes son claros.	Escala de Likert 1-5	Promedio Total

Fuente: Elaboración propia

De existir estudios cualitativos se aplican una lista de verificación consistente en ocho preguntas para ser usadas en la evaluación de estudios cualitativos. Considerando la evaluación bajo una valoración de escala de Likert del 1 al 5, donde 1 es la valoración más baja y 5 la más alta. La tabla 33 referente a formato de listas de preguntas para la evaluación cualitativa de los artículos, muestra datos adicionales como el No. paper, título, id_pregunta, descripción, calificación y promedio para la aplicación en el presente estudio.

Tabla 33: **Formato de listas de preguntas para la evaluación cualitativa de los artículos de RSL.**

No. Paper	Título	Id_Pregunta	Descripción	Calificación	Promedio
		PCT1	¿El diseño de la investigación es adecuado para llevar a cabo el estudio?	Escala de Likert 1-5	

		PCT2	¿El estudio se basa en el cuerpo de conocimiento existente, es decir, analiza explícitamente su contribución a la luz de trabajos anteriores?	Escala de Likert 1-5	
		PCT3	¿Los hallazgos son creíbles?	Escala de Likert 1-5	
		PCT4	¿El proceso de investigación se describe a fondo? ¿Los obstáculos son descritos de manera útil?	Escala de Likert 1-5	
		PCT5	¿Están claros los vínculos entre los datos, la interpretación y las conclusiones?	Escala de Likert 1-5	
		PCT6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	Escala de Likert 1-5	
		PCT7	¿La presentación de informes es clara y coherente?	Escala de Likert 1-5	
		PCT8	¿Son claras las suposiciones, perspectivas teóricas, valores que han configurado la forma y el resultado de la evaluación?	Escala de Likert 1-5	Promedio total

Fuente: Elaboración propia

Se realizó el análisis cuantitativo, cualitativo de los 127 artículos determinados para la RSL aplicando la Tabla 32, formato de listas de preguntas para la evaluación cuantitativa de los artículos de RSL y la Tabla 33, formato de listas de preguntas para la evaluación cualitativa de los artículos de RSL.

Los resultados de análisis de los papers se describen en el Anexo D que detalla el Análisis Cualitativo RSL y en el Anexo E referente al Análisis Cuantitativo RSL.

En el que se dio respuesta a las preguntas planteadas para la evaluación.

Se determinó que 117 artículos cumplen con el análisis cuantitativo o cualitativo, por lo que se consideran para el estudio de RSL del presente trabajo doctoral.

Estrategia de extracción de datos

Después de que se hayan seleccionado los estudios primarios y se haya evaluado su calidad, se extraerán los datos. Los formularios de extracción de datos y la

estrategia que se adoptará para registrarlos se detallan a continuación, permitiendo resumir los aspectos relevantes de la investigación, se denota en la tabla 34. Formulario de extracción de datos, adaptada de (Kitchenham, 2007).

Tabla 34: **Formulario de extracción de datos de artículos científicos para RSL**

Id del Estudio	ID:#
INFORMACIÓN GENERAL	
Título	
Autor (s)	
Año de Publicación	
Tipo de Referencia	Revista/Conferencia/Reporte/workshop
Editor	
País de Estudio	
Entorno de estudio	Industria /Universidad
Tipo de estudio	REPORTE/Encuesta / Experimento / Caso de Estudio, etc.
Artículo Revisado por pares?	SI/NO
Detalle General	
CARACTERISTICAS DEL ESTUDIO E INFORMACIÓN ESPECÍFICA	
Datos y Métodos	
NOTAS SOBRE TEMAS EMERGENTES JUNTO A DETALLES DE SÍNTESIS	
ANÁLISIS DE CRITERIOS	

Fuente: Adaptación de (Kitchenham, 2007)

En la Tabla 35 referente al análisis de criterios inclusivos, se presenta el detalle para el análisis correspondiente a los trece criterios que se han identificado en el presente estudio. Este análisis se realizó por artículo científico.

Tabla 35: **Análisis de Criterios Inclusivos**

ANÁLISIS DE CRITERIOS INCLUSIVOS		
Preguntas	**Criterios de Inclusión usados para responder las preguntas de investigación.**	
Q1. ¿Qué tipos de insiders threat o amenazas internas existen en intranets académicas y cuáles son sus fuentes de datos?	1.- Tipos de insiders threat o amenazas internas existentes en redes de datos.	
	2.- Tipos de insiders threat o amenazas internas existentes en intranets académicas.	
	3.- Principales fuentes de datos de insiders threats.	

	4.- Cuántas investigaciones mencionan considerar insider threat para limitar el control de acceso a usuarios en intranets?	
Q2. Qué herramientas, métodos o procedimientos de recolección de datos se emplean en el análisis de insiders threat, ¿además que métodos de identificación o detección de amenazas se emplean?	1. - ¿Qué herramientas, métodos o procedimientos de recolección de datos se emplean en el análisis de insiders threat?	
	2.- ¿Qué procedimientos se emplean para realizar mediciones de data de insiders threats en intranets académicas?	
	3.- ¿Qué método de detección de mal uso o detección de anomalías o comportamientos anómalos emplea en el contexto de detección de intrusiones de insiders threat?	
	4.- ¿Qué método de detección de mal uso o detección de anomalías o comportamientos anómalos emplea en el contexto de detección de intrusiones de insiders threat en intranets académicas?	
	5.- ¿Qué método se usa para identificar insiders threat en tiempo real (Real Time usage profiling)	
	6.- ¿Qué algoritmo de análisis de data emplean en la identificación de insiders threats?	
	7.- ¿Qué estudios aplican análisis de tramas para la identificación en insiders threat y cómo lo hacen?	
Q3. ¿Qué metodología para identificar,	1. ¿Qué metodología para identificar, evaluar y	

evaluar y controlar insiders threat en intranets académicas se emplea y cuál es la más adecuada?	controlar insiders threat se emplea, ¿cuál es la más adecuada?	
	2. Existen modelos, normas particulares en seguridad en intranets de redes académicas.	

Fuente: Elaboración propia

Selección de estudios primarios.

A continuación, se incluye en la Tabla 36, información referente al listado de papers obtenidos al aplicar la búsqueda en las bases de datos ACM, SCOPUS, IEEE definida en la Tabla 5, considerado para el presente estudio. Entre los datos, están: identificador(IDs), autores, año, título, tipo y fuente.

Tabla 36: **Listado de Papers resultado de aplicar la Estrategia de Búsqueda en las bases de datos ACM, SCOPUS, IEEE.**

ACM					
IDs	**Autores**	**Año**	**Título**	**Tipo**	**Fuente**
1 ACM01	Myers, Justin; Grimaila, Michael R.; Mills, Robert F	2009	Towards Insider Threat Detection Using Web Server Logs (Myers et al., 2009)	Conference Paper	Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence
2 ACM02	Ren, Xueshuang; Wang, Liming	2020	A Hybrid Intelligent System for Insider Threat Detection Using Iterative Attention (Ren & Wang, 2020)	Conference Paper	Proceedings of 2020 the 6th International Conference on Computing and Data Engineering
3 ACM03	Liu, Ming; Xue, Zhi; Xu, Xianghua; Zhong, Changmin; Chen, Jinjun	2018	Host-Based Intrusion Detection System with System Calls: Review and Future Trends (M. Liu et al., 2018)	Article	ACM Comput. Surv.
4 ACM04	Chen, You; Malin, Bradley	2011	Detection of Anomalous Insiders in Collaborative Environments via Relational Analysis of Access Logs (Y. Chen & Malin, 2011)	Conference Paper	Proceedings of the First ACM Conference on Data and Application Security and Privacy
5 ACM05	Liu, Fucheng; Wen, Yu; Zhang, Dongxue; Jiang, Xihe; Xing, Xinyu; Meng, Dan	2019	Log2vec: A Heterogeneous Graph Embedding Based Approach for Detecting Cyber Threats within Enterprise (F. Liu et al., 2019)	Conference Paper	Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security
6 ACM06	Väisänen, Teemu	2017	Categorization of Cyber Security Deception Events for Measuring the Severity Level of Advanced Targeted Breaches (Väisänen, 2017)	Conference Paper	Proceedings of the 11th European Conference on Software Architecture: Companion Proceedings
7 ACM07	Bhilare, Dattatraya S.; Ramani, Ashwini K.; Tanwani, Sanjay K.	2009	Protecting Intellectual Property and Sensitive Information in Academic Campuses from Trusted Insiders: Leveraging Active Directory (Bhilare et al., 2009)	Conference Paper	Proceedings of the 37th Annual ACM SIGUCCS Fall Conference: Communication and Collaboration
8 ACM08	Rattanalerdnusorn, Ekkachan; Pattaranantakul, Montida; Thaenkaew, Phithak; Vorakulpipat, Chalee	2020	IoTDePT: Detecting Security Threats and Pinpointing Anomalies in an IoT Environment(Rattanalerdnusorn et al., 2020)	Conference Paper	Proceedings of the 2020 9th International Conference on Software and Computer Applications

9 ACM09	Sadasivam, Karthik; Samudrala, Banuprasad; Yang, T. Andrew	2005	Design of Network Security Projects Using Honeypots (Sadasivam et al., 2004)	Article	J. Comput. Sci. Coll.
10 ACM10	Wallace, Nathan; Atkison, Travis	2013	Observing Industrial Control System Attacks Launched via Metasploit Framework (Wallace & Atkison, 2013)	Conference Paper	Proceedings of the 51st ACM Southeast Conference
11 ACM11	Thompson, Herbert H; Ford, Richard	2004	Perfect Storm: The Insider, Naivety, and Hostility (Thompson & Ford, 2004)	Article	Queue
12 ACM12	Pisarčík, Peter; Sokol, Pavol	2014	Framework for Distributed Virtual Honeynets (Pisarčík & Sokol, 2014)	Conference Paper	Proceedings of the 7th International Conference on Security of Information and Networks
13 ACM13	Pak, Charles	2008	The near Real Time Statistical Asset Priority Driven (Nrtsapd) Risk Assessment Methodology (Pak, 2008)	Conference Paper	Proceedings of the 9th ACM SIGITE Conference on Information Technology Education
14 ACM14	Hongxia, Li; Lei, Chen	2018	Research on Computer Communication Network Security and Guarantee Ways (H. Li & Chen, 2018)	Conference Paper	Proceedings of the 2018 2nd International Conference on Algorithms, Computing and Systems
15 ACM15	Pak, Charles; Cannady, James	2009	Asset Priority Risk Assessment Using Hidden Markov Models (Pak & Cannady, 2009)	Conference Paper	Pro of the 10th ACM Conference on Information and technolo
16 ACM16	Zhihan Lv, Liang Qiao, Amit Kumar Singh, Qingjun Wang	2021	AI-empowered IoT Security for Smart Cities (Lv et al., 2021)	Journal paper	ACM Transactions on Internet Technology (TOIT), Volume 21, Issue 4
17 ACM17	Sudipta Paul, Subhankar Mishra	2020	LAC : LSTM AUTOENCODER with Community for Insider Threat Detection (Paul & Mishra, 2020)	Conference Paper	ICBDR 2020: 2020 the 4th International Conference on Big Data Research (ICBDR'20)
18 ACM18	Robert Ball, Glenn A. Fink, Chris North	2004	Home-centric visualization of network traffic for security administration (Ball et al., 2004)	Conference Paper	VizSEC/DMSEC '04: Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security
19 ACM19	Wang Daxian, Zhang Jishan, Yu jiujiu	2020	Research on intelligent Firewall for network security (Daxian et al., 2020)	Conference Paper	Proceedings of the 2020 2nd International Conference on Robotics, Intelligent Control and Artificial Intelligence
20 ACM20	Sagar Samtani, Murat Kantarcioglu, Hsinchun Chen	2020	Trailblazing the Artificial Intelligence for Cybersecurity Discipline: A Multi-Disciplinary Research Roadmap (Samtani et al., 2020)	Journal paper	ACM Transactions on Management Information Systems (TMIS), Volume 11, Issue 4
SCOPUS					
21 SCO01	Sarker I.H., Kayes A.S.M., Badsha S., Alqahtani H., Watters P., Ng A.	2020	Cybersecurity data science: an overview from machine learning perspective (Sarker et al., 2020)	Article	Journal of Big Data
22 SCO02	Wen Y., Chen X., Zeng X., Wang W.	2020	Analysis of E-mail Account Probing Attack Based on Graph Mining (Wen et al., 2020)	Article	Scientific Reports
23 SCO03	Singh J., Behal S.	2020	Detection and mitigation of DDoS attacks in SDN: A comprehensive review, research challenges and future directions (J. Singh & Behal, 2020)	Review	Computer Science Review
24 SCO04	Pliatsios D., Sarigiannidis P., Lagkas T., Sarigiannidis A.G.	2020	A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics (Pliatsios et al., 2020)	Article	IEEE Communications Surveys and Tutorials
25 SCO05	Sampath N., Sadhasivam J., Jayavel S., Chindarmony N.S., Sharma S.	2020	Intrusion detection in software defined networking using snort and mirroring (Sampath et al., 2020)	Article	SSRG International Journal of Engineering Trends and Technology
26 SCO06	Mahajan A., Ramotra A.K., Mansotra V., Singh M.	2020	An Automated Framework to Uncover Malicious Traffic for University Campus Network (Mahajan et al., 2020)	Conference Paper	Smart Innovation, Systems and Technologies
27 SCO07	Zhao S., Wei R., Cai L., Yu A., Meng D.	2020	CTLMD: Continuous-Temporal Lateral Movement Detection Using Graph Embedding (S. Zhao et al., 2020)	Conference Paper	Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and

					Lecture Notes in Bioinformatics)
28 SCO08	Kurt Ç., Ayhan Erdem O.	2020	Real-time anomaly detection and mitigation using streaming telemetry in SDN (Kurt & Ayhan Erdem, 2020)	Article	Turkish Journal of Electrical Engineering and Computer Sciences
29 SCO09	Bhati B.S., Chugh G., Al-Turjman F., Bhati N.S.	2020	An improved ensemble based intrusion detection technique using XGBoost (Bhati et al., 2021)	Article	Transactions on Emerging Telecommunications Technologies
30 SCO10	Lin J., Liao L., Wang T., Zhang J., Cheng L.	2020	SDCCP: Control the network using software-defined networking and end-to-end congestion control (J. Lin et al., 2020)	Conference Paper	Concurrency Computation
31 SCO11	Alagrash Y., Mohan N., Gollapalli S.R., Rrushi J.	2019	Machine learning and recognition of user tasks for malware detection (Alagrash et al., 2019)	Conference Paper	Proceedings - 1st IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Application
32 SCO12	Ring M., Wunderlich S., Scheuring D., Landes D., Hotho A.	2019	A survey of network-based intrusion detection data sets (Ring et al., 2019)	Review	Computers and Security
33 SCO13	Jin Q., Wang L.	2019	Intranet User-Level Security Traffic Management with Deep Reinforcement Learning (Jin & Wang, 2019)	Conference Paper	Proceedings of the International Joint Conference on Neural Networks
34 SCO14	Kumar B.K., Raj N., Dhivvya J.P., Muralidharan D.	2019	Fixing network security vulnerabilities in local area network (Kumar et al., 2019)	Conference Paper	Proceedings of the International Conference on Trends in Electronics and Informatics, ICOEI 2019
35 SCO15	Latah M., Toker L.	2019	Artificial intelligence enabled software-defined networking: A comprehensive overview (Latah & Toker, 2018)	Review	IET Networks
36 SCO16	Khan T., Alam M., Akhunzada A., Hur A., Asif M., Khan M.K.	2019	Towards augmented proactive cyberthreat intelligence (Khan et al., 2019)	Article	Journal of Parallel and Distributed Computing
37 SCO17	Hu T., Niu W., Zhang X., Liu X., Lu J., Liu Y.	2019	An Insider Threat Detection Approach Based on Mouse Dynamics and Deep Learning (T. Hu et al., 2019)	Article	Security and Communication Networks
38 SCO18	Xie J., Richard Yu F., Huang T., Xie R., Liu J., Wang C., Liu Y.	2019	A survey of machine learning techniques applied to software defined networking (SDN): Research issues and challenges (Xie et al., 2019)	Review	IEEE Communications Surveys and Tutorials
39 SCO19	Toprak C., Turker C., Erman A.T.	2018	Detection of DHCP Starvation Attacks in Software Defined Networks: A Case Study (Toprak et al., 2018)	Conference Paper	UBMK 2018 - 3rd International Conference on Computer Science and Engineering
40 SCO20	Qin T., He C., Jiang H., Chen R.	2018	Behavior rhythm: An effective model for massive logs characterizing and security monitoring in cloud (T. Qin et al., 2018)	Conference Paper	2018 IEEE Conference on Communications and Network Security, CNS 2018
41 SCO21	Kuo C.-T., Chang V., Lei C.-L.	2018	A feasibility analysis for edge computing fusion in LPWA IoT environment with SDN structure (Kuo et al., 2018)	Conference Paper	Proceedings of 2017 International Conference on Engineering and Technology, ICET 2017
42 SCO22	Tantar E., Tantar A.-A., Kantor M., Engel T.	2018	On Using Cognition for Anomaly Detection in SDN (Tantar et al., 2018)	Conference Paper	Advances in Intelligent Systems and Computing
43 SCO23	Kul G., Upadhyaya S., Hughes A.	2017	Complexity of insider attacks to databases (Kul et al., 2017)	Conference Paper	MIST 2017 - Proceedings of the 2017 International Workshop on Managing Insider Security Threats, co-located with CCS 2017
44 SCO24	Zoughbi S.	2017	Securing government information and data in developing countries (Zoughbi, 2017)	Book	Securing Government Information and Data in Developing Countries
45 SCO25	Rawat D.B., Reddy S.R.	2017	Software Defined Networking Architecture, Security and Energy Efficiency: A Survey (Rawat & Reddy, 2017)	Review	IEEE Communications Surveys and Tutorials
46 SCO26	Cox J.H., Clark R.J., Owen H.L.	2016	Leveraging SDN for ARP security (Cox et al., 2016)	Conference Paper	Conference Proceedings - IEEE SOUTHEASTCON
47 SCO27	Da Silva A.S., Smith P., Mauthe A., Schaeffer-Filho A.	2015	Resilience support in software-defined networking: A survey (A. S. da Silva et al., 2015)	Article	Computer Networks
48 SCO28	Ali S.T., Sivaraman V., Radford A., Jha S.	2015	A Survey of Securing Networks Using Software Defined Networking (S. T. Ali et al., 2015)	Article	IEEE Transactions on Reliability

49 SCO29	Gugelmann D., Gasser F., Ager B., Lenders V.	2015	Hviz: HTTP(S) traffic aggregation and visualization for network forensics (Gugelmann et al., 2015)	Article	Digital Investigation
50 SCO30	Trio Pramono Y.W., Suhardi	2015	Anomaly-based intrusion detection and prevention system on website usage using rule-growth sequential pattern analysis: Case study: Statistics of Indonesia (BPS) website (Trio Pramono & Suhardi, 2015)	Conference Paper	Proceedings - 2014 International Conference on Advanced Informatics: Concept, Theory and Application, ICAICTA 2014
51 SCO31	Sathya R., Thangarajan R.	2015	Efficient anomaly detection and mitigation in software defined networking environment (Sathya & Thangarajan, 2015)	Conference Paper	2nd International Conference on Electronics and Communication Systems, ICECS 2015
52 SCO32	Stiawan D., Idris m.y., Abdullah a.H.	2015	Penetration testing and network auditing: Linux (Stiawan et al., 2015)	Article	Journal of Information Processing Systems
53 SCO33	Gugelmann D., Gasser F., Ager B., Lenders V.	2015	Repetido HViz: HTTP(S) traffic aggregation and visualization for network forensics (Gugelmann et al., 2015)	Conference Paper	Proceedings of the Digital Forensic Research Conference, DFRWS 2015 EU
54 SCO34	Chi P.-W., Kuo C.-T., Ruan H.-M., Chen S.-J., Lei C.-L.	2014	An AMI threat detection mechanism based on SDN networks (Po-Wen et al., 2014)	Conference Paper	SECURWARE 2014 - 8th International Conference on Emerging Security Information, Systems and Technologies
55 SCO35	Čermák M., Čeleda P., Vykopal J.	2014	Detection of DNS traffic anomalies in large networks (Čermák et al., 2014)	Article	Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)
56 SCO36	Kim I.S., Kim M.H.	2012	Agent-based honeynet framework for protecting servers in campus networks (I. S. Kim & Kim, 2012)	Article	IET Information Security
57 SCO37	Nithiyanandam C., Tamilselvan D., Balaji S., Sivaguru V.	2012	Advanced framework of defense system for prevetion of insider's malicious behaviors (Nithiyanandam et al., 2012)	Conference Paper	International Conference on Recent Trends in Information Technology, ICRTIT 2012
58 SCO38	Shimoda A., Mori T., Goto S.	2010	Sensor in the dark: Building untraceable large-scale honeypots using virtualization technologies (Shimoda et al., 2010)	Conference Paper	Proceedings - 2010 10th Annual International Symposium on Applications and the Internet, SAINT 2010
59 SCO39	Gökhan Kul, Shambhu Upadhyaya, Andrew Hughes	2020	An Analysis of Complexity of Insider Attacks to Databases (Kul et al., 2020)	Article	(2021) ACM Transactions on Management Information Systems, 12 (1), art. no. 3391231, . Cited 1 time
60 SCO40	Harshit Gujral, Abhinav Sharma, Pulkit Jain, Shriya Juneja, Sangeeta Mittal	2022	Design and Implementation of a Quantitative Network Health Monitoring and Recovery System (Gujral et al., 2022)	Article	(2022) Wireless Personal Communications
61 SCO41	Ricardo Raimundo, Albérico Rosário	2021	The Impact of Artificial Intelligence on Data System Security: A Literature Review (Raimundo & Rosário, 2021)	Article	(2021) Sensors, 21 (21), art. no. 7029,
62 SCO42	Noe M.Yungaicela Naula, Cesar Varga Rosales, Jesús Arturo Pérez, Díaz Mahdi Zareei	2022	Towards security automation in Software Defined Networks(Review) (Yungaicela-Naula et al., 2022)	Review	Computer Communications Volume 183, 1 February 2022, Pages 64-82
63 SCO43	Li Zhang, Vrizlynn.L. Thing	2021	Three decades of deception techniques in active cyber defense - Retrospect and outlook (L. Zhang & Thing, 2021)	Review	Computers and Security Volume 106, July 2021, Article number 102288
64 SCO44	Jean Paul A. Yaacoub, Javier Hernandez Fernandez, Hassan N. Noura a, Ali Chehab	2021	Security of Power Line Communication systems: Issues, limitations and existing solutions (Yaacoub et al., 2021)	Review	Computer Science Review 39 (2021) 100331
65 SCO45	Talha Ongun, Oliver Spohngellert, Benjamin Miller, Simona Boboila, Alina Oprea, Tina Eliassi-Rad	2021	PORTFILER: Port-Level Network Profiling for Self-Propagating Malware Detection (Ongun et al., 2021)	Review	Computer Science Review, 39, art. no. 100331,

66 SCO46	Mohammad Al-Fawa'reh, Mustafa Al-Fayoumi, Shadi Nashwan, Salam Fraihat	2021	Cyber threat intelligence using PCA-DNN model to detect abnormal network behavior (Al-Fawa'reh et al., 2022)	Article	Egyptian Informatics Journal 23 (2022) 173–185
67 SCO47	Al-Fawa'reh, Mohammad; Ashi, Zain; and Jafar, Mousa Tayseer	2021	Detecting Malicious DNS Queries Over Encrypted Tunnels Using Statistical Analysis and Bi-Directional Recurrent Neural Networks (Mohammad Al-Fawa'reh, 2021)	Article	Journal of Modern Science: Vol. 7 : Iss. 4 , Article 4.
68 SCO48	Song Wang; Juan Fernando Balarezo; Sithamparanatha n Kandeepan; Akram Al-Hourani; Karina Gomez Chavez	2021	Machine Learning in Network Anomaly Detection: A Survey Publisher (S. Wang et al., 2021)	Article	(2021) IEEE Access, 9, pp. 152379-152396.
69 SCO49	Qiaofeng Qin, Konstantinos Poularakis, and Leandros Tassiulas	2020	A Learning Approach with Programmable Data Plane towards IoT Security (Q. Qin et al., 2020)	Conference Paper	(2020) Proceedings - International Conference on Distributed Computing Systems, 2020-November, art. no. 9355643
70 SCO50	Faheem Ullah, Matthew Edwards, Rajiv Ramdhany, Ruzanna Chitchyan, M. Ali Babar, Awais Rashid	2017	Data Exfiltration: A Review of External Attack Vectors and Countermeasures (Ullah et al., 2018)	Review	Journal of Network and Computer Applications, 101
71 SCO51	Dennis Arturo, Kazuya Takemori, Shinichiro Kubota, Kenichi Sugitani, Yasuo Musashi	2009	Towards the Design of Hardware Based Security Device and Communication Implementation (Ludeña Romaña et al., 2009)	Conference Paper	Proceedings of the 2nd International Conference on Intelligent Networks and Intelligent Systems, art. no. 5364834, pp. 250-252
72 SCO52	Suomalainen, J., Julku, J., Heikkinen, A., Rantala, S.J., Yastrebova, A.	2022	Security-driven prioritization for tactical mobile networks (Suomalainen et al., 2022)	Article	Journal of Information Security and Applications, 67, art. no. 103198
73 SCO53	Poddar, R., Babu, H.	2022	Decision Tree Based IoT Attack Detection in Programmabl(Poddar & Babu, 2022) Language (Poddar & Babu, 2022)	Conference Paper	Lecture Notes in Networks and Systems, 450 LNNS, pp. 671-683.
74 SCO54	Deshpande, K., Rao, M.	2022	An Open-Source Framework Unifying Stream and Batch Processing (Deshpande & Rao, 2022)	Conference Paper	Lecture Notes in Networks and Systems, 336, pp. 607-630
75 SCO55	Singh, A., Satapathy, S.C., Roy, A., Gutub, A.	2022	AI-Based Mobile Edge Computing for IoT: Applications, Challenges, and Future Scope (A. Singh et al., 2022)	Article	Arabian Journal for Science and Engineering,
76 SCO56	Sandhu, K.	2021	Handbook of research on advancing cybersecurity for digital transformation (Sandhu, 2021)	Book	Handbook of Research on Advancing Cybersecurity for Digital Transformation, pp. 1-460
IEEE					
77 IEEE01	Shuai Zhao, Mayanka Chandrashekar, Yugyung Lee, Deep Medhi	2015	Real-Time Network Anomaly Detection System Using Machine Learning (S. Zhao et al., 2015)	Article	11th International Conference on the Design of Reliable Communication Networks (DRCN)
78 IEEE02	Hu Ruipeng	2011	Design and Implementation of Campus Network Intrusion Detection System (R. Hu, 2011)	Conference Paper	International Conference on Intelligence Science and Information Engineering
79 IEEE03	Changwei Huang, Jinquan Xiong, Zhengwen Peng	2012	Applied Research on Snort Intrusion Detection Model in The Campus Network (Huang et al., 2012)	Article	IEEE Symposium on Robotics and Applications(ISRA)
80 IEEE04	Mohd Nazri Ismail, Mohd Taha Ismail	2009	Framework of Intrusion Detection System via Snort Application on Campus Network Environment (Ismail & Ismail, 2009)	Conference Paper	International Conference on Future Computer and Communication
81 IEEE05	Yuanyuan Chen, Wang Yao, Jianghua Luo	2016	Research on the active defense security system based on cloud computing of wisdom campus network (Y. Chen et al., 2016)	Conference Paper	28th Chinese Control and Decision Conference (CCDC)

82 IEEE06	Y.Yasami M.Farahmand V.Zargari	2007	An ARP-based Anomaly Detection Algorithm Using Hidden Markov Model in Enterprise Networks (Yasami et al., 2007)	Conference Paper	Conference: Systems and Networks Communications, 2007. ICSNC 2007. Second International
83 IEEE07	Zhao Kai	2012	Research and design of the distributed intrusion detection system based on Snort (K. Zhao, 2012)	Article	2012 International Conference on Computer Science and Electronics Engineering
84 IEEE08	Minoru Ikebe∗, Daiki Shimokawa† and Kazuyuki Yoshida	2016	Proposal of a malicious communication control method using OpenFlow (Ikebe et al., 2016)	Conference Paper	10th International Conference on Complex, Intelligent, and Software Intensive Systems
85 IEEE09	Ms Rita Dewanjee	2016	Intrusion Filtration System(IFS)- mapping Network Security in new way (Dewanjee, 2017)	Conference Paper	10th International Conference on Complex, Intelligent, and Software Intensive Systems
86 IEEE10	Azam Rashid, Muhammad Jawaid Siddique, Shahid Munir Ahmed	2020	Machine and Deep Learning Based Comparative Analysis Using Hybrid Approaches for Intrusion Detection System (Rashid et al., 2020)	Conference Paper	Conference: 2020 3rd International Conference on Advancements in Computational Sciences (ICACS)
87 IEEE11	Ying-Feng Hsu, ZhenYu He, Yuya Tarutani, Morito Matsuoka	2019	Toward an Online Network Intrusion Detection System Based on Ensemble Learning (Hsu et al., 2019)	Conference Paper	12th International Conference on Cloud Computing (CLOUD)
88 IEEE12	Baoyi Wang, Feng Li, Shaomin Zhang	2009	Research On Intrusion Detection Based On Campus Network (B. Wang et al., 2009)	Article	2009 Third International Symposium on Intelligent Information Technology Application
89 IEEE13	Zheng Wu, Debao Xiao, Hui Xu, Xi Peng, Xin Zhuang	2009	Virtual Inline: A Technique of Combining IDS and IPS Together in Response Intrusion (Wu et al., 2009)	Article	2009 First International Workshop on Education Technology and Computer Science
90 IEEE14	'N. Kussul, A..Shelestov, A. Sidorenko, S. Skakun, Y. Veremeenko	2003	Intelligent Multi-Agent Information Security System (Kussul et al., 2003)(Kussul et al., 2003)	Conference Paper	IEEE Iolematiooal Workshop on Inrelligca Dam Acquisition and Advanced Computing System: Technology and Applications 8~10 September ZWI
91 IEEE15	Zhaoli Liu, Tao Qin, Xiaohong Guan, Hezhi Jiang and Chenxu Wang	2018	An Integrated Method for Anomaly Detection From Massive System Logs (Z. Liu, Qin, et al., 2018)	Article	Special section on security and trusted computing for industrial internet of things
92 IEEE16	'Ying-Feng Hsu, Morito Matsuoka	2020	A Deep Reinforcement Learning Approach for Anomaly Netwon System (Hsu & Matsuoka, 2020)	Conference Paper	Conference: 2020 IEEE 9th International Conference on Cloud Networking (CloudNet)
93 IEEE17	Georgios Androulidakis, Vassilis Chatzigiannakis, and Symeon Papavassiliou,	2009	Network Anomaly Detection and Classification via Opportunistic Sampling (Androulidakis et. al., 2009).	Conference Paper	IEEE Network • January/February 2009
94 IEEE18	'Qingyuan Shan	2022	Wireless network intrusion detection model and safety enhancement framework for campus network (Shan, 2022)	Conference Paper	Proceedings of the Fourth International Conference on Smart Systems and Inventive Technology (ICSSIT-2022)
95 IEEE19	LTC Bruce D. Caulkins, Joohan Lee, Morgan Wang	2005	Packet- vs. Session-Based Modeling for Intrusion Detection Systems (Caulkin et al., 2005)	Conference Paper	Conference: Information Technology: Coding and Computing, 2005. ITCC 2005. International Conference on Volume: 1
96 IEEE20	'Li He, Shunzheng Yu, Min Li	2008	Anomaly Detection Based on Available Bandwidth Estimation (L. He et al., 2008)	Conference Paper	2008 IFIP International Conference on Network and Parallel Computing
97 IEEE21	Chao-Hsi Yeh and Chung-Huang Yang	2008	Design and Implementation of Honeypot Systems Based on Open-Source Software (Yeh & Yang, 2008)	Conference Paper	Conference: Intelligence and Security Informatics, 2008. ISI 2008. IEEE International Conference on
98 IEEE22	Jin Q., Wang L.	2019	Repetido Intranet User-Level Security Traffic Management with Deep Reinforcement Learning (Jin & Wang, 2019)	Conference Paper	Proceedings of the International Joint Conference on Neural Networks
99 IEEE23	'Inadyuti Dutt, Samarjeet Borah, Indrakanta Maitra	2018	A Proposed Machine Learning based Scheme for Intrusion Detection (Dutt et al., 2018)	Conference Paper	Proceedings of the 2nd International conference on Electronics, Communication and

					Aerospace Technology (ICECA 2018
100 IEEE24	Hyunhee Park, Meejoung Kim, Chul-Hee Kang	2009	F-TAD: Traffic Anomaly Detection for Sub-networks Using Fisher Linear Discriminant (Park et al., 2009)	Conference Paper	Conference: Third International Conference on Network and System Security, NSS 2009, Gold Coast, Queensland, Australia, October 19-21, 2009 Authors:
101 IEEE25	'Kai Hwang, Ying Chen, Hua Liu	2005	Defending Distributed Systems Against Malicious Intrusions and Network Anomalies (Hwang et al., 2005)	Conference Paper	Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium (IPDPS'05)
102 IEEE26	Ed Amoroso, Eugene Kogan, Brenda McAnderson, Dan Powell, Brian Rexroad, Steve Schuster, and Anthony Stramaglia	1998	Local Area Detection of Incoming War Dial Activity (Amoroso et al., 1998)	Conference Paper	SRDS '98: Proceedings of the The 17th IEEE Symposium on Reliable Distributed Systems
103 IEEE27	'Chris Herringshaw	1997	Detecting Attacks on Networks (Herringshaw, 1997)	Article	ComputerVolume 30Issue 12December 1997 pp 16–17
104 IEEE28	Xinghua Li, Hengyou Zhang, Yinbin Miao, Siqi Ma, Jianfeng Ma, Ximeng Liu, and Kim-Kwang Raymond Choo	2021	CAN Bus Messages Abnormal Detection Using Improved SVDD in Internet of Vehicles (X. Li et al., 2022)	Article	IEEE INTERNET OF THINGS JOURNAL, VOL. 9, NO. 5, MARCH 1, 2022
105 IEEE29	'Gautam Thatte, Urbashi Mitra, and John Heidemann	2011	Parametric Methods for Anomaly Detection in Aggregate Traffic (Thatte et al., 2011)	Article	IEEE/ACM Transactions on Networking 19(2):512 - 525
106 IEEE30	Muralidaran Gangadharan and Kai Hwang	2001	Intranet Security with Micro-Firewalls and Mobile Agents for Proactive Intrusion Response* (Gangadharan & Hwang, 2001)	Conference Paper	Conference: Computer Networks and Mobile Computing, 2001. Proceedings. 2001 International Conference on
107 IEEE31	'G. Androulidakis and S. Papavassiliou	2007	Intelligent Flow-based Sampling for Effective Network Anomaly Detection (Androulidakis & Papavassiliou, 2007)	Conference Paper	Conference: Proceedings of the Global Communications Conference, 2007. GLOBECOM '07
108 IEEE32	G. Androulidakis, V. Chatzigiannakis and S. Papavassiliou	2007	Using Selective Sampling for the Support of Scalable and Efficient Network Anomaly Detection (Androulidakis et al., 2007)	Conference Paper	Conference: Globecom Workshops, 2007 IEEE
109 IEEE33	'Dong Liu, Chunrui Zhang' and Fang Lou	2021	Terminal Security Protection Anomaly Detection Based on Combined Algorithm (D. Liu et al., 2021)	Conference Paper	2021 International Conference on Intelligent Computing, Automation and Applications (ICAA)
110 IEEE34	Geng Tian∗†, Zhiliang Wang∗‡, Xia Yin∗†, Zimu Li∗‡, Xingang Shi∗‡, Ziyi Lu§, Chao Zhou§, Yang Yu∗†, Yingya Guo∗†	2015	Mining Network Traffic Anomaly Based on Adjustable Piecewise Entropy (G. Tian et al., 2016)	Conference Paper	Conference: 2015 IEEE 23rd International Symposium on Quality of Service (IWQoS)
111 IEEE35	'Cong Dong† , Yufan Chen‡ , Yunjian Zhang† , Yuling Liu† , Zhigang Lu † , Pu Dong †∗, and Baoxu Liu†	2021	BEDIM: Lateral Movement Detection In Enterprise Network Through Behavior Deviation Measurement (Dong et al., 2021)	Conference Paper	IEEE 23rd Int Conf on High Performance Computing & Communications; 7th Int Conf on Data Science & Systems; 19th Int Conf on Smart City; 7th Int Conf on Dependability in Sensor, Cloud & Big Data Systems & Application
112 IEEE36	Ali El Attar, Rida Khatoun and Marc Lemercier	2014	Clustering-based Anomaly Detection for Smartphone Applications (el Attar et al., 2014)	Conference Paper	Conference: NOMS 2014 - 2014 IEEE/IFIP Network Operations and Management Symposium
113 IEEE37	'Kazuya Takemori,∗ and Dennis Arturo	2009	Detection of NS Resource Record based DNS Query Request Packet Traffic and SSH	Article	2009 Second International Conference on Intelligent Networks and Intelligent Systems

	Ludena Roma ˜ na˜ ∗ Shinichiro Kubota,† Kenichi Sugitani,† and Yasuo Musashi		Dictionary Attack Activity (Takemori et al., 2009)		
114 IEEE38	Mr.Siddhant Shah, Mr. Shailesh Pramod Bendale	2020	An Intuitive Study: Intrusion Detection Systems and Anomalies, How AI can be used as a tool to enable the majority, in 5G era. (Shah & Pramod Bendale, 2019)	Article	Project: Security in Software Defined Network
115 IEEE39	'Hong han, Xian-liang lu, li-yong ren, bo chen	2006	Taichi: an open intrusion automatic response system based on plugin (Hong et al., 2006)	Conference Paper	Proceedings of the Fifth International Conference on Machine Learning and Cybernetics
116 IEEE40	Jing Tao, Ning Zheng, Waner Wang, Ting Han, Xuna Zhan, Qingxin Luan	2019	A Behavior Sequence Clustering-based Enterprise Network Anomaly Host Recognition Method (Tao et al., 2019)	Conference Paper	Conference: 2019 IEEE International Conference on Big Knowledge (ICBK)
117 IEEE41	Z. Liu, X. Guan, S. Li, T. Qin, C. He	2018	Behavior Rhythm: A New Model for Behavior Visualization and Its Application in System Security Management (Z. Liu, Guan, et al., 2018)	Article	IEEE Access, 6, 73940-73951.
118 IEEE42	Aditya Patel, Sweta Ghaghda, Payal Nagecha	2014	Model for Security in Wired and Wireless Network for Education (Patel et al., 2014)	Conference Paper	Conference: 2014 International Conference on Computing for Sustainable Global Development (INDIACom)
119 IEEE43	'Xinming Ou, Siva Raj Rajagopalan, Sakthiyuvaraja Sakthivelmuruga n	2009	An Empirical Approach to Modeling Uncertainty in Intrusion Analysis (Ou et al., 2009)	Conference Paper	2009 Annual Computer Security Applications Conference
120 IEEE44	K. Giotis, G. Androulidakis, V. Maglaris	2014	Leveraging SDN for Efficient Anomaly Detection and Mitigation on Legacy Networks (Giotis et al., 2014)	Conference Paper	Conference: Third European Workshop on Software Defined Networks (EWSDN) 2014At: Budapest
121 IEEE45	'Muhammad Salahuddien Manggalanny, Kalamullah Ramli	2017	Real Time DNS Traffic Profiling Enhanced Detection Design for National Level Network (Manggalanny & Ramli, 2017)	Conference Paper	2017 International Seminar on Intelligent Technology and Its Application
122 IEEE46	Shuangwu Chen, Xiang Chen, Zhen Yao, Jian Yang, Yangyang Li, and Feng Wu	2020	Evolving Switch Architecture toward Accommodating In-Network Intelligence (S. Chen et al., 2020)	Article	January 2020IEEE Communications Magazine 58(1):33-39
123 IEEE47	'Chang Liu, Zigang Cao, Gang Xiong, Gaopeng Gou, Siu-Ming Yiu, Longtao He	2018	MaMPF: Encrypted Traffic Classification Based on Multi-Attribute Markov Probability Fingerprints (C. Liu et al., 2019)	Conference Paper	Conference: 2018 IEEE/ACM 26th International Symposium on Quality of Service (IWQoS)
124 IEEE48	Likun Liu, Jiantao Shi, Hongli Zhang, and Xiangzhan Yu	2019	No Way to Evade: Detecting Multi-Path Routing Attacks for NIDS (L. Liu et al., 2019)	Conference Paper	Conference: GLOBECOM 2019 - 2019 IEEE Global Communications Conference
125 IEEE49	'Yasuo Musashi,* Florent Hequet,† Dennis Arturo Ludeña Romaña,† Shinichiro Kubota,* and Kenichi Sugitani*	2010	Detection of Host Search Activity in PTR Resource Record Based DNS Query Packet Traffic (Musashi et al., 2010)	Article	Proceedings of the 2010 IEEE International Conference on Information and Automation June 20 - 23,
126 IEEE50	Nan Jiang∗, Jin Cao†, Yu Jin∗, Li Erran Li†, Zhi-Li Zhang∗	2010	Identifying Suspicious Activities through DNS Failure Graph Analysis (Jiang et al., 2010)	Conference Paper	Conference: Network Protocols (ICNP), 2010 18th IEEE International Conference on
127 IEEE51	'Su He, Xin Zhang, Zhihong Jiang, Hao Kang, Hui Wang	2011	TVMonitor: A P2P-TV Content Monitoring Platform (S. He et al., 2011)	Article	2011 Third International Conference on Multimedia Information Networking and Security

Fuente: Elaboración propia

Evaluación de los estudios.

Se evaluaron los artículos científicos empleando el formulario de extracción de datos detallados en la Tabla 34. En este proceso se consideró los 13 criterios inclusivos descritos en la Tabla 35. Para al final tener como resultado lo descrito en el Anexo C referente a RSL de “Amenazas internas en intranets académicas”, donde se muestra los datos de los artículos y señala los criterios a los que responde.

Se describe el proceso.

Extracción y síntesis de los datos requeridos.

Para la extracción y síntesis de los datos, se utilizó el formulario detallado en la tabla 34 referente a la estrategia de extracción de datos (ACM, SCOPUS, IEEE). En la tabla 37 se muestra un ejemplo de su aplicación.

Este proceso se realizó con los 117 artículos considerados para la RSL.

Tabla 37: **Ejemplo de aplicación del formulario estrategia de extracción de datos (ACM, SCOPUS, IEEE.)**

Id del Estudio	ID:# ID:1
INFORMACIÓN GENERAL	
Título	Software-Defined Networking (SDN) Definition - Open Networking Foundation
Autor (s)	OPEN NETWORKING FOUNDATION
Año de Publicación	2007
Tipo de Referencia	Revista/Conferencia/Reporte/workshop
Editor	ONF
País de Estudio	USA
Entorno de estudio	Industria /Universidad
Tipo de estudio	REPORTE/Encuesta / Experimento / Caso de Estudio, etc.
Artículo Revisado por pares?	SI/NO
Detalle General	Da una visión general del funcionamiento de SDN, atributos y metas en Redes de Campus. El Role de SDN y OpenFlow, Arquitectura simplificada con mayor flexibilidad.
CARACTERISTICAS DEL ESTUDIO E INFORMACIÓN ESPECÍFICA	
Datos y Métodos	Estudio descriptivo. No aplica.
NOTAS SOBRE TEMAS EMERGENTES JUNTO A DETALLES DE SÍNTESIS	
OpenFlow basada en SDN introduce un paradigma de flujo multicapa, que provee mayor control. Políticas granulares que pueden ser aplicadas para individuos o en grupos de flujos en el controlador central, desacoplando políticas del hardware, para diferentes departamentos, diferentes tipos de acceso o usuarios remotos. Políticas de seguridad basadas en contexto del usuario dinámicamente aplicado. Permitirá a las políticas para ser desacoplado del perímetro físico, lo cual es especialmente importante para los móviles Redes de campus son inherentemente múltiples usuarios y deben ser virtualizados para garantizar la aplicación de políticas distintas para los distintos usuarios. SDN basados en OpenFlow proporciona virtualización de la red y la aplicación de políticas granulares de una manera mucho más simple que los métodos convencionales basados en protocolos MPLS y VRF-Lite.	

ANÁLISIS DE CRITERIOS
Criterio de inclusión 2. Hace referencia a Q1

Fase 3: Revisión de la documentación

Escritura de la revisión del reporte.

Los papers evaluados y revisados proceden de tres bases de datos ampliamente utilizadas en investigaciones estas son: ACM, SCOPUS e IEEE. En total se obtuvieron 127 papers, como se pueden observar en la Tabla 36, después de la evaluación se identificaron ocho papers que no daban respuesta a las preguntas, ni a los criterios de inclusión de la investigación o se repetían en los resultados de las búsquedas por lo que no se tomaron en cuenta, tampoco se incluyeron dos libros debido a la generalidad de sus tópicos, sin embargo, se encuentran incluidos en este resumen del resultado de las búsquedas en las bases de datos. En total se han considerado 117 artículos en la RSL siendo este valor el 100%.

La búsqueda en la base de datos ACM se realizó el 6/04/2022 dando como resultado 20 papers, la búsqueda en la base de datos SCOPUS se realizó el 9/06/2022 dando como resultado 56 papers y por último la búsqueda en la base de datos IEEE se realizó el 02/07/2022 dando como resultado 51 papers. El periodo de publicación de los papers comprende desde 1997 al 2022. Cada paper se identifica además según la base de datos, y se incluye una numeración, esta identificación se mantendrá en todo el documento.

La Tabla 38, resume el resultado de las búsquedas en las bases de datos. Muestra los artículos considerados para el presente estudio. Los artículos descartados son los duplicados, sin acceso o no relevantes para el estudio.

Los artículos relevantes son aquellos que cumplieron con los criterios de selección y dan respuesta a las preguntas planteadas.

Tabla 38: **Resumen del Resultado de las Búsquedas en las bases de datos.**

Nombre de la Base de datos	Resultados de búsqueda	Artículos descartados	Artículos relevantes
ACM	20	-	20
SCOPUS	56	SCO05, SCO21, SCO24, SCO41, SCO33, SCO54, SCO55, SCO56	48
IEEE	51	IEEE22, IEEE28	49
TOTAL	**127**	**10**	**117**

Fuente: Elaboración propia

La investigación busca dar respuesta a las preguntas y sus criterios de inclusión definidos anteriormente, a continuación, se presentarán los resultados de cada pregunta y criterio.

Q1. ¿Qué tipos de insiders threat o amenazas internas existen en intranets académicas y cuáles son sus fuentes de datos?

Esta pregunta considera cuatro criterios, según se describe.

Q1.1 Tipos de insiders threat o amenazas internas existentes en redes de datos

Tras la revisión se realizó un listado de todas las amenazas en general mencionadas en la literatura, en la Tabla 39 se puede apreciar los tipos de insiders threat o amenazas internas existentes en redes de datos, detallando: tipo, fuente interna o externa o si no se menciona. El total muestra el número de artículos en los que está presente, porcentaje y los códigos de los papers en los que se identificaron.

Tabla 39: **Q1.1 Tipos de insiders threat o amenazas internas existentes en redes de datos**

Tipos de Ataques o amenazas	Fuente: Interna, externa o no menciona	Total	%	Papers
DDoS, DoS	Interna Externa	46	39.31%	**ACM**: 6, 8, 10, 11, 12, 15, 19, 3 **SCO**: 40, 3, 4, 9, 10, 13, 15, 18, 19, 25, 27, 28, 29, 31, 32, 35, 36, 37, 38, 42, 44, 45, 48, 47, 22, 26, 49 **IEEE**: 6, 11, 17, 21, 25, 31, 32, 35, 38, 39, 42
Malware	Externa Interna	30	25.64%	**ACM:** 1, 6, 8, 11, 15, 18, 19 **SCO:** 40, 4, 3, 11, 15, 29, 32, 36, 37, 38, 44, 45, 48, 50 **IEEE:** 6, 10, 17, 25, 31, 32, 36, 38, 42
Robo de información	Externa Interna	15	12.82%	**ACM:** 14, 5, 17, 20 **SCO:** 17, 9, 11, 13, 23, 28, 29, 50 **IEEE:** 6, 35, 36
Ataques Fingerprint	Interna	13	11.11%	**ACM:** 10 **SCO:** 39, 40, 3, 13, 31, 32, 36, 37 **IEEE:** 21, 25, 32, 39
Robo de identidad y credenciales	Interna	13	11.11%	**ACM:** 14, 5, 17, 20 **SCO:** 17, 39, 11, 23, 25, 32, 37 **IEEE:** 35, 42
Administradores maliciosos o descontentos	Interna	11	9.4%	**ACM:** 6, 13, 18 **SCO:** 17, 40, 14, 23, 43, 44 **IEEE:** 6, 27
Envenenamiento de registros DNS, ARP, IP	Interna	9	7.69%	**ACM:** 15 **SCO:** 9, 37, 44, 47, 26 **IEEE:** 6, 13, 45
Vulnerabilidades informáticas	Interna	9	7.69%	**SCO:** 40, 14, 28, 36, 45, 50 **IEEE:** 10, 26, 35
Abuso de acceso	Interna	8	6.84%	**ACM:** 15 **SCO:** 17, 39, 9, 23, 25, 37

				IEEE: 35
Amenazas Persistentes avanzadas (APT)	Interna Externa	5	4.27%	**ACM:** 5 **SCO:** 16, 42, 43 **IEEE:** 45
Código malicioso, Inyección SQL	Externa Interna	5	4.27%	**ACM:** 11, 10, 15 **SCO:** 40, 16
Errores y desconocimiento de usuarios	Interna	5	4.27%	**ACM:** 14, 13, 15, **SCO:** 17, 39
Phishing	Externa Interna	5	4.27%	**SCO:** 40, 37, 43, 44, 50
Ataque de usuario Root (U2R)	Interna	4	3.42%	**SCO:** 9, 31 **IEEE:** 11, 25
Personas con información privilegiada	Interna	4	3.42%	**ACM:** 1 **SCO:** 13, 37, 43
Remote to local attack R2L	Interna	4	3.42%	**SCO:** 9, 31 **IEEE:** 11, 25
Sabotaje de sistemas y recursos	Interna	4	3.42%	**ACM:** 10, 17, 19 **SCO:** 13
Destrucción de datos	Externa Interna	3	2.56%	**ACM:** 14, **SCO:** 17, 13
Ingeniería social	Externa Interna	3	2.56%	**SCO:** 37, 43 **IEEE:** 35
Ataque de día 0	Externa	2	1.7%	**ACM:** 10, 3
Fraude	Interna	2	1.7%	**SCO:** 39, 23
Man in the Middle	Externa Interna	2	1.7%	**SCO:** 26 **IEEE:** 13
Ataques de diccionario	Externa	1	0.85%	**IEEE:** 25
Ataques de enrutamiento	Interna	1	0.85%	**IEEE:** 48
Ataques de Hackers	Externa Interna	1	0.85%	**ACM:** 18
Ataques de Sondeo	Externa Interna	1	0.85%	**SCO:** 9
Ataques físicos	Interna	1	0.85%	**SCO:** 50
Cross Site Scripting	Interna	1	0.85%	**SCO:** 50
Inanición DHCP	Interna	1	0.85%	**SCO:** 19
Packet sniffing	Externa Interna	1	0.85%	**SCO:** 9

Fuente: Elaboración propia

Para dar respuesta a esta pregunta se tomó en cuenta todas las amenazas mencionadas en los papers en revisión indistinto de su origen interno o externo, pues según la literatura, las amenazas externas debido a las habilidades de los atacantes pueden escalar y penetrar la seguridad de una red fácilmente convirtiéndose en una amenaza interna o insider, esto debido a la combinación de diferentes técnicas de ataque e ingeniería social como se menciona en IEEE30.

Como se puede observar en la Tabla 39 referente a Q1.1 Tipos de insiders threat o amenazas internas existentes en redes de datos. La amenaza interna que más veces ha sido considerada en las investigaciones según la RSL es el ataque de denegación de servicio (DoS) y su variante denegación de servicio distribuido (DDoS) con el 39.31%. Seguido de ataques derivados de malware con el 25.64% entre los cuales destacan virus, gusanos, troyanos entre otros. La amenaza conocida como ransomware, mencionada en SCO45, SCO06 y SCO44 con un índice de daño alto,

aprovecha vulnerabilidades existentes en los sistemas que no se encuentran actualizados, como ejemplo el ransomware Wanacry detallado en SCO45.

También se observa que la amenaza de tipo abuso de acceso, se relaciona con robo de información con un porcentaje de 12.82% o destrucción de datos sensibles e ingeniería social. El abuso de acceso por parte de empleados que se valen de sus credenciales o técnicas de ingeniería social para así obtener permisos y acceso a información que no le corresponde y proceder al robo o secuestro de esta. Estos temas destacan en SCO23 y SCO50, como los objetivos comunes de los insiders.

El desconocimiento de normas de seguridad, principalmente políticas y errores por parte de empleados se menciona en “errores y desconocimiento de usuarios” con el 4.27% como una de las amenazas más importantes para la seguridad con el que pueden aprovechar los atacantes para poder acceder a la red y perpetrar ataques más elaborados como lo señalan en ACM13 y ACM15.

Conclusión: las amenazas internas en redes de datos que más se mencionan como resultado de la RSL en la pregunta Q1.1 son los ataques de denegación de servicio y sus variantes denegación de servicio distribuido con el 39.31%, malware para distintas acciones entre los que destacan Ransomware con el 25.64%. Robo de información con el 12.82%, Ataques Fingerprint y Robo de identidad y credenciales con el 11.11%, Administradores maliciosos o descontentos con el 9.4%, Vulnerabilidades informáticas con el 7.69%, Abuso de acceso con el 6.84% y otras con menor porcentaje.

Q1.2 Tipos de insiders threat o amenazas internas existentes en intranets académicas.

Para dar respuesta a este criterio de inclusión se realizó un listado de todas las amenazas internas existentes en intranets académicas mencionadas en la literatura, luego, se realizó un conteo de las veces que cada amenaza fue mencionada y tratada en los papers, en la Tabla 40 referente a Q1.2 Tipos de insiders threat o amenazas internas existentes en intranets académicas, se muestra el tipo de ataque o amenaza, fuente: Interna, externa o no se menciona. El total como resultado del conteo, porcentaje y los códigos de los papers.

Tabla 40: **Q1.2 Tipos de insiders threat o amenazas internas existentes en intranets académicas.**

Tipos de Ataques o amenazas	Fuente: Interna, externa o no menciona	Total	%	Papers

DoS, DDoS	Externa Interna	16	13.68%	**SCO:** 2, 46, 6, 51 **IEEE:** 3, 5, 8, 12, 24, 29, 37, 42, 43, 44, 49, 50
Malware	Interna Externa	9	7.69%	**SCO:** 2, 51 **IEEE:** 2, 4, 5, 12, 18, 24, 50
Ataques de sondeo de red y aplicaciones	Externa Interna	7	5.98%	**SCO:** 2 **IEEE:** 5, 8, 12, 24, 42, 49
Abuso de acceso	Interna	4	3.42%	**IEEE:** 12, 18, 40, 42
Robo de propiedad intelectual (información)	Externa Interna	3	2.57%	**ACM:** 7 **SCO:** 51 **IEEE:** 3
Ataques de Penetración	Externa	3	2.57%	**SCO:** 2, 46 **IEEE:** 3
Errores de empleados o desconocimiento	Interna	2	1.71%	**ACM:** 7 **IEEE:** 2
Administradores maliciosos o descontentos	Interna	2	1.71%	**ACM:** 7 **IEEE:** 2
Phishing	Interna	2	1.71%	**SCO:** 2 **IEEE:** 49
Ataques Web	Externa Interna	2	1.71%	**SCO:** 46 **IEEE:** 5
Ataques de fuerza Bruta	Externa Interna	2	1.71%	**SCO:** 46, 6
Vulnerabilidades de los sistemas	Interna	2	1.71%	**IEEE:** 2, 44
Destrucción de datos	Interna	2	1.71%	**IEEE:** 3, 42
Ransomware	Externa	1	0.85%	**SCO:** 6
Ataques Heartbleed	Interna	1	0.85%	**SCO:** 46
Sabotaje	Externa Interna	1	0.85%	**IEEE:** 3
Remote to local attack R2L	Interna	1	0.85%	**IEEE:** 12
Ataque de usuario Root U2R	Interna	1	0.85%	**IEEE:** 12
Ataques de diccionario	Externa Interna	1	0.85%	**IEEE:** 37
Ataques Físicos	Interna	1	0.85%	**IEEE:** 37
Ataques de monitoreo	Externa Interna	1	0.85%	**IEEE:** 40

Fuente: Elaboración propia

Conclusión:

Las amenazas internas en redes académicas que más han sido mencionadas según el criterio Q1.2 son los ataques de denegación de servicio y su variante denegación de servicio distribuido con el 13.68%. Malware con el 7.69%, debido al ámbito en donde se desarrollan las actividades educativas es más fácil la propagación de malware por medios físicos es decir unidades extraíbles de los estudiantes y docentes convirtiéndose en una amenaza bastante común en este tipo de redes como se menciona en IEEE18. Ataques de sondeo de red y aplicaciones con 5.98%. Y otras amenazas en menor proporción como: abuso de acceso con 3.42%, robo de propiedad intelectual (información) con el 2.57%, se relaciona con el acceso no autorizado y ataques de sondeo de correo electrónico o puertos, aunque este tipo de amenaza puede provenir del exterior rápidamente puede escalar y convertirse en una

amenaza interna donde los objetivos más comunes son el robo de información de personas con perfiles altos de gerencia como un rector o un jefe de investigación, pero también la información referente a los estudiantes es un objetivo común como se menciona en SCO02.

Además de ataques de penetración con 2.57% y otras amenazas en menor porcentaje.

Q1.3 Principales fuentes de datos de insiders threats.

Entre las preguntas de investigación se analizaron las principales fuentes de datos de insider threat o amenazas internas existentes en intranets académicas. Identificándose tres tipos de fuentes o conjuntos de datos para el manejo de investigaciones de amenazas internas en la literatura, estas son: psicología de usuario, fuente externa y fuente propia.

La fuente psicología de usuario se menciona una única vez en la literatura, en ACM02, hace referencia al comportamiento de empleados o estudiantes ya sea personal o de uso de los recursos de la institución considerando registros de eventos heterogéneos de múltiples dominios, datos psicológicos e información funcional que están disponibles en la organización objetivo.

Las fuentes externas son datos disponibles y de libre acceso, listos para su uso en los que se encuentran datos pertenecientes a diferentes ataques, dentro de estos se encuentran datos de ataques externos, ataques internos, anomalías, registros de acceso, comportamiento de usuarios. Este tipo de datos son de gran ayuda para el entrenamiento de sistemas de detección de intrusos y puesta a prueba de los diferentes sistemas, algoritmos o metodologías propuestas según las necesidades de los investigadores.

De ello resalta el uso del conjunto de datos KDD99 y sus variantes NSL-KDD, Kyoto KDD-Cup, en ACM03, SCO01, SCO09, SCO15, SCO18, SCO31, SCO46, IEEE10, IEEE11, IEEE16, IEEE46, con un porcentaje del 9,4%. Este conjunto de datos KDD99 evalúa la capacidad de su IDS en conjuntos de datos sin procesar y normalizados, contiene 41 características para evaluar métodos de detección de anomalías, donde los ataques se clasifican en cuatro clases principales, como denegación de servicio (DoS), remoto a local (R2L), usuario a remoto (U2R), y sondeo.

El conjunto de datos UNSW-NB15 en IEEE10, IEEE11, IEEE16, IEEE46, con 3,41% es un tráfico sintético con comportamiento malicioso incluye nueve tipos de ataques

como backdoors, DoS, exploits, worms y fuzzers. Está compuesto por 49 características extraídas con herramientas como Argus, Bro-IDS, entre otras.

El conjunto de datos CERT r4.2, descrito en ACM02, ACM05, ACM17, con 2,56 %, conjunto de datos sintético generado en la Universidad Carnegie Mellon, integra diferentes tipos de registros de eventos, incluyendo inicio de sesión/ cierre de sesión, correo electrónico, dispositivo, archivo y HTTP, que capturan los rastros de movimiento de 1000 usuarios en una organización durante 17 meses. Entre ellos hay 7323 instancias de actividad anómalas inyectadas manualmente por expertos en dominios, que representan tres escenarios de amenazas internas.

Para evaluar las principales fuentes de datos externos de insiders threats se realizó un listado y conteo de las menciones en la literatura como se detalla en la Tabla 41, donde se incluye: nombre, descripción, total como resultado del conteo, porcentaje (%) y los códigos de los papers que hacen referencia a la fuente de datos externa.

Tabla 41: **Q1.3 Principales fuentes de datos externos de insiders threats.**

Nombre	Descripción	Total	%	Papers
Conjunto de datos KDD99, NSL-KDD, Kyoto KDD-Cup	El conjunto de datos KDD99 se adopta para evaluar la capacidad de su IDS en conjuntos de datos sin procesar y normalizados, lo que demuestra la tasa de detección mejorada. KDD'99 contiene 41 características para evaluar métodos de detección de anomalías, donde los ataques se clasifican en cuatro clases principales, como denegación de servicio (DoS), remoto a local (R2L), usuario a remoto (U2R), y sondeo.	11	9,4%	**ACM:** 3 **SCO:** 1, 9, 15, 18, 31, 46 **IEEE:** 10, 11, 16, 46
Conjunto de datos UNSW-NB15	Es creado con el uso de la herramienta IXIA Perfect Storm en un pequeño entorno emulado durante 31 horas. La generación de tráfico sintético con comportamiento malicioso incluye nueve tipos de ataques como backdoors, DoS, exploits, worms y fuzzers. Está compuesto por 49 características extraídas con herramientas como Argus, Bro-IDS, entre otras.	4	3.41%	**IEEE:** 10, 11, 16, 46
CERT r4.2	Es un conjunto de datos sintéticos que se creó como parte de un proyecto en la Universidad Carnegie Mellon. Integra diferentes tipos de registros de eventos, incluyendo inicio de sesión/ cierre de sesión, correo electrónico, dispositivo, archivo y HTTP, que capturan los rastros de movimiento de 1000 usuarios en una organización durante 17 meses. Entre ellos hay 7323 instancias de actividad anómalas inyectadas manualmente por expertos en dominios, que representan tres escenarios de amenazas internas.	3	2.56%	**ACM**: 2, 5, 17
Conjunto de datos integral de eventos de ciberseguridad (LANL)	Conjunto de datos integral de eventos de ciberseguridad del Laboratorio Nacional de Los Álamos (LANL). Este conjunto de datos proviene de los Eventos Integrales de Seguridad Cibernética producidos en LANL. Se recopila de los registros de eventos informáticos internos de LANL durante 58 días. LANL anonimizó identificadores cruciales; por lo tanto, se puede acceder públicamente a este conjunto de datos.	3	2.56%	**ACM:** 5 **SCO:** 13 **IEEE:** 35
Conjunto de datos DARPA - 1999	Los conjuntos de datos de DARPA y la Universidad de Nuevo México son los dos conjuntos de datos más utilizados para la evaluación de HIDS. Esos dos	2	1.7%	**ACM:** 3 **IEEE:** 19

	conjuntos de datos solo tienen unos pocos tipos de ataques con una escala de datos pequeña. Creados en el Massachusetts Institute of Technology (MIT) LincolnLab, recogen 7 y 5 semanas de datos de tcpdump sin procesar, respectivamente. Incluyen cuatro tipos de ataques: probe, remote to local, denial of service (DoS), y user to root.			
CAIDA07 – 08, CAIDA DDoS 2007	CAIDA'07 y CAIDA'08 contienen tráfico de ataques DDoS y rastros de tráfico normal. Por lo tanto, el conjunto de datos CAIDA DDoS se puede utilizar para evaluar el modelo de detección de ataques DDoS basado en machine learning.	2	1.7%	**SCO:** 1 **IEEE:** 44
Conjunto de datos ICXS-CSE-CICIDS2018	Es un conjunto de datos generado bajo un enfoque sistemático que se basa en el concepto de perfiles con descripciones detalladas de los escenarios que se desean emular. Según los autores los perfiles α definen escenarios de ataque, mientras que los perfiles β caracterizan el comportamiento normal del usuario, como escribir correos electrónicos o navegar por la web. Instituto Canadiense de Seguridad Cibernética (CIC) proporcionó el conjunto de datos CSE-CICIDS2018, ICIDS2018 incluye siete escenarios de ataque diferentes: Fuerza bruta, Heartbleed, Botnet, DoS, DDoS, ataques web e infiltración de la red desde el interior. La infraestructura de ataque incluye 50 máquinas y la organización de víctimas tiene 5 departamentos e incluye 420 máquinas y 30 servidores. El conjunto de datos incluye las capturas de tráfico de red y registros del sistema de cada máquina, junto con 80 características extraídas del tráfico capturado utilizando CICFlowMeter-V3.	2	1.7%	**SCO:** 46, 49
Registro de acceso a EHR	Registro de salud electrónica, este es un conjunto de datos privados de registros de acceso a EHR reales de un gran centro médico académico, el cual no se menciona.	1	0.85%	**ACM**: 4
Conjuntos de datos públicos de acceso	Datos sin mucha especificación más allá de registros de acceso.	1	0.85%	**ACM**: 4
Listas negras de IP maliciosas	Monitoreo de la darknet (es decir, un conjunto de espacios de direcciones IP no utilizados anunciados a nivel mundial) que se considera como una consecuencia de la actividad maliciosa.	1	0.85%	**ACM**: 8
Black hat USA 2011 doc Simatic S7-1200	Presentado por el investigador de seguridad Dillon Beresford contiene ataques contra el controlador lógico programable (PLC) que en su mayoría son DoS, este documento se llama Simatic S7-1200	1	0.85%	**ACM:** 10
Sistema de control de supervisión y adquisición de datos (SCADA)	El sistema SCADA es una herramienta de automatización y control industrial utilizada en los procesos productivos que puede controlar, supervisar, recopilar datos, analizar datos y generar informes a distancia mediante una aplicación informática. Su principal función es la de evaluar los datos con el propósito de subsanar posibles errores.	1	0.85%	**ACM:** 20
Conjunto de datos Firefox-DS	El conjunto de datos de Firefox es un conjunto de datos HIDS recientemente desarrollado que está disponible públicamente. Creado utilizando técnicas modernas de prueba de penetración como Metasploit, el conjunto de datos contiene trazas de llamadas al sistema normales y anómalas de varios programas.	1	0.85%	**ACM:** 3
ADFA-LD (Linux Dataset)	El ADFA Linux Dataset (ADFA-LD) se creó en el sistema operativo Linux con vulnerabilidades preestablecidas. El conjunto de datos ADFA-LD solo contiene números de llamada al sistema.	1	0.85%	**ACM:** 3
ADFA-WD (Windows Dataset)	ADFA-WD. Microsoft Windows es un sistema informático personal ampliamente utilizado. Como una extensión de ADFA-WD, ADFA-WD: SAA está diseñado para probar la efectividad de HIDS contra "ataques sigilosos basados en Windows" mediante la "elaboración de ataques sigilosos, como Doppelganger, Chimera y Chameleon.	1	0.85%	**ACM:** 3

Conjunto de datos dinámicos de ratón públicos en Github	Características biométricas únicas de dispositivos de entrada como teclados y ratones, el mouse y el teclado se utilizan principalmente como fuente de datos	1	0.85%	**SCO:**17
Bases de datos de vulnerabilidades disponibles en internet	Información relevante acerca de vulnerabilidades conocidas a ciertos sistemas como software o hardware	1	0.85%	**SCO:**49
Repositorios de incidentes de seguridad (RISI)	El Repositorio de Incidentes de Seguridad Industrial (RISI) contiene 228 incidentes notificados que datan de 1982 a 2014, por lo tanto, RISI incluye eventos como incidentes accidentales relacionados con el ciberespacio, así como eventos deliberados como ataques internos y externos	1	0.85%	**SCO:**4
Conjunto de datos DGArchive	Sin especificación	1	0.85%	**SCO:** 47
Conjunto de datos CIRAeCICEDoHBrw2020	Proporcionado por el Instituto Canadiense de Ciberseguridad, analiza el tráfico de DoH en una aplicación para distinguir benigno de malicioso DoH	1	0.85%	**SCO:** 47
Conjunto de datos Cooja Network Simulator	Sin mucha especificación	1	0.85%	**SCO:** 49
Conjuntos de datos de intrusiones estándar	Datos sin muchas especificaciones	1	0.85%	**IEEE:** 23
Flujo de datos en formato IPFix de la red de campus Tsinghua	Flujo en formato IPFIX recopilados de un enrutador de borde de la Red de Campus de la Universidad de Tsinghua para el período del 10 de diciembre de 2014 al 13 de diciembre. La relación de muestreo es de 1:1	1	0.85%	**IEEE:** 34
Conjunto de datos VPNLog	VPNLog Este conjunto de datos proviene de los registros de inicio de sesión de VPN de una empresa.	1	0.85%	**IEEE:** 35
Conjunto de datos Ground Truth	Herramienta para la creación de conjuntos de datos	1	0.85%	**IEEE:** 47

Fuente: Elaboración propia

Finalmente, en lo que se refiere a la fuente de datos propia, son capturas en las redes de datos o a su vez una combinación de datos propio con fuentes de datos externas para así conformar una nueva fuente propia adecuada para las investigaciones.

En (Androulidakis et. al., 2009), con el 1.47 %, se menciona la captura de datos de una red de campus operativo del enlace entre la Universidad Técnica Nacional de Atenas (NTUA) y la Red Griega de Investigación y Tecnología (GRNET) que conecta el campus universitario a Internet. Este enlace tiene un tráfico promedio de 250 Mbps, con servicios de red estándar web, correo electrónico y FTP y aplicaciones P2P.

En la Tabla 42, se muestra con mayor detalle las fuentes de datos propios de insider threat, se menciona: nombre, descripción, herramienta o proceso, total de papers identificados en la literatura, el porcentaje que corresponde y los papers en los que se identifican este tipo de fuentes de datos.

Tabla 42: **Q1.3 Fuentes de datos propios de insider threat.**

Nombre	Descripción	Herramienta/ Proceso	Total	%	Papers
Sin especificar	Datos realistas que se han recopilado de una red real de campus universitarios operativos que consta de más de 4000 anfitriones. Captura de datos del vínculo entre la Universidad Técnica Nacional de	Sin mencionar	2	1.7%	IEEE31 IEEE32

	Atenas (NTUA) y la Red Griega de Investigación y Tecnología (GRNET) que conecta el campus universitario con Internet.				
Sin especificar	Los registros tomados por diferentes herramientas y el valor de los registros de aplicaciones han sido reconocidos como una herramienta valiosa en la detección de eventos, de hecho, los archivos de registro son una fuente de datos importante en esta actividad insider, así como los datos de muchas fuentes diferentes ayudan a definir el comportamiento de una persona con información privilegiada.	Sin mencionar	1	0.85%	ACM01
Datos propios más los datos de CERT r4.2	Obtención de información, como inicio de sesión autenticación/ cierre de sesión, acceso a archivos, uso de correo electrónico y navegación web. Se evalúa el sistema propuesto utilizando el conjunto de datos de amenazas internas CERT r4.2	Sin mencionar	1	0.85%	ACM02
Sin especificar	Las fuentes de datos, como los contenidos generados por el usuario dentro de una organización, los datos biométricos, los IoTSE y los repositorios de codificación pública han recibido mucha menos atención	Sin mencionar	1	0.85%	ACM20
Conjunto de datos de sondeo de correo electrónico	El conjunto de datos original es el registro de datos de inicio de sesión de correo electrónico recopilado de una red de campus. Contiene registros de tráfico de inicios de sesión fallidos. Cada registro incluye la hora de inicio de sesión, la dirección IP de inicio de sesión, el segmento de red de la dirección IP, el nombre de usuario del correo electrónico de inicio de sesión y otros campos, se forma el conjunto de datos de sondeo de correo electrónico de la red del campus.	Sin mencionar	1	0.85%	SCO02
Sin especificar	Fuente propia: registros masivos recopilados del centro de red del campus de la Universidad Xian Jiaotong	Sin mencionar	1	0.85%	SCO20
Sin especificar	Tráfico del puerto TCP 80 de 1,8 mil clientes en una red universitaria durante un período de 24 h. En total, esto corresponde a 205 GB de tráfico de descarga y 7,4 GB de tráfico de carga de 5,7 millones de solicitudes HTTP	Sin mencionar	1	0.85%	SCO29
Conjunto de datos de registro	El conjunto de datos de registro obtenido de la Subdirección de Comunicación de Redes y Datos (BPS)	Almacenó los comportamientos de los usuarios del 28 de febrero al 6 de marzo de 2014.	1	0.85%	SCO30
Datos propios más los datos de ITD UTM	Conjunto de datos: The Intrusion Threat Detection-Universiti Teknologi Malaysia (ITD UTM), sin más especificaciones	Sin mencionar	1	0.85%	SCO32
Sin especificar	Captura en la red de la Universidad de Masaryk y CESNET, la porción de flujos que utilizan el puerto 53 en todo el tráfico.	Sin mencionar	1	0.85%	SCO35
Sin especificar	Para recopilar datos de un entorno corporativo del mundo real, colaboran con un banco nacional con sede en los Estados Unidos para recopilar registros de consultas SQL de su servidor de base de datos.	Sin mencionar	1	0.85%	SCO39
Datos propios (sin especificar) en	Registros de Zeek recopilados en dos redes universitarias University of Virginia	Sin mencionar	1	0.85%	SCO45

conjunto con datos externos	y Virginia Tech. Se utilizaron trazas de malware público para cuatro familias de SPM y variantes propias del malware WannaCry en un entorno virtual.				
Sin especificar	Los datos de flujo de red en tiempo real recopilados de la red de todo el campus de la Universidad de Missouri-Kansas City. El tráfico de red real se recopiló en el centro de datos del campus de la Universidad de Missouri-Kansas City (UMKC).	Sin mencionar	1	0.85%	IEEE01
Sin especificar	Recopilación principalmente dos tipos de registros del sistema: uno es el registro del sistema de los servidores reales y el otro es el registro de anomalías etiquetado del servidor de destino.	Sin mencionar	1	0.85%	IEEE15
Datos propios en conjunto con datos externos	Utilización de NSL-KDD, UNSW-NB15, AWID, Conjunto de datos de registro del sistema de C. Palo Alto Networks (PANW) y un registro de red de campus real, a nuestro entorno de red de campus, que consta de aproximadamente 300 millones de registros diarios de tráfico de red y es aproximadamente 100 veces más grande que los conjuntos de datos sintéticos.	Sin mencionar	1	0.85%	IEEE16
Sin especificar	Captura de datos de una red de campus operativo. Más específicamente, el vínculo entre la Universidad Técnica Nacional de Atenas (NTUA) y la Red Griega de Investigación y Tecnología (GRNET) que conecta el campus universitario a Internet. Este enlace tiene un tráfico promedio de 250 Mb / s, que contiene una rica combinación de tráfico de red que transporta servicios de red estándar como Web, correo electrónico y ftp, así como tráfico de aplicaciones p2p.	Sin mencionar	1	0.85%	IEEE17
Sin especificar	Datos de la Universidad de Corea. Se utiliza el tráfico que no representa el tráfico generado por la red troncal de Internet	Sin mencionar	1	0.85%	IEEE24
Sin especificar	Utilización de un conjunto de datos, que contiene una mezcla de aplicaciones normales y anormales (dos clusters de aplicaciones normales y tres clusters de aplicaciones maliciosas)	Sin mencionar	1	0.85%	IEEE36
Datos propios en conjunto con datos externos	Conjunto de datos: NSL-KDD, UNSW-NB15 y el registro de la red de Palo Alto recolectado en una red de campus (sin especificar)	Sin mencionar	1	0.85%	IEEE11

Fuente: Elaboración propia

Conclusión: En la RSL se ha podido identificar tres tipos de fuentes de datos: Psicología de usuarios, fuente de datos externa y fuentes de datos propias. Como se observa en la Tabla 36 las principales fuentes de datos externos de insiders threats, más utilizadas en la literatura con un porcentaje de 9.4% es el conjunto de datos KDD99, NSL-KDD, Kyoto KDD-Cup que es principalmente utilizado para la evaluación de sistemas de detección de intrusos, donde los ataques se clasifican en denegación de servicio (DoS), remoto a local (R2L), usuario a remoto (U2R), y sondeo.

El conjunto de datos UNSW-NB15 con 3,41% genera tráfico sintético con comportamiento malicioso incluye ataques como backdoors, DoS, exploits, worms y fuzzers. Y el conjunto de datos CERT r4.2, con 2,56 % es un conjunto de datos sintético generado en la Universidad Carnegie Mellon, integra registros de eventos incluyendo inicio de sesión/ cierre de sesión, correo electrónico, dispositivo, archivo y HTTP en las que hay instancias de actividad anómalas de amenazas internas.

Por otro lado, las fuentes de datos propios de insider threat como se observa en la Tabla 42, son datos capturados en las redes de datos o a su vez una combinación de estos datos con fuentes de datos externas para así conformar una nueva fuente propia adecuada para las investigaciones.

En fuentes de datos propias por lo general no especifican nombres del conjunto de datos, más se señala el origen de los datos, y una idea general del tráfico y los datos, no se repiten más que en el caso de datos de campus universitarios de la Universidad Técnica Nacional de Atenas (NTUA) y la Red Griega de Investigación y Tecnología (GRNET) que conecta el campus universitario con Internet. Además, tenemos un conjunto de gran cantidad de datos compilados en redes de campus que incluyen tráfico como: sondeo de correo electrónico, registros de tráfico de inicios de sesión fallidos, tráfico del puerto TCP, solicitudes HTTP, flujos que utilizan el puerto 53 en todo el tráfico, etc.

De la RSL, se determinó que, si bien existen diferentes fuentes de datos externas que se utilizan para el análisis de pruebas en lo que se refiere a datos propios de amenazas internas en redes de campus académicas son muy limitadas y no se da mayor detalle al respecto, existiendo un vacío en el conocimiento. Por lo que se debe realizar un análisis de amenazas internas en una intranet de un campus universitario con el objetivo de capturar data propia e identificarla con mayor detalle para el control, lo que sustenta la presente investigación que servirá de base para estudios futuros.

Q1.4 ¿Cuántas investigaciones mencionan considerar insider threat para limitar el control de acceso a usuarios en intranets?

Durante la revisión de la literatura se identificaron 17 papers que mencionaron el control de acceso como medida ante amenazas en sus redes, estos son: ACM04, ACM05, ACM06, ACM07, ACM11, ACM14, ACM19, SCO07, SCO08, SCO13, SCO34, SCO37, SCO44, SCO26, SCO50 e IEEE01, IEEE39; como se observa en a Tabla 43, se incluye: métodos de control de acceso, descripción, total, porcentaje (%) y papers.

Tabla 43: Papers que mencionan considerar insider threat para limitar el control de acceso a usuarios en intranets.

Menciones de control de acceso				
Métodos de control de acceso	**Descripción**	**Total**	**%**	**Papers**
Utilización de firewall de red.	Menciona que la tecnología de firewall de red se utiliza para fortalecer el control de acceso entre redes, evitar que los usuarios de redes externas ingresen a la red a través de medios ilegales, acceder a los recursos de la red interna y proteger el entorno operativo.	3	2.56%	ACM14 ACM19 IEEE39
	El firewall tradicional se encuentra entre dos o más redes. Se implementa filtrado de paquetes ACL (lista de control de acceso) como una técnica de defensa importante que protege la seguridad de la red interna. Las políticas de control de acceso supervisan los datos que fluyen mediante reglas de acceso.			
	Un firewall tiene un alto control de acceso sobre el tráfico de red. Si el sistema de respuesta a intrusiones colabora con el firewall, puede bloquear la mayoría de los ataques.			
Variantes de control de acceso: AMM, RBAC, TBAC, TeBAC para evitar exposiciones.	Existen tecnologías que se han desarrollado para proteger la información de personas internas, incluidas las muchas variantes de control de acceso para evitar exposiciones. El modelo de matriz de acceso (AMM), El control de acceso basado en roles (RBAC), modelo de control de acceso basado en tareas (TBAC), El control de acceso basado en equipos (TeBAC).	2	1.7%	ACM04 SCO50
Control de inicio de sesión	Se menciona que se puede analizar las operaciones de inicio de sesión del usuario para detectar las anomalías	2	1.7%	ACM05 SCO07
	Hay mucho trabajo centrado en el comportamiento anormal de inicio de sesión de los usuarios o hosts en movimiento lateral.			
Honeypots para entender el comportamiento de usuarios.	La utilización de honeypots y sus variantes puede ayudar a entender el comportamiento de los usuarios de la red.	1	0.85%	ACM06
Registros específicos de cada plataforma	La mayoría de los servidores y aplicaciones están protegidos por mecanismos de control de acceso y registro que a menudo son específicos de la plataforma.	1	0.85%	ACM07
Denegar acceso según niveles de confianza	Menciona que el problema es la confianza con los usuarios por lo que denegar a los usuarios el acceso a otros datos es un punto que se trata.	1	0.85%	ACM11
Patrones de comportamiento.	Menciona la utilización de herramientas para la captura de patrones de comportamiento.	1	0.85%	SCO08
Gestión de recursos de red en función de las credenciales y política de seguridad.	Los métodos defensivos genéricos se pueden dividir en tres tipos: técnicas de autenticación para identificar las entidades en un sistema y entre sistemas, control de acceso para proporcionar o limitar selectivamente los recursos de red en función de las credenciales y política de seguridad que se manifiesta como un cierto conjunto de reglas para mejorar la inmunidad del sistema contra las amenazas internas.	1	0.85%	SCO13
Gestión de acceso con herramientas criptográficas	Menciona la utilización de herramientas criptográficas como la autenticación mutua que asegura las identidades de cada extremo en una comunicación, el cifrado y la gestión de claves, que impone el control de acceso	1	0.85%	SCO34
Framework para prevención de comportamientos maliciosos de usuarios internos.	Este articulo menciona, mediante el monitoreo y control tanto del acceso del usuario para abordar las amenazas internas.	1	0.85%	SCO37
Problemas de autenticación	Los problemas de autenticación si no se abordan adecuadamente, pueden verse comprometidos por un empleado interno y obtener privilegios de acceso.	1	0.85%	SCO44

Control de Direcciones MAC para tener acceso.	Los piratas informáticos pueden utilizar direcciones MAC para obtener acceso.	1	0.85%	SCO26

Fuente: Elaboración propia

Conclusión:

En relación con las investigaciones que consideran insider threat para limitar el control de acceso a usuarios en intranets, el 2.56% utiliza firewall de red en ACM14, para fortalecer el control de acceso entre redes, evitar que los usuarios de redes externas ingresen a la red a través de medios ilegales, acceder a los recursos de la red interna y proteger el entorno operativo. Se menciona además en ACM19, el uso de filtrado de paquetes ACL como una técnica de defensa importante que protege la seguridad de la red interna, políticas de control de acceso que supervisan los datos que fluyen mediante reglas de acceso. IEEE39, menciona la importancia de combinar el sistema de respuesta a intrusiones con el firewall, para bloquear la mayoría de los ataques.

Se presenta variantes de control de acceso para evitar exposiciones, en 1.7 % en ACM04 y SCO50 que hace referencia a tecnologías desarrolladas como AMM, RBAC, TBAC, TeBAC para proteger la información de personas internas, incluidas variantes de control de acceso para evitar exposiciones.

Control de inicio de sesión para detectar anomalías en base al comportamiento anormal de los usuarios o hosts considerándose en el 1.7% como menciona ACM05 y SCO07.

ACM05 presenta políticas de control de acceso, en tres categorías; obligatorio, basado en roles y discrecional, como mecanismos de autenticación y autorización para garantizar que solo los usuarios legítimos con las credenciales requeridas puedan acceder a los datos.

En otros estudios se mencionan en el 0.85% donde se hace referencia a honeypots para entender el comportamiento de usuarios en ACM06. Registros específicos de cada plataforma en ACM07. Denegar acceso según niveles de confianza en ACM11. Patrones de comportamiento en SCO08. Gestión de recursos de red en función de las credenciales y política de seguridad en SCO13. Gestión de acceso con herramientas criptográficas en SCO34. Framework para prevención de comportamientos maliciosos de usuarios internos en SCO37. Problemas de autenticación en SCO44 y Control de Direcciones MAC para tener acceso en SCO26.

De lo revisado destacan métodos de control de acceso basados en firewall, ACL, mecanismos de autenticación y autorización para garantizar que solo los usuarios

legítimos puedan acceder a los datos. Estudios como el presente permite hacer una revisión del estado del arte determinar métodos y/o técnicas utilizadas en el control de amenazas internas, dando la pauta para conocer su tratamiento.

Q2. ¿Qué herramientas, métodos o procedimientos de recolección de datos se emplean en el análisis de insiders threat, además que métodos de identificación o detección de amenazas se emplean?

Esta pregunta considera siete criterios desde Q2.1 a Q2.7.

Q2.1 ¿Qué herramientas, métodos o procedimientos de recolección de datos se emplean en el análisis de insiders threat?

Como se mencionó en el criterio de inclusión Q1.3 un tipo de fuente de datos para el entrenamiento de los sistemas o algoritmos utilizados en la literatura es la fuente propia, esta se complementa con herramientas, métodos o procedimientos para la toma de datos, la Tabla 44 describe herramientas o métodos de recolección de datos, total, porcentaje y papers.

Tabla 44: **Q2.1 Herramientas o métodos de recolección de datos**

Herramientas / Métodos	Total	%	Papers
Captura en formatos pcap mediante puertos espejo; herramientas TCPDump, Ethereal, TCPReplay.	14	11.97%	**ACM:** 9 **SCO:** 8, 12, 28, 29, 32, 38, 46, 47, 26 **IEEE:** 2, 3, 8, 19
Utilización de IDS y sus variantes (HIDS, NIDS, AIDS, SIEM, SNORT, SEBEK).	11	9.4%	**ACM:** 1, 6, 8, 14, 22 **SCO:** 16, 36 **IEEE:** 3, 4, 6, 45
Herramienta o método sin especificar.	10	8.55%	**SCO**: 2, 11, 22 **IEEE:** 1, 14, 36, 37, 40, 47, 49
Utilización de Honeypots y sus variantes (Honeynets, Honeytokens, entre otros).	5	4.27%	**ACM:** 6, 9, 12 **SCO:** 36 **IEEE:** 5
Sistema de monitoreo de amenazas (NICTER); Wireshark.	3	2.56%	**ACM:** 8, 10, 26
Utilización de protocolos Sflow y Openflow.	2	1.71%	**SCO:** 8, 46
Utilización de Winpcap.	2	1.71%	**IEEE:** 7, 51
Herramienta propia sin especificaciones.	1	0.85%	**ACM:** 7
Métodos estadísticos de recolección de datos (recolección métrica) Ej: Flowsense.	1	0.85%	**SCO:** 8
Herramientas propias basadas en SDN de Microsoft.	1	0.85%	**SCO:** 28
Herramienta Switched port analyzer	1	0.85%	**SCO:** 37
Programa Bind 9.2.6	1	0.85%	**SCO:** 51
Método propio en base a herramientas como Flume, HDFS (Hadoop Distributed file System) y Spark	1	0.85%	**IEEE:** 15
Utilización de un sistema de análisis de comportamiento de red NBA	1	0.85%	**IEEE:** 20
Utilización de método propio (WISEMon)	1	0.85%	**IEEE:** 24
Threat Intrusion Detection and Prevention Engine (TIDPE) (Propuesta)	1	0.85%	**SCO:** 6

Fuente: Elaboración propia

Conclusión: Como resultado de la RSL se obtuvo que el conjunto de herramientas TCPdump, Ethereal y TCPReplay para la captura datos en formatos PCAP mediante puertos espejo son las más utilizadas representando un porcentaje de 11.97%. Seguido de la utilización de IDS y sus variantes (HIDS, NIDS, AIDS, SIEM, SNORT, SEBEK) con un porcentaje 9.4%, estas se relacionan ya que ciertos IDS utilizan TCPdump para la captura de datos y su posterior análisis. Sin embargo, llama la atención que en tercer lugar con el 8.55% se realice una captura de datos con herramientas o métodos sin especificar, se resalta que este porcentaje es bastante cercano al de los primeros lugares como se observa en la Tabla 44.

Como apartado final, SCO28 resalta el uso de nuevas herramientas o métodos propios que no se especifican y que se sugieren como alternativa a mecanismos tradicionales de captura de paquetes, como la duplicación de puertos (puerto espejo) considerándoles inviables desde una perspectiva de escala y costo, al necesitar el uso de puertos físicos.

Q2.2 ¿Qué procedimientos se emplean para realizar mediciones de data de insiders threats en intranets académicas?

Durante la RSL se detectó cuatro papers que dan respuesta a este criterio, los dos primeros respecto a redes en general, SCO35, e IEEE36 y los dos restantes en redes de campus ACM07 e IEEE03.

Conclusión: Respecto a los procedimientos que se emplean para realizar mediciones de data de insiders threats, se ha identificado cuatro papers con un porcentaje de 3.42% que dan respuesta a este criterio. Los dos primeros referente a redes en general, SCO35, e IEEE36 y en los dos restantes en redes de campus ACM07 e IEEE03.

En redes de campus, ACM07 propone un enfoque de bajo costo hacia amenazas internas. La solución captura las acciones extremadamente detalladas de los usuarios de la red en todas las aplicaciones y las correlaciona con el contexto del directorio para rastrear y hacer cumplir las políticas institucionales en toda la red del campus. Con el software "Real Time Analyzer" analiza las transacciones capturadas para proporcionar inteligencia y mitigar las amenazas internas. El módulo analiza e informa las excepciones, así como automatiza las auditorías operativas y de seguridad.

IEEE03 analiza los paquetes de datos de acuerdo con el modelo de protocolo de paquetes TCP/IP mediante la tecnología de detección SNORT. El valor de algunos campos especiales y el protocolo correspondiente coinciden, a fin de determinar el protocolo, y luego el patrón de ataque de detección se corresponde con la coincidencia de patrón.

De los resultados se determina que, si bien se hacen referencia a los procedimientos para realizar mediciones de data de insiders threats en intranets académicas, estos son sin muchas especificaciones. Entonces resalta el hecho que es un campo en el que no se ha desarrollado muchos estudios, ni existe un estándar para realizar este tipo de procesos.

Q2.3 ¿Qué método de detección de mal uso o detección de anomalías o comportamientos anómalos emplea en el contexto de detección de intrusiones de insiders threat?

La Tabla 45 muestra los resultados obtenidos durante la revisión en este criterio, se utilizó el mismo proceso que en lo criterios anteriores es decir se definió la herramienta, método o tipo de algoritmo utilizado, así como el total de menciones que se contabilizaron en la revisión, además junto a esto se detalla los papers en lo que se menciona su utilización.

Tabla 45: **Q2.3 Método/Herramientas de detección de mal uso o detección de anomalías de intrusiones de insiders threat.**

Métodos/Herramientas	Total de menciones	Porcentaje	Papers
Uso de IDS y sus variaciones	50	42.74%	**ACM:** 1, 10, 12, 14, 18, 20, 16, 3 **SCO:** 1, 40, 4, 9, 12, 18, 16, 25, 27, 30, 31, 32, 34, 36, 37, 43, 44, 46, 48, 6, 7, 26, 50 **IEEE:** 7, 9, 10, 11, 13, 16, 19, 21, 23, 25, 26, 27, 30, 32, 33, 38, 39, 45, 48
Inteligencia Artificial, Aprendizaje automático, CNN, KNN, RNN, PCA, SVM, ML, DL	34	29.06%	**ACM:** 2, 4, 8, 5, 17, 18, 19, 20, 16, 3 **SCO:** 39, 40, 4, 3, 11, 12, 13, 15, 18, 28, 42, 45, 46, 48, 47, 49 **IEEE:** 10, 11, 23, 32, 35, 38, 45, 46
Comparación de comportamiento de usuarios	13	11.11%	**ACM:** 2, 3 **SCO:** 17, 39, 11, 13, 23, 16 **IEEE:** 6, 20, 32, 33, 36
Frames de monitoreo y detección	10	8.55%	**ACM:** 2, 4, 5 **SCO:** 35, 39, 13, 38 **IEEE:** 24, 31, 47
Uso de honeypots, honeynets honeytokens	8	6.84%	**ACM:** 6, 12 **SCO:** 16, 36, 38, 43 **IEEE:** 13, 21
Firewall	6	5.13%	**ACM:** 14, 19 **SCO:** 16 **IEEE:** 21 30, 39
Minería de datos	6	5.13%	**ACM:** 3 **SCO:** 12, 20, 16, 28, 30
Modelo oculto de Márkov	4	3.42%	**ACM:** 3 **SCO:** 11, 22 **IEEE:** 6

Soluciones SDN, Conjunción Sflow y Openflow	4	3.42%	**SCO:** 8**,** 10, 25, 22
Entropía	3	2.56%	**SCO:** 31 **IEEE:** 34, 49
Analizadores de vulnerabilidades en red	2	1.71%	**SCO:** 14, 40
Modelo basado en gráficos	1	0.85%	**ACM:** 2
Modelo basado en reglas	1	0.85%	**ACM:** 2
Relación de concordancia de reglas	1	0.85%	**ACM:** 2
Proyección espectral de datos	1	0.85%	**ACM:** 4
Uso de reglas bayesianas	1	0.85%	**ACM:** 3
Uso del algoritmo de ventana deslizante	1	0.85%	**ACM:** 3
Modelo de bolsa de palabras	1	0.85%	**ACM:** 3
Método basado en secuencias de enumeración (STIDE)	1	0.85%	**ACM:** 3
Uso de teoría de conjuntos aproximados	1	0.85%	**ACM:** 3
Soluciones basadas en la teoría de la información	1	0.85%	**SCO:** 3
Criptografía y soluciones basadas en certificados	1	0.85%	**SCO:** 19

Fuente: Elaboración propia

Conclusión: En base a los resultados se concluye que la utilización de sistemas de detección de intrusos (IDS) y sus diferentes variantes como son NIDS y HIDS, entre otros, con un porcentaje de 42.74% son los más utilizados para la detección de anomalías con captura de datos en formato PCAP. Seguido se presenta la utilización de algoritmos de inteligencia artificial, aprendizaje automático, aprendizaje profundo representando el 29.06% para el entrenamiento de los sistemas o herramientas que los investigadores proponen. Una mención para considerar en tercer lugar con el 11.11% es la comparación de comportamiento de los usuarios en diferentes horas del día según las funciones que realicen esto se podría relacionar con un tipo de fuente de datos como los son las fuentes de datos de psicología de usuarios.

Q2.4 ¿Qué método de detección de mal uso o detección de anomalías o comportamientos anómalos se emplea en el contexto de detección de intrusiones de insiders threat en intranets académicas?

La Tabla 46 describe Q2.4 Métodos/Herramientas de detección de anomalías de insiders threat en intranets académicas, mostrando los resultados obtenidos durante la revisión en este criterio. Se definió la herramienta, método o tipo de algoritmo utilizado, así como el total de menciones que se contabilizaron en la revisión, junto a esto se detalla los papers en lo que se menciona su utilización.

Tabla 46: **Q2.4 Métodos/Herramientas de detección de anomalías de insiders threat en intranets académicas.**

Métodos/Herramientas	Total de menciones	Porcentaje	Papers
Uso de IDS y sus variaciones	14	11.97%	**SCO:** 29, 51 **IEEE:** 2, 3, 4, 5, 8, 12, 14, 24, 42, 43, 44, 50
Uso de honeypots, honeynets, honeytokens	3	2.56%	**ACM:** 9 **IEEE:** 5, 14

Inteligencia Artificial, Aprendizaje automático, CNN, KNN, RNN, PCA, SVM, ML, DL	3	2.56%	**IEEE:** 1, 3, 14
Comparación de comportamiento de usuarios	2	1.71%	**SCO:** 2 **IEEE:** 40
Minería de datos y gráficos	2	1.71%	**SCO:** 2 **IEEE:** 12
Marcos de monitoreo y detección	2	1.71%	**IEEE:** 1, 17
Herramientas de monitoreo	2	1.71%	**IEEE:** 1, 18
Entropía	2	1.71%	**IEEE:** 17, 37
Heurística	1	0.85%	**SCO:** 29
Firewall	1	0.85%	**IEEE:** 5
Soluciones SDN, Conjunción Sflow y Openflow	1	0.85%	**IEEE:** 8

Fuente: Elaboración propia

Conclusión: Tras la revisión se concluye que el método más utilizado para la detección de anomalías en redes académicas son los sistemas de detección de intrusos y sus diferentes variantes con un porcentaje de 11.97%, tiene relación a que estos sistemas suelen trabajar como herramientas de captura de datos en formatos PCAP lo que es de gran ayuda para el análisis posterior en base a las necesidades de los investigadores en el ambiente académico. De los resultados, en segundo lugar, se nombra al uso de honeypots, honeynets, honeytokens en un porcentaje del 2.56% como mencionan ACM09, IEEE05, IEEE14. En igual porcentaje métodos donde se aplica Inteligencia Artificial, aprendizaje automático, CNN, KNN, RNN, PCA, SVM, ML, DL, como se menciona en IEEE01, IEEE03, IEEE14.

Y en tercer lugar la comparación de comportamiento de usuarios con el 1.71%, SCO02, e IEEE40.

Q2.5 ¿Qué método se usa para identificar insiders threat en tiempo real (Real Time usage profiling)?

Los resultados de este criterio se describen en la Tabla 47, donde se incluye: nombre, descripción, característica, total de menciones, porcentaje y papers de la RSL en que se identificaron.

Tabla 47: **Q2.5 Métodos para identificar insiders threat en tiempo real.**

METODOS O HERRAMIENTAS PARA DETECCION EN TIEMPO REAL					
Nombre	**Descripción**	**Característica**	**Total**	**%**	**Papers**
IDS/IPS	Sistemas de detección de intrusos y sistemas de prevención de intrusos; basado en coincidencia de reglas, SNORT.	Herramienta	5	4.27%	**SCO:** 40, 9 **IEEE:** 3, 4, 5
CADS	Sistema de detección de anomalías basado en la comunidad, un marco de aprendizaje no supervisado para detectar amenazas internas basado en información registrada en los registros de acceso (logs) de entornos colaborativos (CIS).	Herramienta Propuesta	1	0.85%	**ACM:** 4
Sin mencionar	El enfoque propuesto proporciona una solución de bajo costo y rápida implementación, ya que no se requieren cambios en la red. La propuesta de	Enfoque Propuesto	1	0.85%	**ACM:** 7

	seguimiento y alerta en tiempo real garantiza la alerta temprana y también detiene proactivamente las transacciones en curso sin degradar el rendimiento. (Sin probar aún)				
Sin mencionar	Red virtual distribuída. Consiste en un centro de control maestro y una serie de honeynets virtuales basados en la virtualización a nivel de sistema operativo.	Herramienta Propuesta	1	0.85%	**ACM:** 12
NRTSAPD	Metodología de evaluación de riesgos de NRTSAPD la cual proporciona un enfoque de evaluación de riesgos rápido para que la administración se dé cuenta del estado actual del riesgo.	Metodología (Enfoque)	1	0.85%	**ACM:** 13
Sin mencionar	Detección de intrusiones en tiempo real, sin más especificaciones	Herramientas sin especificar	1	0.85%	**ACM:** 19
Sin mencionar	Mecanismo de detección de uso indebido basado en reglas, sin especificar.	Herramientas sin especificar	1	0.85%	**SCO:** 39
Sin especificar	Plataforma de detección y mitigación de anomalías, en tiempo real y basada en modelos sin especificar.	Herramienta propuesta	1	0.85%	**SCO: 8**
Sin especificar	Esquema de administración de seguridad de ciclo de vida completo a nivel de usuario para el tráfico de intranet, desde la detección de anomalías hasta la ejecución de mitigación en línea.	Método Propuesto	1	0.85%	**SCO:** 13
Collasoft y Cascade	Herramientas para la captura de datos y lectura de archivos Pcap en línea.	Herramientas	1	0.85%	**SCO:** 32
SIEM	Proporciona un análisis en tiempo real de la vulnerabilidad de la red y la aplicación mediante la interpretación y visualización de los registros.	Herramienta	1	0.85%	**SCO:** 6
Network Flow Guard for ARP (NFGA)	Adecuada para denegar la suplantación de ARP en tiempo real.	Herramienta Propuesta	1	0.85%	**SCO:** 26
Apache Kafka y Apache Storm en conjunto con SDN.	Encargadas para el procesamiento de big data para satisfacer la creciente necesidad de procesamiento en tiempo real de datos de transmisión. Trabaja en conjunto al sistema propuesto.	Herramienta Propuesta	1	0.85%	**IEEE:** 1
Análisis dinámico y estático	Resultado de su investigación en literatura. Sistema para detectar y prevenir ataques de inyección SQL utilizando técnicas de análisis híbrido dinámico y estático.	Método	1	0.85%	**IEEE:** 38
Sin mencionar	Diseño mejorado para detectar tráfico DNS malicioso para redes de alta velocidad, a gran escala, a nivel nacional, casi en tiempo real.	Herramienta Propuesta	1	0.85%	**IEEE:** 45
RealSecure de Internet Security Systems	Sistemas en tiempo real en internet, sin más especificaciones.	Herramientas	1	0.85%	**IEEE:** 27

Fuente: Elaboración propia

Conclusión: La RSL determinó los métodos que se usan para identificar insiders threat en tiempo real, respecto del criterio Q2.5, determinándose como el principal método, la utilización de sistemas de detección y prevención de intrusos basado en coincidencia de reglas, principalmente SNORT en un porcentaje de 4.27%, citado en SCO40, SCO09, IEEE03, IEEE04, IEEE05. Además de varias propuestas con 0.85 % como ACM04, CADS que es un sistema de detección de anomalías basado en un marco de aprendizaje no supervisado para detectar amenazas internas, o la propuesta de un nuevo algoritmo de predicción de

anomalías en SCO08 donde se señala que la medición de la red es uno de los temas clave para la detección y mitigación de intrusiones en tiempo real.

Y otras en las que no se menciona el nombre, y que se proponen como de seguimiento y alerta en tiempo real como en ACM07, también honeypots virtuales para la detección de intrusos en ACM12. Se incluye nuevos sistemas o herramientas para la mitigación de ataques externos o internos en general o específicos a tiempo real, que han ido evolucionando como en IEEE27 donde los sistemas de red basados en Internet e intranet se convierten en herramientas invaluables que las empresas pueden utilizar para compartir información y realizar negocios con socios en línea. No se debe olvidar que los hackers también han aprendido a utilizar estos sistemas para acceder a redes privadas y sus recursos por lo que la utilización de un sistema en tiempo real puede ayudar a combatir ataques.

Q2.6 ¿Qué algoritmo de análisis de data emplean en la identificación de insiders threats?

La RSL menciona la utilización de algoritmos para diferentes tipos de investigación o propuestas, cabe indicar que la utilidad de estos algoritmos es distinta, pero con un solo objetivo como la detección de anomalías en red por parte de usuarios externos e internos o malos usos de aplicaciones. A continuación, se presentan los algoritmos utilizados en las investigaciones y propuestas revisadas en la Tabla 48 con parámetros que incluyen: nombre, descripción, total, porcentaje y papers.

Tabla 48: **Q2.6 Algoritmo de análisis de data para la identificación de insiders threats.**

Nombre	Descripción	Total	%	Papers
Algoritmos de Machine Learning (ML) aprendizaje automático, como k-NN, Naive Bayes, k-means y k-medoids, CNN, SVM, DT, NB, Random forest	Algoritmos utilizados en conjunto con un IDS para clasificar los flujos de tráfico como normales y anormales y encontrar un conjunto de hosts con comportamientos anómalos.	10	8.55%	**SCO:** 9, 18, 23 **IEEE:** 1, 10, 15, 23, 33, 45, 46
Algoritmo propio propuesto	Algoritmo de fuente propia utilizado en las diferentes investigaciones.	7	5.98%	**ACM:** 8 **SCO:** 2, 8, 22, 49 **IEEE:** 29, 49
Algoritmos de detección propios de un IDS	En el núcleo de cualquier sistema de detección de intrusos está el algoritmo de detección. El algoritmo de detección es responsable de la identificación de patrones y/o eventos secuenciados en el tiempo que pueden ser maliciosos.	5	4.27%	**ACM:** 1, 17 **IEEE:** 3, 11, 48
Sin especificar	Se menciona la utilización, pero no se detalla el funcionamiento o datos referentes al algoritmo.	4	3.42%	**SCO:** 19 **IEEE:** 2, 27, 34

Algoritmos de agrupación (Método de Lovaina)	En la interconexión y modularidad, se puede deducir diferentes comunidades en un conjunto de datos.	2	1.71%	**ACM:** 2, 17
Algoritmo de Clustering propuesto; diferentes versiones	Una versión más eficiente que el tradicional algoritmo de clustering.	2	1.71%	**ACM:** 5 **IEEE:** 36
El aprendizaje Monte Carlo, Q-learning, Deep Q Networks	Algoritmos de aprendizaje por refuerzo más comunes utilizados para detectar tráfico de botnet.	2	1.71%	**SCO:** 1 **IEEE:** 16
Threshold Random Walk con Credit-Based Algorithm (TRW-CB)	Propuesta realizada por los investigadores, pero no se detalla el funcionamiento ni especifica las líneas de código; se menciona en otra investigación.	2	1.71%	**SCO:** 25, 28
Algoritmo de limitación de velocidad.	Propuesta realizada por los investigadores, pero no se detalla el funcionamiento ni especifica las líneas de código; se menciona en otra investigación.	2	1.71%	**SCO:** 25, 28
Algoritmo de la detección máxima de entropía.	Propuesta realizada por los investigadores, pero no se detalla el funcionamiento ni especifica las líneas de código; se menciona en otra investigación.	2	1.71%	**SCO:** 25, 28
Network Advertisement (NETAD)	Propuesta realizada por los investigadores, pero no se detalla el funcionamiento ni especifica las líneas de código; se menciona en otra investigación.	2	1.71%	**SCO:** 25, 28
Algoritmo genético (GA)	El algoritmo genético (GA) y la eliminación de características recursivas se puede emplear en la aplicación de detección de anomalías.	2	1.71%	**SCO:** 48 **IEEE:** 42
Algoritmo de aprendizaje de reglas RIPPER y LEARD	Algoritmos de minería de datos utilizados para la revisión del desarrollo de un HIDS.	1	0.85%	**ACM:** 3
Algoritmos de redes neuronales Levenberg-Marquardt y Error Back-Propagation	Resultado de la investigación propia; mención rápida de la utilización en la literatura.	1	0.85%	**SCO:** 4
Algoritmo Intrusion Weighted Particle	Utilizado para el análisis de redes SCADA, basado en Cuckoo Search Optimization (IWP-CSO), se utiliza para extraer y optimizar las características obtenidas del conjunto de datos.	1	0.85%	**SCO:** 4
Algoritmo, llamado Hierarchical Neuron Architecture based Neural Network (HNA-NN),	Se emplea en el análisis de redes SCADA, se utiliza para realizar la clasificación en función de características optimizadas.	1	0.85%	**SCO:** 4
Shannon Entropy, Joint Entropy, Generalized Entropy, Conditional Entropy, ϕ-entropy,	Algoritmos relacionados al cálculo de la entropía como métrica de medición en la detección de ataques DDoS en SDN.	1	0.85%	**SCO:** 3
Algoritmo Deep Deterministic Policy Gradient (DDPG)	Algoritmo de entrenamiento de defensa frente a amenazas internas	1	0.85%	**SCO:** 13
Asociación FP-Tree. y algoritmo de rulegrowth	Utilizado para mejorar la efectividad de la detección de anomalías en el sistema de detección de intrusiones con la minería de reglas; eficiente para la minería de patrones de reglas secuenciales.	1	0.85%	**SCO:** 30
Versión binaria del Bat Algorithm (BBA)	Es un algoritmo heurístico inspirado en el comportamiento de ecolocalización de los murciélagos.	1	0.85%	**SCO:** 31
Modificación del algoritmo estándar de medición de flujos de tráfico DNS	Modificación utilizada para la detección de anomalías mediante flujos estándar, detección de anomalías mediante flujos extendidos, detección de resolutores DNS abiertos, detección de uso del solucionador de DNS externo, detección de consultas de dominios de malware.	1	0.85%	**SCO:** 35
Algoritmo de reglas de asociación AR_Tree	Utilizado para detectar el comportamiento de intrusión en la red del campus.	1	0.85%	**IEEE:** 12
Algoritmos de predicción de tráfico	Utilizados en análisis de tráfico de red a corto plazo para búferes de enrutamiento de extremo a extremo de red.	1	0.85%	**IEEE:** 18
Algoritmo cusum (cumulative sum)	Algoritmo no paramétrico para la detección de ataques.	1	0.85%	**IEEE:** 31
Algoritmo de Análisis de Componentes Principales (PCA)	PCA tiene como objetivo la reducción de la dimensionalidad de un conjunto de datos en el que hay un gran número de variables interrelacionadas.	1	0.85%	**IEEE:** 32
Algoritmo de boceto de recuento bidireccional	Los enfoques de detección de anomalías se centran en la aplicación de algoritmos existentes en entornos SDN. Como método detallado para detectar un ataque DDoS.	1	0.85%	**IEEE:** 44

Fuente: Elaboración propia

Conclusión: En base a los resultados obtenidos en la Tabla 48, se destaca que los algoritmos para el análisis de data en la identificación de insiders más utilizados en la literatura son algoritmos de machine learning, aprendizaje profundo, como k-NN, Naive Bayes, k-means y k-medoids, CNN, SVM, DT, NB, Random forest con un porcentaje del 8.55%, independientemente de la función para los que se configuren tienen el mismo objetivo común, la detección de anomalías. Mediante la utilización de este tipo de algoritmos se desarrollan algoritmos propios algo que se refleja como el segundo tipo más utilizado en la literatura con el 5.98 %. Como tercer lugar se mencionan algoritmos de detección propios de un IDS para la identificación de patrones y/o eventos secuenciados maliciosos con el 4.27%.

Considerando que varios de los algoritmos identificados en la literatura corresponden a subcategorías dentro del campo del aprendizaje automático (como aprendizaje supervisado, redes neuronales y aprendizaje por refuerzo), y que inicialmente fueron reportados de manera desglosada en la Tabla 48, se procedió a una reclasificación metodológica en la Tabla 49. Esta reorganización agrupa los algoritmos según su enfoque técnico principal, con el fin de facilitar una interpretación más estructurada, homogénea y alineada con los estándares metodológicos de la literatura especializada.

Tabla 49: **Q2.6 Agrupación metodológica de algoritmos para la identificación de insiders threats en redes académicas.**

Categoría	Descripción	Total de papers	% sobre total	Referencias
Algoritmos de aprendizaje supervisado	k-NN, Naive Bayes, SVM, DT, Random Forest	6	5.13	SCO: 9, 18, 23, IEEE: 1, 10, 15
Algoritmos de aprendizaje no supervisado	k-means, k-medoids	4	3.42	IEEE: 23, 33, 45, 46
Redes neuronales	CNN, Levenberg-Marquardt, HNA-NN	4	3.42	ACM: 3, SCO: 4
Aprendizaje por refuerzo	Q-learning, Deep Q Networks, DDPG	3	2.56	SCO: 1, 13, IEEE: 16
Algoritmos evolutivos / bioinspirados	Genético (GA), Bat Algorithm (BBA), IWP-CSO	3	2.56	SCO: 4, 31, IEEE: 42
Entropía	Shannon, Joint, Generalized, Conditional, ϕ-entropy	1	0.85	SCO: 3

Reglas de asociación / minería de datos	FP-Tree, RuleGrowth, AR_Tree, RIPPER, LEARD	3	2.56	ACM: 3, SCO: 30, IEEE: 12
PCA y CUSUM	Análisis de Componentes Principales, Cusum	2	1.71	IEEE: 31, 32
Algoritmos propios (sin clasificar)	Algoritmos desarrollados en la investigación	7	5.98	ACM: 8, SCO: 2, 8, 22, 49, IEEE: 29, 49
Algoritmos de detección propios IDS	Algoritmos nativos de IDS como SNORT	5	4.27	ACM: 1, 17, IEEE: 3, 11, 48
Otros específicos	TRW-CB, NETAD, DNS modificados, Sketching, etc.	6	5.13	SCO: 25, 28, 35, IEEE: 18, 44

La tabla 49 presenta una reclasificación de los algoritmos empleados en la identificación de amenazas internas en intranets académicas, agrupados según su enfoque metodológico y características técnicas.

Los algoritmos más utilizados pertenecen al aprendizaje automático supervisado (5.13%) y a las redes neuronales y aprendizaje profundo (4.27%), seguidos por algoritmos de detección integrados en IDS (4.27%) y por propuestas personalizadas desarrolladas por los propios investigadores (5.98%). También se emplean enfoques menos frecuentes como algoritmos evolutivos o bioinspirados, medidas de entropía, reglas de asociación, reducción de dimensionalidad (PCA) y clustering optimizado, todos con porcentajes individuales inferiores al 3%.

Esta diversidad metodológica confirma la ausencia de un estándar consolidado en el campo, lo que refuerza la necesidad de desarrollar marcos sistemáticos, replicables y adaptables para el control de amenazas internas en entornos académicos.

Q2.7 ¿Qué estudios aplican análisis de tramas para la identificación en insiders threat y cómo lo hacen?

Se han identificado 14 papers que mencionan el análisis de trazas o paquetes durante el proceso de sus investigaciones, la Tabla 50 muestra los resultados obtenidos acerca del análisis de tramas para la identificación en insiders threat y cómo lo hacen, junto con el título del estudio, el método o herramienta, la descripción, el total de artículos, porcentaje (%) y el número de papers.

Tabla 50: **Q2.7 ¿Qué estudios aplican análisis de tramas para la identificación en insiders threat y cómo lo hacen?**

Título	Método/herramienta	Descripción	Total	%	Papers / ID
Advanced framework of defense system for	IDS SNORT - BRO	Se utiliza Snort para el análisis de paquetes y la gestión de redes de gráficos	2	1.71%	**SCO:** 37

prevention of insider's malicious behaviors		de tráfico multi-router. Para examinar el tráfico de flujo se utiliza Wireshark y Snort para capturar el tráfico de la red de interfaz.			
Real Time DNS Traffic Profiling Enhanced Detection Design for National Level Network		Utilización de BRO IDS, con el objetivo de realizar análisis de tráfico pasivo y facilitar el proceso de creación de perfiles para identificar tráfico malo.			**IEEE:** 45
Efficient anomaly detection and mitigation in software defined networking environment	Análisis de paquetes DNS	En un ambiente DNS la selección de características en general como direcciones IP de origen se utiliza para que el análisis respectivo se pueda realizar rápidamente. Concretamente en el campo de detección de anomalías.	2	1.71%	**SCO:** 31
Detection of DNS traffic anomalies in large networks		Para obtener información más específica sobre el tráfico DNS después de un incidente externo o interno, es necesario almacenar todos los campos de paquetes DNS importantes, como las direcciones de origen y destino, el nombre de dominio consultado o los datos de respuesta.			**SCO:** 35
PORTFILER: Port-Level Network Profiling for Self-Propagating Malware Detection	Análisis de paquetes con método propio.	Mención a un método propio referente a características de estadísticas de tráfico: se extraen varias características de estadísticas de tráfico: número de IP internas y externas distintas que se comunican en ese puerto, número de conexiones y número de nuevas IP externas distintas (que no se han contactado antes) por puerto. Se espera observar un aumento en estas características durante los períodos con altas actividades de SPM.	2	1.71%	**SCO:** 45 **SCO:** 49
A Learning Approach with Programmable Data Plane towards IoT Security		Las evaluaciones que utilizan trazas de red de diferentes protocolos de IoT muestran beneficios significativos en precisión, eficiencia y universalidad sobre los métodos de vanguardia. Se concluye que el método propuesto hace elecciones adecuadas de los campos de encabezado logrando un mejor nivel de precisión de detección de ataque (intrusión).			
A Hybrid Intelligent System for Insider Threat Detection Using Iterative Attention	Registros de eventos	Con el fin de abordar los desafíos de los datos de registro sucios e inconsistentes, se analiza cada registro de eventos en un conjunto de campos predefinidos, capturando la información fundamental de cada evento. Cada campo es normalizado por un identificador único, como userID. y agrupando según categorías definidas en el paper.	1	0.85%	**ACM:** 2
Protecting Intellectual Property and Sensitive Information in Academic Campuses from Trusted Insiders: Leveraging Active Directory	Minería de datos	Otro enfoque para observar lo que está sucediendo en una empresa es capturar el tráfico de red y el análisis de paquetes. La utilización de herramientas como un IDS o minería de datos analiza el tráfico de red definiendo algunas reglas basadas en atributos.	1	0.85%	**ACM:** 7
IoTDePT: Detecting Security Threats and Pinpointing Anomalies in an IoT Environment	Análisis y comparación de los encabezados de los paquetes	Se basa en el encabezado del paquete, comprueba si el host de origen intenta establecer una conexión con las direcciones IP de destino que pertenece a un espacio de direcciones IP no utilizado en la darknet. Si es así, se emite una alerta a las organizaciones correspondientes para proporcionar una notificación sobre esta posible infección de malware o ataque.	1	0.85%	**ACM:** 8

Design of Network Security Projects Using Honeypots	Honeypots y sus variantes	Menciona la utilización de herramientas como Honeypots que se ha desplegado en instituciones educativas como herramienta de estudio; con el fin de analizar el tráfico de la red.	1	0.85%	**ACM:** 9
Hviz: HTTP(S) traffic aggregation and visualization for network forensics	Análisis de tráfico HTTP	Menciona que la investigación del tráfico HTTP es cada vez más importante en la ciencia forense digital, ya que HTTP se ha establecido como el protocolo principal en las redes corporativas para la comunicación cliente-servidor.	1	0.85%	**SCO:** 29
Design and Implementation of Campus Network Intrusion Detection System	Evaluación de segmentos de trama ethernet	Mediante la cabecera Ethernet, se puede identificar si se trata de paquete IP, paquete ARP o paquete RARP. Mediante el segmento de protocolo de cabecera IP, se puede identificar si se trata de protocolo TCP o protocolo UDP. Mediante la información del puerto de la cabecera TCP, se puede determinar el tipo de protocolo de la capa superior. Seleccionando un tipo de protocolo específico, o un indicador específico, o un ID de puerto específico, se puede determinar el comportamiento del paquete de red.	1	0.85%	**IEEE:** 2
Applied Research on Snort Intrusion Detection Model in The Campus Network	Análisis de protocolos de comunicación	En el análisis de protocolos se utiliza el protocolo de comunicación de red de las reglas específicas y analiza la información en el lugar correspondiente.	1	0.85%	**IEEE:** 3
Packet- vs. Session-Based Modeling for Intrusion Detection Systems	Análisis del Segmento TCP de las cabeceras de los paquetes	Se utiliza la información del segmento TCP siendo los primeros 20 bytes la información del encabezado del segmento TCP lo necesario para la investigación.	1	0.85%	**IEEE:** 19

Fuente: Elaboración propia

Conclusión: Catorce papers representan el 11.97% del total de artículos en la RSL que hacen referencia al análisis de tramas para la identificación en insiders threat y cómo lo hacen. De los cuales el 1.71% destaca la utilización de la herramienta IDS a través de SNORT y BRO IDS empleados para el análisis de los paquetes e identificación de anomalías, estos trabajan con reglas de concordancia de ataques conocidos como se menciona en SCO37 e IEEE45. En igual porcentaje destaca el análisis de paquetes DNS en SCO31, SCO35, así como el análisis de paquetes con método propio como se resalta en SCO45 donde las evaluaciones que utilizan trazas de red de diferentes protocolos de IoT muestran beneficios significativos en precisión, eficiencia y universalidad sobre los métodos de vanguardia o toman otros datos necesarios para sus investigaciones como señala SCO49.

Los resultados restantes, en el 0.85%, realizan análisis de paquetes definiendo reglas basadas en atributos como en ACM07. Toman información de cabeceras para el análisis en ACM08, e IEEE02. Se considera información de los primeros 20 bytes del segmento TCP en IEEE19. Además, usan honeypots para analizar tráfico en ACM09, usan tráfico en base a protocolos como HTTP en SCO29 y define un protocolos de comunicación de red basado en reglas específicas en el paper IEEE03.

Q3. ¿Qué metodología para identificar, evaluar y controlar insiders threat en intranets académicas se emplea y cuál es la más adecuada?

Q3.1 ¿Qué metodología para identificar, evaluar y controlar insiders threat se emplea? ¿cuál es la más adecuada?

Una tendencia hacia la seguridad de redes es la identificación de eventos anormales o anómalos mediante la utilización de herramientas o métodos, esto en concordancia a una metodología ya establecida o una adaptación de esta. Sin embargo, durante la RSL se pudo evidenciar ampliamente que la tendencia se dirige hacia el uso de una metodología propia propuesta por los investigadores, un método propio o por otro lado un conjunto de pasos que se siguen en cierto orden para cumplir con la detección o mitigación de eventos anómalos o en si de ataques perpetrados tanto desde dentro o fuera de una red de campus o institucional como se observa en la Tabla 51, donde se detalla: nombre, descripción, total, porcentaje y papers.

Tabla 51: **Q3.1 ¿Qué metodología para identificar, evaluar y controlar insiders threat se emplea? ¿cuál es la más adecuada?**

METODOLOGIA DE IDENTIFICACION, CONTROL DE INSIDERS THREAT				
Nombre	**Descripción**	**Total**	**%**	**Papers**
Metodología propia	Conjunto de pasos ordenados con el objetivo de mitigación, detección de eventos anómalos según las necesidades de los investigadores, o parámetros definidos en la propuesta presentada.	62	52.99%	**ACM:** 1, 2, 3, 4, 5, 8, 9, 12, 17. **SCO:** 2, 9, 11, 13, 14, 16, 17, 19, 20, 23, 22, 25, 26, 27, 28, 29, 30, 31, 32, 34, 36, 37, 40, 44, 46, 47, 49, 50 **IEEE:** 1, 4, 8, 9, 11, 12, 13, 15, 16, 19, 21, 23, 24, 25, 30, 32, 33, 34, 35, 36, 39, 40, 43, 45, 48.
Active Directory	Extracción de datos de detalles de los activos a los que se accede, La ruta de acceso, el patrón de acceso, información sobre el movimiento de datos confidenciales a través de la Red del Campus, el tipo de inicio de sesión y los controles de acceso para posterior análisis forense.	1	0.85%	**ACM:** 7
Metodología General	Conjunto de pasos generales para la detección de actividad sospechosa del usuario en la red.	1	0.85%	**SCO:** 39
Sin especificar	Resultado de la investigación una mención general de aspectos de seguridad.	1	0.85%	**SCO:** 4
Metodología OpenTM	Metodología para la estimación de tráfico basada en pull obteniendo datos de flujo de OpenFlow.	1	0.85%	**SCO:** 8
Metodologías de detección IDPS	Incluyen la utilización de sistemas de detección de intrusos y sistemas de prevención de intrusos	1	0.85%	**SCO:** 30
OWASP 2013	Clasificación de amenazas de aplicaciones web OWASP 2013 en el registro de acceso al tráfico de usuarios.	1	0.85%	**SCO:** 30
Propuesta de seguridad DarkPorts	Propuesta de seguridad que combina honeypots, puertos virtuales y puertos físicos.	1	0.85%	**SCO:** 38

Threat Intrusion Detection and Prevention Engine (TIDPE)	Marco propuesto para la detección y prevención de amenazas	1	0.85%	**SCO:** 6
Metodología tradicional contra ataques DDoS	Conjunto de pasos para combatir ataques DDoS	1	0.85%	**IEEE:** 44

Fuente: Elaboración propia

Conclusión: De la RSL se determinó con un porcentaje de 52.14% la utilización de una metodología propia detallada como un conjunto de pasos ordenados con el objetivo de mitigar, detectar eventos anómalos considerando las necesidades y tipos de redes en las que se desarrolla las investigaciones. Se menciona un conjunto de metodologías con el 0.85% como Active Directory empleada para la detección de activos e información sobre datos confidenciales en un campus para posterior análisis forense como señala ACM07. OpenTM para la estimación de tráfico basada en pull obteniendo datos de flujo de OpenFlow descrito en SCO08. OWASP 2013 para la clasificación de amenazas de aplicaciones web en SCO30. Propuesta de seguridad DarkPorts, combina honeypots, puertos virtuales y puertos físicos en SCO38. Threat Intrusion Detection and Prevention Engine (TIDPE) para detección y prevención de amenazas detallado en SCO06. Metodología tradicional contra ataques DDoS en IEEE44.

Sin embargo, no se especifica una metodología, como la más adecuada, en la mayoría se utiliza metodologías propias para identificar, evaluar y controlar insiders threat.

Q3.2 ¿Existen modelos, normas particulares en seguridad en intranets de redes académicas?

A continuación, se presenta la Tabla 52 con los resultados obtenidos en este criterio, incluyen: nombre, descripción, total, porcentaje y papers.

Tabla 52: **Q3.2 ¿Existen modelos, normas particulares en seguridad en intranets de redes académicas?**

MODELOS, NORMAS EN SEGURIDAD DE REDES ACADEMICAS				
Nombre	**Descripción**	**Total**	**%**	**Papers**
Firewall institucional	Deniega acceso a recursos institucionales basado en reglas	10	8.55%	**SCO:** 36, 38, 51 **IEEEE:** 2, 3, 5, 12, 19, 21, 30
IDS, IPS y sus variantes	Sistemas que analizan el tráfico de la red y en caso de detectar una concordancia entre el tráfico y las reglas definidas lanza una alerta al administrador de la red o bloquea la amenaza.	7	5.98%	**SCO:** 51 **IEEE:** 2, 4, 5, 12, 19, 21
Tecnología Antivirus	Software licenciado especializado en la protección de virus y demás tipos de ataques.	2	1.71%	**IEEE:** 3, 5
Tecnología de cifrado	Protección de datos de la red como medida de ciberseguridad.	2	1.71%	**IEEE:** 3, 19
Método propio propuesto	Método de autoría de los investigadores propuesto en los papers.	2	1.71%	**IEEE:** 5, 29

Modelo de seguridad propuesto	Conjunto de normas propuesta para su implementación en redes de datos.	1	0.85%	**IEEE:** 42

Fuente: Elaboración propia

Conclusión: En cuanto a si existen modelos, normas particulares en seguridad en intranets de redes académicas se observó la utilización de un Firewall con el objetivo de denegar acceso a recursos institucionales basado en reglas en un 8.55%. En un porcentaje del 5.98% los sistemas de detección y prevención de intrusos (IDS, IPS y sus variantes), analizan el tráfico de la red y en caso de detectar una concordancia entre el tráfico y las reglas definidas lanza una alerta al administrador de la red o bloquea la amenaza. En un porcentaje del 1.71% tecnología antivirus o de cifrado, ya sea para la protección de virus o como medida de ciberseguridad.

Se identificó además un método propio propuesto en IEEE05, IEEE29, donde se emplea el firewall y el centro de seguridad en la nube de comunicación de cifrado en tiempo real, de acuerdo con la política de seguridad para hacer frente al comportamiento de intrusión como se detalla en IEEE05.

IEEE42, propone un modelo de seguridad que incluye el empleo del BYOD (traiga su propio dispositivo) para el trabajo además de un dispositivo emitido por la empresa. Se propone un conjunto de datos para una red de campus, autenticación basada en MAC e IP, Campus Wi-Fi: acceso a la red sin interrupciones en todo el campus con el mismo SSID, separación de datos confidenciales de datos comunes y también formación de todos los usuarios de la red para dar a conocer la seguridad informática y los riesgos asociados a la violación de la seguridad.

En la Tabla 53 se resume el número de papers de la RSL que dan respuesta a las tres preguntas, planteadas y los que no se relacionan.

Tabla 53: **Número de papers basados en las preguntas**

Preguntas	Número de papers relacionados (Y)	Número de papers no relacionados (N)
Q1 ¿Qué tipos de insiders threat o amenazas internas existen en intranets académicas y cuáles son sus fuentes de datos?	**104**	**23**
Q2. Qué herramientas, métodos o procedimientos de recolección de datos se emplean en el análisis de insiders threat, ¿además que métodos de identificación o detección de amenazas se emplean?	**112**	**15**
Q3. Qué metodología para identificar, evaluar y controlar insiders threat en intranets académicas se emplea y cuál es la más adecuada?	**77**	**50**

Fuente: Elaboración propia

Conclusión de la revisión sistemática de literatura

Respecto a las amenazas internas en intranets académicas y cuáles son sus fuentes de datos, según Q1.1.

Se consideran cuatro preguntas:

Las amenazas internas en redes de datos que se mencionan en la pregunta Q1.1 son los ataques de DoS y sus variantes DDoS con el 39.31%. En relación con Q1.2 las amenazas internas en redes académicas que más han sido mencionadas son los ataques de DoS y DDoS con el 13.68%.

Con relación a Q1.3 Principales fuentes de datos de insiders threats. En la RSL se ha podido identificar tres tipos de fuentes de datos: Psicología de usuarios, fuente de datos externa y fuentes de datos propias. Las principales fuentes de datos externos de insiders threats, más utilizadas en la literatura con un porcentaje de 9.4% es el conjunto de datos KDD99, NSL-KDD, Kyoto KDD-Cup que es principalmente utilizado para la evaluación de sistemas de detección de intrusos, donde los ataques se clasifican en denegación de servicio (DoS), remoto a local (R2L), usuario a remoto (U2R), y sondeo.

El conjunto de datos UNSW-NB15 con 3,41% genera tráfico sintético con comportamiento malicioso incluye ataques como backdoors, DoS, exploits, worms y fuzzers. Y el conjunto de datos CERT r4.2, con 2,56 % es un conjunto de datos sintético generado en la Universidad Carnegie Mellon, integra registros de eventos incluyendo inicio de sesión/ cierre de sesión, correo electrónico, dispositivo, archivo y HTTP en las que hay instancias de actividad anómalas de amenazas internas.

Por otro lado, las fuentes de datos propios de insider threat son datos capturados en las redes de datos o a su vez una combinación de estos datos con fuentes de datos externas para así conformar una nueva fuente propia adecuada para las investigaciones.

De la RSL, se determinó que, si bien existen diferentes fuentes de datos externas que se utilizan para el análisis de pruebas en lo que se refiere a datos propios de amenazas internas en redes de campus académicas son muy limitadas y no se da mayor detalle al respecto, por lo que se determinó la necesidad de realizar un análisis de amenazas internas en una intranet de un campus universitario con el objetivo de capturar data propia e identificarla con mayor detalle para el control en el presente estudio de investigación y que servirá de base para estudios futuros.

Respecto a Q1.4 se detecta 17 investigaciones que consideran insider threat para limitar el control de acceso a usuarios en intranets. Entre ellas, en un porcentaje del

2.56% se menciona la utilización de firewall de red en ACM14, donde se utiliza para fortalecer el control de acceso entre redes. Se menciona además en ACM19, el uso de filtrado de paquetes ACL (lista de control de acceso) como una técnica de defensa importante que protege la seguridad de la red interna, políticas de control de acceso que supervisan los datos que fluyen mediante reglas de acceso. IEEE39, menciona la importancia de combinar el sistema de respuesta a intrusiones con el firewall, para bloquear la mayoría de los ataques.

En conclusión, destacan métodos de control de acceso basados en firewall, ACL, mecanismos de autenticación y autorización para garantizar que solo los usuarios legítimos puedan acceder a los datos. Estudios como el presente permite hacer una revisión del estado del arte, determinar métodos /técnicas utilizadas en el control de amenazas internas, dando la pauta para conocer su tratamiento.

Respecto a Q2. ¿Qué herramientas, métodos o procedimientos de recolección de datos se emplean en el análisis de insiders threat, además que métodos de identificación o detección de amenazas se emplean?

De los resultados se resalta el empleo de un IDS para el análisis de la captura de datos y su posterior análisis. Con relación a los procedimientos para realizar mediciones de data de insiders threats en intranets académicas, se ha identificado el análisis de paquetes de datos de acuerdo con el modelo de protocolo de paquetes TCP/IP mediante la tecnología de detección SNORT, basado en el valor de algunos campos especiales a fin de determinar el protocolo, y luego el patrón de ataque de detección que se corresponde con la coincidencia de patrón.

Respecto a los procedimientos para realizar mediciones de data de insiders threat se determina que si bien se hacen referencia a los procedimientos para realizar mediciones de data de insiders threats en intranets académicas, resalta el hecho que es un campo en el que no se ha desarrollado estudios, ni existe un estándar para realizar este tipo de procesos, además en los resultados obtenidos no se define un procedimiento para realizar mediciones de datos esto debido a que cada paper realiza un método propio sin muchas especificaciones, ni se ha identificado un método estándar.

En Q2.3 acerca de la detección de mal uso o de anomalías o comportamientos anómalos que se emplea en el contexto de detección de intrusiones de insiders

threat. Se concluye que la utilización de sistemas de detección de intrusos (IDS) y sus diferentes variantes como los son NIDS Y HIDS entre otros son los más utilizados con un porcentaje de 42.74% para la detección de anomalías en conjunto de la captura de datos en formato PCAP.

Con relación a Q2.4, método de detección de mal uso o detección de anomalías o comportamientos anómalos que se emplea en el contexto de detección de intrusiones de insiders threat en intranets académicas. Tras la revisión se concluye que el método más utilizado para la detección de anomalías en redes académicas son los sistemas de detección de intrusos y sus diferentes variantes con un porcentaje de 11.97%, tiene relación a que estos sistemas suelen trabajar como herramientas de captura de datos en formatos PCAP para su posterior análisis.

Respecto a los métodos que se usa para identificar insiders threat en tiempo real según Q2.5, el principal método es la utilización de sistemas de detección y prevención de intrusos basado en coincidencia de reglas, principalmente SNORT en un porcentaje de 4.27%, pues la medición de la red es uno de los temas clave para la detección y mitigación de intrusiones en tiempo real.

En base a los resultados de Q.2.6, se destaca que los algoritmos para el análisis de data en la identificación de insiders más utilizados en la literatura son algoritmos de Machine Learning, aprendizaje automático, aprendizaje profundo, como k-NN, Naive Bayes, k-means y k-medoids, CNN, SVM, DT, NB, Random forest con un porcentaje del 8.55%, para la detección de anomalías. Además, se desarrollan algoritmos propios algo que se refleja como el segundo tipo más utilizado en la literatura con el 5.98 %. Como tercer lugar se menciona Algoritmos de detección propios de un IDS para la identificación de patrones y/o eventos secuenciados maliciosos con el 4.27%.

En Q.2.7 el 11.97% del total de artículos en la RSL hace referencia al análisis de tramas para la identificación en insiders threat y cómo lo hacen. De los cuales el 1.71% destacan la utilización de la herramienta IDS a través de SNORT y BRO IDS empleados para el análisis de los paquetes e identificación de anomalías, estos trabajan con reglas de concordancia de ataques conocidos.

En base a los resultados de RSL, se selecciona la herramienta de análisis de data en la intranet, SNORT, utilizado para el análisis de la intranet en el presente trabajo doctoral, para aplicarse en la parte práctica del estudio.

Respecto a Q3. ¿Qué metodología para identificar, evaluar y controlar insiders threat en intranets académicas se emplea y cuál es la más adecuada?

La RSL determinó con un porcentaje de 52.14% la utilización de una metodología propia detallada como un conjunto de pasos ordenados con el objetivo de mitigar, detectar eventos anómalos considerando las necesidades y tipos de redes en las que se desarrolla las investigaciones. Con lo que se determina que no existe una metodología estándar que se aplique en este contexto.

En cuanto Q3.2 si existen modelos, normas particulares en seguridad en intranets de redes académicas se observó la utilización de un Firewall con el objetivo de denegar acceso a recursos institucionales basado en reglas en un 8.55%. En un porcentaje del 5.98% los sistemas de detección y prevención de intrusos (IDS, IPS y sus variantes), analizan el tráfico de la red y en caso de detectar una concordancia entre el tráfico y las reglas definidas lanza una alerta al administrador de la red o bloquea la amenaza. En un porcentaje del 1.71% tecnología antivirus o de cifrado se emplea ya sea para la protección de virus o como medida de ciberseguridad.

ANEXO C. RSL DE "AMENAZAS INTERNAS EN INTRANETS ACADÉMICAS"

A continuación, se describen los resultados de la RSL de "Amenazas internas en intranets académicas", en la Tabla 54, donde se detalla el identificador del paper, el título, autores, año, título de la fuente, tipo de documento, tipo de estudio, y las preguntas Q1, Q2 y Q3, donde se indican los papers que se relacionan.

Tabla 54: RSL DE "AMENAZAS INTERNAS EN INTRANETS ACADÉMICAS"

Id_paper	Title	Authors	Year	Source title	Document Type	Studio Type	Q1	Q2	Q3
SCO01	Cybersecurity data science: an overview from machine learning perspective	Sarker I.H., Kayes A.S.M., Badsha S., Alqahtani H., Watters P., Ng A.	2020	Journal of Big Data	Article	Reporte	Q1.1 Q1.3	Q2.1 Q2.3 Q2.6	Ninguna
SCO02	Analysis of E-mail Account Probing Attack Based on Graph Mining	Wen Y., Chen X., Zeng X., Wang W.	2020	Scientific Reports	Article	Caso de estudio	Q1.2 Q1.3	Q2.1 Q2.4 Q2.6	Q3.1
SCO03	Detection and mitigation of DDoS attacks in SDN: A comprehensive review, research challenges and future directions	Singh J., Behal S.	2020	Computer Science Review	Review	Reporte	Q1.1	Q2.3 Q2.6	
SCO04	A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics	Pliatsios D., Sarigiannidis P., Lagkas T., Sarigiannidis A.G.	2020	IEEE Communications Surveys and Tutorials	Article	Encuesta	Q1.1 Q1.3	Q2.3 Q2.6	Q3.1
SCO05	Intrusion detection in software defined networking using snort and mirroring	Sampath N., Sadhasivam J., Jayavel S., Chindarmony N.S., Sharma S.	2020	SSRG International Journal of Engineering Trends and Technology	Article		Ninguna	Ninguna	Ninguna
SCO06	An Automated Framework to Uncover Malicious Traffic for University Campus Network	Mahajan A., Ramotra A.K., Mansotra V., Singh M.	2020	Smart Innovation, Systems and Technologies	Conference Paper	Caso de estudio	Q1.2	Q2.1 Q2.3 Q2.5	Q3.1
SCO07	CTLMD: Continuous-Temporal Lateral Movement Detection Using Graph Embedding	Zhao S., Wei R., Cai L., Yu A., Meng D.	2020	Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)	Conference Paper	Reporte	Q1.4	Q2.3	Ninguna
SCO08	Real-time anomaly detection and mitigation using streaming telemetry in SDN	Kurt Ç., Ayhan Erdem O.	2020	Turkish Journal of Electrical Engineering and Computer Sciences	Article	Experimento	Ninguna	Q2.1 Q2.3 Q2.5 Q2.6	Q3.1
SCO09	An improved ensemble based intrusion detection technique using XGBoost	Bhati B.S., Chugh G., Al-Turjman F., Bhati N.S.	2020	Transactions on Emerging Telecommunications Technologies	Article	Experimento	Q1.1 Q1.3	Q2.3 Q2.5 Q2.6	Q3.1

SCO10	SDCCP: Control the network using software-defined networking and end-to-end congestion control	Lin J., Liao L., Wang T., Zhang J., Cheng L.	2020	Concurrency Computation	Conference Paper	Experimento	Q1.1	Q2.3	Q3.1
SCO11	Machine learning and recognition of user tasks for malware detection	Alagrash Y., Mohan N., Gollapalli S.R., Rrushi J.	2019	Proceedings - 1st IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications, TPS-ISA 2019	Conference Paper	Combinado	Q1.1	Q2.1 Q2.3 Q2.6	Q3.1
SCO12	A survey of network-based intrusion detection data sets	Ring M., Wunderlich S., Scheuring D., Landes D., Hotho A.	2019	Computers and Security	Review	Encuesta	Q1.3	Q2.1 Q2.3	Ninguna
SCO13	Intranet User-Level Security Traffic Management with Deep Reinforcement Learning	Jin Q., Wang L.	2019	Proceedings of the International Joint Conference on Neural Networks	Conference Paper	Experimento	Q1.1 Q1.3 Q1.4	Q2.3 Q2.5 Q2.6	Q3.1
SCO14	Fixing network security vulnerabilities in local area network	Kumar B.K., Raj N., Dhivvya J.P., Muralidharan D.	2019	Proceedings of the International Conference on Trends in Electronics and Informatics, ICOEI 2019	Conference Paper	Experimento	Q1.1	Q2.3	Q3.1
SCO15	Artificial intelligence enabled software-defined networking: A comprehensive overview	Latah M., Toker L.	2019	IET Networks	Review	Reporte	Q1.1 Q1.3	Q2.3	Ninguna
SCO16	Towards augmented proactive cyberthreat intelligence	Khan T., Alam M., Akhunzada A., Hur A., Asif M., Khan M.K.	2019	Journal of Parallel and Distributed Computing	Article	Experimento	Q1.1	Q2.1 Q2.3	Q3.1
SCO17	An Insider Threat Detection Approach Based on Mouse Dynamics and Deep Learning	Hu T., Niu W., Zhang X., Liu X., Lu J., Liu Y.	2019	Security and Communication Networks	Article	Experimento	Q1.1 Q1.3	Q2.3	Q3.1
SCO18	A survey of machine learning techniques applied to software defined networking (SDN): Research issues and challenges	Xie J., Richard Yu F., Huang T., Xie R., Liu J., Wang C., Liu Y.	2019	IEEE Communications Surveys and Tutorials	Review	Reporte	Q1.1 Q1.3	Q2.3 Q2.6	Ninguna
SCO19	Detection of DHCP Starvation Attacks in Software Defined Networks: A Case Study	Toprak C., Turker C., Erman A.T.	2018	UBMK 2018 - 3rd International Conference on Computer Science and Engineering	Conference Paper	Caso de estudio	Q1.1	Q2.3 Q2.6	Q3.1
SCO20	Behavior rhythm: An effective model for massive logs characterizing and security monitoring in cloud	Qin T., He C., Jiang H., Chen R.	2018	2018 IEEE Conference on Communications and Network Security, CNS 2018	Conference Paper	Experimento	Q1.3	Q2.3	Q3.1

SCO21	A feasibility analysis for edge computing fusion in LPWA IoT environment with SDN structure	Kuo C.-T., Chang V., Lei C.-L.	2018	Proceedings of 2017 International Conference on Engineering and Technology, ICET 2017	Conference Paper	Reporte	Ninguna	Ninguna	Ninguna
SCO22	On Using Cognition for Anomaly Detection in SDN	Tantar E., Tantar A.-A., Kantor M., Engel T.	2018	Advances in Intelligent Systems and Computing	Conference Paper	Reporte	Q1.1	Q2.1 Q2.3 Q2.6	Q3.1
SCO23	Complexity of insider attacks to databases	Kul G., Upadhyaya S., Hughes A.	2017	MIST 2017 - Proceedings of the 2017 International Workshop on Managing Insider Security Threats, co-located with CCS 2017	Conference Paper	Reporte	Q1.1	Q2.3 Q2.6	Q3.1
SCO24	Securing government information and data in developing countries	Zoughbi S.	2017	Securing Government Information and Data in Developing Countries	Book		Ninguna	Ninguna	Ninguna
SCO25	Software Defined Networking Architecture, Security and Energy Efficiency: A Survey	Rawat D.B., Reddy S.R.	2017	IEEE Communications Surveys and Tutorials	Review	Reporte	Q1.1	Q2.3 Q2.6	Q3.1
SCO26	Leveraging SDN for ARP security	Cox J.H., Clark R.J., Owen H.L.	2016	Conference Proceedings - IEEE SOUTHEASTCON	Conference Paper	Experimento	Q1.1 Q1.4	Q2.1 Q2.3 Q2.5	Q3.1
SCO27	Resilience support in software-defined networking: A survey	Da Silva A.S., Smith P., Mauthe A., Schaeffer-Filho A.	2015	Computer Networks	Article	Encuesta	Q1.1	Q2.3	Q3.1
SCO28	A Survey of Securing Networks Using Software Defined Networking	Ali S.T., Sivaraman V., Radford A., Jha S.	2015	IEEE Transactions on Reliability	Article	Reporte	Q1.1 Q1.4	Q2.1 Q2.3 Q2.6	Q3.1
SCO29	Hviz: HTTP(S) traffic aggregation and visualization for network forensics	Gugelmann D., Gasser F., Ager B., Lenders V.	2015	Digital Investigation	Article	Experimento	Q1.1 Q1.3	Q2.1 Q2.4 Q2.7	Q3.1
SCO30	Anomaly-based intrusion detection and prevention system on website usage using rule-growth sequential pattern analysis: Case study: Statistics of Indonesia (BPS) website	Trio Pramono Y.W., Suhardi	2015	Proceedings - 2014 International Conference on Advanced Informatics: Concept, Theory and Application, ICAICTA 2014	Conference Paper	Caso de estudio	Q1.3	Q2.3 Q2.6	Q3.1
SCO31	Efficient anomaly detection and mitigation in software defined networking environment	Sathya R., Thangarajan R.	2015	2nd International Conference on Electronics and Communication Systems, ICECS 2015	Conference Paper	Experimento	Q1.1 Q1.3	Q2.3 Q2.6 Q2.7	Q3.1
SCO32	Penetration testing and network auditing: Linux	Stiawan D., Idris m.y., Abdullah a.H.	2015	Journal of Information Processing Systems	Article	Experimento	Q1.1 Q1.3	Q2.3 Q2.5	Q3.1

SCO33	REPETIDO HViz: HTTP(S) traffic aggregation and visualization for network forensics	Gugelmann D., Gasser F., Ager B., Lenders V.	2015	Proceedings of the Digital Forensic Research Conference, DFRWS 2015 EU	Conference Paper	Experimento	Q1.1 Q1.3	Q2.1 Q2.4 Q2.7	Q3.1
SCO34	An AMI threat detection mechanism based on SDN networks	Chi P.-W., Kuo C.-T., Ruan H.-M., Chen S.-J., Lei C.-L.	2014	SECURWARE 2014 - 8th International Conference on Emerging Security Information, Systems and Technologies	Conference Paper	Experimento	Q1.4	Q2.3	Q3.1
SCO35	Detection of DNS traffic anomalies in large networks	Čermák M., Čeleda P., Vykopal J.	2014	Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)	Article	Reporte	Q1.1 Q1.3	Q2.1 Q2.3 Q2.6 Q2.7	Ninguna
SCO36	Agent-based honeynet framework for protecting servers in campus networks	Kim I.S., Kim M.H.	2012	IET Information Security	Article	Caso de estudio	Q1.1	Q2.1 Q2.3	Q3.1 Q3.2
SCO37	Advanced framework of defense system for prevetion of insider's malicious behaviors	Nithiyanandam C., Tamilselvan D., Balaji S., Sivaguru V.	2012	International Conference on Recent Trends in Information Technology, ICRTIT 2012	Conference Paper	Reporte	Q1.1 Q1.4	Q2.1 Q2.3 Q2.7	Q3.1
SCO38	Sensor in the dark: Building untraceable large-scale honeypots using virtualization technologies	Shimoda A., Mori T., Goto S.	2010	Proceedings - 2010 10th Annual International Symposium on Applications and the Internet, SAINT 2010	Conference Paper	Experimento	Q1.1	Q2.1 Q2.3	Q3.1 Q3.2
SCO39	An Analysis of Complexity of Insider Attacks to Databases	Gökhan Kul, Shambhu Upadhyaya, Andrew Hughes	2020	(2021) ACM Transactions on Management Information Systems, 12 (1), art. no. 3391231, . Cited 1 time		Experimento	Q1.1 Q1.3	Q2.3 Q2.5	Q3.1
SCO40	Design and Implementation of a Quantitative Network Health Monitoring and Recovery System	Harshit Gujral, Abhinav Sharma, Pulkit Jain, Shriya Juneja, Sangeeta Mittal	2022	(2022) Wireless Personal Communications	Article	Experimento	Q1.1 Q1.3	Q2.3 Q2.5	Q3.1
SCO41	The Impact of Artificial Intelligence on Data System Security: A Literature Review	Ricardo Raimundo, Albérico Rosário	2021	(2021) Sensors, 21 (21), art. no. 7029,	Article	Reporte	Ninguna	Ninguna	Ninguna
SCO42	Towards security automation in Software Defined Networks(Review)	Noe M.Yungaicela Naula, Cesar Varga Rosales, Jesús Arturo Pérez, Díaz Mahdi Zareei	2022	Computer Communications Volume 183, 1 February 2022, Pages 64-82	Review	Reporte	Q1.1	Q2.3	Ninguna

SCO43	Three decades of deception techniques in active cyber defense - Retrospect and outlook	Li Zhang, Vrizlynn.L. Thing	2021	Computers and Security Volume 106, July 2021, Article number 102288	Review	Reporte	Q1.1	Q2.3	Ninguna
SCO44	Security of Power Line Communication systems: Issues, limitations and existing solutions	Jean Paul A. Yaacoub, Javier Hernandez Fernandez, Hassan N. Noura a, Ali Chehab	2021	Computer Science Review 39 (2021) 100331	Review	Reporte	Q1.1 Q1.4	Q2.3	Q3.1
SCO45	PORTFILER: Port-Level Network Profiling for Self-Propagating Malware Detection	Talha Ongun, Oliver Spohngellert, Benjamin Miller, Simona Boboila, Alina Oprea, Tina Eliassi-Rad	2021	Computer Science Review, 39, art. no. 100331,	Review	Reporte	Q1.1 Q1.3	Q2.3 Q2.7	Ninguna
SCO46	Cyber threat intelligence using PCA-DNN model to detect abnormal network behavior	Mohammad Al-Fawa'reh, Mustafa Al-Fayoumi, Shadi Nashwan, Salam Fraihat	2021	Egyptian Informatics Journal 23 (2022) 173–185	Article	Experimento	Q1.2 Q1.3	Q2.1 Q2.2 Q2.3	Q3.1
SCO48	Machine Learning in Network Anomaly Detection: A Survey Publisher: IEEE PDF	Song Wang; Juan Fernando Balarezo; Sithamparanathan Kandeepan; Akram Al-Hourani; Karina Gomez Chavez	2021	(2021) IEEE Access, 9, pp. 152379-152396.	Article	Encuesta	Q1.1 Q1.3	Q2.3 Q2.6	Ninguna
SCO47	Detecting Malicious DNS Queries Over Encrypted Tunnels Using Statistical Analysis and Bi-Directional Recurrent Neural Networks	Al-Fawa'reh, Mohammad; Ashi, Zain; and Jafar, Mousa Tayseer	2021	Journal of Modern Science: Vol. 7 : Iss. 4 , Article 4.	Article	Experimento	Q1.1 Q1.3	Q2.1 Q2.3	Q3.1
SCO49	A Learning Approach with Programmable Data Plane towards IoT Security	Qiaofeng Qin, Konstantinos Poularakis, and Leandros Tassiulas	2020	(2020) Proceedings - International Conference on Distributed Computing Systems, 2020-November, art. no. 9355643	Conference Paper	Experimento	Q1.1 Q1.3	Q2.3 Q2.6 Q2.7	Q3.1
SCO50	Data Exfiltration: A Review of External Attack Vectors and Countermeasures	Faheem Ullah, Matthew Edwards, Rajiv Ramdhany, Ruzanna Chitchyan, M. Ali Babar, Awais Rashid	2017	Journal of Network and Computer Applications, 101	Review	Reporte	Q1.1 Q1.4	Q2.3	Q3.1
SCO51	Towards the Design of Hardware Based Security Device and Communication Implementation	Dennis Arturo, Kazuya Takemori, Shinichiro Kubota, Kenichi Sugitani, Yasuo Musashi	2009	Proceedings of the 2nd International Conference on Intelligent Networks and Intelligent Systems, art. no. 5364834, pp. 250-252	Conference Paper	Reporte	Q1.2	Q2.1 Q2.4	Q3.2

ACM									
ACM01	Towards Insider Threat Detection Using Web Server Logs	Myers, Justin; Grimaila, Michael R.; Mills, Robert F.	2009	Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies	conferencePaper	Combinado	Q1.1 Q1.3	Q2.1 Q2.3 Q2.6	Q3.1
ACM02	A Hybrid Intelligent System for Insider Threat Detection Using Iterative Attention	Ren, Xueshuang; Wang, Liming	2020	Proceedings of 2020 the 6th International Conference on Computing and Data Engineering	conferencePaper	Combinado	Q1.3	Q2.3 Q2.6 Q2.7	Q3.1
ACM03	Host-Based Intrusion Detection System with System Calls: Review and Future Trends	Liu, Ming; Xue, Zhi; Xu, Xianghua; Zhong, Changmin; Chen, Jinjun	2018	ACM Comput. Surv.	journalArticle	Reporte	Q1.1 Q1.3	Q2.3 Q2.5 Q2.6	Q3.1
ACM04	Detection of Anomalous Insiders in Collaborative Environments via Relational Analysis of Access Logs	Chen, You; Malin, Bradley	2011	Proceedings of the First ACM Conference on Data and Application Security and Privacy	conferencePaper	Experimento	Q1.3 Q1.4	Q2.3 Q2.5	Q3.1
ACM05	Log2vec: A Heterogeneous Graph Embedding Based Approach for Detecting Cyber Threats within Enterprise	Liu, Fucheng; Wen, Yu; Zhang, Dongxue; Jiang, Xihe; Xing, Xinyu; Meng, Dan	2019	Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security	conferencePaper	Experimento	Q1.1 Q1.3 Q1.4	Q2.3 Q2.6	Q3.1
ACM06	Categorization of Cyber Security Deception Events for Measuring the Severity Level of Advanced Targeted Breaches	Väisänen, Teemu	2017	Proceedings of the 11th European Conference on Software Architecture: Companion Proceedings	conferencePaper	Experimento	Q1.1	Q2.1 Q2.3	Ninguna
ACM07	Protecting Intellectual Property and Sensitive Information in Academic Campuses from Trusted Insiders: Leveraging Active Directory	Bhilare, Dattatraya S.; Ramani, Ashwini K.; Tanwani, Sanjay K.	2009	Proceedings of the 37th Annual ACM SIGUCCS Fall Conference: Communication and Collaboration	conferencePaper	Combinado	Q1.2 Q1.3	Q2.4 Q2.1 Q2.2 Q2.5	Q3.1
ACM08	IoTDePT: Detecting Security Threats and Pinpointing Anomalies in an IoT Environment	Rattanalerdnusorn, Ekkachan; Pattaranantakul, Montida; Thaenkaew, Phithak; Vorakulpipat, Chalee	2020	Proceedings of the 2020 9th International Conference on Software and Computer Applications	conferencePaper	Combinado	Q1.1 Q1.3	Q2.1 Q2.3 Q2.6 Q2.7	Q3.1
ACM09	Design of Network Security Projects Using Honeypots	Sadasivam, Karthik; Samudrala, Banuprasad; Yang, T. Andrew	2005	J. Comput. Sci. Coll.	journalArticle	Reporte	Ninguna	Q2.1 Q2.4 Q2.7	Q3.1
ACM10	Observing Industrial Control System Attacks Launched via Metasploit Framework	Wallace, Nathan; Atkison, Travis	2013	Proceedings of the 51st ACM Southeast Conference	conferencePaper	Experimento	Q1.1 Q1.3	Q2.1 Q2.3	Ninguna

ACM11	Perfect Storm: The Insider, Naivety, and Hostility	Thompson, Herbert H; Ford, Richard	2004	Queue	journalArticle	Combinado	Q1.1 Q1.4		
ACM12	Framework for Distributed Virtual Honeynets	Pisarčík, Peter; Sokol, Pavol	2014	Proceedings of the 7th International Conference on Security of Information and Networks	conferencePaper	Experimento	Q1.1	Q2.1 Q2.3 Q2.5	Q3.1
ACM13	The near Real Time Statistical Asset Priority Driven (Nrtsapd) Risk Assessment Methodology	Pak, Charles	2008	Proceedings of the 9th ACM SIGITE Conference on Information Technology Education	conferencePaper	Experimento	Q1.1	Q2.5	Ninguna
ACM14	Research on Computer Communication Network Security and Guarantee Ways	Hongxia, Li; Lei, Chen	2018	Proceedings of the 2018 2nd International Conference on Algorithms, Computing and Systems	conferencePaper	Reporte	Q1.1 Q1.3	Q2.4	Ninguna
ACM15	Asset Priority Risk Assessment Using Hidden Markov Models	Pak, Charles; Cannady, James	2009	Proceedings of the 10th ACM Conference on SIG-Information Technology Education	conferencePaper	Experimento	Q1.1	Q2.3	Ninguna
Id_paper	**Title**	**Authors**	**Year**	**Source title**	**Document Type**	**Studio Type**	**Q1**	**Q2**	**Q3**
ACM17	LAC : LSTM AUTOENCODER with Community for Insider Threat Detection	Sudipta Paul, Subhankar Mishra	2020	ICBDR 2020: 2020 the 4th International Conference on Big Data Research (ICBDR'20)	conferencePaper	Experimento	Q1.1 Q1.3	Q2.3 Q2.6	Q3.1
ACM193	Repetido Host-Based Intrusion Detection System with System Calls: Review and Future Trends	Ming Liu, Zhi Xue, Xianghua Xu, Changmin Zhong, Jinjun Chen	2019	ACM Computing Surveys (CSUR), Volume 51, Issue 5	Journal paper				
ACM18	Home-centric visualization of network traffic for security administration	Robert Ball, Glenn A. Fink, Chris North	2004	VizSEC/DMSEC '04: Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security	conferencePaper	Reporte	Q1.1	Q2.3	Ninguna
ACM19	Research on intelligent Firewall for network security	Wang Daxian, Zhang Jishan, Yu jiujiu	2020	Proceedings of the 2020 2nd International Conference on Robotics, Intelligent Control and Artificial Intelligence	conferencePaper	Experimento	Q1.1 Q1.4	Q2.3 Q2.5	Ninguna
ACM20	Trailblazing the Artificial Intelligence for Cybersecurity Discipline: A Multi-Disciplinary Research Roadmap	Sagar Samtani, Murat Kantarcioglu, Hsinchun Chen	2020	ACM Transactions on Management Information Systems (TMIS), Volume 11, Issue 4	Journal paper	Reporte	Q1.1 Q1.3	Q2.1 Q2.3	Ninguna
ACM16	AI-empowered IoT Security for Smart Cities AI-empowered IoT Security for Smart Cities	Zhihan Lv, Liang Qiao, Amit Kumar Singh, Qingjun Wang	2021	ACM Transactions on Internet Technology (TOIT), Volume 21, Issue 4	Journal paper	Experimento	Ninguna	Q2.3	Ninguna

IEEE									
IEEE01	Real-Time Network Anomaly Detection System Using Machine Learning	Shuai Zhao, Mayanka Chandrashekar, Yugyung Lee, Deep Medhi	2015	11th International Conference on the Design of Reliable Communication Networks (DRCN)	Article	Experimento	Q1.3	Q2.1 Q2.4 Q2.5 Q2.6	Q3.1
IEEE02	Design and Implementation of Campus Network Intrusion Detection System	Hu Ruipeng	2011	nternational Conference on Intelligence Science and Information Engineering	conferencePaper	Reporte	Q1.2	Q2.1 Q2.4 Q2.6 Q2.7	Q3.2
IEEE03	Applied Research on Snort Intrusion Detection Model in The Campus Network	Changwei Huang, Jinquan Xiong, Zhengwen Peng	2012	EEE Symposium on Robotics and Applications(ISRA)	Article	Reporte	Q1.2	Q2.1 Q2.2 Q2.4 Q2.5 Q2.6 Q2.7	Q3.2
IEEE04	Framework of Intrusion Detection System via Snort Application on Campus Network Environment	Mohd Nazri Ismail, Mohd Taha Ismail	2009	International Conference on Future Computer and Communication	conferencePaper	Experimento	Q1.2	Q2.1 Q2.4 Q2.5	Q3.1 Q3.2
IEEE05	Research on the active defense security system based on cloud computing of wisdom campus network	Yuanyuan Chen, Wang Yao, Jianghua Luo	2016	28th Chinese Control and Decision Conference (CCDC)	conferencePaper	Reporte	Q1.2	Q2.1 Q2.4 Q2.5	Q3.2
IEEE06	An ARP-based Anomaly Detection Algorithm Using Hidden Markov Model in Enterprise Networks	Y.Yasami M.Farahmand V.Zargari	2007	Conference: Systems and Networks Communications, 2007. ICSNC 2007. Second International	conferencePaper	Reporte	Q1.1	Q2.1 Q2.3	Ninguna
IEEE07	Research and design of the distributed intrusion detection system based on Snort	Zhao Kai	2012	2012 International Conference on Computer Science and Electronics Engineering	Article	Reporte	Ninguna	Q2.1 Q2.3	Ninguna
IEEE08	Proposal of a malicious communication control method using OpenFlow	Minoru IKEBE∗, Daiki SHIMOKAWA† and Kazuyuki YOSHIDA	2016	10th International Conference on Complex, Intelligent, and Software Intensive Systems	conferencePaper	Experimento	Q1.2	Q2.1 Q2.4	Q3.1
IEEE09	Intrusion Filtration System(IFS)-mapping Network Security in new way	Ms Rita Dewanjee	2016	International conference on Signal Processing, Communication, Power and Embedded System (SCOPES)	Conference Paper	Experimento	Ninguna	Q2.3	Q3.1
IEEE10	Machine and Deep Learning Based Comparative Analysis Using Hybrid Approaches for Intrusion Detection System	Azam Rashid, Muhammad Jawaid Siddique, Shahid Munir Ahmed	2020	Conference: 2020 3rd International Conference on Advancements in Computational Sciences (ICACS)	conferencePaper	Experimento	Q1.1 Q1.3	Q2.3 Q2.6	Ninguna
IEEE11	Toward an Online Network Intrusion Detection System Based on Ensemble Learning	Ying-Feng Hsu, ZhenYu He, Yuya Tarutani, Morito Matsuoka	2019	12th International Conference on Cloud Computing (CLOUD)	Conference Paper	Experimento	Q1.1 Q1.3	Q2.3 Q2.6	Q3.1

IEEE12	Research On Intrusion Detection Based On Campus Network	Baoyi Wang, Feng Li, Shaomin Zhang	2009	2009 Third International Symposium on Intelligent Information Technology Application	Article	Experimento	Q1.2	Q2.4 Q2.6	Q3.1 Q3.2
IEEE13	Virtual Inline: A Technique of Combining IDS and IPS Together in Response Intrusion	Zheng Wu, Debao Xiao, Hui Xu, Xi Peng, Xin Zhuang	2009	2009 First International Workshop on Education Technology and Computer Science	Article	Reporte	Q1.1	Q2.3	Q3.1
IEEE14	Intelligent Multi-Agent Information Security System	N. Kussul, A..Shelestov, A. Sidorenko, S. Skakun, Y. Veremeenko	2003	IEEE Iolematiooal Workshop on Inrelligca Dam Acquisition and Advanced Computing System: Technology and Applications 8~10 September ZWI	Conference Paper	Experimento	Ninguna	Q2.1 Q2.4	Ninguna
IEEE15	An Integrated Method for Anomaly Detection From Massive System Logs	Zhaoli Liu, Tao Qin, Xiaohong Guan, Hezhi Jiang and Chenxu Wang	2018	Special section on security and trusted computing for industrial internet of things	Article	Experimento	Q1.3	Q2.1 Q2.3 Q2.6	Q3.1
IEEE16	A Deep Reinforcement Learning Approach for Anomaly Network Intrusion Detection System	Ying-Feng Hsu, Morito Matsuoka	2020	Conference: 2020 IEEE 9th International Conference on Cloud Networking (CloudNet)	Conference Paper	Experimento	Q1.3	Q2.3 Q2.6	Q3.1
IEEE17	Network Anomaly Detection and Classification via Opportunistic Sampling	Georgios Androulidakis, Vassilis Chatzigiannakis, and Symeon Papavassiliou,	2009	IEEE Network • January/February 2009	Article	Reporte	Q1.1 Q1.3	Q2.4	Ninguna
IEEE18	Wireless network intrusion detection model and safety enhancement framework for campus network	Qingyuan Shan	2022	Proceedings of the Fourth International Conference on Smart Systems and Inventive Technology (ICSSIT-2022)	Conference Paper	Experimento	Q1.2	Q2.4 Q2.6	Ninguna
IEEE19	Packet- vs. Session-Based Modeling for Intrusion Detection Systems	LTC Bruce D. Caulkins, Joohan Lee, Morgan Wang	2005	Conference: Information Technology: Coding and Computing, 2005. ITCC 2005. International Conference onVolume: 1	Conference Paper	Experimento	Q1.3	Q2.1 Q2.3 Q2.7	Q3.1 Q3.2
IEEE20	Anomaly Detection Based on Available Bandwidth Estimation	Li He, Shunzheng Yu, Min Li	2008	2008 IFIP International Conference on Network and Parallel Computing	Conference Paper	Reporte	Ninguna	Q2.1 Q2.3	Ninguna
IEEE21	Design and Implementation of Honeypot Systems Based on Open-Source Software	Chao-Hsi Yeh and Chung-Huang Yang	2008	Conference: Intelligence and Security Informatics, 2008. ISI 2008. IEEE International Conference on	Conference Paper	Reporte	Q1.1	Q2.3	Q3.1 Q3.2
IEEE23	A Proposed Machine Learning based Scheme for Intrusion Detection	Inadyuti Dutt, Samarjeet Borah, Indrakanta Maitra	2018	Proceedings of the 2nd International conference on Electronics, Communication and Aerospace Technology (ICECA 2018	Conference Paper	Experimento	Q1.3	Q2.3 Q2.6	Q3.1

IEEE24	F-TAD: Traffic Anomaly Detection for Sub-networks Using Fisher Linear Discriminant	Hyunhee Park, Meejoung Kim, Chul-Hee Kang	2009	Conference: Third International Conference on Network and System Security, NSS 2009, Gold Coast, Queensland, Australia, October 19-21, 2009 Authors:	Conference Paper	Experimento	Q1.2 Q1.3	Q2.1 Q2.3 Q2.4	Q3.1
IEEE25	Defending Distributed Systems Against Malicious Intrusions and Network Anomalies*	Kai Hwang, Ying Chen, Hua Liu	2005	Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium (IPDPS'05)	Conference Paper	Experimento	Q1.1	Q2.3	Q3.1
IEEE26	Local Area Detection of Incoming War Dial Activity	Ed Amoroso, Eugene Kogan, Brenda McAnderson, Dan Powell, Brian Rexroad, Steve Schuster, and Anthony Stramaglia	1998	SRDS '98: Proceedings of the The 17th IEEE Symposium on Reliable Distributed Systems	Conference Paper	Experimento	Q1.1	Q2.3	Ninguna
IEEE27	Detecting Attacks on Networks	Chris Herringshaw	1997	ComputerVolume 30Issue 12December 1997 pp 16–17	Article	Reporte	Q1.1	Q2.3 Q2.5 Q2.6	Q3.1
IEEE28	CAN Bus Messages Abnormal Detection Using Improved SVDD in Internet of Vehicles	Xinghua Li, Hengyou Zhang, Yinbin Miao, Siqi Ma , Jianfeng Ma, Ximeng Liu, and Kim-Kwang Raymond Choo	2021	IEEE INTERNET OF THINGS JOURNAL, VOL. 9, NO. 5, MARCH 1, 2022	Article		Ninguna	Ninguna	Ninguna
IEEE29	Parametric Methods for Anomaly Detection in Aggregate Traffic	Gautam Thatte, Urbashi Mitra, and John Heidemann	2011	IEEE/ACM Transactions on Networking 19(2):512 - 525	Article	Reporte	Q1.2	Q2.4 Q2.6	Q3.2
IEEE30	Intranet Security with Micro-Firewalls and Mobile Agents for Proactive Intrusion Response*	Muralidaran Gangadharan and Kai Hwang	2001	Conference: Computer Networks and Mobile Computing, 2001. Proceedings. 2001 International Conference on	Conference Paper	Reporte	Ninguna	Q2.3	Q3.1 Q3.2
IEEE31	Intelligent Flow-based Sampling for Effective Network Anomaly Detection	G. Androulidakis and S. Papavassiliou	2007	Conference: Proceedings of the Global Communications Conference, 2007. GLOBECOM '07	Conference Paper	Experimento	Q1.1 Q1.3	Q2.3 Q2.6	Ninguna
IEEE32	Using Selective Sampling for the Support of Scalable and Efficient Network Anomaly Detection	G. Androulidakis, V. Chatzigiannakis and S. Papavassiliou	2007	Conference: Globecom Workshops, 2007 IEEE	Conference Paper	Reporte	Q1.1 Q1.3	Q2.3 Q2.6	Q3.1
IEEE33	Terminal Security Protection Anomaly Detection Based on Combined Algorithm	Dong Liu, Chunrui Zhang' and Fang Lou	2021	2021 International Conference on Intelligent Computing, Automation and Applications (ICAA)	Conference Paper	Experimento	Ninguna	Q2.3 Q2.6	Q3.1

IEEE34	Mining Network Traffic Anomaly Based on Adjustable Piecewise Entropy	Geng Tian∗†, Zhiliang Wang∗‡, Xia Yin∗†, Zimu Li∗‡, Xingang Shi∗‡, Ziyi Lu§, Chao Zhou§, Yang Yu∗†, Yingya Guo∗†	2015	Conference: 2015 IEEE 23rd International Symposium on Quality of Service (IWQoS)	Conference Paper	Experimento	Q1.3	Q2.3 Q2.6	Q3.1
IEEE35	BEDIM: Lateral Movement Detection In Enterprise Network Through Behavior Deviation Measurement	Cong Dong† , Yufan Chen‡ , Yunjian Zhang† , Yuling Liu† , Zhigang Lu † , Pu Dong †∗, and Baoxu Liu†	2021	IEEE 23rd Int Conf on High Performance Computing & Communications; 7th Int Conf on Data Science & Systems; 19th Int Conf on Smart City; 7th Int Conf on Dependability in Sensor, Cloud & Big Data Systems & Application	Conference Paper	Experimento	Q1.1 Q1.3	Q2.3	Q3.1
IEEE36	Clustering-based Anomaly Detection for Smartphone Applications	Ali El Attar, Rida Khatoun and Marc Lemercier	2014	Conference: NOMS 2014 - 2014 IEEE/IFIP Network Operations and Management Symposium	Conference Paper	Reporte	Q1.1 Q1.3	Q2.1 Q2.2 Q2.3 Q2.6	Q3.1
IEEE37	Detection of NS Resource Record based DNS Query Request Packet Traffic and SSH Dictionary Attack Activity	Kazuya Takemori,∗ and Dennis Arturo Ludena Roma ˜ na˜ ∗ Shinichiro Kubota,† Kenichi Sugitani,† and Yasuo Musashi	2009	2009 Second International Conference on Intelligent Networks and Intelligent Systems	Article	Experimento	Q1.2	Q2.1 Q2.4	Ninguna
IEEE38	An Intuitive Study: Intrusion Detection Systems and Anomalies, How AI can be used as a tool to enable the majority, in 5G era.	Mr.Siddhant Shah, Mr. Shailesh Pramod Bendale	2020	Project: Security in Software Defined Network	Article	Reporte	Q1.1	Q2.3 Q2.5 Q2.6	Ninguna
IEEE39	TAICHI: AN OPEN INTRUSION AUTOMATIC RESPONSE SYSTEM BASED ON PLUGIN	HONG HAN, XIAN-LIANG LU, LI-YONG REN, BO CHEN	2006	Proceedings of the Fifth International Conference on Machine Learning and Cybernetics	Conference Paper	Reporte	Q1.1 Q1.4	Q2.3	Q3.1
IEEE40	A Behavior Sequence Clustering-based Enterprise Network Anomaly Host Recognition Method	Jing Tao, Ning Zheng, Waner Wang, Ting Han, Xuna Zhan, Qingxin Luan	2019	Conference: 2019 IEEE International Conference on Big Knowledge (ICBK)	Conference paper	Experimento	Q1.2	Q2.1 Q2.4	Q3.1
IEEE41									
IEEE42	Model for Security in Wired and Wireless Network for Education	Aditya Patel, Sweta Ghaghda, Payal Nagecha	2014	Conference: 2014 International Conference on Computing for Sustainable Global Development (INDIACom)	Conference paper	Encuesta	Q1.1 Q1.2	Q2.4 Q2.6	Q3.2

IEEE43	An Empirical Approach to Modeling Uncertainty in Intrusion Analysis	Xinming Ou, Siva Raj Rajagopalan, Sakthiyuvaraja Sakthivelmurugan	2009	2009 Annual Computer Security Applications Conference	Conference Paper	Reporte	Q1.2	Q2.4	Q3.1
IEEE44	Leveraging SDN for Efficient Anomaly Detection and Mitigation on Legacy Networks	K. Giotis, G. Androulidakis, V. Maglaris	2014	Conference: Third European Workshop on Software Defined Networks (EWSDN) 2014At: Budapest	Conference paper	Experimento	Q1.2 Q1.3	Q2.4 Q2.6	Q3.1
IEEE45	Real Time DNS Traffic Profiling Enhanced Detection Design for National Level Network	Muhammad Salahuddien Manggalanny, Kalamullah Ramli	2017	2017 International Seminar on Intelligent Technology and Its Application	Conference Paper	Experimento	Q1.1	Q2.1 Q2.3 Q2.5 Q2.6 Q2.7	Q3.1
IEEE46	Evolving Switch Architecture toward Accommodating In-Network Intelligence	Shuangwu Chen, Xiang Chen, Zhen Yao, Jian Yang, Yangyang Li, and Feng Wu	2020	January 2020IEEE Communications Magazine 58(1):33-39	Article	Experimento	Q1.3	Q2.3 Q2.6	Ninguna
IEEE47	MaMPF: Encrypted Traffic Classification Based on Multi-Attribute Markov Probability Fingerprints	Chang Liu, Zigang Cao, Gang Xiong, Gaopeng Gou, Siu-Ming Yiu, Longtao He	2018	Conference: 2018 IEEE/ACM 26th International Symposium on Quality of Service (IWQoS)	Conference Paper	Reporte	Q1.3	Q2.1 Q2.3	Ninguna
IEEE48	No Way to Evade: Detecting Multi-Path Routing Attacks for NIDS	Likun Liu, Jiantao Shi, Hongli Zhang, and Xiangzhan Yu	2019	Conference: GLOBECOM 2019 - 2019 IEEE Global Communications Conference	Conference Paper	Experimento	Q1.1	Q2.3 Q2.6	Q3.1
IEEE49	Detection of Host Search Activity in PTR Resource Record Based DNS Query Packet Traffic	Yasuo Musashi,* Florent Hequet,† Dennis Arturo Ludeña Romaña,† Shinichiro Kubota,* and Kenichi Sugitani*	2010	Proceedings of the 2010 IEEE International Conference on Information and Automation June 20 - 23,	Article	Experimento	Q1.2	Q2.1 Q2.3 Q2.6	Ninguna
IEEE50	Identifying Suspicious Activities through DNS Failure Graph Analysis	Nan Jiang∗, Jin Cao†, Yu Jin∗, Li Erran Li†, Zhi-Li Zhang∗	2010	Conference: Network Protocols (ICNP), 2010 18th IEEE International Conference on	Conference Paper	Experimento	Q1.2	Q2.4	Ninguna
IEEE51	TVMonitor: A P2P-TV Content Monitoring Platform	Su He, Xin Zhang, Zhihong Jiang, Hao Kang, Hui Wang	2011	2011 Third International Conference on Multimedia Information Networking and Security	Article	Reporte	Ninguna	Q2.1	Ninguna

Fuente. Elaboración propia.

ANEXO D. ANÁLISIS CUALITATIVO RSL.

En la Tabla 55, se detallan los parámetros considerados para el Análisis Cualitativo de los papers previo al análisis de la RSL. Incluyen: Número de paper, Título, Id_Pregunta, Descripción, Calificación y Promedio.

Tabla 55: **ANÁLISIS CUALITATIVO RSL.**

No. Paper	Título	Id_Pregunta	Descripción	Calificación	Promedio
SCO01	Cybersecurity data science: an overview from machine learning perspective	PCT1	¿El diseño de la investigación es adecuado para llevar a cabo el estudio?	5	
		PCT2	¿El estudio se basa en el cuerpo de conocimiento existente, es decir, analiza explícitamente su contribución a la luz de trabajos anteriores?	5	
		PCT3	¿Los hallazgos son creíbles?	3	
		PCT4	¿El proceso de investigación se describe a fondo? ¿Los obstáculos son descritos de manera útil?	4	
		PCT5	¿Están claros los vínculos entre los datos, la interpretación y las conclusiones?	5	
		PCT6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	5	
		PCT7	¿La presentación de informes es clara y coherente?	5	
		PCT8	¿Son claras las suposiciones, perspectivas teóricas, valores que han configurado la forma y el resultado de la evaluación?	3	4.375
ACM01	Towards Insider Threat Detection Using Web Server Logs	PCT1	¿El diseño de la investigación es adecuado para llevar a cabo el estudio?	3	
		PCT2	¿El estudio se basa en el cuerpo de conocimiento existente, es decir, analiza explícitamente su contribución a la luz de trabajos anteriores?	5	
		PCT3	¿Los hallazgos son creíbles?	3	
		PCT4	¿El proceso de investigación se describe a fondo? ¿Los obstáculos son descritos de manera útil?	5	
		PCT5	¿Están claros los vínculos entre los datos, la interpretación y las conclusiones?	5	
		PCT6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	5	

		PCT7	¿La presentación de informes es clara y coherente?	5	
		PCT8	¿Son claras las suposiciones, perspectivas teóricas, valores que han configurado la forma y el resultado de la evaluación?	5	4.5
ACM06	**Categorization of Cyber Security Deception Events for Measuring the Severity Level of Advanced Targeted Breaches**	PCT1	¿El diseño de la investigación es adecuado para llevar a cabo el estudio?	3	
		PCT2	¿El estudio se basa en el cuerpo de conocimiento existente, es decir, analiza explícitamente su contribución a la luz de trabajos anteriores?	5	
		PCT3	¿Los hallazgos son creíbles?	3	
		PCT4	¿El proceso de investigación se describe a fondo? ¿Los obstáculos son descritos de manera útil?	3	
		PCT5	¿Están claros los vínculos entre los datos, la interpretación y las conclusiones?	4	
		PCT6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PCT7	¿La presentación de informes es clara y coherente?	3	
		PCT8	¿Son claras las suposiciones, perspectivas teóricas, valores que han configurado la forma y el resultado de la evaluación?	3	3.375
ACM07	Protecting Intellectual Property and Sensitive Information in Academic Campuses from Trusted Insiders: Leveraging Active Directory	PCT1	¿El diseño de la investigación es adecuado para llevar a cabo el estudio?	4	
		PCT2	¿El estudio se basa en el cuerpo de conocimiento existente, es decir, analiza explícitamente su contribución a la luz de trabajos anteriores?	5	
		PCT3	¿Los hallazgos son creíbles?	3	
		PCT4	¿El proceso de investigación se describe a fondo? ¿Los obstáculos son descritos de manera útil?	5	
		PCT5	¿Están claros los vínculos entre los datos, la interpretación y las conclusiones?	3	
		PCT6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PCT7	¿La presentación de informes es clara y coherente?	3	
		PCT8	¿Son claras las suposiciones, perspectivas teóricas, valores que han configurado la forma y el resultado de la evaluación?	5	3.875
ACM08		PCT1	¿El diseño de la investigación es adecuado para llevar a cabo el estudio?	5	

	IoTDePT: Detecting Security Threats and Pinpointing Anomalies in an IoT Environment	PCT2	¿El estudio se basa en el cuerpo de conocimiento existente, es decir, analiza explícitamente su contribución a la luz de trabajos anteriores?	4	
		PCT3	¿Los hallazgos son creíbles?	5	
		PCT4	¿El proceso de investigación se describe a fondo? ¿Los obstáculos son descritos de manera útil?	4	
		PCT5	¿Están claros los vínculos entre los datos, la interpretación y las conclusiones?	5	
		PCT6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	5	
		PCT7	¿La presentación de informes es clara y coherente?	5	
		PCT8	¿Son claras las suposiciones, perspectivas teóricas, valores que han configurado la forma y el resultado de la evaluación?	4	4.625
ACM09	Observing Industrial Control System Attacks Launched via Metasploit Framework	PCT1	¿El diseño de la investigación es adecuado para llevar a cabo el estudio?	3	
		PCT2	¿El estudio se basa en el cuerpo de conocimiento existente, es decir, analiza explícitamente su contribución a la luz de trabajos anteriores?	5	
		PCT3	¿Los hallazgos son creíbles?	3	
		PCT4	¿El proceso de investigación se describe a fondo? ¿Los obstáculos son descritos de manera útil?	5	
		PCT5	¿Están claros los vínculos entre los datos, la interpretación y las conclusiones?	3	
		PCT6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	5	
		PCT7	¿La presentación de informes es clara y coherente?	4	
		PCT8	¿Son claras las suposiciones, perspectivas teóricas, valores que han configurado la forma y el resultado de la evaluación?	3	3.875
ACM11	Perfect Storm: The Insider, Naivety, and Hostility	PCT1	¿El diseño de la investigación es adecuado para llevar a cabo el estudio?	3	
		PCT2	¿El estudio se basa en el cuerpo de conocimiento existente, es decir, analiza explícitamente su contribución a la luz de trabajos anteriores?	3	
		PCT3	¿Los hallazgos son creíbles?	3	
		PCT4	¿El proceso de investigación se describe a fondo? ¿Los obstáculos son descritos de manera útil?	4	

		PCT5	¿Están claros los vínculos entre los datos, la interpretación y las conclusiones?	3	
		PCT6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PCT7	¿La presentación de informes es clara y coherente?	4	
		PCT8	¿Son claras las suposiciones, perspectivas teóricas, valores que han configurado la forma y el resultado de la evaluación?	4	3.375
ACM14	Research on Computer Communication Network Security and Guarantee Ways	PCT1	¿El diseño de la investigación es adecuado para llevar a cabo el estudio?	4	
		PCT2	¿El estudio se basa en el cuerpo de conocimiento existente, es decir, analiza explícitamente su contribución a la luz de trabajos anteriores?	3	
		PCT3	¿Los hallazgos son creíbles?	3	
		PCT4	¿El proceso de investigación se describe a fondo? ¿Los obstáculos son descritos de manera útil?	3	
		PCT5	¿Están claros los vínculos entre los datos, la interpretación y las conclusiones?	4	
		PCT6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	4	
		PCT7	¿La presentación de informes es clara y coherente?	4	
		PCT8	¿Son claras las suposiciones, perspectivas teóricas, valores que han configurado la forma y el resultado de la evaluación?	5	3.75
ACM20	Home-centric visualization of network traffic for security administration	PCT1	¿El diseño de la investigación es adecuado para llevar a cabo el estudio?	4	
		PCT2	¿El estudio se basa en el cuerpo de conocimiento existente, es decir, analiza explícitamente su contribución a la luz de trabajos anteriores?	3	
		PCT3	¿Los hallazgos son creíbles?	4	
		PCT4	¿El proceso de investigación se describe a fondo? ¿Los obstáculos son descritos de manera útil?	4	
		PCT5	¿Están claros los vínculos entre los datos, la interpretación y las conclusiones?	3	
		PCT6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	4	
		PCT7	¿La presentación de informes es clara y coherente?	4	

		PCT8	¿Son claras las suposiciones, perspectivas teóricas, valores que han configurado la forma y el resultado de la evaluación?	5	3.875
ACM21	Research on intelligent Firewall for network security	PCT1	¿El diseño de la investigación es adecuado para llevar a cabo el estudio?	3	
		PCT2	¿El estudio se basa en el cuerpo de conocimiento existente, es decir, analiza explícitamente su contribución a la luz de trabajos anteriores?	3	
		PCT3	¿Los hallazgos son creíbles?	3	
		PCT4	¿El proceso de investigación se describe a fondo? ¿Los obstáculos son descritos de manera útil?	3	
		PCT5	¿Están claros los vínculos entre los datos, la interpretación y las conclusiones?	3	
		PCT6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PCT7	¿La presentación de informes es clara y coherente?	3	
		PCT8	¿Son claras las suposiciones, perspectivas teóricas, valores que han configurado la forma y el resultado de la evaluación?	2	2.875
ACM22	Trailblazing the Artificial Intelligence for Cybersecurity Discipline: A Multi-Disciplinary Research Roadmap	PCT1	¿El diseño de la investigación es adecuado para llevar a cabo el estudio?	3	
		PCT2	¿El estudio se basa en el cuerpo de conocimiento existente, es decir, analiza explícitamente su contribución a la luz de trabajos anteriores?	4	
		PCT3	¿Los hallazgos son creíbles?	4	
		PCT4	¿El proceso de investigación se describe a fondo? ¿Los obstáculos son descritos de manera útil?	4	
		PCT5	¿Están claros los vínculos entre los datos, la interpretación y las conclusiones?	4	
		PCT6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	4	
		PCT7	¿La presentación de informes es clara y coherente?	4	
		PCT8	¿Son claras las suposiciones, perspectivas teóricas, valores que han configurado la forma y el resultado de la evaluación?	4	3.875
ACM03		PCT1	¿El diseño de la investigación es adecuado para llevar a cabo el estudio?	4	

	Host-Based Intrusion Detection System with System Calls: Review and Future Trends	PCT2	¿El estudio se basa en el cuerpo de conocimiento existente, es decir, analiza explícitamente su contribución a la luz de trabajos anteriores?	4	
		PCT3	¿Los hallazgos son creíbles?	4	
		PCT4	¿El proceso de investigación se describe a fondo? ¿Los obstáculos son descritos de manera útil?	4	
		PCT5	¿Están claros los vínculos entre los datos, la interpretación y las conclusiones?	4	
		PCT6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	4	
		PCT7	¿La presentación de informes es clara y coherente?	5	
		PCT8	¿Son claras las suposiciones, perspectivas teóricas, valores que han configurado la forma y el resultado de la evaluación?	4	4.125
SCO04	A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics	PCT1	¿El diseño de la investigación es adecuado para llevar a cabo el estudio?	5	
		PCT2	¿El estudio se basa en el cuerpo de conocimiento existente, es decir, analiza explícitamente su contribución a la luz de trabajos anteriores?	5	
		PCT3	¿Los hallazgos son creíbles?	4	
		PCT4	¿El proceso de investigación se describe a fondo? ¿Los obstáculos son descritos de manera útil?	4	
		PCT5	¿Están claros los vínculos entre los datos, la interpretación y las conclusiones?	3	
		PCT6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	4	
		PCT7	¿La presentación de informes es clara y coherente?	5	
		PCT8	¿Son claras las suposiciones, perspectivas teóricas, valores que han configurado la forma y el resultado de la evaluación?	4	4.25
SCO03	Detection and mitigation of DDoS attacks in SDN: A comprehensive review, research challenges and future directions	PCT1	¿El diseño de la investigación es adecuado para llevar a cabo el estudio?	4	
		PCT2	¿El estudio se basa en el cuerpo de conocimiento existente, es decir, analiza explícitamente su contribución a la luz de trabajos anteriores?	4	
		PCT3	¿Los hallazgos son creíbles?	5	
		PCT4	¿El proceso de investigación se describe a fondo? ¿Los obstáculos son descritos de manera útil?	4	

		PCT5	¿Están claros los vínculos entre los datos, la interpretación y las conclusiones?	5	
		PCT6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PCT7	¿La presentación de informes es clara y coherente?	5	
		PCT8	¿Son claras las suposiciones, perspectivas teóricas, valores que han configurado la forma y el resultado de la evaluación?	3	4.125
SCO12	A survey of network-based intrusion detection data sets	PCT1	¿El diseño de la investigación es adecuado para llevar a cabo el estudio?	4	
		PCT2	¿El estudio se basa en el cuerpo de conocimiento existente, es decir, analiza explícitamente su contribución a la luz de trabajos anteriores?	5	
		PCT3	¿Los hallazgos son creíbles?	4	
		PCT4	¿El proceso de investigación se describe a fondo? ¿Los obstáculos son descritos de manera útil?	4	
		PCT5	¿Están claros los vínculos entre los datos, la interpretación y las conclusiones?	4	
		PCT6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PCT7	¿La presentación de informes es clara y coherente?	5	
		PCT8	¿Son claras las suposiciones, perspectivas teóricas, valores que han configurado la forma y el resultado de la evaluación?	4	4.125
SCO15	Artificial intelligence enabled software-defined networking: A comprehensive overview	PCT1	¿El diseño de la investigación es adecuado para llevar a cabo el estudio?	3	
		PCT2	¿El estudio se basa en el cuerpo de conocimiento existente, es decir, analiza explícitamente su contribución a la luz de trabajos anteriores?	5	
		PCT3	¿Los hallazgos son creíbles?	3	
		PCT4	¿El proceso de investigación se describe a fondo? ¿Los obstáculos son descritos de manera útil?	4	
		PCT5	¿Están claros los vínculos entre los datos, la interpretación y las conclusiones?	4	
		PCT6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	4	
		PCT7	¿La presentación de informes es clara y coherente?	4	

		PCT8	¿Son claras las suposiciones, perspectivas teóricas, valores que han configurado la forma y el resultado de la evaluación?	3	3.75
SCO14	Fixing network security vulnerabilities in local area network	PCT1	¿El diseño de la investigación es adecuado para llevar a cabo el estudio?	3	
		PCT2	¿El estudio se basa en el cuerpo de conocimiento existente, es decir, analiza explícitamente su contribución a la luz de trabajos anteriores?	4	
		PCT3	¿Los hallazgos son creíbles?	3	
		PCT4	¿El proceso de investigación se describe a fondo? ¿Los obstáculos son descritos de manera útil?	3	
		PCT5	¿Están claros los vínculos entre los datos, la interpretación y las conclusiones?	4	
		PCT6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PCT7	¿La presentación de informes es clara y coherente?	3	
		PCT8	¿Son claras las suposiciones, perspectivas teóricas, valores que han configurado la forma y el resultado de la evaluación?	4	3.375
SCO18	A survey of machine learning techniques applied to software defined networking (SDN): Research issues and challenges	PCT1	¿El diseño de la investigación es adecuado para llevar a cabo el estudio?	4	
		PCT2	¿El estudio se basa en el cuerpo de conocimiento existente, es decir, analiza explícitamente su contribución a la luz de trabajos anteriores?	5	
		PCT3	¿Los hallazgos son creíbles?	4	
		PCT4	¿El proceso de investigación se describe a fondo? ¿Los obstáculos son descritos de manera útil?	4	
		PCT5	¿Están claros los vínculos entre los datos, la interpretación y las conclusiones?	3	
		PCT6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	4	
		PCT7	¿La presentación de informes es clara y coherente?	4	
		PCT8	¿Son claras las suposiciones, perspectivas teóricas, valores que han configurado la forma y el resultado de la evaluación?	4	4
SCO21		PCT1	¿El diseño de la investigación es adecuado para llevar a cabo el estudio?	4	

	A feasibility analysis for edge computing fusion in LPWA IoT environment with SDN structure	PCT2	¿El estudio se basa en el cuerpo de conocimiento existente, es decir, analiza explícitamente su contribución a la luz de trabajos anteriores?	4	
		PCT3	¿Los hallazgos son creíbles?	3	
		PCT4	¿El proceso de investigación se describe a fondo? ¿Los obstáculos son descritos de manera útil?	4	
		PCT5	¿Están claros los vínculos entre los datos, la interpretación y las conclusiones?	4	
		PCT6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	4	
		PCT7	¿La presentación de informes es clara y coherente?	3	
		PCT8	¿Son claras las suposiciones, perspectivas teóricas, valores que han configurado la forma y el resultado de la evaluación?	4	3.75
SCO23	Complexity of insider attacks to databases	PCT1	¿El diseño de la investigación es adecuado para llevar a cabo el estudio?	4	
		PCT2	¿El estudio se basa en el cuerpo de conocimiento existente, es decir, analiza explícitamente su contribución a la luz de trabajos anteriores?	4	
		PCT3	¿Los hallazgos son creíbles?	4	
		PCT4	¿El proceso de investigación se describe a fondo? ¿Los obstáculos son descritos de manera útil?	4	
		PCT5	¿Están claros los vínculos entre los datos, la interpretación y las conclusiones?	4	
		PCT6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	4	
		PCT7	¿La presentación de informes es clara y coherente?	4	
		PCT8	¿Son claras las suposiciones, perspectivas teóricas, valores que han configurado la forma y el resultado de la evaluación?	4	4
SCO27	Resilience support in software-defined networking: A survey	PCT1	¿El diseño de la investigación es adecuado para llevar a cabo el estudio?	4	
		PCT2	¿El estudio se basa en el cuerpo de conocimiento existente, es decir, analiza explícitamente su contribución a la luz de trabajos anteriores?	5	
		PCT3	¿Los hallazgos son creíbles?	4	
		PCT4	¿El proceso de investigación se describe a fondo? ¿Los obstáculos son descritos de manera útil?	3	

		PCT5	¿Están claros los vínculos entre los datos, la interpretación y las conclusiones?	3	
		PCT6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PCT7	¿La presentación de informes es clara y coherente?	4	
		PCT8	¿Son claras las suposiciones, perspectivas teóricas, valores que han configurado la forma y el resultado de la evaluación?	4	3.75
SCO28	A Survey of Securing Networks Using Software Defined Networking	PCT1	¿El diseño de la investigación es adecuado para llevar a cabo el estudio?	4	
		PCT2	¿El estudio se basa en el cuerpo de conocimiento existente, es decir, analiza explícitamente su contribución a la luz de trabajos anteriores?	5	
		PCT3	¿Los hallazgos son creíbles?	4	
		PCT4	¿El proceso de investigación se describe a fondo? ¿Los obstáculos son descritos de manera útil?	3	
		PCT5	¿Están claros los vínculos entre los datos, la interpretación y las conclusiones?	4	
		PCT6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PCT7	¿La presentación de informes es clara y coherente?	4	
		PCT8	¿Son claras las suposiciones, perspectivas teóricas, valores que han configurado la forma y el resultado de la evaluación?	4	3.875
SCO32	Penetration testing and network auditing: Linux	PCT1	¿El diseño de la investigación es adecuado para llevar a cabo el estudio?	3	
		PCT2	¿El estudio se basa en el cuerpo de conocimiento existente, es decir, analiza explícitamente su contribución a la luz de trabajos anteriores?	3	
		PCT3	¿Los hallazgos son creíbles?	3	
		PCT4	¿El proceso de investigación se describe a fondo? ¿Los obstáculos son descritos de manera útil?	3	
		PCT5	¿Están claros los vínculos entre los datos, la interpretación y las conclusiones?	3	
		PCT6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PCT7	¿La presentación de informes es clara y coherente?	3	

		PCT8	¿Son claras las suposiciones, perspectivas teóricas, valores que han configurado la forma y el resultado de la evaluación?	3	3
SCO34	A Survey of Securing Networks Using Software Defined Networking	PCT1	¿El diseño de la investigación es adecuado para llevar a cabo el estudio?	3	
		PCT2	¿El estudio se basa en el cuerpo de conocimiento existente, es decir, analiza explícitamente su contribución a la luz de trabajos anteriores?	4	
		PCT3	¿Los hallazgos son creíbles?	4	
		PCT4	¿El proceso de investigación se describe a fondo? ¿Los obstáculos son descritos de manera útil?	3	
		PCT5	¿Están claros los vínculos entre los datos, la interpretación y las conclusiones?	3	
		PCT6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PCT7	¿La presentación de informes es clara y coherente?	4	
		PCT8	¿Son claras las suposiciones, perspectivas teóricas, valores que han configurado la forma y el resultado de la evaluación?	4	3.5
SCO35	Detection of DNS traffic anomalies in large networks	PCT1	¿El diseño de la investigación es adecuado para llevar a cabo el estudio?	3	
		PCT2	¿El estudio se basa en el cuerpo de conocimiento existente, es decir, analiza explícitamente su contribución a la luz de trabajos anteriores?	3	
		PCT3	¿Los hallazgos son creíbles?	3	
		PCT4	¿El proceso de investigación se describe a fondo? ¿Los obstáculos son descritos de manera útil?	3	
		PCT5	¿Están claros los vínculos entre los datos, la interpretación y las conclusiones?	4	
		PCT6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PCT7	¿La presentación de informes es clara y coherente?	4	
		PCT8	¿Son claras las suposiciones, perspectivas teóricas, valores que han configurado la forma y el resultado de la evaluación?	3	3.25
SCO37		PCT1	¿El diseño de la investigación es adecuado para llevar a cabo el estudio?	4	

	Advanced framework of defense system for prevetion of insider's malicious behaviors	PCT2	¿El estudio se basa en el cuerpo de conocimiento existente, es decir, analiza explícitamente su contribución a la luz de trabajos anteriores?	3	
		PCT3	¿Los hallazgos son creíbles?	4	
		PCT4	¿El proceso de investigación se describe a fondo? ¿Los obstáculos son descritos de manera útil?	4	
		PCT5	¿Están claros los vínculos entre los datos, la interpretación y las conclusiones?	4	
		PCT6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PCT7	¿La presentación de informes es clara y coherente?	4	
		PCT8	¿Son claras las suposiciones, perspectivas teóricas, valores que han configurado la forma y el resultado de la evaluación?	3	3.625
SCO42	Towards security automation in Software Defined Networks(Review)	PCT1	¿El diseño de la investigación es adecuado para llevar a cabo el estudio?	3	
		PCT2	¿El estudio se basa en el cuerpo de conocimiento existente, es decir, analiza explícitamente su contribución a la luz de trabajos anteriores?	4	
		PCT3	¿Los hallazgos son creíbles?	4	
		PCT4	¿El proceso de investigación se describe a fondo? ¿Los obstáculos son descritos de manera útil?	3	
		PCT5	¿Están claros los vínculos entre los datos, la interpretación y las conclusiones?	3	
		PCT6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PCT7	¿La presentación de informes es clara y coherente?	4	
		PCT8	¿Son claras las suposiciones, perspectivas teóricas, valores que han configurado la forma y el resultado de la evaluación?	3	3.375
SCO43	Three decades of deception techniques in active cyber defense - Retrospect and outlook	PCT1	¿El diseño de la investigación es adecuado para llevar a cabo el estudio?	4	
		PCT2	¿El estudio se basa en el cuerpo de conocimiento existente, es decir, analiza explícitamente su contribución a la luz de trabajos anteriores?	4	
		PCT3	¿Los hallazgos son creíbles?	4	
		PCT4	¿El proceso de investigación se describe a fondo? ¿Los obstáculos son descritos de manera útil?	4	

		PCT5	¿Están claros los vínculos entre los datos, la interpretación y las conclusiones?	4	
		PCT6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PCT7	¿La presentación de informes es clara y coherente?	4	
		PCT8	¿Son claras las suposiciones, perspectivas teóricas, valores que han configurado la forma y el resultado de la evaluación?	4	3.875
SCO44	Security of Power Line Communication systems: Issues, limitations and existing solutions	PCT1	¿El diseño de la investigación es adecuado para llevar a cabo el estudio?	3	
		PCT2	¿El estudio se basa en el cuerpo de conocimiento existente, es decir, analiza explícitamente su contribución a la luz de trabajos anteriores?	4	
		PCT3	¿Los hallazgos son creíbles?	4	
		PCT4	¿El proceso de investigación se describe a fondo? ¿Los obstáculos son descritos de manera útil?	4	
		PCT5	¿Están claros los vínculos entre los datos, la interpretación y las conclusiones?	4	
		PCT6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	4	
		PCT7	¿La presentación de informes es clara y coherente?	4	
		PCT8	¿Son claras las suposiciones, perspectivas teóricas, valores que han configurado la forma y el resultado de la evaluación?	4	3.875
SCO48	Machine Learning in Network Anomaly Detection: A Survey	PCT1	¿El diseño de la investigación es adecuado para llevar a cabo el estudio?	5	
		PCT2	¿El estudio se basa en el cuerpo de conocimiento existente, es decir, analiza explícitamente su contribución a la luz de trabajos anteriores?	5	
		PCT3	¿Los hallazgos son creíbles?	4	
		PCT4	¿El proceso de investigación se describe a fondo? ¿Los obstáculos son descritos de manera útil?	4	
		PCT5	¿Están claros los vínculos entre los datos, la interpretación y las conclusiones?	4	
		PCT6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	4	
		PCT7	¿La presentación de informes es clara y coherente?	5	

		PCT8	¿Son claras las suposiciones, perspectivas teóricas, valores que han configurado la forma y el resultado de la evaluación?	4	4.375
SCO47	Detecting Malicious DNS Queries Over Encrypted Tunnels Using Statistical Analysis and Bi-Directional Recurrent Neural Networks	PCT1	¿El diseño de la investigación es adecuado para llevar a cabo el estudio?	4	
		PCT2	¿El estudio se basa en el cuerpo de conocimiento existente, es decir, analiza explícitamente su contribución a la luz de trabajos anteriores?	4	
		PCT3	¿Los hallazgos son creíbles?	4	
		PCT4	¿El proceso de investigación se describe a fondo? ¿Los obstáculos son descritos de manera útil?	4	
		PCT5	¿Están claros los vínculos entre los datos, la interpretación y las conclusiones?	4	
		PCT6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PCT7	¿La presentación de informes es clara y coherente?	5	
		PCT8	¿Son claras las suposiciones, perspectivas teóricas, valores que han configurado la forma y el resultado de la evaluación?	4	4
SCO06	An Automated Framework to Uncover Malicious Traffic for University Campus Network	PCT1	¿El diseño de la investigación es adecuado para llevar a cabo el estudio?	4	
		PCT2	¿El estudio se basa en el cuerpo de conocimiento existente, es decir, analiza explícitamente su contribución a la luz de trabajos anteriores?	3	
		PCT3	¿Los hallazgos son creíbles?	4	
		PCT4	¿El proceso de investigación se describe a fondo? ¿Los obstáculos son descritos de manera útil?	5	
		PCT5	¿Están claros los vínculos entre los datos, la interpretación y las conclusiones?	4	
		PCT6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	4	
		PCT7	¿La presentación de informes es clara y coherente?	4	
		PCT8	¿Son claras las suposiciones, perspectivas teóricas, valores que han configurado la forma y el resultado de la evaluación?	5	4.125
SCO22	On Using Cognition for Anomaly Detection in SDN	PCT1	¿El diseño de la investigación es adecuado para llevar a cabo el estudio?	3	

		PCT2	¿El estudio se basa en el cuerpo de conocimiento existente, es decir, analiza explícitamente su contribución a la luz de trabajos anteriores?	3	
		PCT3	¿Los hallazgos son creíbles?	4	
		PCT4	¿El proceso de investigación se describe a fondo? ¿Los obstáculos son descritos de manera útil?	4	
		PCT5	¿Están claros los vínculos entre los datos, la interpretación y las conclusiones?	4	
		PCT6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PCT7	¿La presentación de informes es clara y coherente?	4	
		PCT8	¿Son claras las suposiciones, perspectivas teóricas, valores que han configurado la forma y el resultado de la evaluación?	4	3.625
SCO26	Leveraging SDN for ARP security	PCT1	¿El diseño de la investigación es adecuado para llevar a cabo el estudio?	4	
		PCT2	¿El estudio se basa en el cuerpo de conocimiento existente, es decir, analiza explícitamente su contribución a la luz de trabajos anteriores?	3	
		PCT3	¿Los hallazgos son creíbles?	4	
		PCT4	¿El proceso de investigación se describe a fondo? ¿Los obstáculos son descritos de manera útil?	3	
		PCT5	¿Están claros los vínculos entre los datos, la interpretación y las conclusiones?	4	
		PCT6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	4	
		PCT7	¿La presentación de informes es clara y coherente?	4	
		PCT8	¿Son claras las suposiciones, perspectivas teóricas, valores que han configurado la forma y el resultado de la evaluación?	4	3.75
SCO50	Data Exfiltration: A Review of External Attack Vectors and Countermeasures	PCT1	¿El diseño de la investigación es adecuado para llevar a cabo el estudio?	5	
		PCT2	¿El estudio se basa en el cuerpo de conocimiento existente, es decir, analiza explícitamente su contribución a la luz de trabajos anteriores?	5	
		PCT3	¿Los hallazgos son creíbles?	4	
		PCT4	¿El proceso de investigación se describe a fondo? ¿Los obstáculos son descritos de manera útil?	4	

		PCT5	¿Están claros los vínculos entre los datos, la interpretación y las conclusiones?	4	
		PCT6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	4	
		PCT7	¿La presentación de informes es clara y coherente?	5	
		PCT8	¿Son claras las suposiciones, perspectivas teóricas, valores que han configurado la forma y el resultado de la evaluación?	5	4.5
SCO51	Towards the Design of Hardware Based Security Device and Communication Implementation	PCT1	¿El diseño de la investigación es adecuado para llevar a cabo el estudio?	3	
		PCT2	¿El estudio se basa en el cuerpo de conocimiento existente, es decir, analiza explícitamente su contribución a la luz de trabajos anteriores?	3	
		PCT3	¿Los hallazgos son creíbles?	3	
		PCT4	¿El proceso de investigación se describe a fondo? ¿Los obstáculos son descritos de manera útil?	3	
		PCT5	¿Están claros los vínculos entre los datos, la interpretación y las conclusiones?	3	
		PCT6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PCT7	¿La presentación de informes es clara y coherente?	3	
		PCT8	¿Son claras las suposiciones, perspectivas teóricas, valores que han configurado la forma y el resultado de la evaluación?	4	3.125
IEEE02	Design and Implementation of Campus Network Intrusion Detection System	PCT1	¿El diseño de la investigación es adecuado para llevar a cabo el estudio?	3	
		PCT2	¿El estudio se basa en el cuerpo de conocimiento existente, es decir, analiza explícitamente su contribución a la luz de trabajos anteriores?	3	
		PCT3	¿Los hallazgos son creíbles?	4	
		PCT4	¿El proceso de investigación se describe a fondo? ¿Los obstáculos son descritos de manera útil?	3	
		PCT5	¿Están claros los vínculos entre los datos, la interpretación y las conclusiones?	4	
		PCT6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PCT7	¿La presentación de informes es clara y coherente?	3	

		PCT8	¿Son claras las suposiciones, perspectivas teóricas, valores que han configurado la forma y el resultado de la evaluación?	4	3.375
IEEE03	Applied Research on Snort Intrusion Detection Model in The Campus Network	PCT1	¿El diseño de la investigación es adecuado para llevar a cabo el estudio?	3	
		PCT2	¿El estudio se basa en el cuerpo de conocimiento existente, es decir, analiza explícitamente su contribución a la luz de trabajos anteriores?	2	
		PCT3	¿Los hallazgos son creíbles?	3	
		PCT4	¿El proceso de investigación se describe a fondo? ¿Los obstáculos son descritos de manera útil?	3	
		PCT5	¿Están claros los vínculos entre los datos, la interpretación y las conclusiones?	4	
		PCT6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PCT7	¿La presentación de informes es clara y coherente?	3	
		PCT8	¿Son claras las suposiciones, perspectivas teóricas, valores que han configurado la forma y el resultado de la evaluación?	4	3.125
IEEE04	Framework of Intrusion Detection System via Snort Application on Campus Network Environment	PCT1	¿El diseño de la investigación es adecuado para llevar a cabo el estudio?	3	
		PCT2	¿El estudio se basa en el cuerpo de conocimiento existente, es decir, analiza explícitamente su contribución a la luz de trabajos anteriores?	3	
		PCT3	¿Los hallazgos son creíbles?	3	
		PCT4	¿El proceso de investigación se describe a fondo? ¿Los obstáculos son descritos de manera útil?	3	
		PCT5	¿Están claros los vínculos entre los datos, la interpretación y las conclusiones?	3	
		PCT6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PCT7	¿La presentación de informes es clara y coherente?	3	
		PCT8	¿Son claras las suposiciones, perspectivas teóricas, valores que han configurado la forma y el resultado de la evaluación?	3	3
IEEE05		PCT1	¿El diseño de la investigación es adecuado para llevar a cabo el estudio?	3	

	Research on the active defense security system based on cloud computing of wisdom campus network	PCT2	¿El estudio se basa en el cuerpo de conocimiento existente, es decir, analiza explícitamente su contribución a la luz de trabajos anteriores?	3	
		PCT3	¿Los hallazgos son creíbles?	2	
		PCT4	¿El proceso de investigación se describe a fondo? ¿Los obstáculos son descritos de manera útil?	3	
		PCT5	¿Están claros los vínculos entre los datos, la interpretación y las conclusiones?	4	
		PCT6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PCT7	¿La presentación de informes es clara y coherente?	4	
		PCT8	¿Son claras las suposiciones, perspectivas teóricas, valores que han configurado la forma y el resultado de la evaluación?	3	3.125
IEEE07	Research and design of the distributed intrusion detection system based on Snort	PCT1	¿El diseño de la investigación es adecuado para llevar a cabo el estudio?	3	
		PCT2	¿El estudio se basa en el cuerpo de conocimiento existente, es decir, analiza explícitamente su contribución a la luz de trabajos anteriores?	3	
		PCT3	¿Los hallazgos son creíbles?	3	
		PCT4	¿El proceso de investigación se describe a fondo? ¿Los obstáculos son descritos de manera útil?	3	
		PCT5	¿Están claros los vínculos entre los datos, la interpretación y las conclusiones?	3	
		PCT6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PCT7	¿La presentación de informes es clara y coherente?	3	
		PCT8	¿Son claras las suposiciones, perspectivas teóricas, valores que han configurado la forma y el resultado de la evaluación?	3	3
IEEE09	Intrusion Filtration System(IFS)- mapping Network Security in new way	PCT1	¿El diseño de la investigación es adecuado para llevar a cabo el estudio?	3	
		PCT2	¿El estudio se basa en el cuerpo de conocimiento existente, es decir, analiza explícitamente su contribución a la luz de trabajos anteriores?	3	
		PCT3	¿Los hallazgos son creíbles?	3	
		PCT4	¿El proceso de investigación se describe a fondo? ¿Los obstáculos son descritos de manera útil?	3	

		PCT5	¿Están claros los vínculos entre los datos, la interpretación y las conclusiones?	4	
		PCT6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PCT7	¿La presentación de informes es clara y coherente?	4	
		PCT8	¿Son claras las suposiciones, perspectivas teóricas, valores que han configurado la forma y el resultado de la evaluación?	4	3.375
IEEE13	Virtual Inline: A Technique of Combining IDS and IPS Together in Response Intrusion	PCT1	¿El diseño de la investigación es adecuado para llevar a cabo el estudio?	3	
		PCT2	¿El estudio se basa en el cuerpo de conocimiento existente, es decir, analiza explícitamente su contribución a la luz de trabajos anteriores?	3	
		PCT3	¿Los hallazgos son creíbles?	3	
		PCT4	¿El proceso de investigación se describe a fondo? ¿Los obstáculos son descritos de manera útil?	2	
		PCT5	¿Están claros los vínculos entre los datos, la interpretación y las conclusiones?	3	
		PCT6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PCT7	¿La presentación de informes es clara y coherente?	4	
		PCT8	¿Son claras las suposiciones, perspectivas teóricas, valores que han configurado la forma y el resultado de la evaluación?	3	3
IEEE17	Network Anomaly Detection and Classification via Opportunistic Sampling	PCT1	¿El diseño de la investigación es adecuado para llevar a cabo el estudio?	3	
		PCT2	¿El estudio se basa en el cuerpo de conocimiento existente, es decir, analiza explícitamente su contribución a la luz de trabajos anteriores?	3	
		PCT3	¿Los hallazgos son creíbles?	3	
		PCT4	¿El proceso de investigación se describe a fondo? ¿Los obstáculos son descritos de manera útil?	3	
		PCT5	¿Están claros los vínculos entre los datos, la interpretación y las conclusiones?	4	
		PCT6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	2	
		PCT7	¿La presentación de informes es clara y coherente?	3	

		PCT8	¿Son claras las suposiciones, perspectivas teóricas, valores que han configurado la forma y el resultado de la evaluación?	4	3.125
IEEE19	Packet- vs. Session-Based Modeling for Intrusion Detection Systems	PCT1	¿El diseño de la investigación es adecuado para llevar a cabo el estudio?	3	
		PCT2	¿El estudio se basa en el cuerpo de conocimiento existente, es decir, analiza explícitamente su contribución a la luz de trabajos anteriores?	2	
		PCT3	¿Los hallazgos son creíbles?	4	
		PCT4	¿El proceso de investigación se describe a fondo? ¿Los obstáculos son descritos de manera útil?	3	
		PCT5	¿Están claros los vínculos entre los datos, la interpretación y las conclusiones?	3	
		PCT6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PCT7	¿La presentación de informes es clara y coherente?	4	
		PCT8	¿Son claras las suposiciones, perspectivas teóricas, valores que han configurado la forma y el resultado de la evaluación?	4	3.25
IEEE21	Design and Implementation of Honeypot Systems Based on Open-Source Software	PCT1	¿El diseño de la investigación es adecuado para llevar a cabo el estudio?	3	
		PCT2	¿El estudio se basa en el cuerpo de conocimiento existente, es decir, analiza explícitamente su contribución a la luz de trabajos anteriores?	2	
		PCT3	¿Los hallazgos son creíbles?	3	
		PCT4	¿El proceso de investigación se describe a fondo? ¿Los obstáculos son descritos de manera útil?	3	
		PCT5	¿Están claros los vínculos entre los datos, la interpretación y las conclusiones?	4	
		PCT6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PCT7	¿La presentación de informes es clara y coherente?	3	
		PCT8	¿Son claras las suposiciones, perspectivas teóricas, valores que han configurado la forma y el resultado de la evaluación?	3	3
IEEE26		PCT1	¿El diseño de la investigación es adecuado para llevar a cabo el estudio?	2	

	Local Area Detection of Incoming War Dial Activity	PCT2	¿El estudio se basa en el cuerpo de conocimiento existente, es decir, analiza explícitamente su contribución a la luz de trabajos anteriores?	2	
		PCT3	¿Los hallazgos son creíbles?	2	
		PCT4	¿El proceso de investigación se describe a fondo? ¿Los obstáculos son descritos de manera útil?	3	
		PCT5	¿Están claros los vínculos entre los datos, la interpretación y las conclusiones?	2	
		PCT6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	2	
		PCT7	¿La presentación de informes es clara y coherente?	2	
		PCT8	¿Son claras las suposiciones, perspectivas teóricas, valores que han configurado la forma y el resultado de la evaluación?	2	2.125
IEEE27	Detecting Attacks on Networks	PCT1	¿El diseño de la investigación es adecuado para llevar a cabo el estudio?	3	
		PCT2	¿El estudio se basa en el cuerpo de conocimiento existente, es decir, analiza explícitamente su contribución a la luz de trabajos anteriores?	3	
		PCT3	¿Los hallazgos son creíbles?	3	
		PCT4	¿El proceso de investigación se describe a fondo? ¿Los obstáculos son descritos de manera útil?	3	
		PCT5	¿Están claros los vínculos entre los datos, la interpretación y las conclusiones?	3	
		PCT6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PCT7	¿La presentación de informes es clara y coherente?	3	
		PCT8	¿Son claras las suposiciones, perspectivas teóricas, valores que han configurado la forma y el resultado de la evaluación?	3	3
IEEE30	Intranet Security with Micro-Firewalls and Mobile Agents for Proactive Intrusion Response*	PCT1	¿El diseño de la investigación es adecuado para llevar a cabo el estudio?	3	
		PCT2	¿El estudio se basa en el cuerpo de conocimiento existente, es decir, analiza explícitamente su contribución a la luz de trabajos anteriores?	3	
		PCT3	¿Los hallazgos son creíbles?	3	
		PCT4	¿El proceso de investigación se describe a fondo? ¿Los obstáculos son descritos de manera útil?	4	

		PCT5	¿Están claros los vínculos entre los datos, la interpretación y las conclusiones?	3	
		PCT6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PCT7	¿La presentación de informes es clara y coherente?	4	
		PCT8	¿Son claras las suposiciones, perspectivas teóricas, valores que han configurado la forma y el resultado de la evaluación?	4	3.375
IEEE33	Terminal Security Protection Anomaly Detection Based on Combined Algorithm	PCT1	¿El diseño de la investigación es adecuado para llevar a cabo el estudio?	3	
		PCT2	¿El estudio se basa en el cuerpo de conocimiento existente, es decir, analiza explícitamente su contribución a la luz de trabajos anteriores?	3	
		PCT3	¿Los hallazgos son creíbles?	3	
		PCT4	¿El proceso de investigación se describe a fondo? ¿Los obstáculos son descritos de manera útil?	3	
		PCT5	¿Están claros los vínculos entre los datos, la interpretación y las conclusiones?	3	
		PCT6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PCT7	¿La presentación de informes es clara y coherente?	3	
		PCT8	¿Son claras las suposiciones, perspectivas teóricas, valores que han configurado la forma y el resultado de la evaluación?	3	3
IEEE37	Detection of NS Resource Record based DNS Query Request Packet Traffic and SSH Dictionary Attack Activity	PCT1	¿El diseño de la investigación es adecuado para llevar a cabo el estudio?	3	
		PCT2	¿El estudio se basa en el cuerpo de conocimiento existente, es decir, analiza explícitamente su contribución a la luz de trabajos anteriores?	2	
		PCT3	¿Los hallazgos son creíbles?	4	
		PCT4	¿El proceso de investigación se describe a fondo? ¿Los obstáculos son descritos de manera útil?	4	
		PCT5	¿Están claros los vínculos entre los datos, la interpretación y las conclusiones?	3	
		PCT6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PCT7	¿La presentación de informes es clara y coherente?	4	

		PCT8	¿Son claras las suposiciones, perspectivas teóricas, valores que han configurado la forma y el resultado de la evaluación?	4	3.375
IEEE38	An Intuitive Study: Intrusion Detection Systems and Anomalies, How AI can be used as a tool to enable the majority, in 5G era.	PCT1	¿El diseño de la investigación es adecuado para llevar a cabo el estudio?	3	
		PCT2	¿El estudio se basa en el cuerpo de conocimiento existente, es decir, analiza explícitamente su contribución a la luz de trabajos anteriores?	4	
		PCT3	¿Los hallazgos son creíbles?	4	
		PCT4	¿El proceso de investigación se describe a fondo? ¿Los obstáculos son descritos de manera útil?	3	
		PCT5	¿Están claros los vínculos entre los datos, la interpretación y las conclusiones?	3	
		PCT6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	4	
		PCT7	¿La presentación de informes es clara y coherente?	4	
		PCT8	¿Son claras las suposiciones, perspectivas teóricas, valores que han configurado la forma y el resultado de la evaluación?	4	3.625
IEEE39	TAICHI: AN OPEN INTRUSION AUTOMATIC RESPONSE SYSTEM BASED ON PLUGIN	PCT1	¿El diseño de la investigación es adecuado para llevar a cabo el estudio?	3	
		PCT2	¿El estudio se basa en el cuerpo de conocimiento existente, es decir, analiza explícitamente su contribución a la luz de trabajos anteriores?	3	
		PCT3	¿Los hallazgos son creíbles?	3	
		PCT4	¿El proceso de investigación se describe a fondo? ¿Los obstáculos son descritos de manera útil?	3	
		PCT5	¿Están claros los vínculos entre los datos, la interpretación y las conclusiones?	3	
		PCT6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PCT7	¿La presentación de informes es clara y coherente?	3	
		PCT8	¿Son claras las suposiciones, perspectivas teóricas, valores que han configurado la forma y el resultado de la evaluación?	3	3
IEEE42		PCT1	¿El diseño de la investigación es adecuado para llevar a cabo el estudio?	4	

	Model for Security in Wired and Wireless Network for Education	PCT2	¿El estudio se basa en el cuerpo de conocimiento existente, es decir, analiza explícitamente su contribución a la luz de trabajos anteriores?	4	
		PCT3	¿Los hallazgos son creíbles?	4	
		PCT4	¿El proceso de investigación se describe a fondo? ¿Los obstáculos son descritos de manera útil?	4	
		PCT5	¿Están claros los vínculos entre los datos, la interpretación y las conclusiones?	4	
		PCT6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	4	
		PCT7	¿La presentación de informes es clara y coherente?	4	
		PCT8	¿Son claras las suposiciones, perspectivas teóricas, valores que han configurado la forma y el resultado de la evaluación?	4	4
IEEE43	An Empirical Approach to Modeling Uncertainty in Intrusion Analysis	PCT1	¿El diseño de la investigación es adecuado para llevar a cabo el estudio?	4	
		PCT2	¿El estudio se basa en el cuerpo de conocimiento existente, es decir, analiza explícitamente su contribución a la luz de trabajos anteriores?	3	
		PCT3	¿Los hallazgos son creíbles?	4	
		PCT4	¿El proceso de investigación se describe a fondo? ¿Los obstáculos son descritos de manera útil?	4	
		PCT5	¿Están claros los vínculos entre los datos, la interpretación y las conclusiones?	4	
		PCT6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	4	
		PCT7	¿La presentación de informes es clara y coherente?	4	
		PCT8	¿Son claras las suposiciones, perspectivas teóricas, valores que han configurado la forma y el resultado de la evaluación?	3	3.75
IEEE51	TVMonitor: A P2P-TV Content Monitoring Platform	PCT1	¿El diseño de la investigación es adecuado para llevar a cabo el estudio?	3	
		PCT2	¿El estudio se basa en el cuerpo de conocimiento existente, es decir, analiza explícitamente su contribución a la luz de trabajos anteriores?	3	
		PCT3	¿Los hallazgos son creíbles?	3	
		PCT4	¿El proceso de investigación se describe a fondo? ¿Los obstáculos son descritos de manera útil?	3	

		PCT5	¿Están claros los vínculos entre los datos, la interpretación y las conclusiones?	3	
		PCT6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PCT7	¿La presentación de informes es clara y coherente?	3	
		PCT8	¿Son claras las suposiciones, perspectivas teóricas, valores que han configurado la forma y el resultado de la evaluación?	3	3

Fuente. Adaptación de *Checklist for qualitative studies*(Kitchenham & Charters, 2007)

ANEXO E. ANÁLISIS CUANTITATIVO RSL

En la Tabla 56, se detallan los parámetros considerados para el Análisis Cuantitativo de los papers, previo al análisis de la RSL. Incluyen: Número de paper, Título, Id_Pregunta, Descripción, Calificación y Promedio.

Tabla 56: **ANÁLISIS CUANTITATIVO RSL.**

No. Paper	Título	Id_Pregunta	Descripción	Calificación	Promedio
SCO02	Analysis of E-mail Account Probing Attack Based on Graph Mining	PC1	¿Están claramente establecidos los objetivos para el estudio?	5	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	1	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	5	
		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	3	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	3	
		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	5	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	5	
		PC8	¿Se describen los métodos estadísticos?	3	
		PC9	¿Están justificados los métodos estadísticos?	2	
		PC10	¿Es claro el propósito del análisis?	5	
		PC11	¿Son creíbles los resultados?	5	
		PC12	¿Hay una descripción completa del proceso de investigación?	5	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	5	
		PC14	Los reportes son claros.	5	4.07142857
ACM02	A Hybrid Intelligent System for Insider Threat Detection Using Iterative Attention	PC1	¿Están claramente establecidos los objetivos para el estudio?	5	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	4	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	4	

		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	5	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	4	
		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	4	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	5	
		PC8	¿Se describen los métodos estadísticos?	4	
		PC9	¿Están justificados los métodos estadísticos?	5	
		PC10	¿Es claro el propósito del análisis?	5	
		PC11	¿Son creíbles los resultados?	5	
		PC12	¿Hay una descripción completa del proceso de investigación?	5	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	5	
		PC14	Los reportes son claros.	4	4.57142857
ACM04	Detection of Anomalous Insiders in Collaborative Environments via Relational Analysis of Access Logs	PC1	¿Están claramente establecidos los objetivos para el estudio?	5	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	5	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	5	
		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	4	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	5	
		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	4	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	3	
		PC8	¿Se describen los métodos estadísticos?	5	
		PC9	¿Están justificados los métodos estadísticos?	4	
		PC10	¿Es claro el propósito del análisis?	5	
		PC11	¿Son creíbles los resultados?	5	

		PC12	¿Hay una descripción completa del proceso de investigación?	5	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	5	
		PC14	Los reportes son claros.	5	4.64285714
ACM10	Observing Industrial Control System Attacks Launched via Metasploit Framework	PC1	¿Están claramente establecidos los objetivos para el estudio?	5	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	3	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	3	
		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	4	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	5	
		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	5	
		PC8	¿Se describen los métodos estadísticos?	2	
		PC9	¿Están justificados los métodos estadísticos?	2	
		PC10	¿Es claro el propósito del análisis?	5	
		PC11	¿Son creíbles los resultados?	5	
		PC12	¿Hay una descripción completa del proceso de investigación?	5	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	5	
		PC14	Los reportes son claros.	5	4.07142857
ACM12	Framework for Distributed Virtual Honeynets	PC1	¿Están claramente establecidos los objetivos para el estudio?	5	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	4	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	4	
		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	5	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	5	

		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	4	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	3	
		PC8	¿Se describen los métodos estadísticos?	5	
		PC9	¿Están justificados los métodos estadísticos?	5	
		PC10	¿Es claro el propósito del análisis?	4	
		PC11	¿Son creíbles los resultados?	4	
		PC12	¿Hay una descripción completa del proceso de investigación?	4	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	4	
		PC14	Los reportes son claros.	5	4.35714286
ACM13	The near Real Time Statistical Asset Priority Driven (Nrtsapd) Risk Assessment Methodology	PC1	¿Están claramente establecidos los objetivos para el estudio?	5	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	4	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	4	
		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	4	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	4	
		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	4	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	3	
		PC8	¿Se describen los métodos estadísticos?	4	
		PC9	¿Están justificados los métodos estadísticos?	4	
		PC10	¿Es claro el propósito del análisis?	5	
		PC11	¿Son creíbles los resultados?	4	
		PC12	¿Hay una descripción completa del proceso de investigación?	5	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	5	
		PC14	Los reportes son claros.	4	4.21428571

ACM15	Asset Priority Risk Assessment Using Hidden Markov Models	PC1	¿Están claramente establecidos los objetivos para el estudio?	5	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	4	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	4	
		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	4	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	4	
		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	4	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	3	
		PC8	¿Se describen los métodos estadísticos?	4	
		PC9	¿Están justificados los métodos estadísticos?	4	
		PC10	¿Es claro el propósito del análisis?	5	
		PC11	¿Son creíbles los resultados?	4	
		PC12	¿Hay una descripción completa del proceso de investigación?	5	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	5	
		PC14	Los reportes son claros.	5	4.28571429
ACM05	Log2vec: A Heterogeneous Graph Embedding Based Approach for Detecting Cyber Threats within Enterprise	PC1	¿Están claramente establecidos los objetivos para el estudio?	4	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	4	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	3	
		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	4	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	5	
		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	4	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	4	
		PC8	¿Se describen los métodos estadísticos?	5	

		PC9	¿Están justificados los métodos estadísticos?	5	
		PC10	¿Es claro el propósito del análisis?	5	
		PC11	¿Son creíbles los resultados?	4	
		PC12	¿Hay una descripción completa del proceso de investigación?	5	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	4	
		PC14	Los reportes son claros.	4	4.28571429
ACM17	LAC : LSTM AUTOENCODER with Community for Insider Threat Detection	PC1	¿Están claramente establecidos los objetivos para el estudio?	5	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	5	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	4	
		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	4	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	4	
		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	4	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	4	
		PC8	¿Se describen los métodos estadísticos?	4	
		PC9	¿Están justificados los métodos estadísticos?	3	
		PC10	¿Es claro el propósito del análisis?	5	
		PC11	¿Son creíbles los resultados?	4	
		PC12	¿Hay una descripción completa del proceso de investigación?	4	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	3	
		PC14	Los reportes son claros.	3	4
ACM23	AI-empowered IoT Security for Smart Cities	PC1	¿Están claramente establecidos los objetivos para el estudio?	4	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	4	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	4	

		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	5	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	4	
		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	4	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	4	
		PC8	¿Se describen los métodos estadísticos?	4	
		PC9	¿Están justificados los métodos estadísticos?	4	
		PC10	¿Es claro el propósito del análisis?	4	
		PC11	¿Son creíbles los resultados?	5	
		PC12	¿Hay una descripción completa del proceso de investigación?	4	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	4	
		PC14	Los reportes son claros.	4	4.14285714
SCO17	An Insider Threat Detection Approach Based on Mouse Dynamics and Deep Learning	PC1	¿Están claramente establecidos los objetivos para el estudio?	4	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	4	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	3	
		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	3	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	5	
		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	4	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	3	
		PC8	¿Se describen los métodos estadísticos?	4	
		PC9	¿Están justificados los métodos estadísticos?	4	
		PC10	¿Es claro el propósito del análisis?	4	
		PC11	¿Son creíbles los resultados?	5	

		PC12	¿Hay una descripción completa del proceso de investigación?	4	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	5	
		PC14	Los reportes son claros.	5	4.07142857
SCO39	An Insider Threat Detection Approach Based on Mouse Dynamics and Deep Learning	PC1	¿Están claramente establecidos los objetivos para el estudio?	5	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	5	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	4	
		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	4	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	4	
		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	4	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	5	
		PC8	¿Se describen los métodos estadísticos?	3	
		PC9	¿Están justificados los métodos estadísticos?	3	
		PC10	¿Es claro el propósito del análisis?	5	
		PC11	¿Son creíbles los resultados?	5	
		PC12	¿Hay una descripción completa del proceso de investigación?	5	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	5	
		PC14	Los reportes son claros.	5	4.42857143
SCO40	Design and Implementation of a Quantitative Network Health Monitoring and Recovery System	PC1	¿Están claramente establecidos los objetivos para el estudio?	5	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	4	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	5	
		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	3	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	5	

		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	4	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	4	
		PC8	¿Se describen los métodos estadísticos?	3	
		PC9	¿Están justificados los métodos estadísticos?	3	
		PC10	¿Es claro el propósito del análisis?	5	
		PC11	¿Son creíbles los resultados?	4	
		PC12	¿Hay una descripción completa del proceso de investigación?	5	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	4	
		PC14	Los reportes son claros.	5	4.21428571
SCO08	Real-time anomaly detection and mitigation using streaming telemetry in SDN	PC1	¿Están claramente establecidos los objetivos para el estudio?	4	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	4	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	3	
		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	3	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	5	
		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	4	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	5	
		PC8	¿Se describen los métodos estadísticos?	3	
		PC9	¿Están justificados los métodos estadísticos?	3	
		PC10	¿Es claro el propósito del análisis?	5	
		PC11	¿Son creíbles los resultados?	4	
		PC12	¿Hay una descripción completa del proceso de investigación?	5	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	4	
		PC14	Los reportes son claros.	5	4.07142857

SCO09	An improved ensemble based intrusion detection technique using XGBoost	PC1	¿Están claramente establecidos los objetivos para el estudio?	4	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	4	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	4	
		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	3	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	5	
		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	4	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	4	
		PC8	¿Se describen los métodos estadísticos?	2	
		PC9	¿Están justificados los métodos estadísticos?	2	
		PC10	¿Es claro el propósito del análisis?	5	
		PC11	¿Son creíbles los resultados?	4	
		PC12	¿Hay una descripción completa del proceso de investigación?	4	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	4	
		PC14	Los reportes son claros.	5	3.85714286
SCO11	Machine learning and recognition of user tasks for malware detection	PC1	¿Están claramente establecidos los objetivos para el estudio?	5	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	4	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	4	
		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	4	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	5	
		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	3	
		PC8	¿Se describen los métodos estadísticos?	2	

		PC9	¿Están justificados los métodos estadísticos?	2	
		PC10	¿Es claro el propósito del análisis?	5	
		PC11	¿Son creíbles los resultados?	4	
		PC12	¿Hay una descripción completa del proceso de investigación?	5	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	4	
		PC14	Los reportes son claros.	5	3.92857143
SCO10	SDCCP: Control the network using software-defined networking and end-to-end congestion control	PC1	¿Están claramente establecidos los objetivos para el estudio?	5	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	3	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	3	
		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	4	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	5	
		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	4	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	4	
		PC8	¿Se describen los métodos estadísticos?	3	
		PC9	¿Están justificados los métodos estadísticos?	2	
		PC10	¿Es claro el propósito del análisis?	5	
		PC11	¿Son creíbles los resultados?	4	
		PC12	¿Hay una descripción completa del proceso de investigación?	3	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	4	
		PC14	Los reportes son claros.	5	3.85714286
SCO13	Intranet User-Level Security Traffic Management with Deep Reinforcement Learning	PC1	¿Están claramente establecidos los objetivos para el estudio?	5	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	3	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	4	

		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	4	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	5	
		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	4	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	3	
		PC8	¿Se describen los métodos estadísticos?	3	
		PC9	¿Están justificados los métodos estadísticos?	4	
		PC10	¿Es claro el propósito del análisis?	5	
		PC11	¿Son creíbles los resultados?	4	
		PC12	¿Hay una descripción completa del proceso de investigación?	5	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	4	
		PC14	Los reportes son claros.	5	4.14285714
SCO19	Detection of DHCP Starvation Attacks in Software Defined Networks: A Case Study	PC1	¿Están claramente establecidos los objetivos para el estudio?	4	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	3	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	3	
		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	3	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	5	
		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	4	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	3	
		PC8	¿Se describen los métodos estadísticos?	3	
		PC9	¿Están justificados los métodos estadísticos?	2	
		PC10	¿Es claro el propósito del análisis?	5	
		PC11	¿Son creíbles los resultados?	4	

		PC12	¿Hay una descripción completa del proceso de investigación?	4	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	4	
		PC14	Los reportes son claros.	4	3.64285714
SCO20	Behavior rhythm: An effective model for massive logs characterizing and security monitoring in cloud	PC1	¿Están claramente establecidos los objetivos para el estudio?	3	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	3	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	3	
		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	3	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	3	
		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	3	
		PC8	¿Se describen los métodos estadísticos?	3	
		PC9	¿Están justificados los métodos estadísticos?	3	
		PC10	¿Es claro el propósito del análisis?	3	
		PC11	¿Son creíbles los resultados?	3	
		PC12	¿Hay una descripción completa del proceso de investigación?	3	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	3	
		PC14	Los reportes son claros.	3	3
SCO16	Towards augmented proactive cyberthreat intelligence	PC1	¿Están claramente establecidos los objetivos para el estudio?	4	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	4	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	3	
		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	3	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	5	

		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	3	
		PC8	¿Se describen los métodos estadísticos?	3	
		PC9	¿Están justificados los métodos estadísticos?	3	
		PC10	¿Es claro el propósito del análisis?	4	
		PC11	¿Son creíbles los resultados?	4	
		PC12	¿Hay una descripción completa del proceso de investigación?	4	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	5	
		PC14	Los reportes son claros.	4	3.71428571
SCO20	Software Defined Networking Architecture, Security and Energy Efficiency: A Survey	PC1	¿Están claramente establecidos los objetivos para el estudio?	4	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	5	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	4	
		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	4	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	4	
		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	3	
		PC8	¿Se describen los métodos estadísticos?	4	
		PC9	¿Están justificados los métodos estadísticos?	4	
		PC10	¿Es claro el propósito del análisis?	5	
		PC11	¿Son creíbles los resultados?	4	
		PC12	¿Hay una descripción completa del proceso de investigación?	4	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	4	
		PC14	Los reportes son claros.	3	3.92857143

SCO29	Hviz: HTTP(S) traffic aggregation and visualization for network forensics	PC1	¿Están claramente establecidos los objetivos para el estudio?	5	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	4	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	3	
		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	3	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	4	
		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	4	
		PC8	¿Se describen los métodos estadísticos?	2	
		PC9	¿Están justificados los métodos estadísticos?	2	
		PC10	¿Es claro el propósito del análisis?	4	
		PC11	¿Son creíbles los resultados?	5	
		PC12	¿Hay una descripción completa del proceso de investigación?	4	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	5	
		PC14	Los reportes son claros.	4	3.71428571
SCO30	Anomaly-based intrusion detection and prevention system on website usage using rule-growth sequential pattern analysis: Case study: Statistics of Indonesia (BPS) website	PC1	¿Están claramente establecidos los objetivos para el estudio?	5	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	4	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	4	
		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	3	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	5	
		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	3	
		PC8	¿Se describen los métodos estadísticos?	4	

		PC9	¿Están justificados los métodos estadísticos?	4	
		PC10	¿Es claro el propósito del análisis?	5	
		PC11	¿Son creíbles los resultados?	4	
		PC12	¿Hay una descripción completa del proceso de investigación?	5	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	4	
		PC14	Los reportes son claros.	4	4.07142857
SCO31	Efficient anomaly detection and mitigation in software defined networking environment	PC1	¿Están claramente establecidos los objetivos para el estudio?	4	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	3	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	3	
		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	3	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	5	
		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	4	
		PC8	¿Se describen los métodos estadísticos?	3	
		PC9	¿Están justificados los métodos estadísticos?	3	
		PC10	¿Es claro el propósito del análisis?	4	
		PC11	¿Son creíbles los resultados?	5	
		PC12	¿Hay una descripción completa del proceso de investigación?	4	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	5	
		PC14	Los reportes son claros.	3	3.71428571
SCO36	Agent-based honeynet framework for protecting servers in campus networks	PC1	¿Están claramente establecidos los objetivos para el estudio?	5	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	4	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	3	

		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	3	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	5	
		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	3	
		PC8	¿Se describen los métodos estadísticos?	3	
		PC9	¿Están justificados los métodos estadísticos?	4	
		PC10	¿Es claro el propósito del análisis?	5	
		PC11	¿Son creíbles los resultados?	4	
		PC12	¿Hay una descripción completa del proceso de investigación?	5	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	4	
		PC14	Los reportes son claros.	4	3.92857143
SCO38	Sensor in the dark: Building untraceable large-scale honeypots using virtualization technologies	PC1	¿Están claramente establecidos los objetivos para el estudio?	4	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	2	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	3	
		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	3	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	5	
		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	4	
		PC8	¿Se describen los métodos estadísticos?	3	
		PC9	¿Están justificados los métodos estadísticos?	2	
		PC10	¿Es claro el propósito del análisis?	4	
		PC11	¿Son creíbles los resultados?	4	

		PC12	¿Hay una descripción completa del proceso de investigación?	3	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	5	
		PC14	Los reportes son claros.	3	3.42857143
SCO45	PORTFILER: Port-Level Network Profiling for Self-Propagating Malware Detection	PC1	¿Están claramente establecidos los objetivos para el estudio?	4	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	3	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	3	
		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	3	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	5	
		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	4	
		PC8	¿Se describen los métodos estadísticos?	3	
		PC9	¿Están justificados los métodos estadísticos?	3	
		PC10	¿Es claro el propósito del análisis?	5	
		PC11	¿Son creíbles los resultados?	4	
		PC12	¿Hay una descripción completa del proceso de investigación?	4	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	4	
		PC14	Los reportes son claros.	4	3.71428571
SCO36	Cyber threat intelligence using PCA-DNN model to detect abnormal network behavior	PC1	¿Están claramente establecidos los objetivos para el estudio?	4	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	4	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	4	
		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	4	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	5	

		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	4	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	4	
		PC8	¿Se describen los métodos estadísticos?	4	
		PC9	¿Están justificados los métodos estadísticos?	3	
		PC10	¿Es claro el propósito del análisis?	4	
		PC11	¿Son creíbles los resultados?	4	
		PC12	¿Hay una descripción completa del proceso de investigación?	4	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	4	
		PC14	Los reportes son claros.	3	3.92857143
SCO07	CTLMD: Continuous-Temporal Lateral Movement Detection Using Graph Embedding	PC1	¿Están claramente establecidos los objetivos para el estudio?	4	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	3	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	3	
		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	3	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	5	
		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	3	
		PC8	¿Se describen los métodos estadísticos?	3	
		PC9	¿Están justificados los métodos estadísticos?	3	
		PC10	¿Es claro el propósito del análisis?	3	
		PC11	¿Son creíbles los resultados?	3	
		PC12	¿Hay una descripción completa del proceso de investigación?	4	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	3	
		PC14	Los reportes son claros.	4	3.35714286

SCO49	A Learning Approach with Programmable Data Plane towards IoT Security	PC1	¿Están claramente establecidos los objetivos para el estudio?	3	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	3	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	4	
		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	3	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	5	
		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	4	
		PC8	¿Se describen los métodos estadísticos?	2	
		PC9	¿Están justificados los métodos estadísticos?	2	
		PC10	¿Es claro el propósito del análisis?	4	
		PC11	¿Son creíbles los resultados?	4	
		PC12	¿Hay una descripción completa del proceso de investigación?	4	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	4	
		PC14	Los reportes son claros.	3	3.42857143
IEEE01	Real-Time Network Anomaly Detection System Using Machine Learning	PC1	¿Están claramente establecidos los objetivos para el estudio?	3	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	3	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	3	
		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	3	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	5	
		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	4	
		PC8	¿Se describen los métodos estadísticos?	3	

		PC9	¿Están justificados los métodos estadísticos?	3	
		PC10	¿Es claro el propósito del análisis?	4	
		PC11	¿Son creíbles los resultados?	4	
		PC12	¿Hay una descripción completa del proceso de investigación?	4	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	4	
		PC14	Los reportes son claros.	4	3.57142857
IEEE06	An ARP-based Anomaly Detection Algorithm Using Hidden Markov Model in Enterprise Networks	PC1	¿Están claramente establecidos los objetivos para el estudio?	3	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	3	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	3	
		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	3	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	5	
		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	3	
		PC8	¿Se describen los métodos estadísticos?	3	
		PC9	¿Están justificados los métodos estadísticos?	3	
		PC10	¿Es claro el propósito del análisis?	3	
		PC11	¿Son creíbles los resultados?	4	
		PC12	¿Hay una descripción completa del proceso de investigación?	4	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	4	
		PC14	Los reportes son claros.	4	3.42857143
IEEE08	Proposal of a malicious communication control method using OpenFlow	PC1	¿Están claramente establecidos los objetivos para el estudio?	4	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	2	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	3	

		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	3	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	5	
		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	3	
		PC8	¿Se describen los métodos estadísticos?	3	
		PC9	¿Están justificados los métodos estadísticos?	3	
		PC10	¿Es claro el propósito del análisis?	4	
		PC11	¿Son creíbles los resultados?	3	
		PC12	¿Hay una descripción completa del proceso de investigación?	4	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	4	
		PC14	Los reportes son claros.	3	3.35714286
IEEE10	Machine and Deep Learning Based Comparative Analysis Using Hybrid Approaches for Intrusion Detection System	PC1	¿Están claramente establecidos los objetivos para el estudio?	4	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	4	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	5	
		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	4	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	5	
		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	4	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	3	
		PC8	¿Se describen los métodos estadísticos?	3	
		PC9	¿Están justificados los métodos estadísticos?	3	
		PC10	¿Es claro el propósito del análisis?	4	
		PC11	¿Son creíbles los resultados?	4	

		PC12	¿Hay una descripción completa del proceso de investigación?	3	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	4	
		PC14	Los reportes son claros.	5	3.92857143
IEEE11	Toward an Online Network Intrusion Detection System Based on Ensemble Learning	PC1	¿Están claramente establecidos los objetivos para el estudio?	4	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	4	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	3	
		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	3	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	5	
		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	4	
		PC8	¿Se describen los métodos estadísticos?	3	
		PC9	¿Están justificados los métodos estadísticos?	3	
		PC10	¿Es claro el propósito del análisis?	4	
		PC11	¿Son creíbles los resultados?	4	
		PC12	¿Hay una descripción completa del proceso de investigación?	4	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	4	
		PC14	Los reportes son claros.	4	3.71428571
IEEE12	Research On Intrusion Detection Based On Campus Network	PC1	¿Están claramente establecidos los objetivos para el estudio?	3	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	4	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	3	
		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	3	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	5	

		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	3	
		PC8	¿Se describen los métodos estadísticos?	2	
		PC9	¿Están justificados los métodos estadísticos?	2	
		PC10	¿Es claro el propósito del análisis?	4	
		PC11	¿Son creíbles los resultados?	3	
		PC12	¿Hay una descripción completa del proceso de investigación?	3	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	4	
		PC14	Los reportes son claros.	3	3.21428571
IEEE14	Intelligent Multi-Agent Information Security System	PC1	¿Están claramente establecidos los objetivos para el estudio?	3	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	2	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	2	
		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	3	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	5	
		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	4	
		PC8	¿Se describen los métodos estadísticos?	3	
		PC9	¿Están justificados los métodos estadísticos?	3	
		PC10	¿Es claro el propósito del análisis?	3	
		PC11	¿Son creíbles los resultados?	3	
		PC12	¿Hay una descripción completa del proceso de investigación?	3	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	4	
		PC14	Los reportes son claros.	3	3.14285714

IEEE15	An Integrated Method for Anomaly Detection From Massive System Logs	PC1	¿Están claramente establecidos los objetivos para el estudio?	4	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	4	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	4	
		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	4	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	5	
		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	4	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	4	
		PC8	¿Se describen los métodos estadísticos?	3	
		PC9	¿Están justificados los métodos estadísticos?	3	
		PC10	¿Es claro el propósito del análisis?	4	
		PC11	¿Son creíbles los resultados?	4	
		PC12	¿Hay una descripción completa del proceso de investigación?	4	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	4	
		PC14	Los reportes son claros.	4	3.92857143
IEEE16	Intelligent Multi-Agent Information Security System	PC1	¿Están claramente establecidos los objetivos para el estudio?	4	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	4	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	4	
		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	4	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	5	
		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	4	
		PC8	¿Se describen los métodos estadísticos?	3	

		PC9	¿Están justificados los métodos estadísticos?	3	
		PC10	¿Es claro el propósito del análisis?	4	
		PC11	¿Son creíbles los resultados?	4	
		PC12	¿Hay una descripción completa del proceso de investigación?	4	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	4	
		PC14	Los reportes son claros.	4	3.85714286
IEEE18	Wireless network intrusion detection model and safety enhancement framework for campus network	PC1	¿Están claramente establecidos los objetivos para el estudio?	3	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	2	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	3	
		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	3	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	3	
		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	3	
		PC8	¿Se describen los métodos estadísticos?	2	
		PC9	¿Están justificados los métodos estadísticos?	2	
		PC10	¿Es claro el propósito del análisis?	4	
		PC11	¿Son creíbles los resultados?	2	
		PC12	¿Hay una descripción completa del proceso de investigación?	4	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	4	
		PC14	Los reportes son claros.	4	3
IEEE20	Anomaly Detection Based on Available Bandwidth Estimation	PC1	¿Están claramente establecidos los objetivos para el estudio?	3	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	2	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	4	

		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	4	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	5	
		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	3	
		PC8	¿Se describen los métodos estadísticos?	2	
		PC9	¿Están justificados los métodos estadísticos?	2	
		PC10	¿Es claro el propósito del análisis?	4	
		PC11	¿Son creíbles los resultados?	3	
		PC12	¿Hay una descripción completa del proceso de investigación?	4	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	4	
		PC14	Los reportes son claros.	4	3.35714286
IEEE23	A Proposed Machine Learning based Scheme for Intrusion Detection	PC1	¿Están claramente establecidos los objetivos para el estudio?	4	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	3	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	3	
		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	3	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	5	
		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	4	
		PC8	¿Se describen los métodos estadísticos?	3	
		PC9	¿Están justificados los métodos estadísticos?	3	
		PC10	¿Es claro el propósito del análisis?	4	
		PC11	¿Son creíbles los resultados?	4	

		PC12	¿Hay una descripción completa del proceso de investigación?	4	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	4	
		PC14	Los reportes son claros.	4	3.64285714
IEEE24	F-TAD: Traffic Anomaly Detection for Sub-networks Using Fisher Linear Discriminant	PC1	¿Están claramente establecidos los objetivos para el estudio?	4	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	4	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	4	
		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	4	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	5	
		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	3	
		PC8	¿Se describen los métodos estadísticos?	3	
		PC9	¿Están justificados los métodos estadísticos?	3	
		PC10	¿Es claro el propósito del análisis?	4	
		PC11	¿Son creíbles los resultados?	4	
		PC12	¿Hay una descripción completa del proceso de investigación?	4	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	4	
		PC14	Los reportes son claros.	4	3.78571429
IEEE25	Defending Distributed Systems Against Malicious Intrusions and Network Anomalies*	PC1	¿Están claramente establecidos los objetivos para el estudio?	4	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	4	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	4	
		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	4	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	5	

		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	4	
		PC8	¿Se describen los métodos estadísticos?	4	
		PC9	¿Están justificados los métodos estadísticos?	4	
		PC10	¿Es claro el propósito del análisis?	4	
		PC11	¿Son creíbles los resultados?	4	
		PC12	¿Hay una descripción completa del proceso de investigación?	4	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	4	
		PC14	Los reportes son claros.	4	4
IEEE29	Parametric Methods for Anomaly Detection in Aggregate Traffic	PC1	¿Están claramente establecidos los objetivos para el estudio?	4	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	4	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	4	
		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	4	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	4	
		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	3	
		PC8	¿Se describen los métodos estadísticos?	3	
		PC9	¿Están justificados los métodos estadísticos?	3	
		PC10	¿Es claro el propósito del análisis?	4	
		PC11	¿Son creíbles los resultados?	4	
		PC12	¿Hay una descripción completa del proceso de investigación?	4	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	4	
		PC14	Los reportes son claros.	4	3.71428571

IEEE31	Intelligent Flow-based Sampling for Effective Network Anomaly Detection	PC1	¿Están claramente establecidos los objetivos para el estudio?	4	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	3	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	4	
		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	4	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	5	
		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	4	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	4	
		PC8	¿Se describen los métodos estadísticos?	3	
		PC9	¿Están justificados los métodos estadísticos?	3	
		PC10	¿Es claro el propósito del análisis?	4	
		PC11	¿Son creíbles los resultados?	4	
		PC12	¿Hay una descripción completa del proceso de investigación?	4	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	5	
		PC14	Los reportes son claros.	4	3.92857143
IEEE32	Using Selective Sampling for the Support of Scalable and Efficient Network Anomaly Detection	PC1	¿Están claramente establecidos los objetivos para el estudio?	4	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	4	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	4	
		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	4	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	4	
		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	4	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	3	
		PC8	¿Se describen los métodos estadísticos?	4	

		PC9	¿Están justificados los métodos estadísticos?	4	
		PC10	¿Es claro el propósito del análisis?	4	
		PC11	¿Son creíbles los resultados?	4	
		PC12	¿Hay una descripción completa del proceso de investigación?	4	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	4	
		PC14	Los reportes son claros.	4	3.92857143
IEEE34	Mining Network Traffic Anomaly Based on Adjustable Piecewise Entropy	PC1	¿Están claramente establecidos los objetivos para el estudio?	4	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	4	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	4	
		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	4	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	5	
		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	4	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	4	
		PC8	¿Se describen los métodos estadísticos?	4	
		PC9	¿Están justificados los métodos estadísticos?	4	
		PC10	¿Es claro el propósito del análisis?	4	
		PC11	¿Son creíbles los resultados?	4	
		PC12	¿Hay una descripción completa del proceso de investigación?	4	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	4	
		PC14	Los reportes son claros.	4	4.07142857
IEEE35	BEDIM: Lateral Movement Detection In Enterprise Network Through Behavior Deviation Measurement	PC1	¿Están claramente establecidos los objetivos para el estudio?	4	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	4	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	4	

		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	4	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	4	
		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	4	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	4	
		PC8	¿Se describen los métodos estadísticos?	4	
		PC9	¿Están justificados los métodos estadísticos?	4	
		PC10	¿Es claro el propósito del análisis?	4	
		PC11	¿Son creíbles los resultados?	4	
		PC12	¿Hay una descripción completa del proceso de investigación?	4	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	5	
		PC14	Los reportes son claros.	5	4.14285714
IEEE36	Clustering-based Anomaly Detection for Smartphone Applications	PC1	¿Están claramente establecidos los objetivos para el estudio?	4	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	4	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	4	
		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	4	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	5	
		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	4	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	4	
		PC8	¿Se describen los métodos estadísticos?	4	
		PC9	¿Están justificados los métodos estadísticos?	4	
		PC10	¿Es claro el propósito del análisis?	4	
		PC11	¿Son creíbles los resultados?	4	

		PC12	¿Hay una descripción completa del proceso de investigación?	4	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	4	
		PC14	Los reportes son claros.	4	4.07142857
IEEE40	A Behavior Sequence Clustering-based Enterprise Network Anomaly Host Recognition Method	PC1	¿Están claramente establecidos los objetivos para el estudio?	4	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	4	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	3	
		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	3	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	5	
		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	4	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	4	
		PC8	¿Se describen los métodos estadísticos?	3	
		PC9	¿Están justificados los métodos estadísticos?	3	
		PC10	¿Es claro el propósito del análisis?	5	
		PC11	¿Son creíbles los resultados?	4	
		PC12	¿Hay una descripción completa del proceso de investigación?	5	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	5	
		PC14	Los reportes son claros.	5	4.07142857
IEEE44	Leveraging SDN for Efficient Anomaly Detection and Mitigation on Legacy Networks	PC1	¿Están claramente establecidos los objetivos para el estudio?	4	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	3	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	3	
		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	3	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	5	

		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	4	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	4	
		PC8	¿Se describen los métodos estadísticos?	3	
		PC9	¿Están justificados los métodos estadísticos?	3	
		PC10	¿Es claro el propósito del análisis?	4	
		PC11	¿Son creíbles los resultados?	4	
		PC12	¿Hay una descripción completa del proceso de investigación?	4	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	4	
		PC14	Los reportes son claros.	4	3.71428571
IEEE45	Real Time DNS Traffic Profiling Enhanced Detection Design for National Level Network	PC1	¿Están claramente establecidos los objetivos para el estudio?	4	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	4	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	3	
		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	3	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	5	
		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	4	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	4	
		PC8	¿Se describen los métodos estadísticos?	3	
		PC9	¿Están justificados los métodos estadísticos?	3	
		PC10	¿Es claro el propósito del análisis?	3	
		PC11	¿Son creíbles los resultados?	4	
		PC12	¿Hay una descripción completa del proceso de investigación?	4	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	3	
		PC14	Los reportes son claros.	3	3.57142857

IEEE46	Evolving Switch Architecture toward Accommodating In-Network Intelligence	PC1	¿Están claramente establecidos los objetivos para el estudio?	4	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	4	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	2	
		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	2	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	5	
		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	4	
		PC8	¿Se describen los métodos estadísticos?	2	
		PC9	¿Están justificados los métodos estadísticos?	2	
		PC10	¿Es claro el propósito del análisis?	4	
		PC11	¿Son creíbles los resultados?	4	
		PC12	¿Hay una descripción completa del proceso de investigación?	4	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	4	
		PC14	Los reportes son claros.	4	3.42857143
IEEE47	MaMPF: Encrypted Traffic Classification Based on Multi-Attribute Markov Probability Fingerprints	PC1	¿Están claramente establecidos los objetivos para el estudio?	3	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	3	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	3	
		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	3	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	4	
		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	3	
		PC8	¿Se describen los métodos estadísticos?	3	

		PC9	¿Están justificados los métodos estadísticos?	3	
		PC10	¿Es claro el propósito del análisis?	3	
		PC11	¿Son creíbles los resultados?	3	
		PC12	¿Hay una descripción completa del proceso de investigación?	3	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	3	
		PC14	Los reportes son claros.	3	3.07142857
IEEE48	No Way to Evade: Detecting Multi-Path Routing Attacks for NIDS	PC1	¿Están claramente establecidos los objetivos para el estudio?	4	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	4	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	4	
		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	4	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	5	
		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	4	
		PC8	¿Se describen los métodos estadísticos?	3	
		PC9	¿Están justificados los métodos estadísticos?	3	
		PC10	¿Es claro el propósito del análisis?	4	
		PC11	¿Son creíbles los resultados?	4	
		PC12	¿Hay una descripción completa del proceso de investigación?	4	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	4	
		PC14	Los reportes son claros.	4	3.85714286
IEEE49	Detection of Host Search Activity in PTR Resource Record Based DNS Query Packet Traffic	PC1	¿Están claramente establecidos los objetivos para el estudio?	3	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	3	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	3	

		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	3	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	5	
		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	3	
		PC8	¿Se describen los métodos estadísticos?	3	
		PC9	¿Están justificados los métodos estadísticos?	3	
		PC10	¿Es claro el propósito del análisis?	3	
		PC11	¿Son creíbles los resultados?	3	
		PC12	¿Hay una descripción completa del proceso de investigación?	3	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	3	
		PC14	Los reportes son claros.	3	3.14285714
IEEE50	Identifying Suspicious Activities through DNS Failure Graph Analysis	PC1	¿Están claramente establecidos los objetivos para el estudio?	3	
		PC2	¿El estudio se basa en investigaciones previas que lo fundamentan?	3	
		PC3	¿Las variables / métricas tienen una mediación clara en el estudio?	3	
		PC4	Los modelos de valoración de las variables/métricas de estudio están definidas.	3	
		PC5	Si el estudio involucra la evaluación de una tecnología, ¿está claramente definida la tecnología?	4	
		PC6	¿Son las medidas utilizadas en el estudio las más relevantes para responder a las preguntas de investigación?	3	
		PC7	¿Es suficiente el alcance (tamaño y longitud) del estudio para permitir que se identifiquen cambios en los resultados de interés?	3	
		PC8	¿Se describen los métodos estadísticos?	3	
		PC9	¿Están justificados los métodos estadísticos?	3	
		PC10	¿Es claro el propósito del análisis?	3	
		PC11	¿Son creíbles los resultados?	3	

		PC12	¿Hay una descripción completa del proceso de investigación?	3	
		PC13	¿Hay una coherencia entre datos, la interpretación y las conclusiones?	3	
		PC14	Los reportes son claros.	3	3.07142857

Fuente. Adaptación de *Checklist for quantitative studies*(Kitchenham & Charters, 2007)

ANEXO F. CONFIGURACIÓN PARA LAS PRUEBAS REALIZADAS EN EL CAPITULO 5. VALIDACIÓN DE LA PROPUESTA

Este anexo incluye el detalle de las pruebas realizadas en el capítulo 5, validación de la propuesta de la metodología de control de amenazas insiders para intranets académicas detallada en el Capítulo 4 y aplicada en el campus de la ESPOCH. Se incluyen las configuración de las pruebas y análisis realizadas en cada una de ellas:

En la sección 1, se desarrolla la validación en cuatro etapas:

1. Diagnóstico de seguridad con OSSTMM adaptado en el canal humano (1.1).
2. Análisis en tiempo real de la intranet para identificar amenazas (1.2).
3. Evaluación del control de la amenaza DoS en un escenario SDN, mediante políticas ACLs en el controlador Floodlight. Se aplican dos pruebas: sin control y con la implementación del mecanismo de mitigación (1.4).

En la sección 2, se realiza el análisis estadístico, verificando supuestos y validando la hipótesis planteada en el Capítulo 1.

1. Aplicación de la metodología

La intranet del campus académico en estudio está ubicada en el edificio de la Facultad de Informática y Electrónica (FIE) en la Escuela Superior Politécnica de Chimborazo (ESPOCH), universidad del Ecuador.

1.1 Etapa 1. Diagnóstico de seguridad de la intranet académica en el canal humano.

1.1.1 Aplicación de OSSTMM adaptado en el canal humano de la intranet del campus académico.

Se considera 4.1.1 donde se describe la adaptación de la metodología OSSTMM V3.02, se incluye las fases de la metodología propuesta, según se describe en el capítulo 4 inciso 4.1.1 donde se adapta OSSTMM V3.02 para el análisis del canal humano en la intranet académica. Se incluyen las fases de inducción, interacción, evaluación de la confiabilidad y gestión de recursos e intervención para evaluar la seguridad respecto al canal humano e identificar las brechas existentes con el cálculo del RAV.

Esta investigación aplica la prueba de caja gris donde el auditor tiene información limitada del objetivo y este es informado con anterioridad a la ejecución de la prueba (Herzog, 2010). La información se obtiene del personal técnico encargado de los laboratorios y equipos de la intranet

académica, ubicada en el edificio de la FIE, y de las entrevistas al personal de Redes de la Dirección de Tecnologías de la Información y Comunicación (DTIC) de la universidad del Ecuador en análisis, la ESPOCH.

A continuación, se incluye las fases de la metodología propuesta:

1) FASE DE INDUCCIÓN.

1.1) REVISIÓN DE LA POSTURA

Los criterios seleccionados son: políticas, legislación, regulaciones, cultura y relaciones.

1.2.) LOGÍSTICA

- Se considera: equipos de comunicación, comunicaciones y tiempo. Donde los servicios en la intranet son: voz, video y datos.
- La comunicación, se da en español.
- En el tiempo se determina que los docentes y estudiantes poseen un horario en dependencia de sus actividades académicas, a diferencia del sector administrativo que labora en un horario definido.

1.3) VERIFICACIÓN DE DETECCIÓN ACTIVA

- La intranet académica cuenta con los servicios de: acceso a internet y telefonía. Con relación a las políticas institucionales el departamento de Infraestructura y Redes (DTIC) de la ESPOCH únicamente es la encargada de realizar la verificación de la seguridad, monitoreo y supervisión de la red, además del soporte técnico, por lo que no se considera verificación de detección activa.

2) FASE 2: INTERACCIÓN

- Esta fase calcula el valor de la seguridad operacional o porosidad y los valores de los controles de interacción clase A y B, indicados en la Tabla 4 referente a: Porosidad, Controles y Limitaciones en la Metodología OSSTMM(Herzog, 2010).
- La información se obtiene de las entrevistas a los encargados de la red, aplicando la observación y la utilización de los dispositivos de seguridad del edificio, se contabiliza la porosidad total en el canal humano que considera: visibilidad, acceso y confianza, sin embargo, no se especifica cuáles son por confidencialidad.

- Para el cálculo de controles para el acceso a los activos: laboratorios y equipos, se calcula los controles clase A en el canal humano, evaluando: autenticación, indemnización, resistencia, subyugación y continuidad. Y los de clase B, que corresponden a: no-repudio, confidencialidad, privacidad, integridad, sistemas de alarma. Estos datos son ingresados para el cálculo final en el formulario automatizado de la metodología OSSTMM V3.02, adjunto en el Anexo G. Se detalla a continuación:

2.1) AUDITORIA DE LA VISIBILIDAD

- Identificación de acceso, se determina las interacciones de los técnicos a cargo del sitio, con los usuarios de la intranet: estudiantes, docentes y administrativos, así como los procesos que manejan, para proveer acceso en función al tipo de usuario.
- Enumeración personal: Se evalúa el personal dentro del alcance con acceso autorizado o no a los activos, en este caso el cuarto de telecomunicaciones, laboratorios, aulas y equipos.

2.2) VERIFICACIÓN DE ACCESO

- Proceso de acceso: Se determina los procesos y métodos para acceder a los activos de la intranet y escenarios sin que se necesite una autorización.
- Autoridad: Con relación al personal que tiene acceso a los activos en el alcance, solo los técnicos pueden prestar los activos de la intranet, por lo que este punto no se toma en cuenta.
- Autenticación: Se contabiliza los métodos por los cuales se puede interactuar con el personal de recepción y acceso.

2.3) VERIFICACIÓN DE CONFIANZA

- En relación con la autenticidad de los documentos de solicitud de préstamo de laboratorios o equipos, autorizados por los directores de escuela, con firma y sello de legalidad. El abuso de los recursos puede darse ya que no se cuenta con un control detallado de la actividad individual de cada uno de los usuarios de la intranet institucional.

2.4) VERIFICACIÓN DE CONTROLES (CONTROLES DE CLASE B)

Los controles de clase B, se consideran esenciales para proteger los activos de la información y mitigar los riesgos derivados de su exposición, teniendo en cuenta las actividades diarias incluidas en el alcance, las cuales son:

- No repudio: Contabiliza al personal de recepción que identifican y registran adecuadamente el acceso o las interacciones con los activos.
- Confidencialidad: Numera los segmentos de comunicación eficiente con los encargados dentro del alcance.
- Privacidad: Contabiliza los métodos eficientes para asegurar este control.
- Integridad: Registra los métodos eficientes aplicados en el alcance para proteger y asegurar que la información de los activos físicos no pueda ser alterados o manipulados.
- Alarma: Anota los sistemas de advertencia en caso de emergencia.

3) FASE 3: Evaluación de la Confiabilidad y Gestión de Recursos (INVESTIGACIÓN).

3.1) VERIFICACIÓN DE PROCESOS

- Mantenimiento: Se relaciona con la revisión de la postura. Se aplica la lista de verificación de la seguridad, acerca de cursos de capacitación sobre seguridad hacia el personal estudiantes, docentes y administrativos.
- Desinformación y Diligencia: En base a la información de la lista de verificación de la seguridad se determina que no existen cursos de capacitación de seguridad, únicamente cursos impartidos por el proveedor de servicios. No se toma en cuenta este punto.
- Indemnización: Considera los documentos legales a los que deben someterse los estudiantes o docentes para la utilización de ciertos activos o información.

3.2) VERIFICACIÓN DE ENTRENAMIENTO

- Acerca de la capacitación sobre seguridad informática a los trabajadores, como se determina en la fase de inducción no existe capacitación institucional considerada al momento en seguridad. Por lo que no se toma en cuenta.
- Hijacking o secuestro: No se puede aplicar ya que la cantidad de estudiantes supera los 3000.

3.3) VALIDACIÓN DE LA PROPIEDAD

- Mercado negro: Todos los programas utilizados en los laboratorios son distribuidos a los estudiantes si se solicita, solo algunos de estos programas tienen licencias.

- Canales de venta: Al ser distribuidos abiertamente no se tiene control de lo que el estudiante hace con el software.

3.4) REVISIÓN DE SEGREGACIÓN

- Asignación de contención de privacidad: Se identifica cómo se maneja la privacidad.
- Limitaciones: Se considera las fases anteriores, errores y anomalías. Además: vulnerabilidades, debilidades, preocupación, exposición y anomalías para el cálculo final del RAV.

3.5) VERIFICACIÓN DE EXPOSICIÓN

La información requerida en este punto es confidencial por esta razón no se toma en cuenta para la adaptación de la metodología del canal humano.

3.6) EXPLORACIÓN DE INTELIGENCIA COMPETITIVA

Se relaciona con empresas, por lo que no se considera en el presente estudio.

4) FASE 4: INTERVENCIÓN

Mediante el cálculo automático con la herramienta ISECOM, al ingresar los datos se obtiene el estado actual de la seguridad operacional aplicado en el canal humano. En esta fase intervienen:

4.1) VERIFICACIÓN DE CUARENTENA

En intranets académicas, donde la colaboración abierta es esencial, los riesgos asociados a contactos hostiles son bajos. La prioridad es proteger datos personales, gestionar accesos y garantizar la integridad de la información. Por ello, las pruebas de cuarentena no son aplicables en este contexto.

4.2) PRIVILEGIOS DE AUDITORÍA

- Subyugación: Contabilizar los métodos por los cuales se puede interactuar con el personal de recepción.
- Los puntos: identificación, autorización, escalamiento de permisos, discriminación se realizan con previa identificación en concordancia con la fase de inducción.

4.3) CONTINUIDAD DE SERVICIO

- Resistencia: Contabiliza los responsables que permiten acceder sin autorización a los activos del cuarto de telecomunicaciones.

- Continuidad: Registra el total de responsables que genera conflictos en cuanto a retrasos de acceso.

4.4) ALERTAS Y REVISIÓN: FIN DE LA ENCUESTA.

Se incluye revisión y alertas en esta fase al ser la parte final de la metodología, estas se relacionan con controles de la segunda fase, se incluye: verificación de alarmas y almacenamiento, además de recuperación de Información, proporcionando un control adicional y asegurando que todos los incidentes sean registrados, evaluados y gestionados de manera adecuada. La información es confidencial.

El cálculo del RAV indica el estado actual de la seguridad operacional de un canal, calculado de manera automatizada, en la hoja de cálculo del RAV de la web oficial de ISECOM(ISECOM, 2021), donde se ingresan los valores numéricos de cada ítem para obtener los resultados. Al concluir la aplicación de OSSTMM adaptado se obtiene como resultado, el 85.77 RAV, que corresponde a la evaluación de riesgo (RAV) de seguridad, determinando un 13.92% de vulnerabilidades y anomalías que pueden ser aprovechados por un usuario interno.
Se incluye el formulario del cálculo del RAV con los resultados del análisis de seguridad operacional aplicado al canal humano en el Anexo G.

Al existir vulnerabilidades se sigue con la etapa 2, de lo contrario concluiría la aplicación de la metodología.

1.2 Etapa 2. Análisis en tiempo real de la data de la intranet del campus académico en estudio.

Con el propósito de corroborar los resultados obtenidos en la Etapa 1, en la que se identificaron vulnerabilidades en la intranet académica, se llevó a cabo un análisis en tiempo real del tráfico de red en el campus de la ESPOCH, específicamente en el edificio de la FIE.

La metodología se implementó en un entorno de red de alta velocidad (Gigabit Ethernet, hasta 1 Gbps), utilizando puertos espejo (mirror ports) para capturar tráfico de tres VLANs de la intranet. Se implementaron NIDS-SNORT para el análisis del tráfico en tiempo real y NEXPOSE para complementar y validar la auditoría de amenazas internas realizada en la Etapa 1. A través de un escaneo de vulnerabilidades con NEXPOSE en su versión de prueba, se identificaron debilidades en la red y se evaluaron posibles soluciones.

- Análisis de tráfico de la intranet en tiempo real.

El análisis de amenazas internas se efectuó sobre la intranet de la ESPOCH, institución que cuenta con una matriz principal en la ciudad de Riobamba, así como con dos campus adicionales ubicados en Macas y Orellana. En la matriz principal, la infraestructura de red está conformada por:

- Ocho nodos principales, que corresponden a las siete facultades y un nodo administrativo.
- La administración es centralizada y está a cargo del DTIC, quien gestiona y almacena los datos.
- Con aproximadamente 250 switches en total.
- Posee un rango de direcciones IP públicas de clase /24.
- 42 switches exclusivos de la FIE.

Para este estudio, el análisis en tiempo real se llevó a cabo en la intranet del edificio principal de la FIE, considerando los siguientes entornos de acceso:

- Siete laboratorios.
- Dos salas de profesores.
- Un área administrativa.

El monitoreo se centró en las VLANs de Estudiantes, Docentes y Administrativos para capturar y analizar datos de tráfico. Esto permitió identificar amenazas con mayor precisión y evaluar estrategias de control aplicables en investigaciones futuras.

- Infraestructura de red

En la Figura 25, se presenta la infraestructura de la intranet académica, que está compuesta por equipamiento CISCO, específicamente:

- Un switch de distribución WS-3850C-48P.
- Diez switches de acceso 2960-48P.

El servidor HP G9, ubicado en el data center del edificio de la FIE, fue configurado con NIDS-SNORT, siguiendo las especificaciones técnicas establecidas en la documentación oficial de la (SNORT COMMUNITY, 2022). Para el análisis del tráfico de red y la identificación de amenazas

internas, se estableció la conexión del servidor con el switch de distribución, habilitando tres puertos mirror destinados a la captura de paquetes en tiempo real. El periodo de monitoreo comprendió del 2 de mayo al 7 de julio de 2019, seleccionado estratégicamente por corresponder al intervalo de mayor carga en la intranet académica, debido al desarrollo regular de actividades académicas en dicho período.

A continuación, se presenta el escenario de estudio.

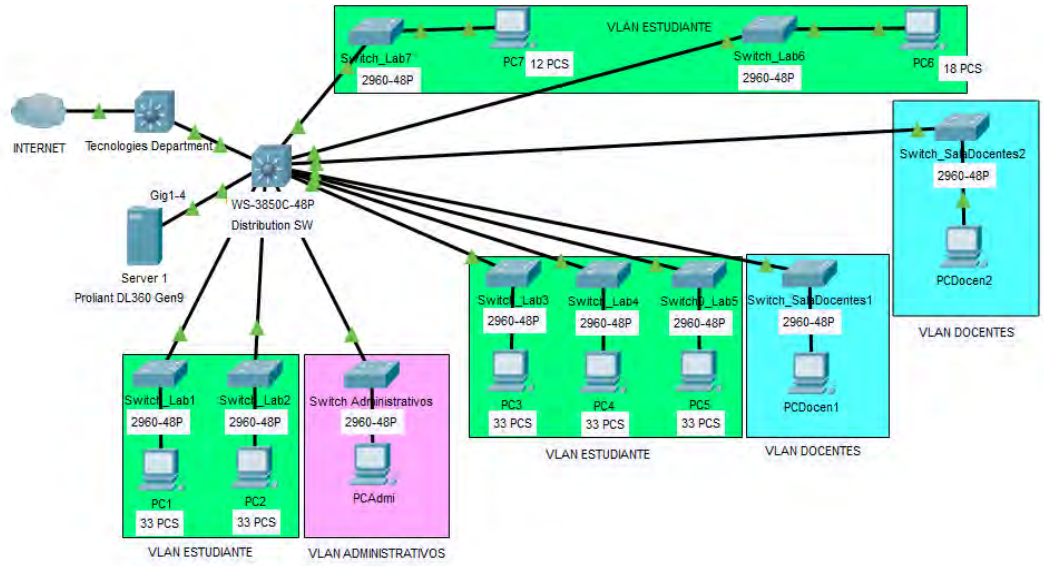


Figura 25: Infraestructura de la Intranet Académica.(Barba-Vera et al., 2024)

Se configura NIDS-SNORT para analizar la red con las reglas de la comunidad y las de usuario NIDS-SNORT aplicadas para el análisis. Ello permite indicar las alertas en consola escuchadas de las VLANs estudiante, docente y administrativo. NIDS-SNORT almacena los paquetes de las alertas en logs, una vez que se detiene para el análisis del paquete. Este proceso se realiza a diario incluyendo los fines de semana.

A continuación, se presentan las Tabla 57, 58 y 59, que incluyen la cantidad de paquetes recibidos, analizados y eliminados en las VLAN de Estudiante, Docente y Administrativo por NIDS-SNORT y sus porcentajes. Se observa que, a pesar de la cantidad de paquetes recibidos, NIDS-SNORT pudo analizarlos, obteniendo una baja tasa de eliminación de paquetes, demostrando la eficiencia de esta herramienta y un adecuado análisis del tráfico de la intranet.

Tabla 57: Análisis del tráfico en la VLAN Estudiante basado en el número de paquetes

VLAN Estudiante		
Nombre	Cantidad	Porcentaje
Paquetes recibidos	27810598653	100%
Paquetes analizados	26884523479	96.75%
Paquetes eliminados	902986272	3.25%

Fuente. Elaboración propia.

Tabla 58: Análisis del tráfico en la VLAN Docente basado en el número de paquetes.

VLAN Docente		
Nombre	Cantidad	Porcentaje
Paquetes recibidos	548884339	100%
Paquetes analizados	545328509	99.35%
Paquetes eliminados	3555783	0.65%

Fuente. Elaboración propia.

Tabla 59: Análisis del tráfico en la VLAN Administrativa basado en el número de paquetes.

VLAN Administrativa		
Nombre	Cantidad	Porcentaje
Paquetes recibidos	389006844	100%
Paquetes analizados	386385688	99.33%
Paquetes eliminados	2620083	0.67%

Fuente. Elaboración propia.

- Interpretación de datos capturados en la intranet

Para interpretar los datos analizados en tiempo real con NIDS-SNORT, se llevó a cabo un análisis de las amenazas identificadas y se compararon los resultados con los obtenidos mediante Nexpose. Esto permitió elaborar un cuadro comparativo detallado (Tabla 59), en el cual se incluyen:

- El Identificador SNORT (SID),
- El tipo de amenaza detectada,
- Las VLANs afectadas, y
- Una descripción de la amenaza.

Además, el análisis con Nexpose proporciona información sobre las vulnerabilidades específicas detectadas en los activos evaluados.

El monitoreo se ejecutó 24 horas al día, siete días a la semana, exceptuando feriados. Durante este proceso, se registraron y analizaron los siguientes parámetros:

- Cantidad de paquetes analizados,
- Alertas generadas,
- Direcciones IP de origen y destino,
- Identificadores de alerta,
- Fecha y hora de cada evento,
- Número total de alertas por día, y
- Observaciones relevantes registradas durante el análisis en las VLANs.

Para el proceso de escaneo, Nexpose fue instalado en un host perteneciente a las VLANs Estudiante y Docente. Se realizó un escaneo completo, utilizando credenciales de acceso autorizadas para evaluar todos los dispositivos en la red. Como resultado, Nexpose generó un informe ejecutivo, en el que se clasificaron las vulnerabilidades detectadas de acuerdo con:

- Nivel de riesgo,
- Sistema operativo afectado,
- Tipo de vulnerabilidad, y
- Medidas de mitigación recomendadas.

Un resumen de este informe se presenta en el Anexo H.

- Comparación de resultados entre NIDS-SNORT y Nexpose

El escaneo y el análisis en tiempo real de la intranet del campus académico permitieron identificar múltiples amenazas y vulnerabilidades en las VLANs Estudiante, Docente y Administrativa. La comparación entre ambas herramientas evidenció una relación significativa entre los ataques detectados por NIDS-SNORT y las vulnerabilidades reportadas por Nexpose.

Los datos de Nexpose fueron extraídos directamente del reporte generado después del escaneo de los objetivos. A partir de este análisis comparativo, se validó el diagnóstico de seguridad de la intranet académica, lo que permitirá seleccionar una amenaza insider específica para su control en la Fase 4 de este estudio.

- Gestión eficiente de reglas en NIDS-SNORT: Identificador SNORT (SID) y número de revisión (rev)

En la Tabla 60, se presenta el SNORT ID (SID), un identificador único que permite una gestión eficiente de reglas en el sistema de detección de intrusiones SNORT. Este mecanismo garantiza que cada regla sea única, evitando conflictos en la identificación de amenazas.

El proceso de asignación del SID sigue un enfoque sistemático, diseñado para optimizar la organización y administración de reglas en el IDS. Adicionalmente, el número de revisión (rev) asociado al SID permite un control detallado de versiones, lo que facilita la actualización frecuente de reglas ante nuevas amenazas emergentes (Jaw & Wang, 2022).

Estas características hacen del SID un elemento esencial para mejorar la precisión, adaptabilidad y rendimiento del sistema de detección de intrusiones en entornos dinámicos.

Tabla 60: Análisis de amenazas detectadas con NIDS-SNORT y vulnerabilidades identificadas con NEXPOSE

Análisis con NIDS-SNORT				**Exploración con Nexpose**
Identificador SNORT	**Amenaza**	**VLANs**	**Descripción**	**Vulnerabilidad**
1-40357:3	Instantaccess.exe Trojan	Estudiante	Redirige a un sitio malicioso que muestra advertencias de que su computadora está infectada y necesita ejecutar el escaneo instant-access.exe inmediatamente . (VSAntivirus, 2005)	Se observó que el 15.339% de las vulnerabilidades encontradas pertenecen a vulnerabilidades web. Que puede ser explotado con malware.
1-31046:6	Exploit kit	Estudiante	Este evento se genera cuando una estructura de URL coincide con la estructura utilizada por el.(SNORT, 2024)	
1-46237:1	Miner64 Trojan	Estudiante Docente	Es un archivo ejecutable que forma parte de BitcoinMiner desarrollado por Ufasoft. Este evento se genera	

Análisis con NIDS-SNORT				Exploración con Nexpose
Identificador SNORT	**Amenaza**	**VLANs**	**Descripción**	**Vulnerabilidad**
			cuando se ejecuta la muestra del minero.(Microsoft, 2014)	
1-45549:1	XMRig Trojan	Estudiante Docente	Este evento se genera cuando XMRig intenta iniciar sesión en una API de grupo de minería jsonrpc (GitHub, 2024)	
1-48080:1	Ramnit Trojan	Estudiante	El troyano Ramnit hace que los equipos infectados funcionen como una red de bots centralizada.(Incibe, n.d.)	
1-46486:1	LittleInstaller Trojan	Estudiante	Este evento se genera cuando una computadora Slimware se comunica con el servidor de control para obtener actualizaciones no deseados.SNORT(2024)	
1-41337:2	Sysch Malware	Estudiante	Una aplicación que realiza en secreto otras acciones que afectan la información personal o confidencial almacenada en el dispositivo y/o el control del dispositivo. Está asociado al sistema operativo Android. SNORT(2024)	
1-35549:1	Zeus Trojan Malware	Estudiante Docente	Este troyano se usa para instalar el ransomware CryptoLocker en la computadora de la víctima. (VirusTotal, 2006)	
1-35030:1	Zbot or Zeus Trojan	Estudiante Docente	Una versión del malware troyano Zeus. Este troyano se usa para instalar el ransomware CryptoLocker	

Análisis con NIDS-SNORT				Exploración con Nexpose
Identificador SNORT	**Amenaza**	**VLANs**	**Descripción**	**Vulnerabilidad**
			en una computadora víctima.SNORT (2024)	
1-25074:1	Banker Trojan	Estudiante	Troyanos que roban información bancaria de un sistema afectado. (kASPERSKY, 2024)	
1-41573:4	Information theft	Estudiante	El tráfico detectado conocido por explotar vulnerabilidades en el navegador Internet Explorer, en el sistema operativo Windows, permite a los atacantes remotos obtener información confidencial a través de un sitio web manipulado, también conocido como "Microsoft Edge Information Disclosure Vulnerability".(Microsoft, 2017)	Más del 40 % de los objetivos activos (usuarios) durante el análisis Nexpose utilizan el sistema operativo Windows 7. Haciéndolos vulnerables a amenazas 1-41573:4, 1-47102:1 y 1-32691:1.
1-47102:1	Exploit Usage	Estudiante Administrativo	Este evento se genera cuando un atacante intenta aprovechar una vulnerabilidad de confusión de tipos en Microsoft Edge o CVE-2018-8298. (Microsoft, 2020)	
1-23605:12	Malicious file.	Estudiante	Nombrado Armadillo, se sabe poca información sobre esta alerta es de origen ruso.(SNORT, 2024)	Se determinó el 15.339% de vulnerabilidades en líneas de código. Que puede ser explotado con inyección de código malicioso.
1-43459:2	Backdoor Doublepulsar and exploit Eternalblue	Estudiante	Implementación de Doublepulsar Backdoor, se puede utilizar para ejecutar	Vulnerabilidades del protocolo SMB. La firma del bloque de mensajes del servidor

Análisis con NIDS-SNORT				Exploración con Nexpose
Identificador SNORT	**Amenaza**	**VLANs**	**Descripción**	**Vulnerabilidad**
			software malicioso en la máquina víctima . Eternalblue es un exploit comúnmente utilizado para explotar vulnerabilidades en el protocolo SMB y relacionado con el ransomware Wannacry. (Fortinet, 2024)	(SMB) está deshabilitada. SMBv1 SMBv2 firma no requerida Se utiliza el protocolo SMBv1 en desuso. MS17-010.
1-46659:2	Exploit Usage	Estudiante	Intento de explotar un doble gratuito en Adobe Acrobat Reader.SNORT(2024)	Vulnerabilidad CVE-2018-4990, la explotación exitosa puede conducir a la ejecución de código malicioso.
1-32691:1	Script usage	Estudiante Docente	Intento de DoS usando Internet Explorer 9. (BetaFred et al., 2019)	Más del 40% de los ordenadores conectados a la intranet utilizan el sistema operativo Windows 7 mediante Internet Explorer. Nexpose determinó que alrededor del 10% de las vulnerabilidades encontradas pertenecen a la categoría DoS.

Fuente. Elaboración propia.

La Tabla 60 muestra la relación entre las amenazas detectadas con NIDS-SNORT en las VLAN Estudiante, Docente y Administrativo, junto con un resumen de las estadísticas de vulnerabilidades identificadas con Nexpose donde se detectó:

- El 15.34% de las vulnerabilidades pertenecen a web que pueden ser explotadas con malware como Instantaccess.exe, Miner64, XMRig, Ramnit, LittleIn-staller, Zbot o Zeus, Banker, Exploit kit.

- Además, más del 40% de los objetivos activos, usuarios de intranet durante el escaneo en la VLAN de Estudiantes, tienen el sistema operativo Windows 7, siendo vulnerables al robo de información al explotar la vulnerabilidad de Microsoft Edge e Internet Explorer.
- Se detectó que el 15.339% pertenecen a vulnerabilidades relacionadas con líneas de código que pueden ser explotadas con inyección de código malicioso.
- Las vulnerabilidades de los protocolos SMBv1 y SMBv2 en las que el protocolo se utiliza sin la firma de identificación SMB, además de que el protocolo está actualmente en desuso, pueden ser explotadas por el exploit Eternalblue y la puerta trasera Doublepulsar, que está relacionada con el conocido ransomware Wannacry. Esto se determinó en la VLAN estudiante.
- La explotación de la vulnerabilidad CVE-2018-4990, puede conducir a la ejecución de código malicioso mediante el uso de un exploit para romper la seguridad del software comercial.
- Alrededor del 10% de las vulnerabilidades encontradas pertenecen a la categoría DoS, esta amenaza fue detectada en el uso de Internet Explorer 9 en las VLANs Docente y Estudiante.

El SID del SNORT posibilita la identificación de amenazas en la intranet del campus académico, permite la búsqueda de soluciones potenciales para cada vulnerabilidad, así como la capacidad de explotar y controlar estas vulnerabilidades y amenazas. Que pueden ser la base para estudios futuros.

1.3 Etapa 4. Implementación de control de la amenaza insider seleccionada: DoS.

Considerando la metodología descrita en el capítulo cuatro, se plantea un escenario SDN con equipos reales y políticas de QoS a través de ACLs para evaluar la incidencia del control de la amenaza interna en el rendimiento.

- **Calidad de Servicio (QoS) y parámetros de rendimiento**.

Se evalúan los parámetros de rendimiento: ancho de banda, latencia, jitter (variaciones en latencia), pérdida de paquetes. Para medir la incidencia de las ACLs al mitigar la amenaza insider DoS en la intranet del campus académico de la ESPOCH.

- **Implementación de Políticas de QoS.**

Para la implementación de políticas de QoS se considera: la experiencia en la implementación de políticas de QoS en redes legacy descrito en la metodología para esta fase en 4.4.2. Es importante categorizar el tráfico para generar tráfico similar al de la intranet en evaluación,

considerando los protocolos TCP en el 80% y UDP en el 20%, respectivamente, esto se considera para la simulación de tráfico con D-ITG. Además, el flujo de etapas del modelo propuesto para el diseño de políticas de QoS en redes convencionales y SDN que se detallada en la Figura 21 del capítulo 4, p. 93. La política de control de la amenaza DoS se implementa en SDN en el controlador FloodLigth.

- **Establecer el escenario de pruebas con tecnología SDN.**

El escenario de pruebas con tecnología SDN se basa en criterios técnicos y analíticos obtenidos del análisis detallado del tráfico en la intranet del campus académico de la ESPOCH. Este escenario está diseñado para simular condiciones realistas y evaluar el impacto de ataques de DoS en un entorno controlado. A través de la implementación de políticas de QoS y el uso de herramientas avanzadas, se busca medir el rendimiento de la red frente a estas amenazas, tomando en cuenta parámetros clave como ancho de banda, latencia, jitter y pérdida de paquetes. A continuación, se detallan los parámetros:

- Data de la intranet.

El análisis previo del tráfico en la intranet proporcionó información crítica sobre los protocolos y el volumen de datos manejados. Las Tablas 56, 57 y 58 describen un alto número de paquetes en las VLANs evaluadas, identificando a TCP (80%) y UDP (20%) como los protocolos predominantes. Este patrón se utilizó como base para la configuración del generador de tráfico D-ITG, recreando condiciones similares a las observadas en la red real. Además, se consideró la velocidad del puerto de red de las computadoras (100 Mbps) para generar paquetes de transmisión adaptados al entorno.

- Generador de tráfico

El generador D-ITG se seleccionó debido a su capacidad para crear tráfico personalizado que imita las condiciones reales de una intranet. Esta herramienta permite inyectar tráfico que simula diferentes escenarios, facilitando la medición precisa de parámetros de rendimiento y proporcionando datos confiables para el análisis.

- Entorno de pruebas SDN

El escenario de pruebas simula un nodo que representa un laboratorio de la intranet de la ESPOCH configurado con equipos físicos en un escenario SDN. Donde se incluye la amenaza insider DoS, que tiene la finalidad de agotar los recursos del sistema informático (ancho de banda

o de procesamiento), logrando así la interrupción temporal o definitiva de los servicios de bases de datos o páginas web, mediante la generación de varias solicitudes en un instante de tiempo al equipo de destino, comprometiendo la disponibilidad. Los protocolos que tienen más prioridad de ser atacados son: SMTP, DNS y NTP (Toainga & Peña, 2019).

Las amenazas más comunes a la capa de transporte son los ataques de DoS, por lo que este tipo de amenazas se considera en la fase de explotación, esto implica denegar el servicio de una página web y el acceso a la misma. Para simular el ataque de DoS, se utiliza la Distribución/Kali Linux Scritp Slowloris – Módulos de Metasploit. Para realizar la explotación, en el escenario se incluye un servidor web apache configurando la página por defecto para realizar las pruebas, siendo esta el objetivo del ataque se utiliza la herramienta Slowloris que permite mediante una línea de comando realizar un ataque DoS, usa tráfico HTTP (Hipertext Transfer Protocol), hace una conexión TCP completa y envía cientos de solicitudes a largo plazo e intervalos regulares. Eventualmente, todas las conexiones se agotarán y ningún otro servidor podrá conectarse hasta que se liberen al menos algunas de las conexiones retenidas.

En la intranet del campus académico se realizó un escaneo del escenario y se obtuvo las direcciones IP por lo que esa información se utiliza en este ataque. La dirección IP del servidor web apache en el escenario es 192.168.0.20/24.

Para realizar el ataque desde Kali Linux, se ingresa al directorio de la herramienta y se ejecuta la línea de comando para el ataque:

Sudo perl ./303lowloris.pl -dns 192.168.0.20 -port 80 -timeout 1 -num 1000 -cache

Esta línea indica que se ejecute un ataque hacia la dirección IP del servidor web enviando 1000 paquetes TCP a través del puerto 80 cada segundo y además que se almacenen los paquetes en cache. La definición del número de paquetes para la ejecución del ataque se realizó en base a los logs almacenados de las alertas detectadas con SNORT durante el análisis del tráfico, pues al revisarlo tuvo una duración de aproximadamente 10 minutos en el que se enviaron alrededor de 5000 paquetes en un segundo. Sin embargo, para la prueba en el escenario de estudio que considera un nodo de la intranet, se adaptó considerándose 1000 paquetes de ataque, para poder recolectar 60 muestras que permitan hacer una valoración estadística y no saturar la conexión en las primeras pruebas con 5000 paquetes.

- Recursos de topología

Se utiliza los equipos SDN descritos en la metodología para el hardware, así como en el software. Esto se detalla en el inciso 4.4.3.

- Controlador

Se emplea el controlador Floodlight, que es multiplataforma, cuenta con Rest API, es de código abierto, de instalación medianamente complejo, compatible con los equipos del escenario de pruebas. Además, tiene más tiempo en el mercado y buena documentación, características relevantes para su implementación.(Barba et al., 2019)

- Pruebas en el escenario de estudio con tecnología SDN.

Las pruebas se realizan en el escenario SDN, como se observa en la figura 24, donde se incluye el plano de control con el servidor SNORT y el controlador Floodlight. En el plano de datos se incluyen Host A, Host B y Kali Linux además de las conexiones entre los equipos. A continuación, las configuraciones se describen en un proceso secuencial por pasos. Mayor detalle puede encontrar en el Anexo I.

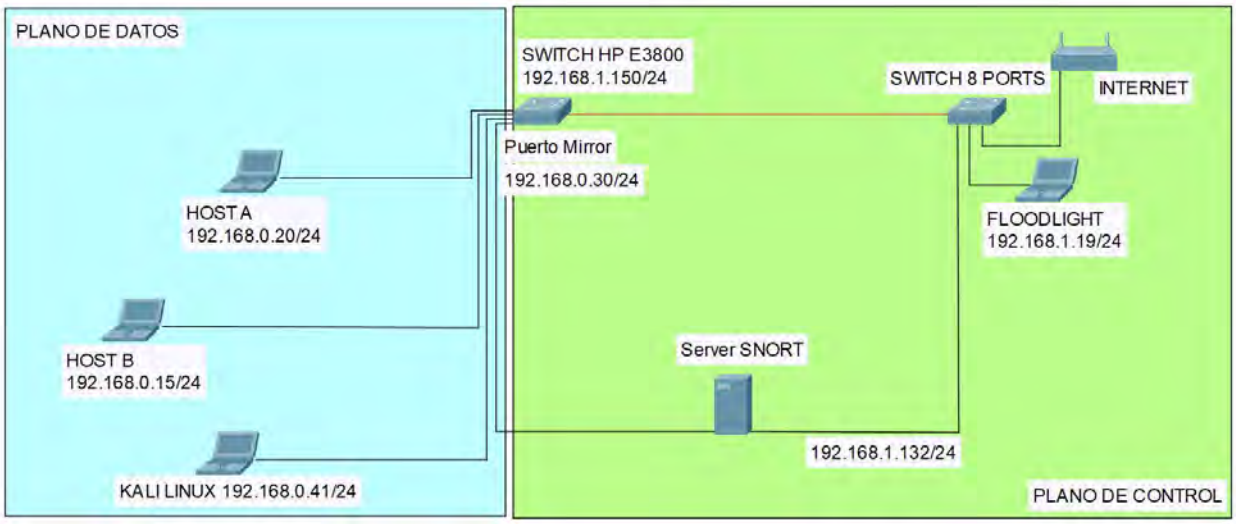


Figura 26: Escenario propuesto

Fuente. Elaboración propia.

Prueba 1: Análisis en el escenario SDN con ataque de DoS y sin control

La prueba se realiza en el escenario SDN descrito en la figura 26. El gráfico muestra una configuración segmentada en dos planos principales: plano de control y de datos, diseñados para analizar el impacto de un ataque DoS en ausencia de políticas de control.

Se incluye un switch HP E3800 que conecta el tráfico del plano de datos con el plano de control a través del puerto *mirror*, lo que permite el monitoreo y análisis del tráfico. El Servidor SNORT recibe datos de la red para detectar anomalías. El controlador Floodlight, ubicado en el plano de control, supervisa el flujo de datos y aplica las políticas configuradas en la red. Este diseño asegura la segregación lógica de roles, el monitoreo efectivo del tráfico, y la simulación de ataques con un enfoque en la detección y mitigación de intrusiones evaluando el rendimiento de la red frente a ataques de tipo DoS, lo que permite establecer parámetros clave para futuras optimizaciones en la gestión de redes de campus académicos empleando tecnología SDN.

A continuación, se describe la conexión entre los componentes:

1. **Configuración de la topología:**
    - Separación del plano de datos del plano de control.
    - Plano de control:
        - Controlador FloodLigth (192.168.0.19/24).
        - Switch SDN HP E3800 (192.168.1.150/24).
        - Servidor SNORT (192.168.1.132/24).
    - Plano de datos:
        - Host A (servidor web) - 192.168.0.20/24.
        - Host B (cliente) - 192.168.0.15/24.
        - Equipo atacante (Kali Linux) - 192.168.0.41/24.
2. **Pruebas estándar:**
    - Ping entre equipos de prueba.
3. **Configuración del entorno:**
    - Levantamiento del controlador Floodlight.
    - Activación de SNORT para detección de anomalías.
    - Observación de flujos generados por Floodlight.
4. **Activación de SNORT:**
    - Monitoreo del tráfico en el plano de control y de datos.
    - Configuración de reglas para detectar amenazas.
5. **Verificación de conexiones:**
    - Ping entre Host A y Host B.
6. **Simulación de ataque DoS:**
    - Uso de Slowloris desde el equipo atacante.
    - Ejecución del ataque DoS dirigido al Host A.

7. **Inyección de tráfico con D-ITG:**
    - Creación de flujos e inyección desde el servidor SDN.
    - Recepción del tráfico en el cliente SDN.
8. **Generación de reportes:**
    - Captura de datos con D-ITG desde el cliente.
    - Análisis de parámetros de rendimiento: ancho de banda, jitter, delay y pérdida de paquetes.

Prueba 2: Análisis en el escenario SDN con ataque de DoS y con la política de control.

El escenario para la prueba 2 se desarrolla en un entorno SDN, similar a la prueba 1, figura 26, con los mismos planos principales: el plano de datos y el plano de control, pero incluye políticas de control diseñadas para mitigar el impacto del ataque de Denegación de Servicio (DoS).

De tal manera que se evalúe el impacto del ataque DoS sobre el servidor web cuando se implementan políticas de control diseñadas para mitigar las anomalías detectadas por SNORT, lo que permite comparar los resultados de esta prueba con los de la Prueba 1, para validar la eficacia de las políticas en un entorno SDN para mantener la estabilidad y disponibilidad de los servicios en la red.

El escenario simula condiciones realistas bajo control, asegurando una evaluación exhaustiva de las medidas de mitigación frente a ataques DoS en un entorno SDN bien estructurado.

A continuación, el detalle de la prueba:

1. **Configuración de la topología:**
    - Separación del plano de datos del plano de control.
    - Plano de control:
        - Controlador FloodLigth (192.168.1.19/24).
        - Switch SDN HP E3800 (192.168.1.150/24).
        - Equipo Ubuntu con SNORT (192.168.1.132/24).
    - Plano de datos:
        - Host A (servidor) - 192.168.0.20/24.
        - Host B (cliente) - 192.168.0.15/24.
        - Equipo atacante (Kali Linux) - 192.168.0.41/24.
2. **Acceso al controlador Floodlight:**

- Observación del switch HP E3800 y hosts desde la interfaz web.

3. **Visualización de la topología:**
   - Generación del escenario SDN por Floodlight.
4. **Flujos generados por Floodlight:**
   - Habilitación de la comunicación entre los equipos del escenario.
5. **Verificación de conexiones:**
   - Comprobación de la comunicación entre Host A y Kali Linux.
6. **Simulación de ataque DoS:**
   - Uso de Slowloris para atacar el Host A.
   - Ejecución del ataque y observación de la línea de comandos.
7. **Implementación de SNORT:**
   - Configuración de reglas de detección de ataques DoS.
   - Ejecución de SNORT y detección del ataque.
8. **Bloqueo del ataque:**
   - Implementación de reglas para bloquear el ataque mediante comandos CURL.
   - Verificación de las reglas desde el controlador Floodlight.
9. **Inyección de tráfico con D-ITG:**
   - Generación de tráfico desde el servidor SDN.
   - Recepción del tráfico en el cliente SDN.
10. **Análisis de datos generados:**
    - Evaluación de parámetros de rendimiento como jitter, ancho de banda, delay y pérdida de paquetes.
    - Realización del análisis estadístico para validar la propuesta.

- **Análisis comparativo de los resultados**

El análisis comparativo de resultados se obtiene con base en la ejecución de dos pruebas experimentales:

Prueba 1: Evaluación del Ataque DoS sin Políticas de Control

- Se ejecuta un ataque Slowloris, enviando 1000 paquetes TCP por segundo al servidor web sin aplicar ninguna medida de mitigación.
- Se miden los parámetros de rendimiento de la red (ancho de banda, latencia, jitter y pérdida de paquetes) antes, durante y después del ataque.
- Los valores observados reflejan un impacto crítico en la estabilidad de la red.

Prueba 2: Evaluación del Ataque DoS con Políticas de Control

- Se repite el mismo ataque Slowloris, pero en este caso con SNORT y Floodlight activados para la detección y mitigación en tiempo real.
- Se aplican reglas de bloqueo en Floodlight y SNORT detecta la anomalía en el tráfico, permitiendo responder al ataque antes de que cause una interrupción grave.
- Se vuelven a medir los mismos parámetros de rendimiento de la red para determinar el impacto del control implementado.

- **Cálculo del Porcentaje de Reducción del Impacto**

El porcentaje de mejora en cada parámetro se calcula usando la siguiente fórmula:
Reducción del Impacto (%)=((Valor Sin Control−Valor Con Control)/ Valor Sin Control))×100.

Ejemplo de cálculo para latencia:

Sin Control: Incremento del 220%
Con Control: Incremento del 15%

Reducción del Impacto=((220−15)/220))×100=85%

Este mismo procedimiento se aplica a jitter, pérdida de paquetes y ancho de banda, comparando los valores antes y después de la mitigación del ataque. Los datos obtenidos permiten estructurar la tabla de análisis comparativo, resaltando la mejora en los parámetros de rendimiento de la red. Los cálculos de la reducción del impacto para cada parámetro de rendimiento se observan como sigue:

- Reducción del impacto en ancho de banda:
  ((75−10)/75)×100=86.67%

- Reducción del impacto en latencia:
  ((220−15)/220)×100=93.18%

- Reducción del impacto en jitter:

((180−5)/180)×100=97.22%

- Reducción del impacto en pérdida de paquetes:
  ((46−3)/46)×100=93.48%

- **Resumen del Análisis Comparativo**

Se detalla en la tabla 61 el análisis comparativo de los parámetros de rendimiento en las pruebas y la reducción del impacto.

Tabla 61*:* Resumen del Análisis comparativo de los parámetros de rendimiento en las pruebas y la reducción del impacto.

Parámetro	Sin Control	Con Control	Reducción del Impacto (%)
Ancho de Banda	75%	10%	**86.67%**
Latencia	220%	15%	**93.18%**
Jitter	180%	5%	**97.22%**
Pérdida de Paquetes	46%	3%	**93.48%**

Fuente. Elaboración propia.

Hallazgo Principal

La integración de SNORT y Floodlight en un entorno SDN reduce significativamente el impacto de los ataques DoS, asegurando la disponibilidad y estabilidad del servicio.

El análisis de validación de la propuesta se realiza utilizando un método estadístico en 3.

2. Recolección de datos

Se seleccionaron 60 muestras por prueba en el escenario físico SDN para garantizar la validez estadística del análisis t-Student, equilibrando rigor académico y factibilidad operativa. Este tamaño muestral, recomendado por la literatura, supera el mínimo de 30 necesario para confiabilidad estadística y permite capturar suficiente variabilidad del sistema, minimizar errores tipo II y cumplir los supuestos de normalidad y homogeneidad de varianzas (Mahat, 2024; Althubaiti, 2023; Kang, 2021). Además, en casos donde los datos no cumplen los supuestos de normalidad, este tamaño es adecuado para pruebas no paramétricas como la prueba U de Mann-

Whitney, que garantiza resultados confiables y válidos bajo condiciones de distribución no normal o datos ordinales (Nuha et al., 2021).

Se realizaron 60 muestras por cada prueba en el escenario físico SDN con la amenaza de DoS, antes de la política de control y con la implementación de la política de control. Evaluando los parámetros de rendimiento de la red: delay, jitter, ancho de banda, pérdida de paquetes; adicional a ello se consideró el porcentaje de pérdida de paquetes y promedio de paquetes por segundo, que corrobora la variable pérdida de paquetes y, promedio de paquetes por segundo que da una idea de la cantidad de paquetes transmitidos, producto de la comunicación en el escenario de estudio.

Los datos están conformados por paquetes de datos TCP en el 80% y 20% de paquetes UPD, empezando desde 4496 hasta 104377 de 512 bytes c/u con un tiempo de duración de 10 segundos. Enviando tráfico desde de 2.19 a 50.96 Mbps.

3.Análisis de datos

1.1 Análisis Descriptivo

Una vez que se recogieron las muestras, se procede a realizar un análisis descriptivo de cada una de las variables analizadas. En la Tabla 62, escenario sin política de control, se muestra el resumen de estadísticos descriptivos para cada una de las variables, los resultados del primer escenario sin política de control se denomina Grupo 0 y en la Tabla 63 compila los resultados del segundo escenario con implementación de Política de Control, Grupo 1.

Tabla 62: Escenario sin política de Control

	N	Media	Mediana	Desv. Desviación	Mínimo	Máximo
Delay	60	1090,1876	1090,4638	,40363	1089,63	1090,57
Jitter	60	,0004	,0004	,00028	,00	,00
Ancho_de_Banda	60	30732,8004	35011,7722	10731,20035	1840,46	42688,79
Promedio_Paquetes_Seg	60	7503,1251	8547,7960	2619,92196	449,33	10422,07
Pérdida_Paquetes	60	6812,9167	2702,0000	8434,42620	2,00	28850,00
Paquetes_perdidos_porcentaje	60	6,7715	3,4300	8,09372	,03	27,04

Fuente. Elaboración propia.

Tabla 63: Escenario con implementación de política de Control

	N	Media	Mediana	Desv. Desviación	Mínimo	Máximo
Delay	60	1063,5976384	1055,5571575	14,71955001	1055,48	1090,14
Jitter	60	,0003992	,0003530	,00024676	,00	,00
Ancho_de_Banda	60	31410,9787711	35906,9230850	10844,83871315	1837,42	43577,12
Promedio_Paquetes_Seg	60	7668,6959890	8766,3386440	2647,66570157	448,59	10638,94
Pérdida_Paquetes	60	5761,1666667	2309,0000000	8218,66324478	,00	28721,00
Paquetes_perdidos_porcentaje	60	5,5553333	2,4400000	7,51089005	,00	25,94

Fuente. Elaboración propia.

Delay: En el contexto de la SDN, el delay es una métrica crucial, ya que la eficiencia en la transmisión de paquetes es fundamental para el rendimiento de las aplicaciones y servicios que dependen de la red. El Grupo 0, sin política de control, mostró un delay promedio de 1090.19 ms. El Grupo 1, con política de control, presentó un delay promedio significativamente menor de 1063.60 ms, destacando el potencial de las políticas de control en la reducción del tiempo de transmisión de paquetes en una SDN. Esta reducción de aproximadamente un 2,5%, destaca el impacto positivo de las políticas de control en la disminución del delay y valida su eficacia como herramientas clave para la optimización de la calidad del servicio (QoS). Este resultado responde a una problemática identificada en estudios previos, como el de Imran et al. (2019), que plantearon la necesidad de políticas de control capaces de abordar no solo la reducción del delay, sino también la sobrecarga computacional y la protección de la red frente a ataques DoS, pero que, hasta el momento, no habían sido validadas en entornos reales, demostrando viabilidad y efectividad de dichas políticas en condiciones reales aportando una perspectiva aplicada que refuerza su relevancia práctica y ofrece una contribución tangible para el desarrollo de soluciones adaptativas en redes SDN.

Jitter: El jitter bajo en ambos grupos es un indicativo positivo, especialmente en un entorno SDN donde la consistencia en el tiempo de transmisión es vital para la sincronización de aplicaciones y servicios distribuidos. La ligera reducción en el jitter observada en el Grupo 1 es resultado de una gestión de tráfico más efectiva proporcionada por las políticas de control implementadas. Estas políticas optimizan la distribución del tráfico y reducen las fluctuaciones temporales (jitter), mejorando la uniformidad en los tiempos de transmisión. Este resultado, aunque sutil, valida la efectividad de las estrategias de control para mitigar la variabilidad en entornos reales y aporta un fundamento sólido para la adopción de SDN en infraestructuras críticas, donde la consistencia temporal es esencial para garantizar el rendimiento y la calidad del servicio.

Ancho de Banda:

El ancho de banda similar en ambos grupos sugiere que la capacidad de transmisión de datos es adecuada en ambos casos. Sin embargo, en un entorno SDN, la eficiencia en la utilización del ancho de banda resulta tan crucial como su capacidad bruta, y las políticas de control desempeñan un papel fundamental en su optimización. Este estudio valida dicha afirmación en un escenario práctico con datos reales, lo que lo diferencia de estudios previos, como el de (Jenny & Sugirtham, 2023), que, aunque destacan la importancia de estas políticas, no cuantifican el valor exacto de mejora. La evidencia empírica presentada en este trabajo no solo corrobora los resultados teóricos existentes, sino que también supera los desafíos de redes operativas, consolidando las políticas de control como herramientas indispensables para la mejora de la calidad del servicio (QoS) y la experiencia del usuario final (QoE). Los hallazgos de este trabajo refuerzan la importancia de implementar soluciones prácticas y adaptativas en redes SDN modernas, maximizando el uso del ancho de banda y asegurando la continuidad operativa en escenarios críticos.

Pérdida de Paquetes:

La reducción en la pérdida de paquetes, desde un 6,77% en el Grupo 0 hasta un 5,56% en el Grupo 1, con una mejora del 1,21%, evidencia de manera clara la efectividad de las políticas de control en la mitigación de interrupciones causadas por ataques DoS y en la mejora de la QoS en entornos SDN. Estos resultados coinciden con investigaciones recientes que destacan el impacto positivo de estas estrategias. Por ejemplo, Wang (2023) presenta DoSDefender, un marco diseñado para reducir la saturación de recursos en el plano de control, mejorando la estabilidad de la red. Sin embargo, dicho estudio no reporta valores específicos sobre la mejora en la pérdida de paquetes. Asimismo, Eliyan & Di Pietro (2021) enfatizan la importancia de monitorear esta métrica en redes SDN, pero tampoco ofrecen datos cuantitativos concretos que respalden la efectividad de las políticas de control.

En contraste, esta tesis proporciona evidencia empírica sólida obtenida en un entorno práctico, consolidando su relevancia al presentar resultados cuantificables que confirman el impacto positivo de las políticas de control en la reducción de la pérdida de paquetes. Esto posiciona la investigación como un aporte significativo a la literatura existente, no solo validando las capacidades teóricas de las redes SDN, sino también ofreciendo un enfoque práctico que aborda las limitaciones de estudios anteriores. Contribuyendo con un enfoque metodológico que guía el

desarrollo de estrategias más robustas y adaptativas, esenciales para responder a los crecientes desafíos en la gestión de redes modernas.

Pérdida de Paquetes (%): Esta métrica proporciona una visión porcentual de la pérdida de paquetes, y los resultados son coherentes con la métrica anterior.

Promedio de Paquetes por Segundo: Esta métrica refleja la capacidad de la red para procesar paquetes bajo demanda. El grupo "Con política de control" procesa un mayor número de paquetes por segundo en comparación con el grupo "Sin política de control", lo que destaca la efectividad de las políticas de control en mantener la operatividad de la red.

En función de los datos analizados, se concluye que la implementación de políticas de control en una red SDN ha demostrado un impacto significativo en la mejora de métricas clave como el delay, el jitter, el ancho de banda y la pérdida de paquetes, lo que contribuye directamente a la optimización de la QoS y la QoE. Este estudio no solo valida la efectividad de estas estrategias en un entorno práctico, sino que también supera las limitaciones de investigaciones previas al aportar resultados cuantificables y aplicables en condiciones reales de operación.

Los hallazgos de esta investigación subrayan la importancia de una gestión de red eficiente, dinámica y proactiva, que aproveche las capacidades de las redes SDN para adaptarse y responder de manera efectiva a condiciones cambiantes y amenazas como los ataques DoS. Este enfoque no solo refuerza la resiliencia de la red, sino que también marca un precedente metodológico para el diseño e implementación de estrategias más robustas y adaptativas, esenciales en la gestión de redes modernas. La contribución de este trabajo establece una base sólida para futuras investigaciones y aplicaciones prácticas en redes SDN, consolidando su relevancia como una solución crítica para enfrentar los desafíos de la conectividad contemporánea.

1.1.1 Gráficos de los resultados e interpretación.

Se incluyen los gráficos de los datos de los parámetros de rendimiento evaluados en los grupos con política de control y sin política de control en la Figura 27.

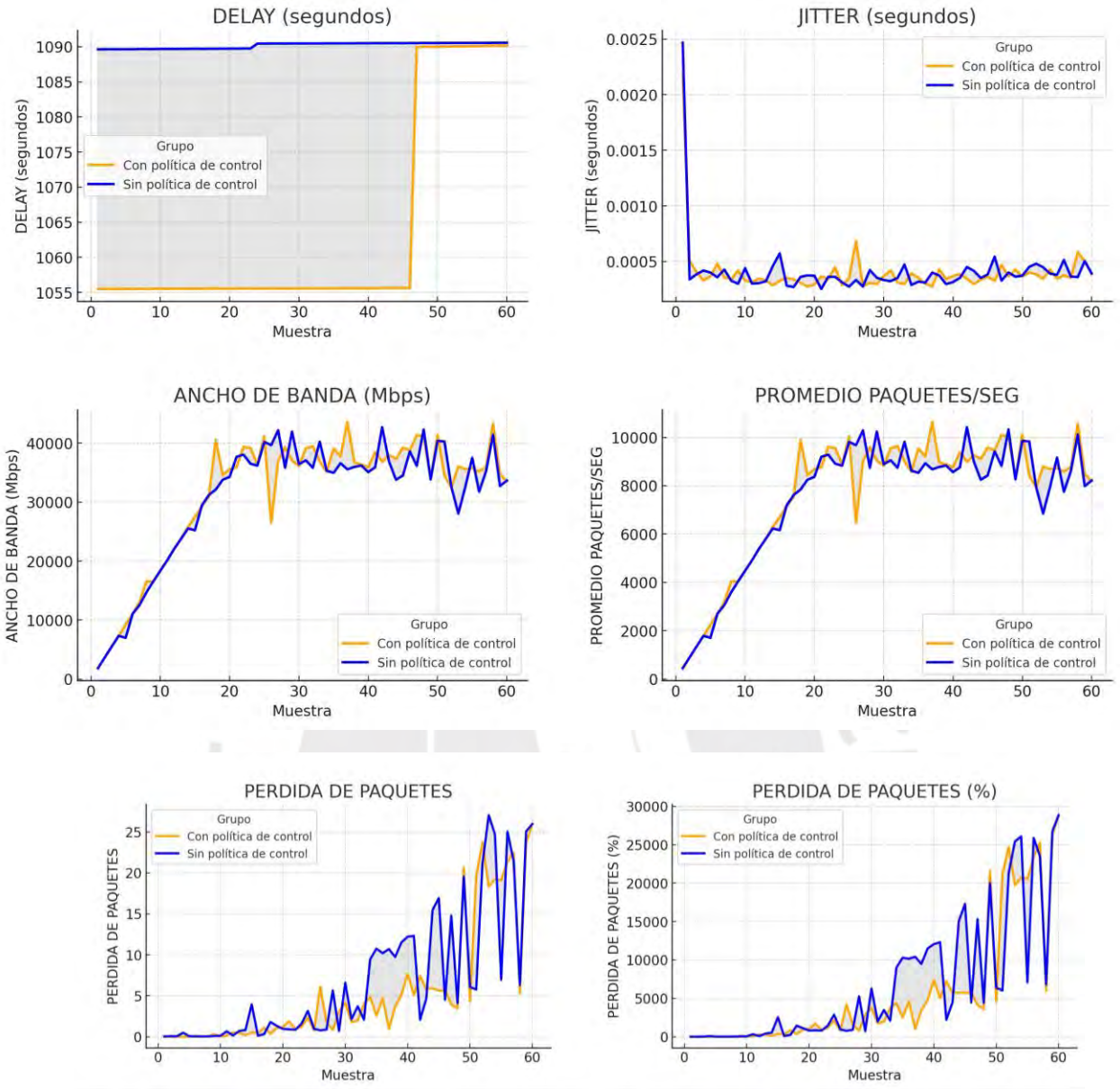


Figura 27: Gráficos de los resultados de las variables de análisis de rendimiento de la red.
Fuente. Elaboración propia.

Los resultados obtenidos de este análisis empírico subrayan la importancia crucial de implementar políticas de control en entornos de red definidos por software, especialmente cuando se enfrentan a amenazas de seguridad como los ataques DoS. El grupo "Con política de control" ha demostrado un rendimiento y una resiliencia notables en todas las métricas evaluadas, principalmente en el delay, lo que valida la efectividad de las estrategias de mitigación empleadas. Estos hallazgos proporcionan una base sólida para la adopción de medidas

proactivas en la protección de infraestructuras de red críticas, asegurando así la integridad y el rendimiento óptimo de la red en presencia de amenazas cibernéticas.

1.2 Comprobación de supuestos estadísticos

Para comparar los dos grupos sin implementación de una regla de control del insider threat DoS y con implementación de esta regla de control en términos de las variables de rendimiento analizadas, se puede considerar la realización de una prueba t de Student para muestras independientes. Sin embargo, antes de aplicar esta prueba, es necesario verificar los siguientes supuestos:

- Normalidad, para determinar si las distribuciones de las variables se aproximan a una distribución normal en cada grupo.
- Homogeneidad de varianzas: Para verificar si las varianzas de las variables en los dos grupos son o no similares.

Para verificar estos supuestos, se aplicará la prueba de Shapiro-Wilk para evaluar la normalidad de la distribución de los datos, considerando que la muestra para cada grupo es de 60 observaciones. La prueba de Levene se aplica para evaluar la homogeneidad de varianzas entre los grupos. Si los supuestos se cumplen, se procederá con la prueba t de Student. Si no se cumplen, se podría considerar una prueba no paramétrica como la prueba U de Mann-Whitney que debe emplearse cuando los datos son ordinales o cuando los tamaños de muestra son pequeños y no se ajustan a una distribución normal(Nuha et al., 2021). En la Tabla 64 y Tabla 65 se muestran los resultados de la prueba de Shapiro-Wilk y de la prueba de Levene respectivamente.

Tabla 64: Resultados de la prueba de Shapiro-Wilk.

Variable	Grupo 0		Grupo 1	
	Estadístico Shapiro-Wilk	P-Valor	Estadístico Shapiro-Wilk	P-Valor
Delay	0.846	0.000	0.837	0.000
Jitter	0.698	0.000	0.530	0.000
Ancho_de_Banda	0.201	0.000	0.195	0.000
Promedio_Paquetes_Seg	0.848	0.000	0.837	0.000
Perdida_Paquetes	0.248	0.000	0.112	0.000
Paquetes_perdidos_porcentaje	0.267	0.000	0.165	0.000

Fuente. Elaboración propia.

Tabla 65: Resultados de la prueba de Levene.

Variable	F	P-Valor
Delay	145.209	0.000
Jitter	0.15	0.88
Ancho_de_Banda	0.002	0.98
Promedio_Paquetes_Seg	0.04	0.98
Perdida_Paquetes	4.06	0.45
Pquetes_perdidos_porcentaje	3.05	0.35

Fuente. Elaboración propia.

Todos los valores de p-valor son menores que 0.05, lo que indica que podemos rechazar la hipótesis nula de normalidad para todas las variables en ambos grupos. Esto significa que las distribuciones de estas variables no siguen una distribución normal ($p < 0.05$).

Con respecto a la homogeneidad de Varianzas, la prueba de Levene indicó que para el "DELAY", las varianzas entre los dos grupos no son homogéneas. Para las demás variables, no hay evidencia suficiente para rechazar la hipótesis nula, indicando que las varianzas entre los grupos son homogéneas.

Dada la violación de los supuestos de normalidad y homogeneidad de varianzas para algunas variables, no es posible aplicar una prueba paramétrica como la prueba t de Student, para comparar los dos grupos, por lo que, se aplicará la prueba no paramétrica de U Mann-Whitney.

3.3 Comparación entre grupos

La prueba de Mann-Whitney U se utiliza para determinar si hay diferencias estadísticamente significativas entre dos grupos independientes cuando los datos no cumplen con los supuestos de normalidad y homogeneidad de varianzas. En la Tabla 66 se muestran los resultados de la prueba aplicada a cada una de las variables:

Tabla 66: Prueba de U-Man Whitney.

Estadísticos de prueba						
	Delay	**Jitter**	**Ancho_de_Banda**	**Promedio_Paquetes_Seg**	**Perdida_Paquetes**	**Paquetes_perdidos_porcentaje**
U de Mann-Whitney	322,000	1669,500	1634,000	1634,000	1654,000	1638,000
W de Wilcoxon	2152,000	3499,500	3464,000	3464,000	3484,000	3468,000
Z	-7,757	-0,685	-0,871	-0,871	-0,766	-0,850
p-valor	0,000	0,493	0,384	0,384	0,443	0,395
a. Variable de agrupación: Escenario						

Fuente. Elaboración propia.

DELAY: Hay evidencia significativa para rechazar la hipótesis nula de que las distribuciones de retraso son iguales en ambos grupos. Esto demuestra que la política de control es efectiva para mitigar los efectos del tráfico excesivo generado por ataques DoS, mejorando la entrega de paquetes y la calidad del servicio (QoS). Este hallazgo valida la hipótesis de la investigación al demostrar que estas políticas están diseñadas específicamente para reducir el delay en condiciones de amenaza.

JITTER, ANCHO DE BANDA, PROMEDIO PAQUETES/SEG, PERDIDA PAQUETES, PERDIDA DE PAQUETES PORCENTAJE: No hay evidencia suficiente para rechazar la hipótesis nula, lo que indica que no hay diferencias significativas entre los dos grupos en estas variables.
Sin embargo, al analizar la descripción de los datos y el análisis estadístico se tiene: Jitter: ambos grupos muestran valores bajos de jitter, con una ligera reducción en el Grupo 1, el análisis estadístico indica que esta mejora no es significativa. A pesar de ello, los resultados destacan la capacidad de las políticas de control para mantener la consistencia temporal en la transmisión de paquetes, lo cual es fundamental para aplicaciones sensibles al tiempo.
Ancho de Banda: el análisis muestra un aumento leve en el ancho de banda utilizado por el Grupo 1 (31.410,98 kbps) en comparación con el Grupo 0 (30.732,80 kbps). Aunque estadísticamente no significativo, este incremento resalta que las políticas de control optimizan la utilización eficiente del ancho de banda, asegurando recursos disponibles en escenarios críticos.
Pérdida de Paquetes: hay una reducción del 6,77% al 5,56% refleja una mejora del 1,21%, aunque no estadísticamente significativa. Este resultado es consistente con investigaciones previas que destacan la importancia de políticas de control para mitigar interrupciones, aunque la implementación práctica no muestra diferencias significativas en condiciones operativas.
Promedio de Paquetes por Segundo: El Grupo 1 procesó un mayor número de paquetes por segundo (7.668,70) frente al Grupo 0 (7.503,13). Si bien este incremento no fue estadísticamente significativo, apoya la efectividad de las políticas de control en el manejo de la operatividad de la red bajo demanda.

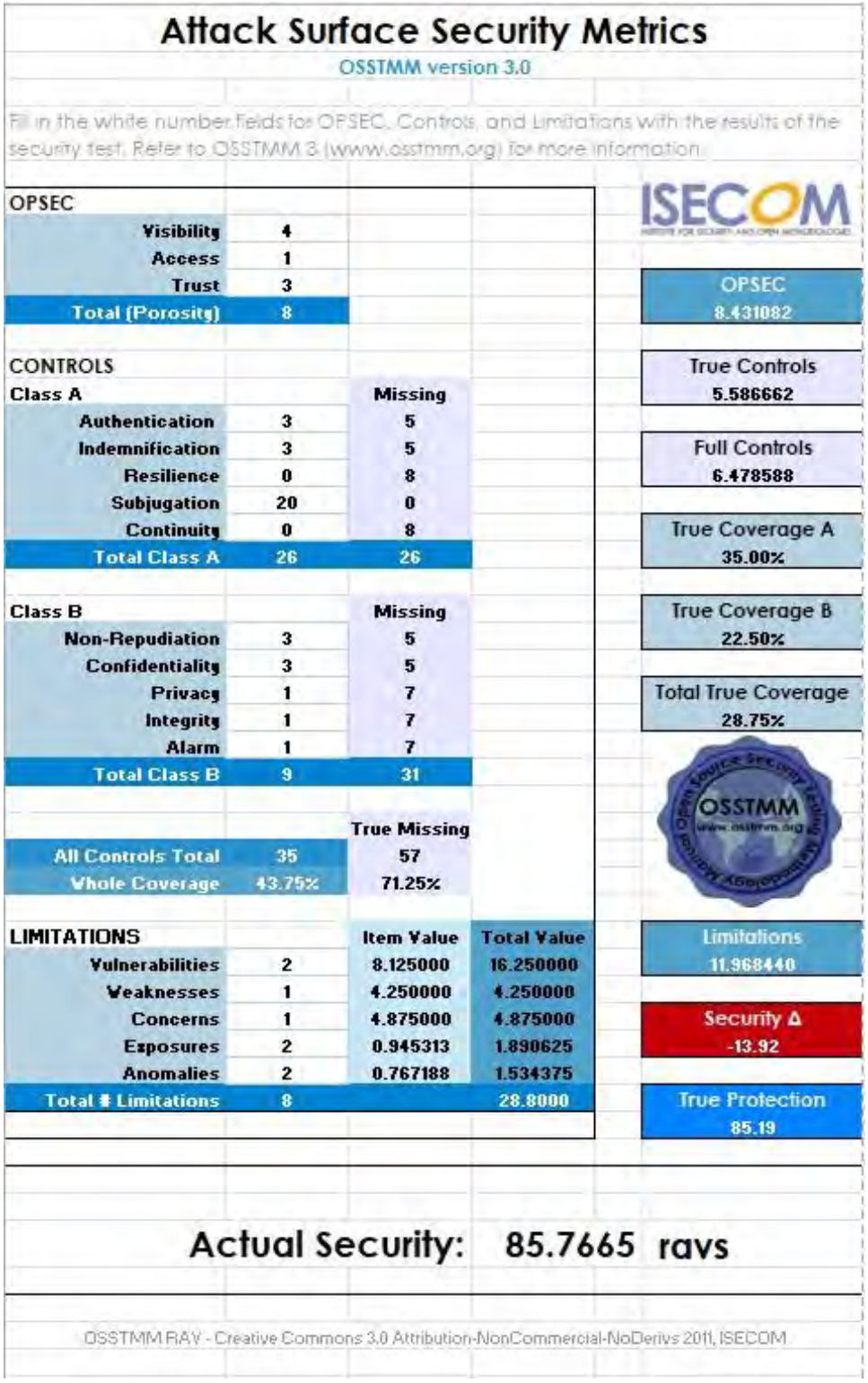
En resumen, la política de control obtiene un impacto significativo en la reducción del retraso (delay), pero no se observan diferencias significativas en las otras variables evaluadas, al realizar

el análisis estadístico, sin embargo, los resultados reflejan un rendimiento consistentemente mejorado en el Grupo 1. Esto resalta la importancia de la políticas de control no solo para mejorar el rendimiento de la red en métricas clave, sino también para consolidar una base empírica en el desarrollo de soluciones prácticas y adaptativas que aborden los crecientes desafíos de la gestión de amenazas en redes modernas.

La mejora del delay, puede deberse a que la política de control está específicamente diseñada para gestionar el control de la amenaza de DoS, que incide en el DELAY, debido a que el exceso de tráfico generado por el ataque puede saturar los enlaces de la red y los dispositivos, causando retrasos en la entrega de paquetes y la política de QoS implementada elimina satisfactoriamente este efecto.

Con lo que se comprueba la hipótesis del presente trabajo doctoral que evalúa “la implementación de políticas de QoS en SDN facilita el control de insiders threat mejorando el rendimiento de la intranet académica” en términos de reducción del retraso causado por ataques DoS, resaltando su importancia en la gestión de amenazas de seguridad.

ANEXO G. FORMULARIO DEL CÁLCULO DEL RAV APLICADO AL CANAL HUMANO.



Attack Surface Security Metrics

OSSTMM version 3.0

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

ISECOM

OPSEC		
Visibility	4	
Access	1	
Trust	3	
Total (Porosity)	8	

OPSEC 8.431082

CONTROLS		
Class A		Missing
Authentication	3	5
Indemnification	3	5
Resilience	0	8
Subjugation	20	0
Continuity	0	8
Total Class A	26	26

True Controls 5.586662

Full Controls 6.478588

True Coverage A 35.00%

Class B		Missing
Non-Repudiation	3	5
Confidentiality	3	5
Privacy	1	7
Integrity	1	7
Alarm	1	7
Total Class B	9	31

True Coverage B 22.50%

Total True Coverage 28.75%

OSSTMM

		True Missing
All Controls Total	35	57
Whole Coverage	43.75%	71.25%

LIMITATIONS		Item Value	Total Value
Vulnerabilities	2	8.125000	16.250000
Weaknesses	1	4.250000	4.250000
Concerns	1	4.875000	4.875000
Exposures	2	0.945313	1.890625
Anomalies	2	0.767188	1.534375
Total # Limitations	8		28.8000

Limitations 11.968440

Security Δ -13.92

True Protection 85.19

Actual Security: 85.7665 ravs

Figura 28: Resultado de la Auditoría del Canal Humano (ISECOM, 2021)

ANEXO H. REPORTE DE NEXPOSE EN LA INTRANET ACADÉMICA.

El análisis de vulnerabilidades con Nexpose instalada en un host perteneciente a las VLANs incluyó la intranet en estudio con un tipo de análisis completo con las credenciales de acceso a los equipos. El proceso tuvo una duración de 24 minutos, tras lo cual se generó un informe ejecutivo que clasificó las vulnerabilidades por nivel de riesgo, sistema operativo, tipo y posibles soluciones.

Las vulnerabilidades en redes de datos se clasifican en tres categorías principales: críticas, graves y moderadas, según su impacto potencial y la facilidad con la que pueden ser explotadas. Esta clasificación es esencial para priorizar los esfuerzos de mitigación y garantizar una gestión de riesgos eficiente. El Sistema de puntuación de vulnerabilidades comunes (CVSS) se utiliza a menudo para evaluar estas vulnerabilidades, donde una puntuación alta indica un riesgo crítico que requiere atención inmediata (Singh y Joshi, 2016). Se describe sus tipos:

2. Vulnerabilidades Críticas, representan los riesgos más altos dentro de una red, ya que pueden permitir a los atacantes tomar control total de los sistemas afectados.
3. Vulnerabilidades Graves, aunque menos urgentes que las críticas, las vulnerabilidades graves aún representan un riesgo significativo para la integridad y disponibilidad de la red.
4. Vulnerabilidades Moderadas, presentan menor riesgo, pero aún pueden comprometer el rendimiento o la seguridad operativa de la red.

Resultados del análisis de Nexpose en la VLAN Estudiantes

El informe indicó la presencia de 400 vulnerabilidades, distribuidas en 30 críticas, 296 graves y 74 moderadas. Identificándose vulnerabilidades críticas en 6 sistemas, mientras que 2 no presentaron ningún problema. El resto de los equipos mostró vulnerabilidades graves y moderadas.

Principales vulnerabilidades y sistemas afectados

- Las vulnerabilidades más comunes fueron generic-icmp-timestamp (21 ocurrencias) y generic-tcp-timestamp (18 ocurrencias).

- La categoría más afectada fue "Apple y Apple Mac OS X", con 200 instancias relacionadas con sistemas operativos obsoletos en laboratorios. También se observó una prevalencia de equipos con Windows 7, que requieren actualizaciones urgentes.
- Varias vulnerabilidades graves están relacionadas con el protocolo SMB (Server Message Block), utilizado para la compartición de archivos e impresoras en red. Estas vulnerabilidades tienen un puntaje de riesgo entre 3000 y 5000 y se deben a la falta de configuración de la firma SMB, lo que facilita ataques de tipo "hombre en el medio". La firma SMB puede configurarse de manera segura para prevenir estos riesgos.
- En el caso de vulnerabilidades según servicios, HTTP (Hypertext Transfer Protocol) fue el más utilizado en los equipos analizados y presentó 71 vulnerabilidades, lo que lo convierte en el principal foco de riesgos detectados.

El informe evidencia la urgencia de implementar actualizaciones en sistemas operativos obsoletos, como Windows 7 y Apple Mac OS X, y mejorar las configuraciones de seguridad en protocolos y servicios críticos. Además, se recomienda configurar adecuadamente la firma SMB para reducir el riesgo de ataques a la red. Este análisis resalta la importancia de un mantenimiento constante y la actualización de sistemas para mitigar vulnerabilidades en redes universitarias.

A continuación, se incluyen páginas del informe en VLAN de estudiantes en las Figuras 29 y 30 referente al resumen ejecutivo de Nexpose en VLAN Estudiante. Vulnerabilidades por categorías y más comunes respectivamente.

Audit Report

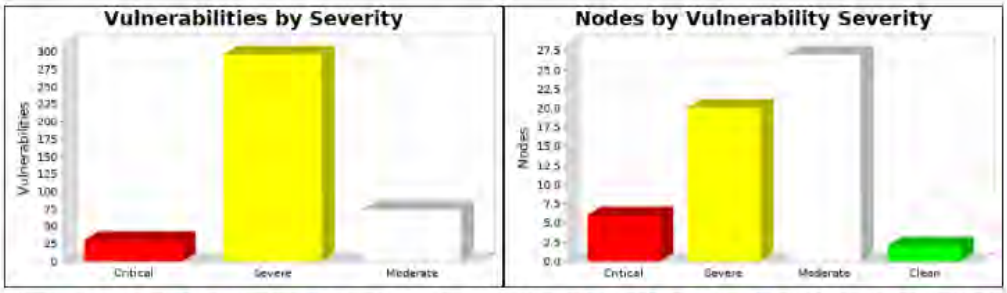
1. Executive Summary

This report represents a security audit performed by Nexpose from Rapid7 LLC. It contains confidential information about the state of your network. Access to this information by unauthorized personnel may allow them to compromise your network.

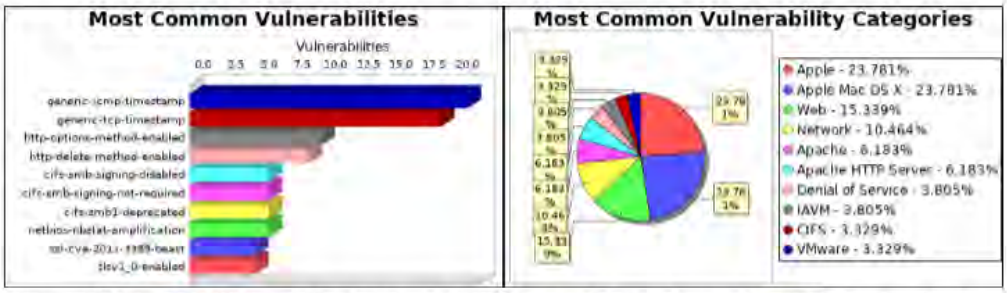
Site Name	Start Time	End Time	Total Time	Status
VLANESTUDIANTE/23	July 29, 2019 10:23, EDT	July 29, 2019 10:48, EDT	24 minutes	Success

There is not enough historical data to display overall asset trend.

The audit was performed on 29 systems, 29 of which were found to be active and were scanned.



There were 400 vulnerabilities found during this scan. Of these, 30 were critical vulnerabilities. Critical vulnerabilities require immediate attention. They are relatively easy for attackers to exploit and may provide them with full control of the affected systems. 296 vulnerabilities were severe. Severe vulnerabilities are often harder to exploit and may not provide the same access to affected systems. There were 74 moderate vulnerabilities discovered. These often provide information to attackers that may assist them in mounting subsequent attacks on your network. These should also be fixed in a timely manner, but are not as urgent as the other vulnerabilities. Critical vulnerabilities were found to exist on 6 of the systems, making them most susceptible to attack. 20 systems were found to have severe vulnerabilities. Moderate vulnerabilities were found on 27 systems. No vulnerabilities were found on the remaining 2 systems.



There were 21 occurrences of the generic-icmp-timestamp vulnerability, making it the most common vulnerability. There were 200 vulnerability instances in the Apple and Apple Mac OS X categories, making them the most common vulnerability categories.

Figura 29: Figura Resumen Ejecutivo de Nexpose en VLAN Estudiante. Vulnerabilidades por categorías.

Fuente. Elaboración a partir del Reporte Nexpose.

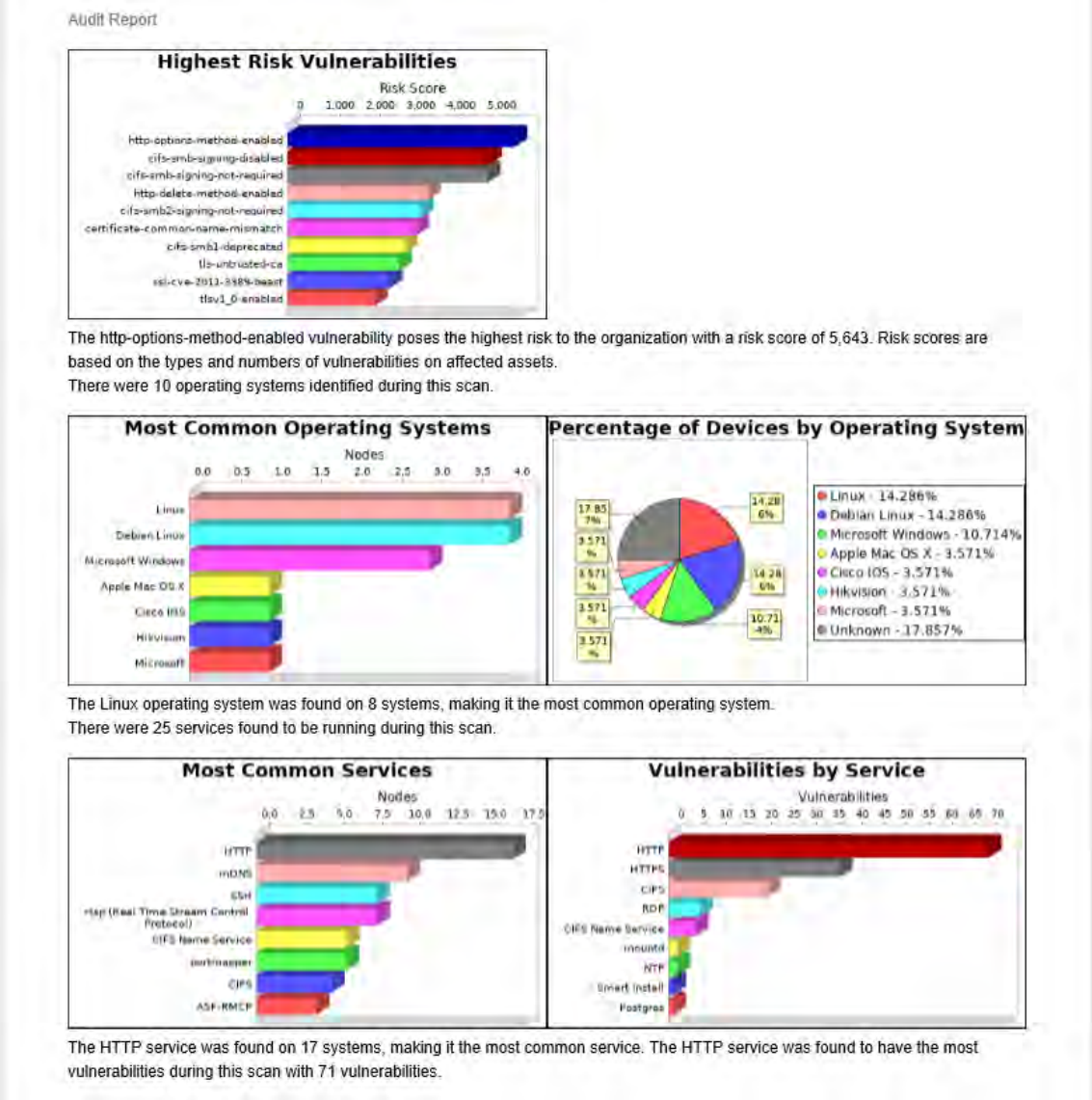


Figura 30: Figura Resumen Ejecutivo de Nexpose en VLAN Estudiante. Vulnerabilidades más comunes.

Fuente. Elaboración a partir del Reporte Nexpose.

Resultados del análisis con Nexpose en la VLAN Docentes.

El análisis realizado en la VLAN Docentes mediante la herramienta Nexpose detectó un total de 682 vulnerabilidades, clasificadas según su nivel de severidad. Se tiene 93 críticas, 555 graves y 34 moderadas. Se encontraron vulnerabilidades críticas en 4 sistemas, mientras que 7 sistemas presentaron vulnerabilidades graves, y 10 sistemas mostraron vulnerabilidades moderadas. Ninguno de los sistemas escaneados estuvo libre de riesgos.

Principales vulnerabilidades y categorías afectadas

- La vulnerabilidad más recurrente fue generic-tcp-timestamp (8 ocurrencias).
- Las categorías más afectadas corresponden a sistemas Apple y Apple Mac OS X, con 400 instancias debidas a versiones obsoletas.
- También se identificó la necesidad de actualizar sistemas operativos Windows 7, predominantes en esta VLAN.
- Varias vulnerabilidades graves, como cifs-smb-signing-disabled, están asociadas al protocolo SMB, con un puntaje de riesgo promedio de 3342. Este protocolo, esencial para la compartición de archivos, no cuenta con configuraciones de firma SMB, lo que facilita ataques de intermediarios.
- Los servicios más afectados en esta VLAN fueron CIFS Name Service, con 14 vulnerabilidades y HTTP, con 11 vulnerabilidades.

El informe destaca la urgencia de actualizar los sistemas operativos, especialmente Apple y Windows 7, para mitigar los riesgos críticos. Además, se recomienda configurar adecuadamente la firma SMB y fortalecer la seguridad en los servicios HTTP y CIFS Name Service. Este análisis subraya la importancia de un mantenimiento continuo y configuraciones robustas en los sistemas de la VLAN Docentes.

A continuación, se incluyen las páginas del informe en VLAN docentes en las Figuras 31 y 32 referente a Resumen Ejecutivo de Nexpose en VLAN Docente. Vulnerabilidades por categorías y más comunes respectivamente.

Audit Report

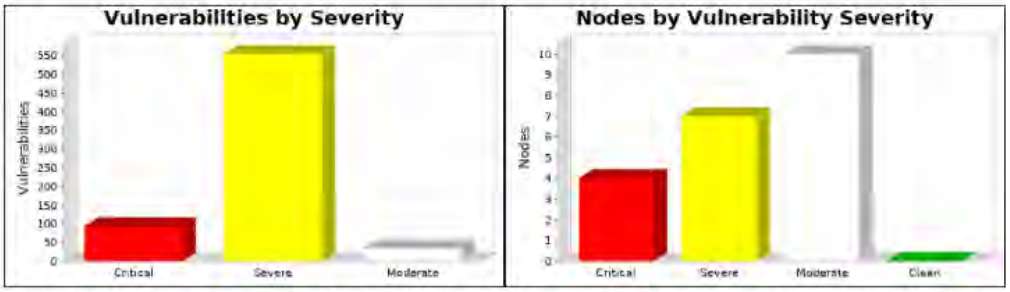
1. Executive Summary

This report represents a security audit performed by Nexpose from Rapid7 LLC. It contains confidential information about the state of your network. Access to this information by unauthorized personnel may allow them to compromise your network.

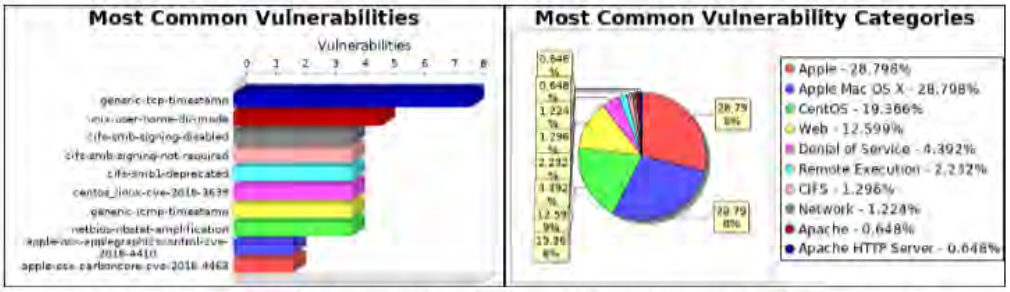
Site Name	Start Time	End Time	Total Time	Status
VlanEstudiante/23202	July 29, 2019 12:10, EDT	July 29, 2019 12:26, EDT	16 minutes	Success

There is not enough historical data to display overall asset trend.

The audit was performed on 10 systems, 10 of which were found to be active and were scanned.



There were 682 vulnerabilities found during this scan. Of these, 93 were critical vulnerabilities. Critical vulnerabilities require immediate attention. They are relatively easy for attackers to exploit and may provide them with full control of the affected systems. 555 vulnerabilities were severe. Severe vulnerabilities are often harder to exploit and may not provide the same access to affected systems. There were 34 moderate vulnerabilities discovered. These often provide information to attackers that may assist them in mounting subsequent attacks on your network. These should also be fixed in a timely manner, but are not as urgent as the other vulnerabilities. Critical vulnerabilities were found to exist on 4 of the systems, making them most susceptible to attack. 7 systems were found to have severe vulnerabilities. Moderate vulnerabilities were found on 10 systems. No systems were free of vulnerabilities.



There were 8 occurrences of the generic-tcp-timestamp vulnerability, making it the most common vulnerability. There were 400 vulnerability instances in the Apple and Apple Mac OS X categories, making them the most common vulnerability categories

Figura 31. Resumen Ejecutivo de Nexpose en VLAN Docente. Vulnerabilidades por categorías.

Fuente. Elaboración a partir del Reporte Nexpose.

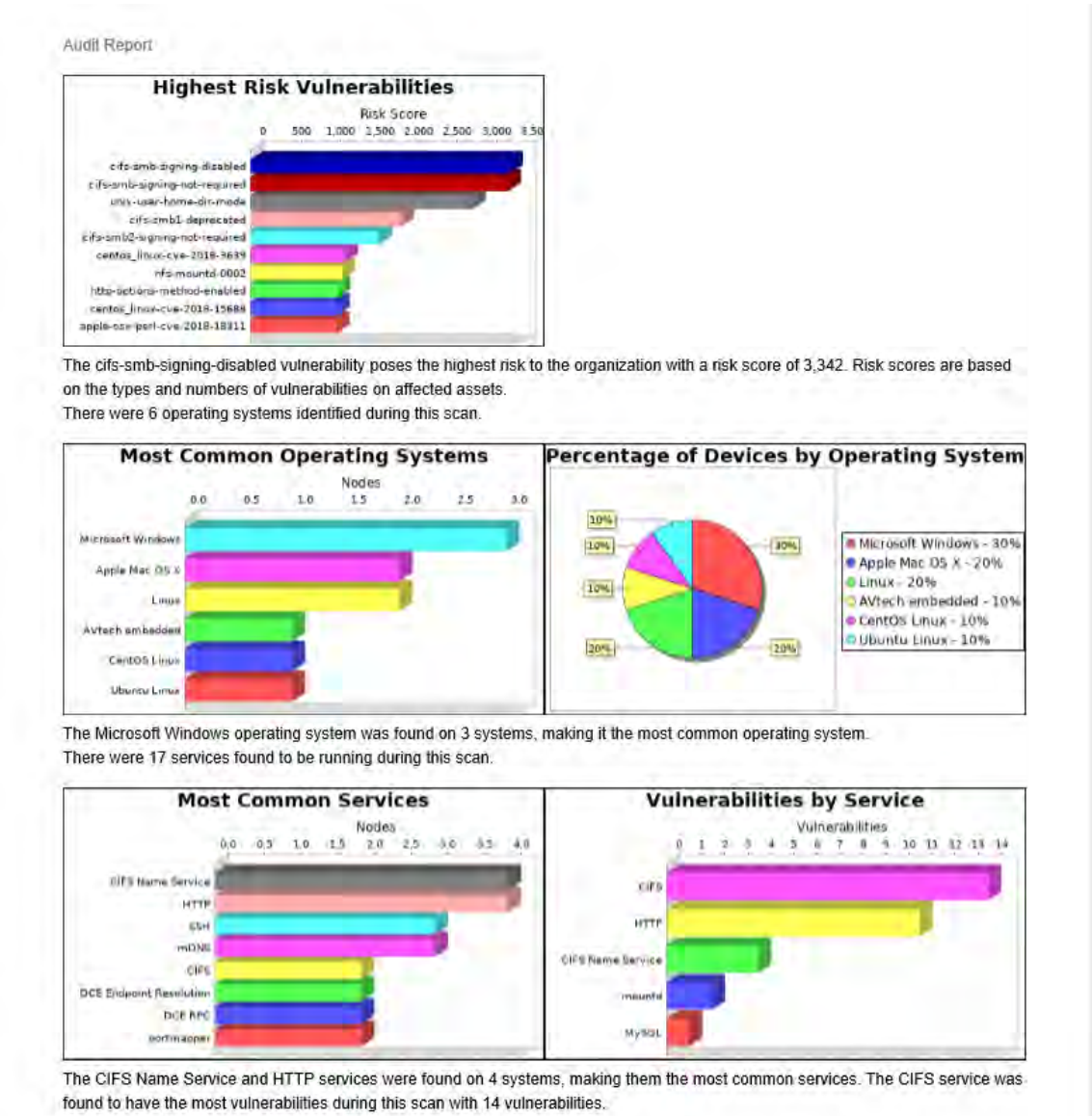


Figura 32. Figura Resumen Ejecutivo de Nexpose en VLAN Docente. Vulnerabilidades más comunes.

Fuente. Elaboración a partir del Reporte Nexpose.

ANEXO I. CONFIGURACIÓN PARA LAS PRUEBAS REALIZADAS EN EL ESCENARIO SDN.

EQUIPOS EMPLEADOS

Se incluye equipos SDN, puede ser un conmutador de 24 puertos

- Hardware, se sugiere el siguiente, pudiendo considerar equipos con características similares:
  - ✓ Un conmutador HP 3800 Series 24G-25FP + J9575, el equipo HP funciona con el protocolo OpenFlow, que permite probar redes SDN, así como también al ambiente tradicional. Tiene un procesador ASIC / ARM @ 350 MHz; Freescale P2020 @ 1200 MHz, 4 Gb de flash y 2 Gb SDRAM. Este dispositivo se observa en la figura 33 del anexo I.

Figura 33: Conmutador Hp 3800
Fuente. Elaboración propia.

  - ✓ 1 switch hp PRO CURVE 1810G-8, para la conexión de equipos servidores, como se muestra en la figura 31.

Figura 34: HP PRO CURVE 1810G-8

Fuente. Elaboración propia.

Para el escenario se implementa equipos físicos, incluye las 5 computadoras (cliente, servidor, controlador, SNORT, atacante (Kali-Linux)), que se tendrán en el escenario de pruebas.

Prueba 1. Análisis en el escenario SDN con ataque de DoS y sin control.

1.- Configuración de la topología:

En la realización de las pruebas como se muestra en la figura se visualiza la separación del plano de datos del plano de control. Donde el plano de control está compuesto por:

- El controlador (FloodLigth) con la dirección ip 192.168.0.19/24 y
- El switch SDN HP E3800 con el direccionamiento de 192.168.1.150/24,
- Y el servidor SNORT con la dirección 192.168.1.132/24.

El plano de datos está conformado por los equipos:

- Host A (servidor web) con dirección IP 192.168.0.20/24 y
- Host B (cliente) con la dirección 192.168.0.15/24, respectivamente.
- Se incluye el equipo atacante implementado en Kali Linux con la dirección 192.168.0.41/24, que simula el ataque DoS.

Se debe enfatizar que los planos de datos y de control están totalmente separados de una manera lógica.

2.-Pruebas estándar:

Una vez que la topología respectiva está instalada es posible realizar pruebas estándar como: ping entre los equipos de pruebas (cliente, servidor).

3.- Configuración del entorno:

Se levanta el controlador Floodlight, que permite la comunicación en el escenario de pruebas. La Figura 35 muestra los flujos generados por Floodlight.

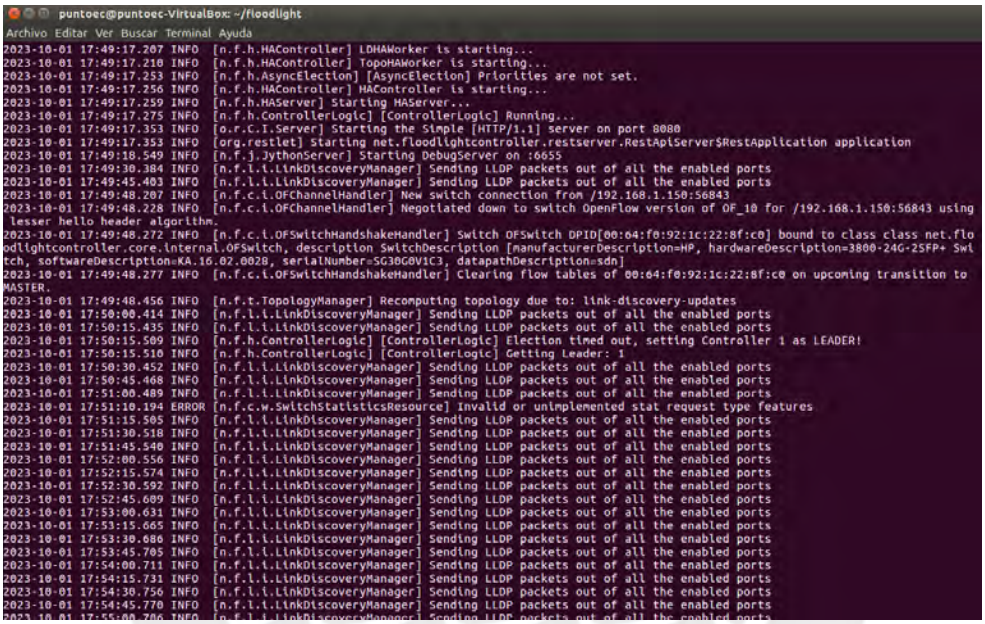


Figura 35: Flujos generados por Floodlight.
Fuente. Reporte Floodlight.

Adicionalmente se observa la topología que genera el controlador FloodLigth, desde la interfaz web del controlador en la Figura 36.

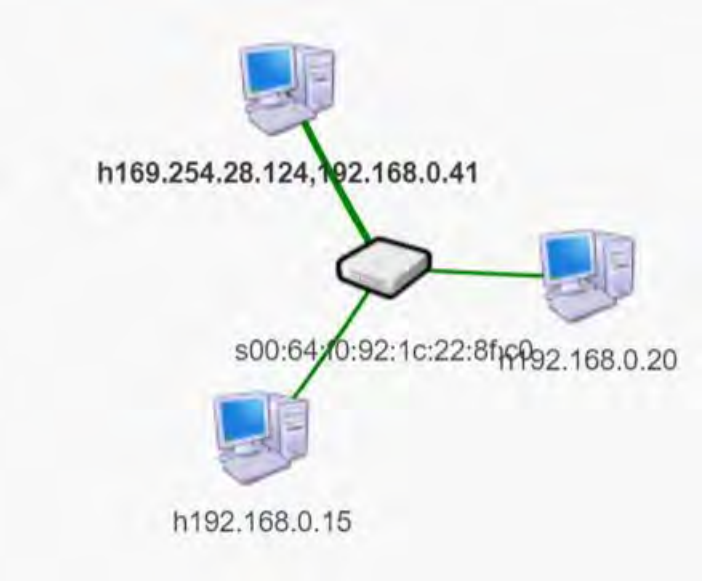


Figura 36: Escenario SDN generado por Floodlight
Fuente. Reporte Floodlight.

4.- Activación de SNORT:

Se activa SNORT que detecta anomalías en la red con la dirección IP 192.168.1.132/24 en el plano de control y 192.168.0.30/24 en el plano de datos a través de un puerto mirror del switch SDN para analizar el tráfico de la intranet y detectar en base a la configuración de reglas de la comunidad y propias las amenazas de la intranet.

Se incluyen las imágenes de la Figura 37, captura de SNORT ejecutándose y Figura 38, socket del SNORT activado.

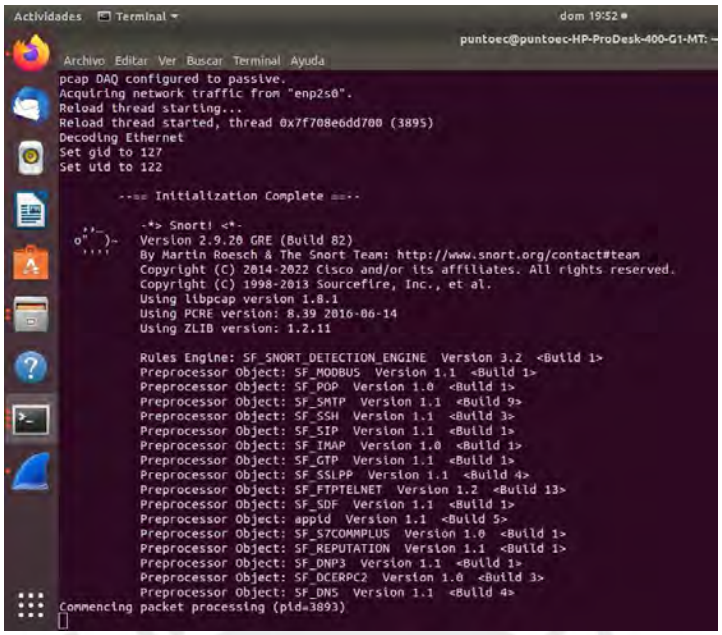


Figura 37: Captura de SNORT ejecutándose.
Fuente. Reporte SNORT

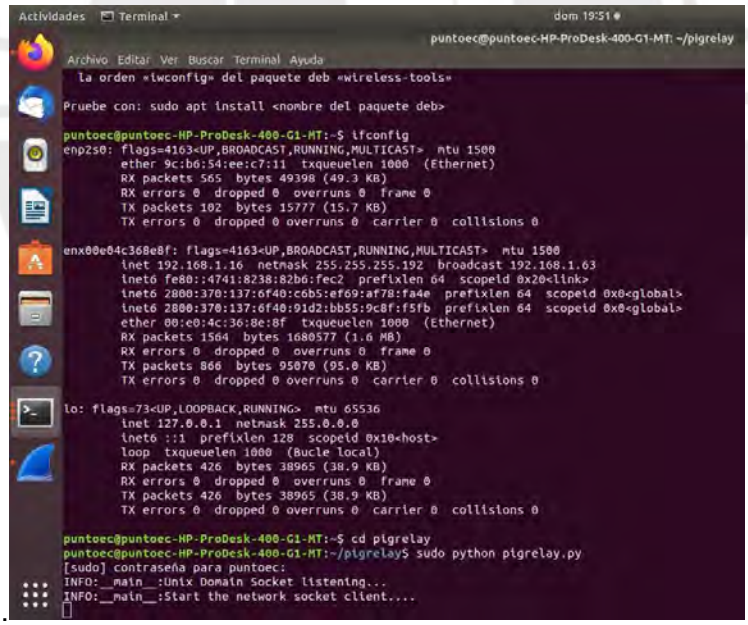
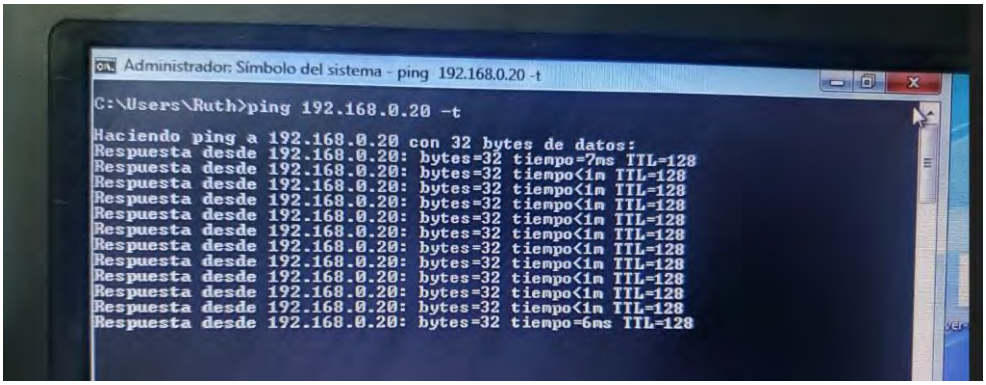


Figura 38: Socket del SNORT activado.
Fuente. Reporte SNORT

5.- Verificación de conexiones:

Se verifica las conexiones, entre los equipos HOST A (servidor web) y HOST B (cliente), las Figuras 39 y 40, señalan comunicación exitosa.

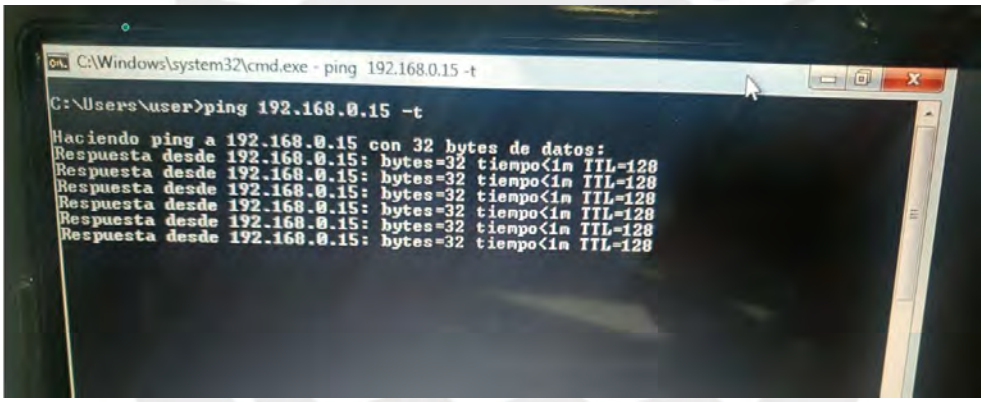


```
C:\Users\Ruth>ping 192.168.0.20 -t

Haciendo ping a 192.168.0.20 con 32 bytes de datos:
Respuesta desde 192.168.0.20: bytes=32 tiempo=7ms TTL=128
Respuesta desde 192.168.0.20: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.20: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.20: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.20: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.20: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.20: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.20: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.20: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.20: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.20: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.20: bytes=32 tiempo=6ms TTL=128
```

Figura 39: Verificación de ping HOST A (servidor web) y HOST B (cliente).

Fuente. Reporte



```
C:\Users\user>ping 192.168.0.15 -t

Haciendo ping a 192.168.0.15 con 32 bytes de datos:
Respuesta desde 192.168.0.15: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.15: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.15: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.15: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.15: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.15: bytes=32 tiempo<1m TTL=128
```

Figura 40: Verificación de ping HOST B (cliente) a HOST A(servidor web).

Fuente. Reporte

6.- Simulación de ataque DoS:

Se levanta Slowloris para la emisión del ataque, en Kali Linux, una vez configurado, se procede a simular el ataque DoS apuntando directamente a la IP del HOST A (Servidor). En la imagen se muestra la línea de comando ejecutada desde el Slowloris, según se observa en la Figura 41.

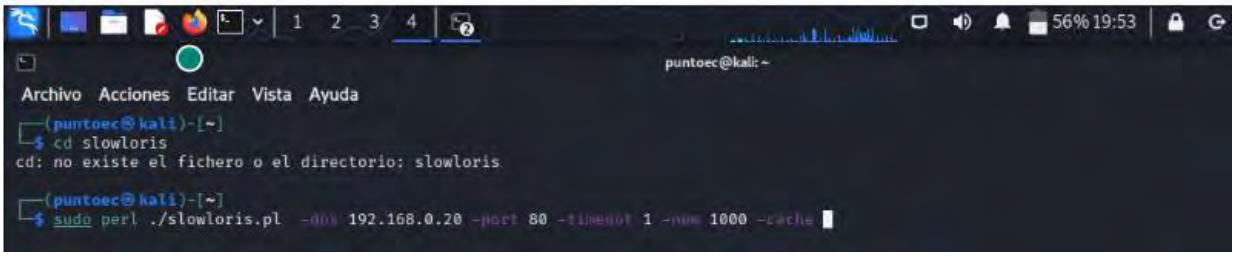


Figura 41: Línea de comando ejecutada desde el Slowloris.

Fuente. Ejecución Slowloris

Ejecución del comando para el ataque Slowloris, Figura 42.

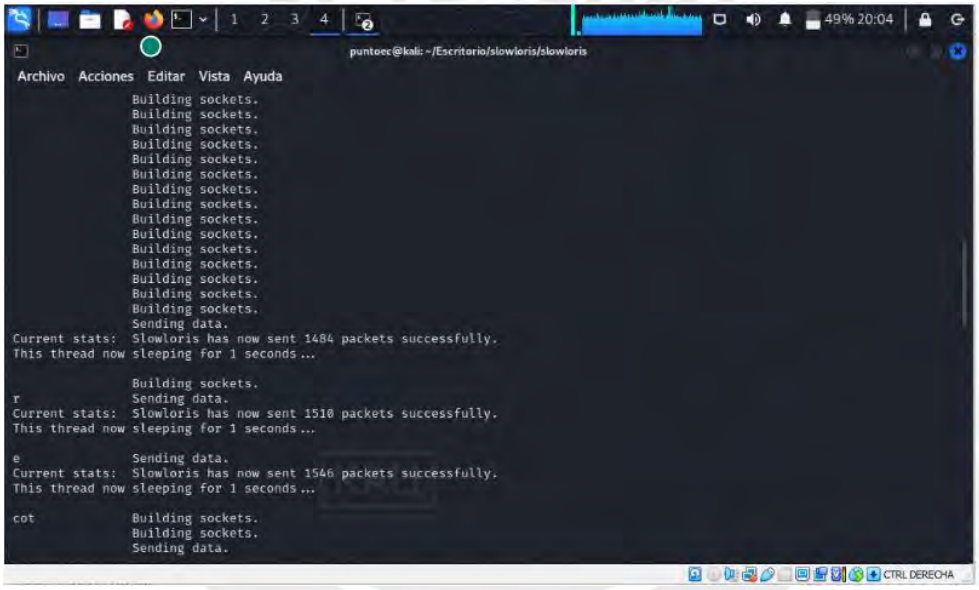


Figura 42: Ejecución del comando para el ataque Slowloris.

Fuente. Ejecución Slowloris

7.- **Inyección de tráfico con D-ITG:**

Se procede con la inyección de tráfico TCP/UDP mediante D-ITG, la misma que se ejecuta en el servidor según las cargas necesarias, distribuyendo por intervalos (60 pruebas) hasta la capacidad del canal 100 Mbps.

En el lado del servidor se crean los flujos y se inyectan, ingresando la dirección ip del cliente, finamente ejecutando los comandos logger y sender como se lo puede visualizar en la Figura 43.

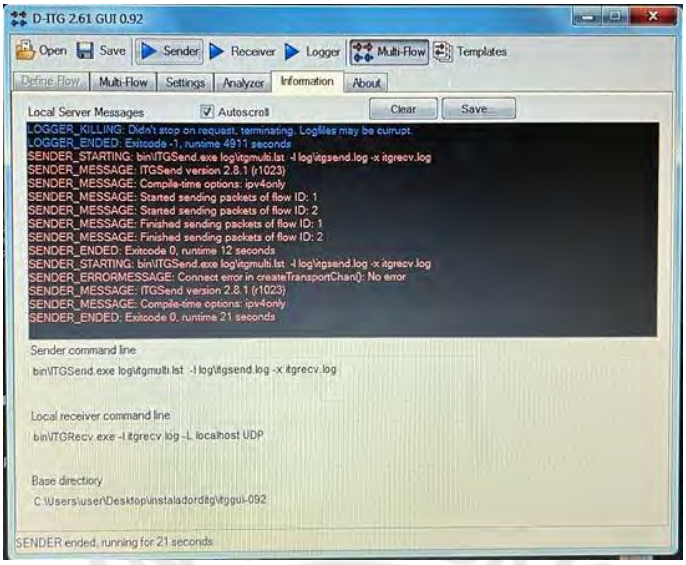


Figura 43: Inyección de tráfico desde el servidor SDN.

Fuente. Ejecución D-ITG

Mientras que en el cliente se activa Receiver y Logger para recibir la transmisión emitida por el servidor, como se observa en la Figura 44.

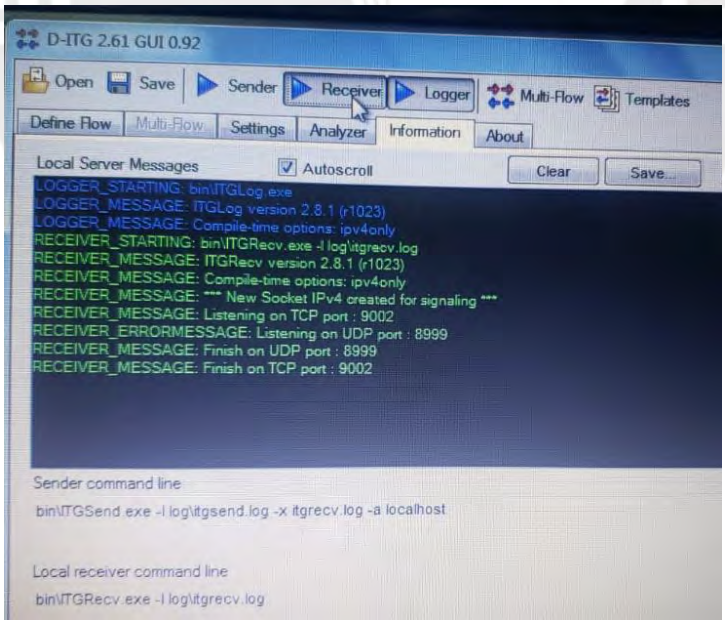


Figura 44: Inyección de tráfico desde el cliente SDN.

Fuente. Ejecución D-ITG

Generación de reportes:

Se muestra el reporte generado en cada una de las pruebas para su análisis, según la Figura 45.

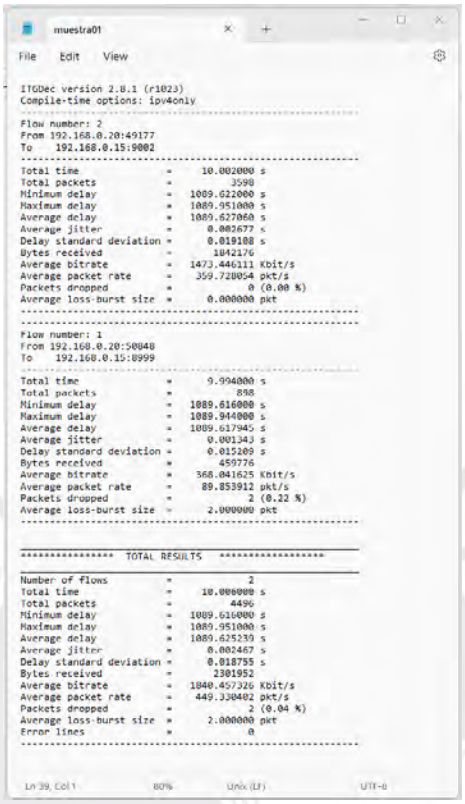


Figura 45: Captura datos con D-ITG SDN desde el cliente.

Fuente. Ejecución D-ITG

Se puede observar los parámetros de rendimiento en la comunicación, evaluándose ancho de banda, jitter, delay y pérdida de paquetes, que se han documentado para el análisis estadístico.

Prueba 2. Análisis en el escenario SDN con ataque de DoS y con la política de control.

1.- Configuración de la topología:

En la realización de la prueba 2, como se muestra en la Figura 46, se visualiza un escenario similar al de la primera prueba, en donde se encuentra la separación del plano de datos del plano de control.

En este segundo escenario el plano de control está compuesto por:

- El controlador (FloodLigth) con la dirección IP 192.168.1.19/24.
- El switch SDN HP E3800 con el direccionamiento de 192.168.1.150/24 y
- Un equipo Ubuntu que incluye la configuración SNORT con direccionamiento 192.168.1.132/24 en el plano de control y con puerto mirror y con enlace al switch HP E3800 en el plano de datos con la dirección 192.168.0.30/24.

Además, en el plano de datos:

Están los equipos HOST A (servidor) con IP 192.168.0.20/24, un equipo HOST B (cliente) con direccionamiento 192.168.0.15/24 y un equipo atacante implementado en Kali Linux a través de Slowloris para la amenaza DoS con IP 192.168.0.41/24.

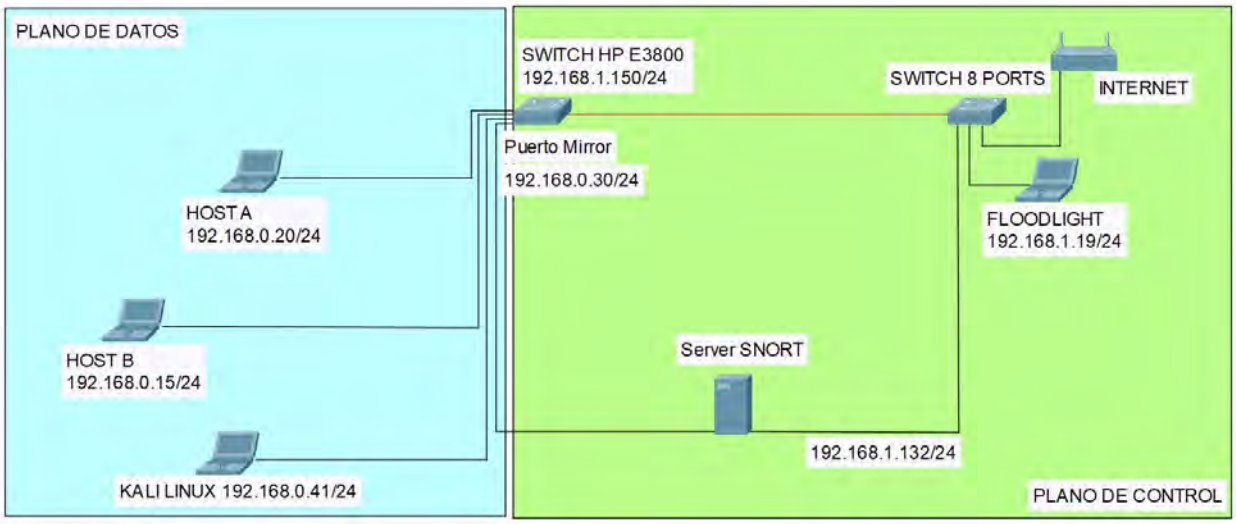


Figura 46: Escenario de pruebas SDN con Ataque DoS y con la política de control.

Fuente. Elaboración propia.

2.- Acceso al controlador Floodlight:

Al acceder vía web al controlador Floodlight, se puede observar el switch HP E3800, y sus características como se observa en la Figura 47.

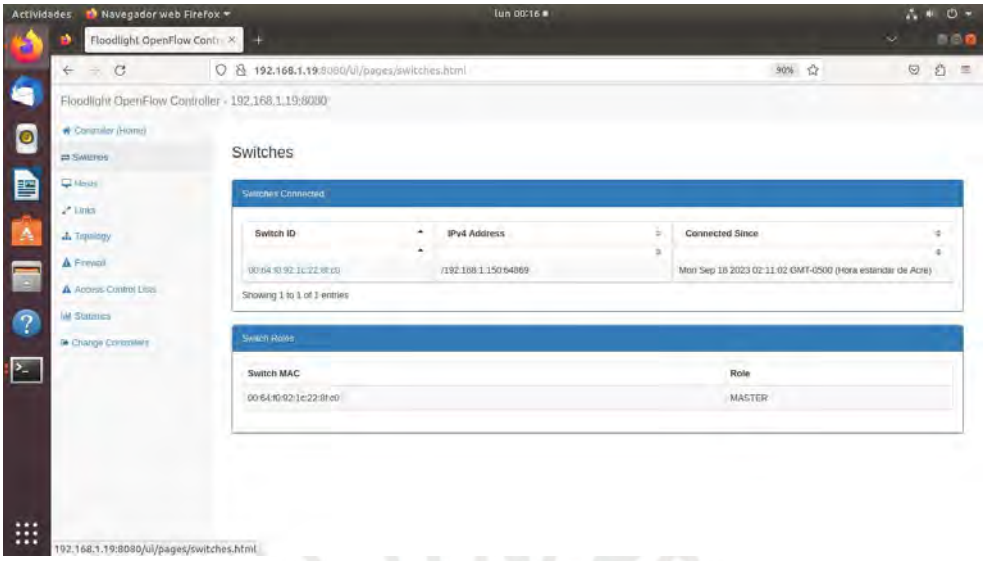


Figura 47: Switch HP E3800, y sus características desde la interfaz web Floodlight.
Fuente. Ejecución interfaz web Floodlight

Así como los hosts que forman parte del escenario SDN y se visualizan en la Figura 48.

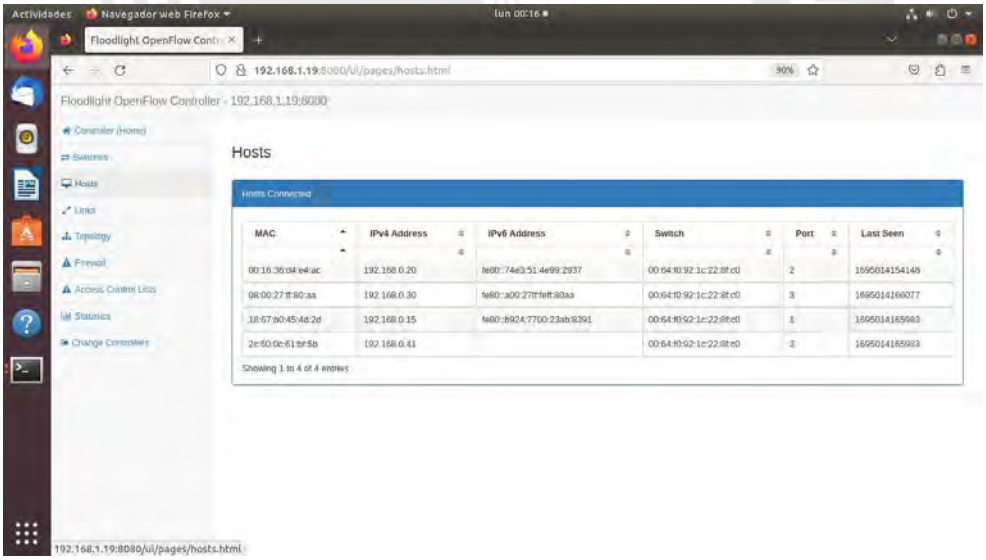


Figura 48: Hosts y sus características desde la interfaz web Floodligth.

Fuente. Ejecución interfaz web Floodlight

3.- Visualización de la topología:

A continuación, se observa la topología que genera el controlador Floodligth, desde la interfaz web del controlador del plano de datos del escenario de pruebas. Observe la Figura 49.

Figura 49: Escenario de pruebas SDN generado por Floodlight con el ataque.
Fuente. Ejecución interfaz web Floodlight

4.- Flujos generados por Floodlight:

Se observan los flujos del controlador Floodlight, en la Figura 50, que habilita la comunicación entre las pcs del escenario de pruebas.

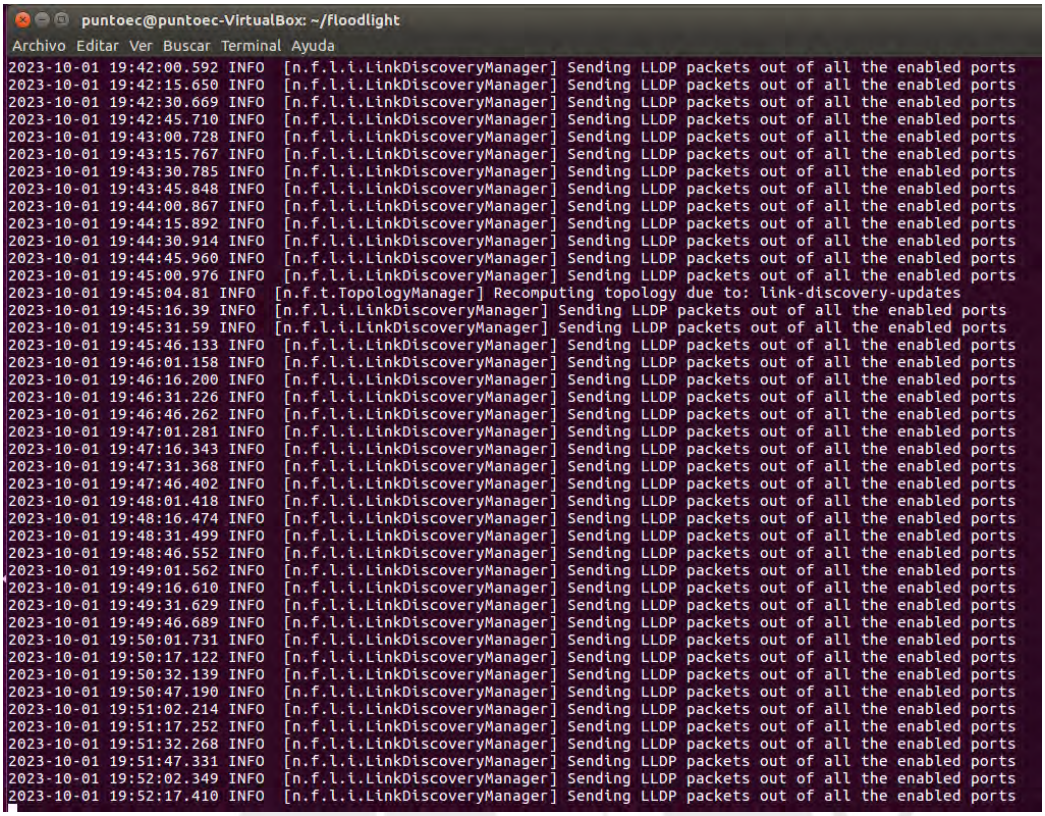


Figura 50: Flujos generados por Floodlight.

Fuente. Ejecución Floodlight

5.- Verificación de conexiones:

Y la verificación de la comunicación entre las computadoras de los equipos HOST A (servidor web) y Kali – Linux (atacante) según figura 51 y viceversa en la Figura 52.

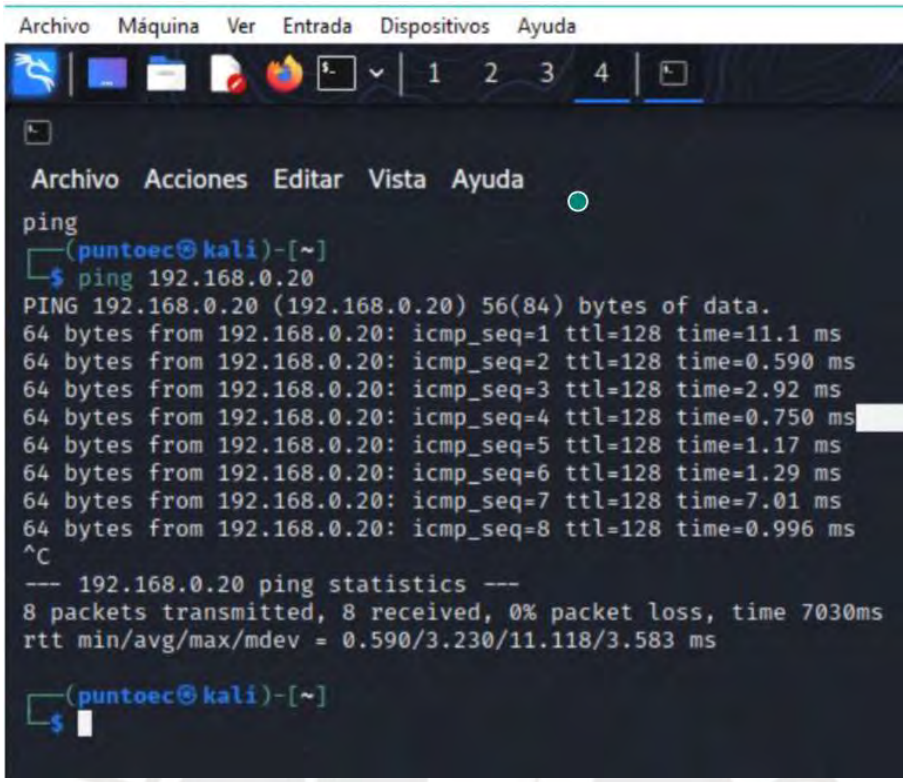


Figura 51: Verificado la conexión exitosa entre los equipos HOST A (servidor web) y Kali – Linux (atacante).

Fuente. Fuente. Ejecución Kali-Linux

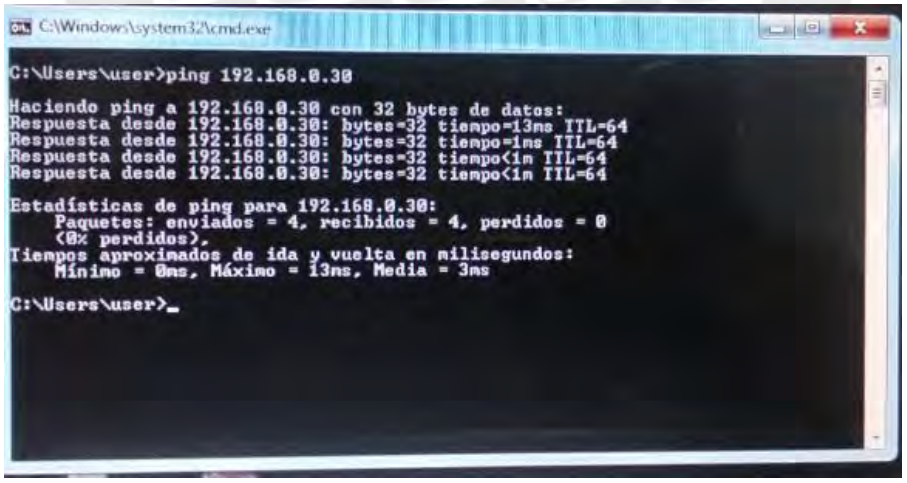


Figura 52: Verificado la conexión exitosa entre los equipos y Kali – Linux (atacante) y HOST A (servidor web).

Fuente. Ejecución Prueba Host A

6.- Simulación de ataque DoS:

Para este escenario de prueba mediante la aplicación Slowloris se procede a simular el ataque DoS apuntando directamente a la ip del HOST A (Servidor), en la imagen se muestra la línea de comando ejecutada desde el Slowloris, según se observa en la Figura 53.

Figura 53: Línea de comando ejecutada desde el Slowloris.
Fuente. Ejecución Slowloris

La ejecución del comando para el ataque Slowloris, se muestra en la Figura 54.

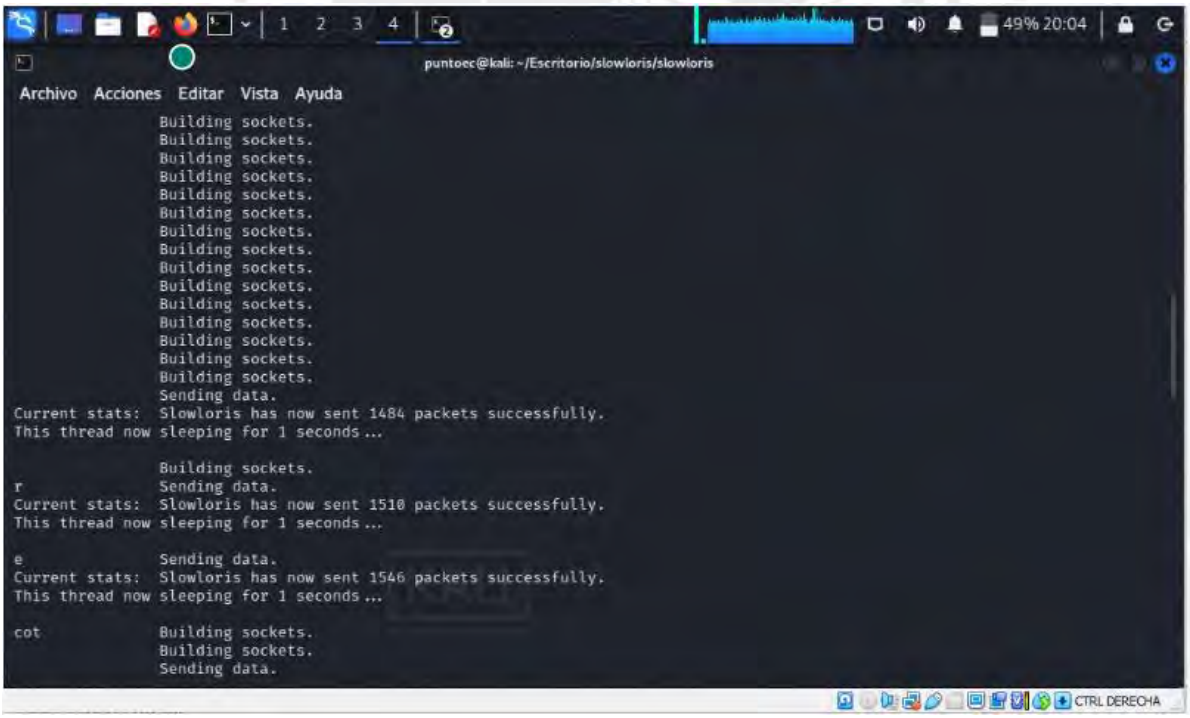


Figura 54: Ejecución del comando para el ataque Slowloris.
Fuente. Ejecución Slowloris

7.- Implementación de SNORT:

Para detectar el ataque, SNORT se implementa en un equipo bajo Ubuntu. Para ello se configura el archivo *rules* como se presenta en la pantalla, incluyendo una regla de detección del ataque DoS observe la Figura 55.

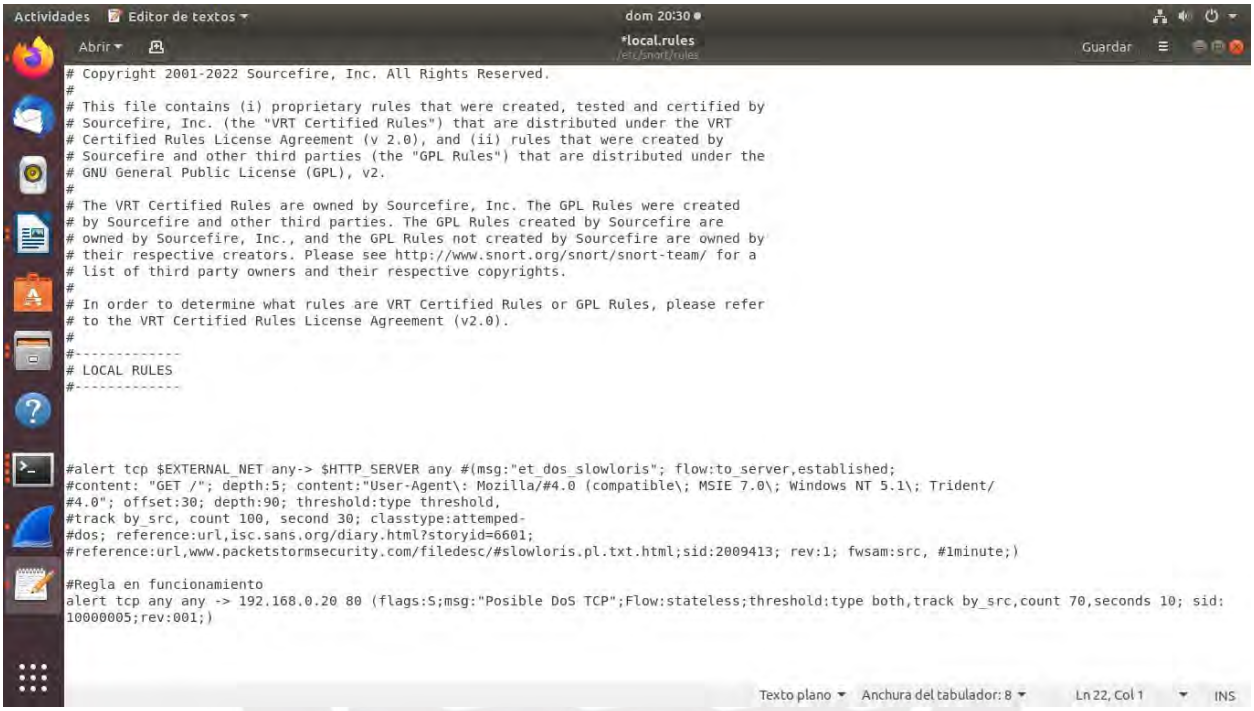


Figura 55: Regla detección de ataque DoS en SNORT.
Fuente. Ejecución SNORT

En la siguiente imagen se ejecuta SNORT, Figura 56.

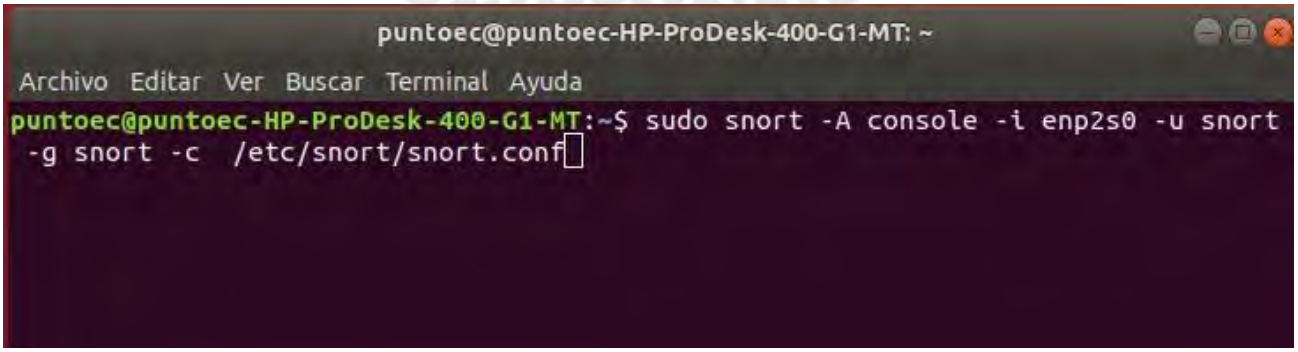


Figura 56: Regla detección de ataque DoS en SNORT.
Fuente. Ejecución SNORT

Y muestra el ataque detectado como se visualiza en la Figura 57, detección de ataque DoS en SNORT.

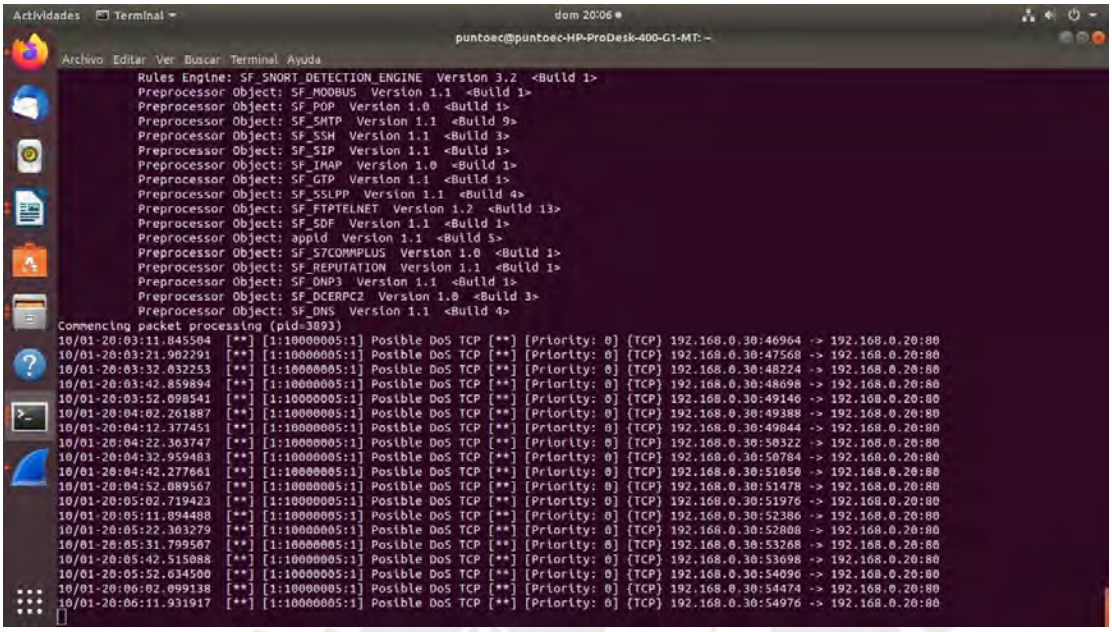


Figura 57: Detección de ataque DoS en SNORT.
Fuente. Ejecución SNORT

8.- Bloqueo del ataque:

Se implementan las reglas para el bloqueo del ataque mediante comandos CURL como se observa en la Figura 58. Con esta regla la comunicación se mantiene con regularidad.

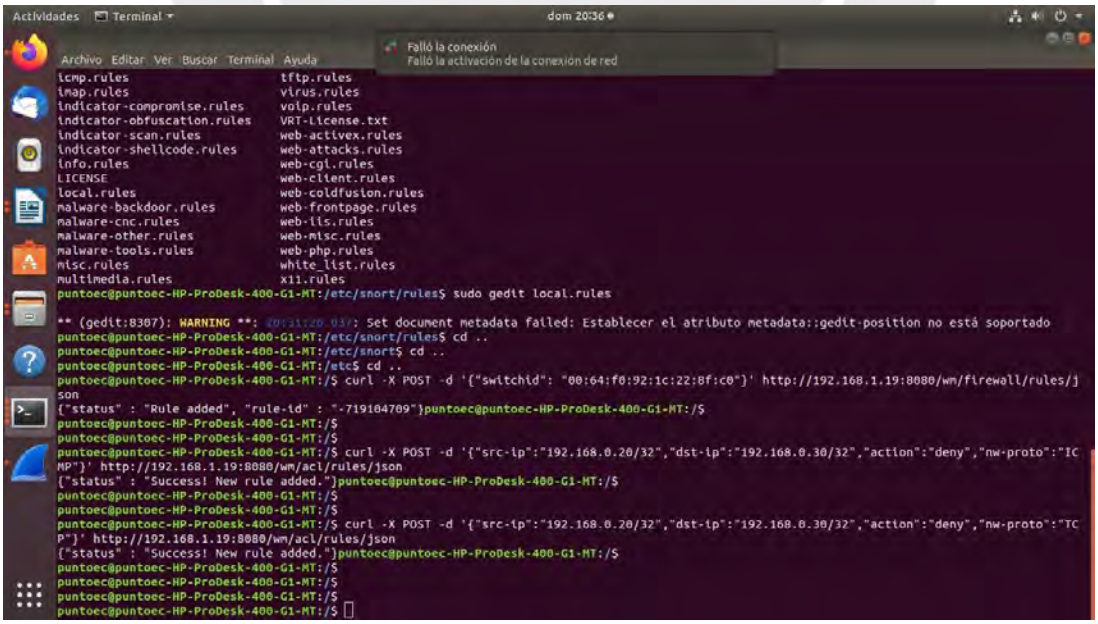


Figura 58: Reglas para el bloqueo del ataque mediante comandos CURL.
Fuente. Ejecución Floodlight

Vía web desde el controlador Floodlight se muestran las reglas añadidas, como se observa en la Figura 59 y 60.

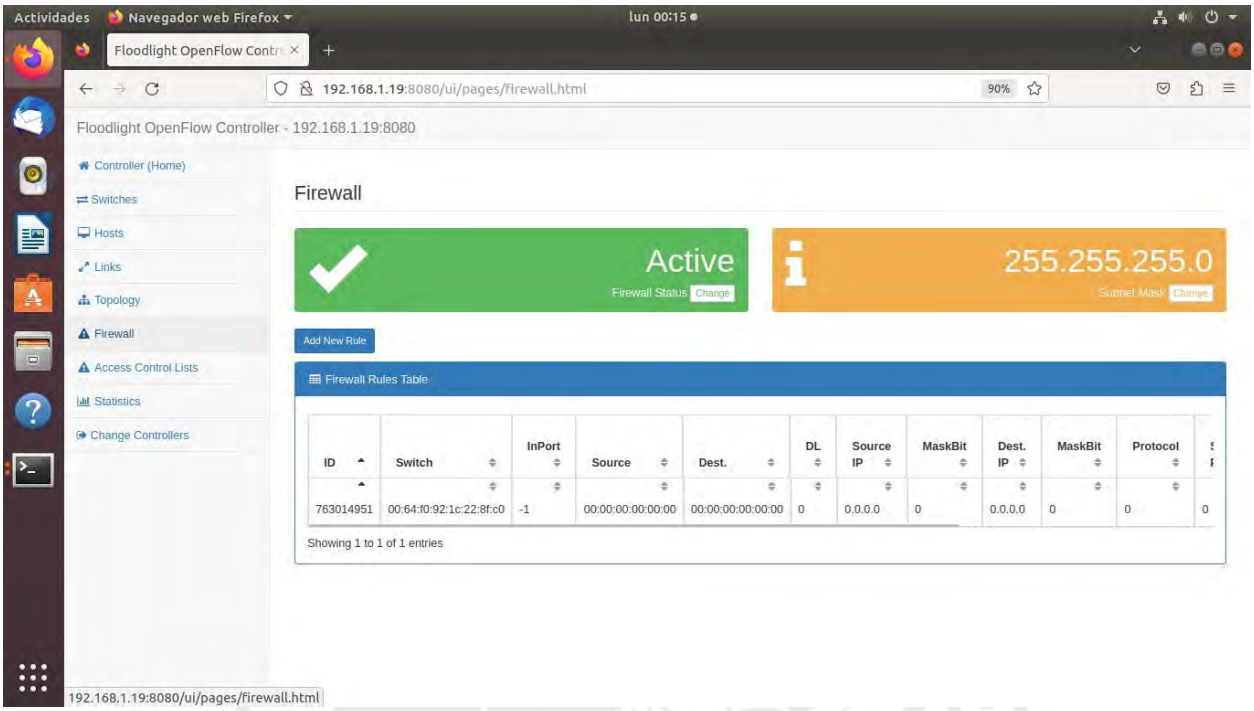


Figura 59: Reglas para el bloqueo del ataque mediante comandos CURL.
Fuente. Ejecución Interfaz Web Floodlight

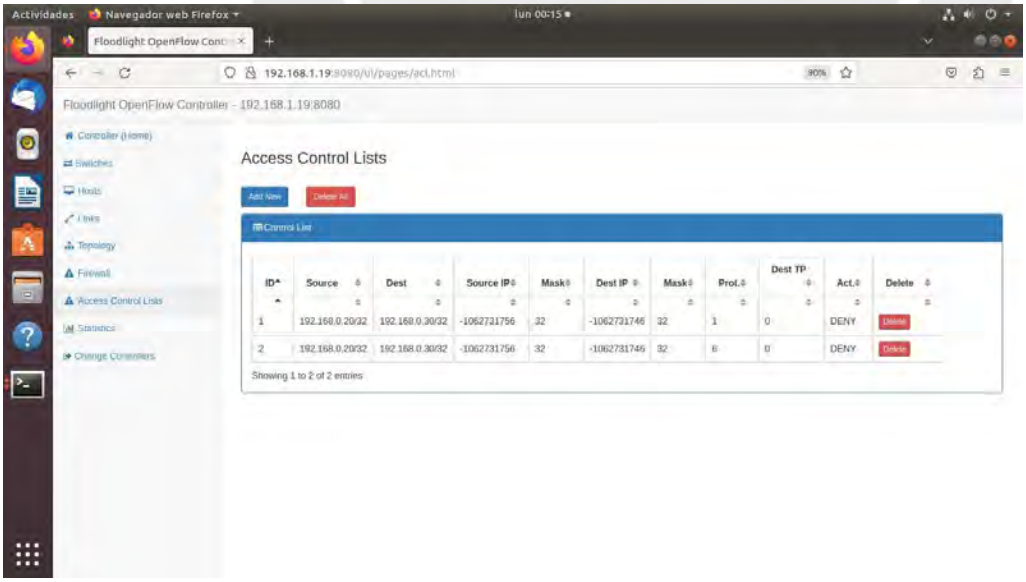


Figura 60: Reglas para el bloqueo del ataque mediante comandos CURL.

Fuente. Ejecución Interfaz Web Floodlight

9.- **Inyección de tráfico con D-ITG:**

Posteriormente con ayuda del generador de tráfico D-ITG, inyectamos tráfico, como dato de prueba se ingresan valores: en TCP y en UDP, teniendo un total de 60 muestras.

En la Figura 61 se muestra en el lado del servidor ejecutando los comandos Logger y Sender se inicia la generación de tráfico.

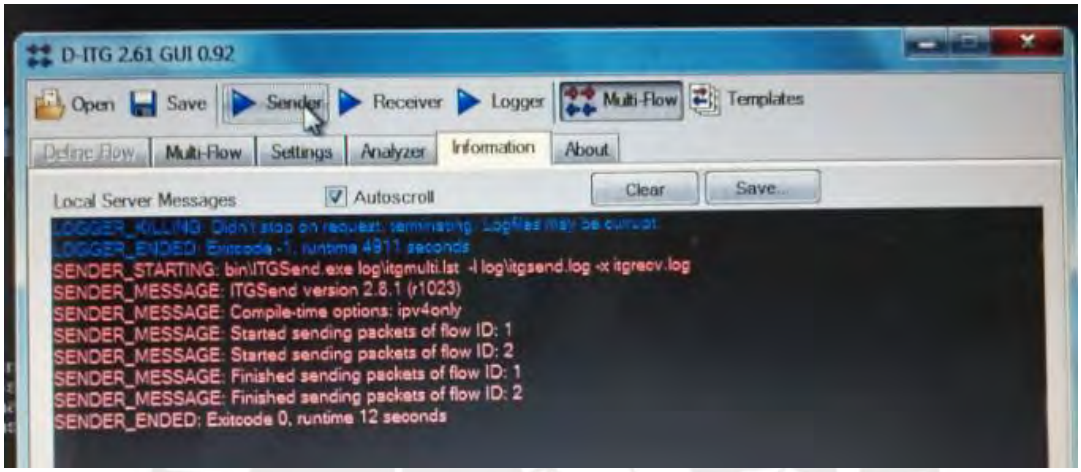


Figura 61: Lado del servidor, ejecutando los comandos Logger y Sender se inicia la generación de tráfico.
Fuente. Ejecución Host Servidor.

Y se procede en el cliente a receptar el tráfico generado ejecutando los comandos Logger y Receiver, como se observa en las Figuras 62 y 63.

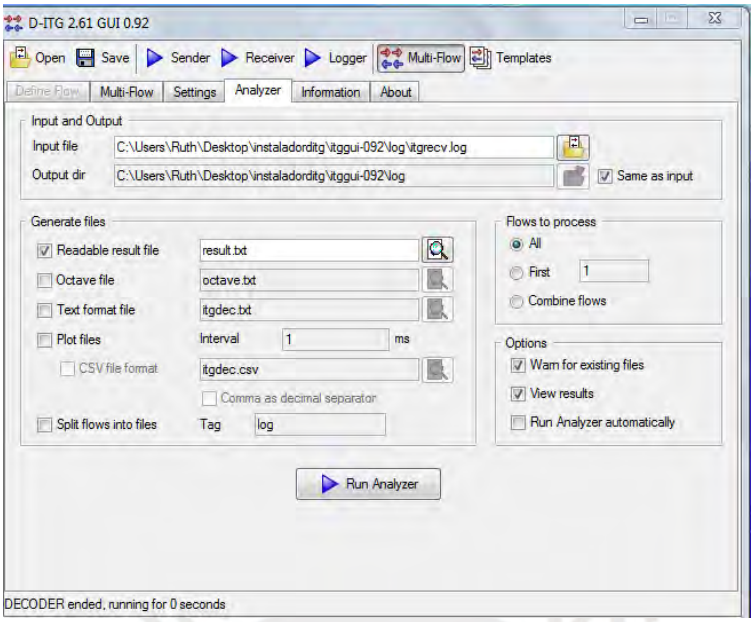


Figura 62: Interfaz D-ITG en el cliente.

Fuente. Ejecución D-ITG en el cliente

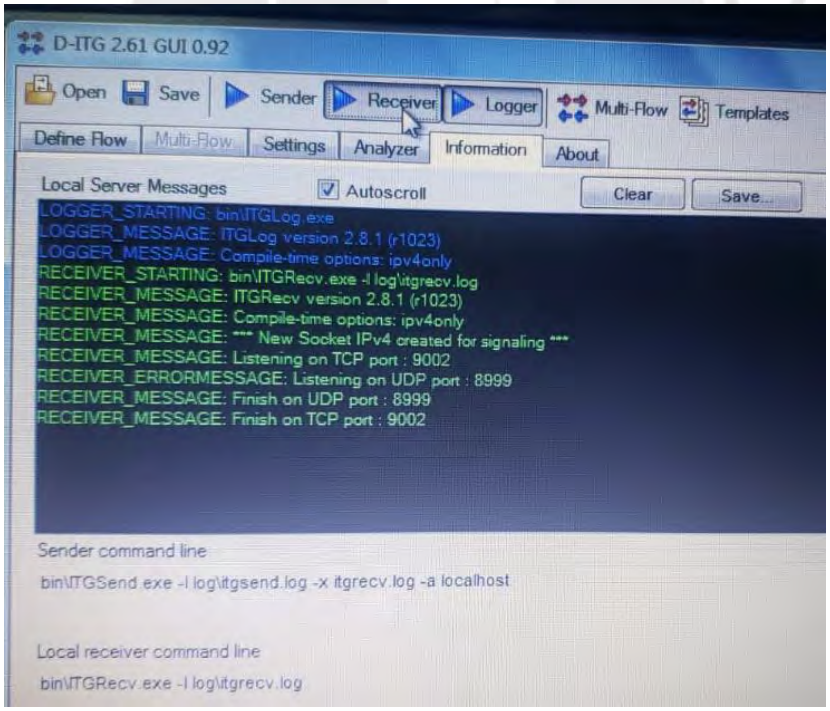


Figura 63: Cliente recepta el tráfico generado ejecutando los comandos Logger y Receiver.
Fuente. Ejecución D-ITG en el cliente

10. Análisis de datos generados:

Finalmente se procede a realizar el análisis de los datos generados como se puede visualizar en la figura 64. Reporte de la transmisión con parámetros de rendimiento, jitter, ancho de banda, delay, pérdida de paquetes.

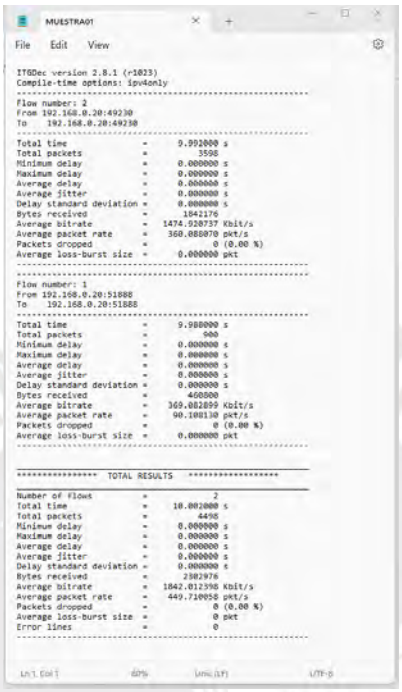


Figura 64: Reporte de la transmisión con parámetros de rendimiento, Jitter, ancho de banda, delay, pérdida de paquetes

Fuente. Ejecución D-ITG en el cliente

ANEXO J. AUTORIZACIÓN INSTITUCIONAL Y RESGUARDO ÉTICO EN EL ANÁLISIS DE LA INTRANET ACADÉMICA

En cumplimiento de los principios éticos y metodológicos que orientan esta investigación doctoral, a continuación, se detalla el procedimiento adoptado para garantizar el manejo adecuado de los datos durante el análisis del tráfico interno de la intranet académica, así como el respaldo institucional que avaló esta fase del estudio.

1. Validación institucional y acompañamiento técnico

El análisis se realizó entre los meses de abril y agosto de 2019, en las instalaciones de la Facultad de Informática y Electrónica de la Escuela Superior Politécnica de Chimborazo (ESPOCH). Es importante señalar que, durante ese periodo, la institución aún no contaba con lineamientos formalmente establecidos en materia de seguridad de la información ni con un comité de ética específico para proyectos tecnológicos.

No obstante, el procedimiento fue autorizado institucionalmente y acompañado técnicamente por el Departamento de Tecnologías de la Información y Comunicación (DTIC). Se contó con la participación directa del Ing. Roberto Morales, en su calidad de Administrador de Red y Coordinador del Área de Redes, y del técnico Miguel Ordóñez, quienes brindaron soporte durante la configuración de la infraestructura tecnológica —en particular del servidor HP Generación 9—, así como durante el desarrollo, validación y seguimiento del análisis ejecutado.

Como respaldo documental de esta gestión, se elaboró un oficio de solicitud formal fechado el 7 de marzo de 2019, en el que se establece el alcance del procedimiento y la necesidad de contar con apoyo institucional para su implementación en el nodo ubicado en el edificio de la Facultad de Informática y Electrónica. Dicho oficio fue archivado y se adjunta en la figura 65 como evidencia de validación institucional.

Recibido:
7 marzo de 2019

Autorizo actividad.

Riobamba, 07 de marzo de 2019

Ingeniero
Roberto Morales
Administrador de Redes - DTIC
Escuela Superior Politécnica de Chimborazo (ESPOCH)

Asunto: Solicitud de respaldo técnico para análisis de intranet académica en el marco de tesis doctoral

De mi consideración:

En el marco del desarrollo de mi tesis doctoral titulada "Políticas de calidad de servicio en Software Defined Network para facilitar el control de amenazas internas mejorando el rendimiento en campus académicos", se ha planificado la ejecución de una fase de análisis técnico del tráfico interno de la intranet académica, con el propósito de identificar posibles amenazas internas y evaluar el nivel actual de seguridad de la red.

El análisis se llevará a cabo en el nodo ubicado en el edificio de la Facultad de Informática y Electrónica de la ESPOCH, por considerarse un entorno representativo para el objeto de estudio. Dicho procedimiento se desarrollará conforme a la metodología OSSTMM V3.02, adaptada al contexto académico. Está previsto que la actividad incluya entrevistas técnicas al personal del área de redes, así como la recopilación de información bajo estrictos criterios de confidencialidad, en el marco de una auditoría de tipo caja gris. En todo momento se garantizará la protección de la identidad de los participantes y la no divulgación de datos sensibles.

En este contexto, solicito muy comedidamente su colaboración y respaldo técnico en la configuración y supervisión de los equipos involucrados, así como su participación como responsable institucional del área de redes, a fin de que este estudio se lleve a cabo con apego a los principios éticos y metodológicos que rigen la investigación científica.

Agradezco de antemano su apoyo y quedo atenta a su confirmación para proceder con las actividades programadas.

Atentamente,

Ing. Ruth Barba Vera

Ing. Ruth Genoveva Barba Vera
Doctoranda Pontificia Universidad Católica del Perú (PUCP)
Técnico Docente – ESPOCH
C.I. 0603611328

Figura 65: Oficio de solicitud y autorización del análisis de la intranet ESPOCH

Fuente. Autor.

2. Enfoque metodológico y criterios de confidencialidad

Para la evaluación de riesgos en el canal humano, se aplicó la metodología OSSTMM V3.02, adaptada al entorno universitario. Esta fue implementada mediante una auditoría de tipo caja gris, en la que el personal participante fue previamente informado y contextualizado sobre los objetivos, alcances y límites del proceso. El procedimiento fue informado de manera explícita, asegurando un consentimiento informado verbal por parte de los involucrados, en conformidad con los principios éticos aplicables.

La recolección de información se llevó a cabo a través de entrevistas estructuradas al personal técnico, particularmente a miembros del DTIC. En resguardo de la confidencialidad institucional y de la privacidad de los participantes, se resolvió no incluir en la tesis el contenido específico de las preguntas ni las respuestas obtenidas, en consideración a la sensibilidad técnica de los datos recopilados.

3. Resultados generales y resguardo de información sensible

El análisis permitió determinar un índice de riesgo (RAV) de 85.77, lo cual indica un nivel de seguridad moderado en la red académica evaluada. Este resultado respalda la pertinencia y necesidad de la propuesta metodológica desarrollada en el presente trabajo.

Para garantizar la seguridad institucional, se ha decidido omitir en el documento los detalles técnicos operativos derivados del análisis, evitando así la exposición de configuraciones sensibles o posibles vectores de vulnerabilidad.

4. Justificación del análisis preliminar

La fase preliminar de análisis del tráfico real de la red fue esencial para identificar vulnerabilidades internas existentes, seleccionar el tipo de amenaza a modelar —en este caso, un ataque de denegación de servicio (DoS)—, y diseñar un escenario de simulación SDN con condiciones técnicas realistas. Para ello, se utilizó equipamiento de red configurado específicamente para esta finalidad.

Cabe destacar que este procedimiento fue ejecutado sin intervención directa en la red operativa de la institución, lo cual garantizó la integridad funcional del entorno académico y la no afectación de los servicios institucionales.

Consideraciones finales

La ejecución de esta fase de la investigación se llevó a cabo con el respaldo expreso del Departamento de Tecnologías de la Información y Comunicación (DTIC), bajo el acompañamiento técnico del Ing. Roberto Morales y del técnico Miguel Ordóñez, y con la aplicación de medidas orientadas a preservar la confidencialidad, proteger la información crítica y asegurar la transparencia metodológica.

En consecuencia, se deja constancia de que el desarrollo de esta fase de investigación se ajustó plenamente a los principios de legalidad institucional, ética investigativa y buenas prácticas profesionales, según los estándares vigentes para proyectos de análisis en redes académicas.