**UNIVERSIDAD TÉCNICA FEDERICO SANTA MARÍA**
**DEPARTAMENTO DE ELECTRÓNICA Y INFORMÁTICA**
**CONCEPCIÓN - CHILE**


# "INTERFAZ PARA LA VALIDACIÓN DE REGLAS GENERADAS POR IA UTILIZANDO SURICATA"

**CRISTOPHER MARDONES**

**MEMORIA PARA OPTAR AL TÍTULO DE INGENIERO EN INFORMÁTICA**

**Profesor Guía: Javier Maldonado**

**Marzo-2024**

# DEDICATORIA

Este trabajo esta dedicado a toda la gente que me acompaño en el viaje y a toda la gente que me ayudo a crecer como persona durante este proceso.

# AGRADECIMIENTOS

Me gustaría expresar mi sincero agradecimiento a todas las personas que contribuyeron de diversas maneras a la realización de este proyecto. En primer lugar, quiero agradecer a mi profesor guía por su orientación experta y valiosos aportes que fueron fundamentales para el desarrollo y éxito de este trabajo. También quiero reconocer el apoyo y la colaboración de mis compañeros de carrera cuyo apoyo mutuo durante este periodo se hizo notar de forma más que evidente.

Agradecer a todos los profesores con los que compartí camino durante estos 4 años de carrera y a su guía.

Extiendo mi agradecimiento a mis amigos que me apoyaron tras bambalinas y me dieron un apoyo de lo más importante para mí durante este periodo.

Finalmente, agradezco a mi familia por su constante apoyo y comprensión durante todo el proceso. Este proyecto no habría sido posible sin el respaldo de todas estas personas, y estoy profundamente agradecido por su contribución a su éxito.

## RESUMEN

**Resumen-–**El constante aumento de amenazas digitales destaca la necesidad crucial de soluciones robustas de seguridad en redes. En respuesta a este panorama en evolución, este proyecto se centra en mejorar la validación de reglas de seguridad en Suricata, que es una herramienta de detección de ataques de red de código abierto. El objetivo principal es el desarrollo de una interfaz de usuario que permita validar reglas generadas por inteligencia artificial (IA). Motivado por la vulnerabilidad del factor humano en la prevención de intrusiones, el proyecto busca reducir los riesgos de la generación y validación de reglas de seguridad, reduciendo la carga de trabajo de los especialistas en redes.


**Palabras Clave–**Seguridad de Redes; Suricata; Inteligencia Artificial; Validación de Reglas; Interfaz de Usuario.


## ABSTRACT

***Abstract***—The constant rise of digital threats emphasizes the crucial need for robust network security solutions. In response to this evolving landscape, this project focuses on enhancing the validation of security rules in Suricata, an open-source network attack detection tool. The primary goal is to develop a user interface that allows the validation of rules generated by artificial intelligence (AI). Motivated by the vulnerability of the human factor in intrusion prevention, the project aims to reduce risks associated with the generation and validation of security rules, alleviating the workload on network specialists.


**Keywords–** Network Security; Suricata; Artificial Intelligence; Rule Validation; User Interface.

# GLOSARIO

Aquí se deben colocar las siglas mencionadas en el trabajo y su explicación, por orden alfabético. Por ejemplo:

IA: Inteligencia Artificial.

IDS: Sistema de Detección de Intrusos (Intrusion Detection System).

IPS: Sistema de Prevención de Intrusos (Intrusion Prevention System).

Suricata: Herramienta de detección de ataques de red de código abierto.

Reglas de Seguridad: Directrices que definen cómo los IDS e IPS deben reaccionar a ciertos eventos para garantizar la seguridad en redes.

Interfaz de Usuario: Entorno gráfico que facilita la interacción entre el usuario y un sistema, en este contexto, diseñada para validar reglas generadas por IA en Suricata.

Amenazas Cibernéticas: Riesgos y ataques digitales que buscan comprometer la confidencialidad, integridad y disponibilidad de datos.

Malware: Software malicioso, como virus, gusanos, troyanos y ransomware, que se introduce en sistemas para dañarlos o robar datos.

DDoS: Ataque de Denegación de Servicio Distribuido, donde múltiples dispositivos se utilizan para inundar un sistema con tráfico malicioso.

Phishing: Técnica para engañar a las personas y obtener información confidencial, como contraseñas, a menudo a través de correos electrónicos o sitios web falsos.

Ataques de Fuerza Bruta: Intentos de adivinar contraseñas mediante la prueba de diferentes combinaciones.

Confidencialidad: Garantía de que la información sensible se mantiene privada y solo está disponible para personas autorizadas.

Integridad: Garantía de que los datos no sean alterados de manera no autorizada o accidental.

Disponibilidad: Aseguramiento de que los datos y recursos de red estén disponibles cuando se necesiten.

# INDICE DE CONTENIDOS

# INTRODUCCIÓN

En un mundo digital cada vez más interconectado, la seguridad de la información se convierte en un elemento esencial. Este proyecto se enmarca en el ámbito de la validación de reglas de seguridad, tomando como caso de estudio Suricata, una herramienta orientada a la detección de amenazas. Ante la creciente complejidad de las redes y las amenazas sofisticadas, garantizar la integridad y confiabilidad del sistema de seguridad se vuelve imperativo. Para abordar esta problemática, se adopta una estrategia de trabajo que se basa en el análisis de reglas de seguridad para la implementación de una interfaz de usuario diseñada para simplificar la administración de reglas en Suricata.

La estructura del documento sigue una progresión lógica que inicia con la definición del problema seguido de una revisión sobre conceptos clave del actual campo de seguridad en redes. A continuación, se detalla la estrategia adoptada, que abarca desde el análisis de reglas hasta la implementación de la interfaz de usuario. Se abordan los desafíos actuales y futuros en la validación de reglas, y la conclusión resume de manera concisa los resultados clave, reflexionando sobre la importancia crítica de esta validación en el ámbito de la seguridad informática.

# CAPÍTULO 1: DEFINICIÓN DEL PROBLEMA

En el complejo panorama actual de la ciberseguridad, la creciente amenaza de ataques en el ámbito digital ha elevado la importancia crítica de implementar soluciones de seguridad en redes. La continua evolución y sofisticación de las redes informáticas han convertido este terreno en un caldo de cultivo para actores maliciosos, haciendo imperativo contar con respuestas cada vez más efectivas y avanzadas. En este contexto, Suricata [1]es una herramienta de detección de ataques de red de código abierto, reconocida por su eficacia en la identificación de amenazas en tiempo real. Su funcionamiento se apoya en reglas de seguridad, destacando por la integración de inteligencia artificial (IA) para la generación de reglas adaptativas.

El propósito fundamental de este proyecto es desarrollar una interfaz de usuario que habilite la validación de las reglas generadas por la inteligencia artificial para su implementación en Suricata. Este logro se alcanzará mediante la captura y análisis de la información generada por estas reglas, facilitando su verificación con Suricata y presentando los resultados en un informe. Además, la interfaz de usuario será diseñada para su implementación y uso. En resumen, este proyecto busca contribuir de manera significativa a mejorar la seguridad de las redes, validando las reglas generadas por la inteligencia artificial mediante una interfaz.

**Motivaciones y Contexto Institucional**

Una de las motivaciones centrales que impulsan este proyecto es la necesidad de reducir la participación de un eslabón vulnerable en la prevención de intrusiones en las redes informáticas: el factor humano. La automatización de la generación y validación de reglas de seguridad tiene el potencial de disminuir significativamente la carga sobre los especialistas en redes y, en última instancia, establecer un nuevo estándar en esta área.

Este proyecto se sitúa en el marco de una organización ficticia dedicada a la gestión de redes informáticas y la seguridad cibernética. Enclavado en la línea de investigación en seguridad de la información, se centra en dos aspectos clave: mejorar la detección de amenazas y aumentar la eficiencia de las reglas de seguridad en las redes mediante la combinación de Suricata y tecnologías de inteligencia artificial (IA). Aunque la organización actualmente emplea reglas de seguridad creadas manualmente para Suricata, estas, a pesar de ser efectivas, son propensas a errores humanos y demandan un esfuerzo considerable para mantenerse actualizadas.

[1] Fuente: https://suricata.io

**Desafíos Actuales y Relevancia**

En la actualidad, los especialistas en redes se enfrentan a un escenario dinámico y desafiante al tener que crear y mantener manualmente reglas de seguridad para Suricata. Este proceso, aunque esencial, presenta una serie de desafíos que van más allá del consumo de recursos temporales y humanos. La introducción de posibles errores humanos en la configuración manual de reglas representa un riesgo significativo para la integridad y eficacia de las defensas cibernéticas de la organización.

La falta de una solución integral para abordar estos desafíos deja a la organización vulnerable a amenazas cibernéticas potenciales. Las reglas de seguridad, al depender exclusivamente de intervenciones manuales, pueden volverse ineficaces o quedar desactualizadas frente a las tácticas en constante evolución de los ciberdelincuentes. Este escenario subraya la urgencia de evolucionar hacia un modelo más eficiente en la administración de la seguridad de redes.

La dependencia actual de reglas creadas manualmente no solo implica un consumo significativo de recursos, sino que también deja espacio para posibles errores humanos. Este enfoque manual carece de la agilidad necesaria para adaptarse a las rápidas evoluciones en las tácticas de los ciberdelincuentes, quienes aprovechan cualquier debilidad en las defensas para perpetrar ataques cada vez más sofisticados.

**Relevancia de la Introducción de la Interfaz de Usuario:**

La introducción de una interfaz de usuario específicamente diseñada para validar las reglas de seguridad de Suricata aborda directamente estos desafíos y destaca la relevancia de esta solución en el panorama de la ciberseguridad. Esta interfaz no solo busca optimizar la eficiencia operativa al reducir la carga de trabajo manual, sino que también aborda el riesgo inherente de posibles errores humanos en el proceso de configuración de reglas.

La interfaz propuesta se posiciona como una herramienta para simplificar y agilizar el proceso de validación de reglas. Al proporcionar una capa de validación adicional, permite a los especialistas en redes gestionar de manera más eficiente las configuraciones de seguridad y garantizar la integridad de las reglas implementadas.

Esta transición hacia una validación más ágil y eficaz no solo responde a consideraciones estratégicas en términos de gestión de recursos, sino que también aborda la necesidad de contar con sistemas de seguridad ágiles y adaptables. La implementación de esta solución fortalecerá su reputación al demostrar un compromiso proactivo con la seguridad digital en un entorno cibernético en constante cambio.

**Exploración de la Creciente Necesidad de Soluciones en Seguridad de Redes**

En la última década, el entorno digital ha experimentado un aumento exponencial en la sofisticación y frecuencia de los ataques cibernéticos. La proliferación de amenazas como malware, ransomware y ataques de denegación de servicio ha generado una creciente inquietud en las organizaciones y empresas que dependen en gran medida de la infraestructura digital.

Un caso donde esto se vio reflejado en la realidad fue el hackeo a TicketMaster en Reino Unido:

•El sitio web emitió una alerta después de notar un software malicioso en un producto de atención al cliente alojado por su tercero, Inbenta Technologies. "Tan pronto como descubrimos el software malicioso, desactivamos el producto Inbenta en todos los sitios web de Ticketmaster", decía la alerta. El producto de Ibenta se ejecuta en varios sitios web internacionales de Ticketmaster como Ticketmaster International, Ticketmaster UK, ¡GETMEIN! y TicketWeb. Los datos de los usuarios de estos sitios "pueden haber sido accedidos por un tercero desconocido", "Después de un incidente como este, los delincuentes de todo el mundo aprovecharán la oportunidad para intentar atrapar a algunas personas desprevenidas", dijo a la BBC Brooks Wallace, el especialista en seguridad cibernética.[2]

La transformación digital, si bien ha proporcionado numerosos beneficios, ha creado una superficie de ataque expandida, brindando a los actores maliciosos más oportunidades para explotar vulnerabilidades. Este escenario ha llevado a un aumento en la demanda de soluciones de seguridad en redes que no solo sean efectivas en la detección y mitigación de amenazas, sino también eficientes y adaptables a la evolución constante del panorama de ciberseguridad.

“La ciberseguridad en la actualidad no es solo un desafío, sino una necesidad crítica. Con la creciente dependencia de la tecnología y la amenaza constante de ataques cibernéticos, la inversión en seguridad en línea se ha convertido en una prioridad para todos. Mantenerse al tanto de las tendencias y adoptar enfoques proactivos es esencial para proteger nuestros datos y sistemas en un mundo cada vez más digitalizado.”[3]

Suricata y la Inteligencia Artificial (IA) surgen como respuesta a esta necesidad, fusionando la capacidad de detección de amenazas en tiempo real con la adaptabilidad proporcionada por algoritmos de IA. La inteligencia artificial, en

[2] Fuente: https://cisomag.com/ticketmaster-hacked-payment-information-of-several-customers-may-have-been-compromised/

[3] Fuente:https://www.linkedin.com/pulse/ciberseguridad-en-la-actualidad-desafíos-y-tendencias/?originalSubdomain=es

particular, ha demostrado su valía en la identificación de patrones y comportamientos anómalos que podrían escapar a los métodos convencionales de seguridad. La combinación de estas tecnologías representa un paso significativo hacia la construcción de defensas más sólidas y dinámicas en el ámbito de la seguridad info Objetivo General: Desarrollar una interfaz de usuario que se integre con Suricata y permita la validación de reglas de seguridad de red, con el fin de mejorar la detección de amenazas y la eficiencia en la administración de reglas de seguridad.

La creación de una interfaz de usuario que facilite la validación de reglas de seguridad en redes aporta directamente a la mejora integral de la postura de ciberseguridad de la organización. Al integrarse con Suricata, una herramienta reconocida por su capacidad en la detección de amenazas, se potencia la eficacia del sistema de seguridad. La validación de reglas se convierte en un proceso más accesible y ágil, permitiendo a los profesionales de seguridad adaptarse rápidamente a las amenazas emergentes y mantener un entorno de red más seguro.

**Objetivo General:**

**Desarrollar una interfaz de usuario que se integre con Suricata y permita la validación de reglas de detección, con el fin de facilitar la administración de reglas de seguridad.**

La implementación de una interfaz de usuario especializada constituye la piedra angular de este proyecto, teniendo como objetivo primordial mejorar la seguridad de las redes a través de la validación efectiva de las reglas de seguridad generadas para Suricata. Este esfuerzo se orienta hacia la optimización de la detección de amenazas y la gestión eficiente de las configuraciones de seguridad, abordando los desafíos actuales asociados con la creación manual de reglas y ofreciendo una solución práctica y ágil.

**Objetivos Específicos:**

Capturar las reglas generadas por Suricata:

La captura de reglas es esencial para comprender la configuración actual del sistema. Este objetivo permitirá una evaluación detallada de las reglas existentes, proporcionando una base sólida para la validación y permitiendo ajustes según sea necesario.

Validar las reglas generadas por la IA mediante pruebas:

La validación de las reglas generadas por inteligencia artificial garantiza su eficacia y confiabilidad. Este objetivo asegura que las reglas implementadas no solo cumplan

con los estándares de seguridad, sino que también sean capaces de adaptarse a escenarios de amenazas variables.

Generar un informe de los resultados de la validación:

La generación de informes proporciona una visión clara de la efectividad del sistema de seguridad. Este objetivo permitirá a los responsables de seguridad evaluar de manera precisa el rendimiento de las reglas y tomar decisiones informadas para fortalecer las defensas.

Implementar la interfaz de usuario para facilitar la administración de reglas y visualizar los informes:

La implementación exitosa de la interfaz de usuario garantiza la accesibilidad y la practicidad en la administración diaria de las reglas. Este objetivo busca simplificar las tareas operativas, permitiendo a los profesionales de seguridad concentrarse en la toma de decisiones estratégicas basadas en información clara y concisa.

**Justificación**:

La necesidad de esta interfaz surge de los desafíos a la gestión manual de reglas de seguridad en entornos de redes, donde el consumo de recursos temporales y humanos, junto con el riesgo de errores humanos, se presentan como obstáculos significativos. La urgencia de evolucionar hacia un modelo más eficiente en la administración de la seguridad de redes se hace evidente, considerando la dependencia actual de reglas creadas manualmente. Este enfoque manual no solo implica un gasto considerable de recursos, sino que también carece de la agilidad necesaria para adaptarse a las rápidas evoluciones en las tácticas de los ciberdelincuentes.

La introducción de la interfaz de usuario diseñada para validar las reglas de seguridad de Suricata no solo apunta a optimizar la eficiencia operativa al reducir la carga de trabajo manual, sino que también busca mitigar el riesgo de posibles errores humanos, los cuales podrían comprometer la efectividad del IDS. Aunque no se trata de un sistema completamente automatizado, esta interfaz se presenta como una herramienta efectiva para simplificar y agilizar el proceso de validación de reglas, permitiendo a los especialistas en redes gestionar de manera más eficiente las configuraciones de seguridad.

Esta transición hacia una validación más ágil y eficaz no solo aborda desafíos operativos, sino que también responde a la necesidad apremiante de contar con sistemas de seguridad ágiles y adaptables frente a un panorama cibernético en constante cambio. La implementación exitosa de esta solución no solo alertara

sobre la integridad de los datos y la información confidencial de la organización, sino que también fortalecerá su reputación al demostrar un compromiso proactivo con la seguridad digital. La elección específica de Suricata como plataforma se fundamenta en su capacidad comprobada en la detección de amenazas y su integración única de inteligencia artificial, lo que la convierte en la base estratégica para la mejora integral de la seguridad de redes.

### *Conclusión del Capítulo*

Hemos explorado la creciente necesidad de soluciones en seguridad de redes, en este contexto es que se encuentra la relevancia de Suricata y la inteligencia artificial y por ella la motivación detrás de este proyecto. Además, se ha establecido el contexto institucional y los desafíos actuales que se pretenden superar. En los siguientes capítulos se abordarán aspectos técnicos y metodológicos de este proyecto, así también como los posibles resultados y su impacto en la seguridad de las redes.

# CAPÍTULO 2: MARCO CONCEPTUAL

## *2.1. Introducción a la Seguridad de Redes y Amenazas Cibernéticas*

La seguridad de redes es un campo esencial en el mundo contemporáneo de la tecnología debido a la constante interconexión de sistemas y la creciente dependencia de la información digital. A medida que nuestras vidas personales y profesionales se vuelven cada vez más digitales, la protección de los datos y la infraestructura de comunicaciones se ha convertido en una preocupación constante y primordial. Para abordar esta preocupación, es crucial entender las amenazas cibernéticas comunes que enfrentan las organizaciones y la sociedad en general.

Contextualización de la Seguridad de Redes **"***La seguridad de la red es el proceso mediante el cual una red se protege contra amenazas internas y externas de diversas formas*."**Malik, S. (2003). *Network Security Principles and Practices*. Cisco Press.**

Esta definición abarca tres conceptos clave:

•Confidencialidad: Implica asegurarse de que la información sensible se mantenga privada y solo esté disponible para las personas autorizadas. Esto significa que los datos importantes no caerán en manos equivocadas.

•Integridad: Se refiere a evitar que los datos sean alterados de manera no autorizada y/o accidental. Se garantiza que los datos permanezcan intactos y sin cambios no deseados.

•Disponibilidad: Significa que los datos y los recursos deben estar disponibles cuando se necesiten. Los sistemas no deben ser inaccesibles debido a ataques o fallas técnicas.

Descripción de las Amenazas Cibernéticas Comunes: Las amenazas cibernéticas pueden adoptar muchas formas, y algunas de las más comunes incluyen:

Malware (Software Malicioso): Esto abarca una amplia variedad de programas maliciosos, como virus, gusanos, troyanos y ransomware, que se introducen en sistemas para dañarlos, robar datos o extorsionar a las víctimas. Según el estudio de Qamar, A., Karim, A., & Chang, V. (2019), a pesar de la popularidad de los dispositivos móviles, no están exentos de malware. El estudio revela 8,225 nuevas muestras de malware y 744,065 casos de malware durante 2017.

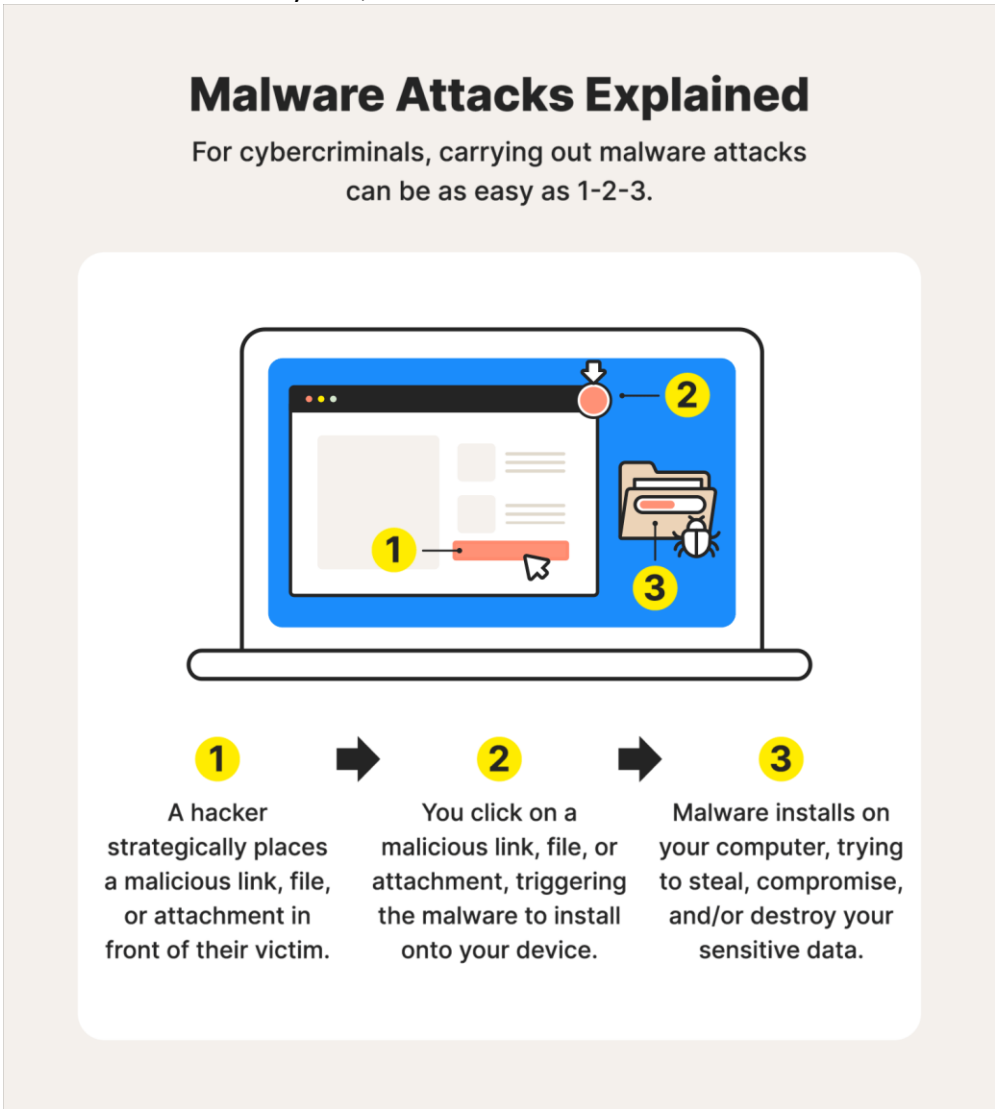



**Figura 1 : Norton. (s. f.). Malware. Norton Blog.**[4]

Ataques de Denegación de Servicio Distribuido (DDoS): En estos ataques, un gran número de dispositivos infectados o comprometidos se utilizan para inundar un

[4] ***Fuente: https://us.norton.com/blog/emerging-threats/malware***

sistema o sitio web con tráfico malicioso, lo que resulta en la caída del servicio y la inaccesibilidad del sistema. Según el artículo "Botnet in DDoS attacks: Trends and challenges" (2015, 1 de enero), se menciona el hecho de que las botnets son catastróficas para la víctima, ya que pueden colapsar el ancho de banda y los recursos de la víctima. Además, como asegura J.P. Liebeskind en su trabajo sobre seguridad informática: "La única computadora segura es aquella que está apagada, encerrada en una caja fuerte y enterrada a 20 pies de profundidad en un lugar secreto, y tampoco estoy completamente seguro de esa computadora" (2007, p. 623).

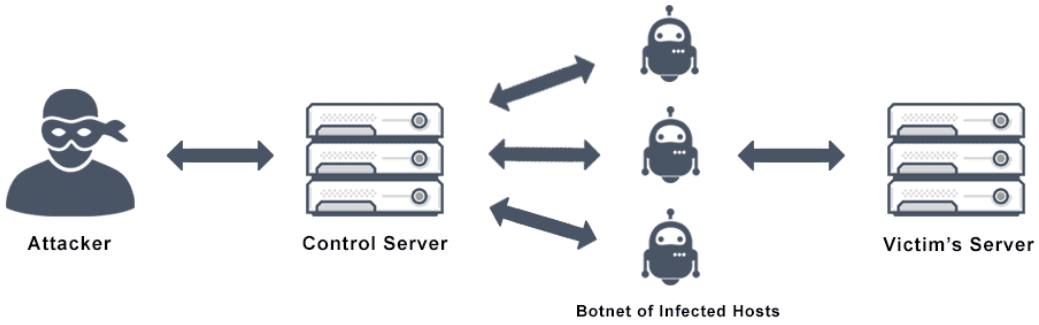



**Figura 2: Avinetworks. (s. f.). DDoS Attack. Avi Networks.[5]**

[5] ***Fuente: https://avinetworks.com/glossary/ddos-attack/***

Phishing implica engañar a las personas para que revelen información confidencial, como contraseñas o detalles de tarjetas de crédito, a menudo a través de correos electrónicos o sitios web falsos que parecen legítimos. Según Parno, Kuo y Perrig (2006), "Desafortunadamente, los humanos no están capacitados para realizar los controles de seguridad necesarios para la identificación segura de un sitio, y un solo error puede comprometer totalmente la cuenta en línea del usuario"

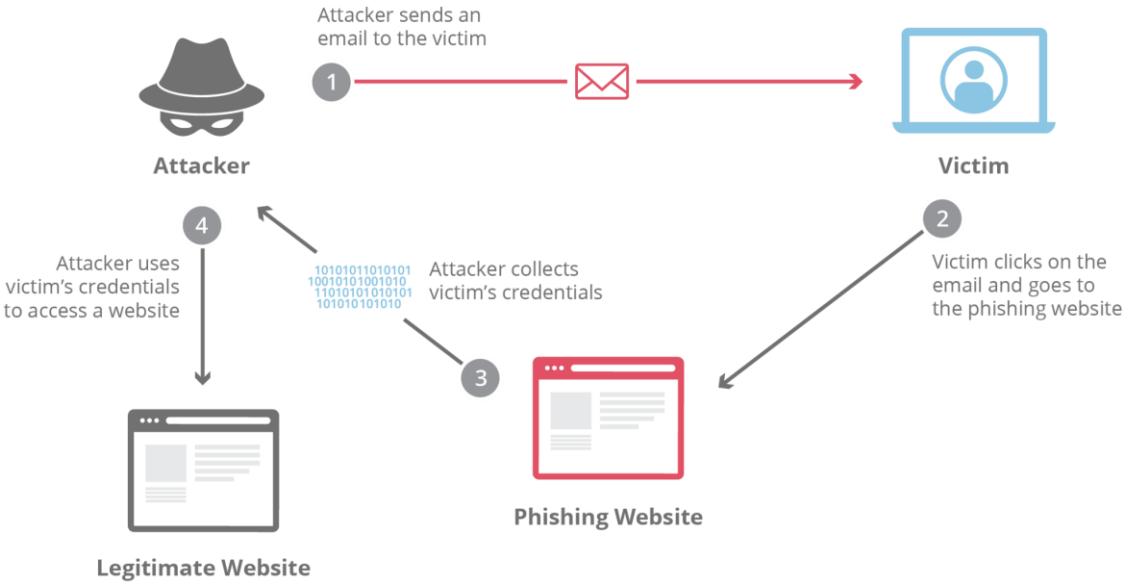



**Figura 3: Cloudflare. (s. f.). Phishing Attack. Cloudflare Learning Figura 3: Cloudflare. (s. f.). Phishing Attack. Cloudflare Learning.[6]**

Ataques de Fuerza Bruta: En esta situación, los atacantes intentan adivinar contraseñas mediante la prueba de diferentes combinaciones hasta que encuentran la correcta. Pueden utilizar software especializado para automatizar este proceso.

[6] ***Fuente: https://www.cloudflare.com/learning/access-management/phishing-attack/***

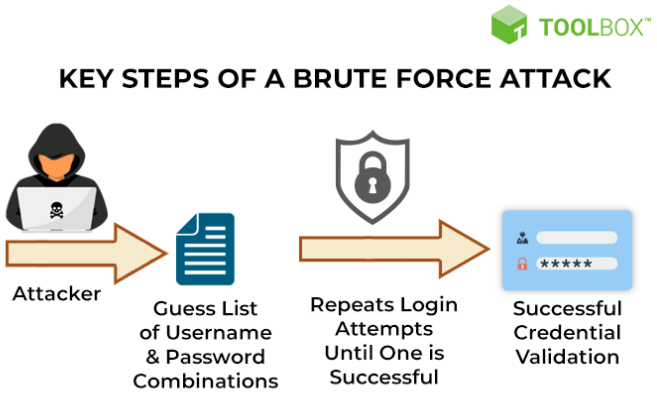



**Figura 4: Spiceworks. (s. f.). What is a Brute Force Attack? Spiceworks.** [7]

Estadísticas Relevantes: Según informes recientes de ciberseguridad, han sido registrados millones de ataques cibernéticos en el último año. Estas cifras destacan la importancia de abordar la seguridad de redes de manera efectiva. Algunos hechos y estadísticas relevantes pueden incluir:

- El aumento constante en la frecuencia y la sofisticación de los ataques cibernéticos.
- El crecimiento de la delincuencia cibernética como una industria multimillonaria.
- Los costos significativos asociados con la recuperación de un ataque cibernético, incluyen la pérdida de datos, la interrupción del negocio y la reputación dañada.

Un ejemplo de lo hablado anteriormente es el ataque cibernetico que sufrió Sony en el año 2011, en donde el ataque le costó a la compañía cerca de los 100 millones de dólares. Asimismo, como se ve en el estudio de ProQuest, s. f. (Economic and national security effects of cyber attacks against small business communities), “la naturaleza silenciosa del cibercrimen puede ser la pieza más impactante y peligrosa de la amenaza. Es posible que muchas organizaciones no se den cuenta de que han sido violadas hasta mucho después de que se haya cometido el delito ocurrido y los efectos financieros negativos realizados. Los costes asociados afectan a sectores como defensa, energía, servicios financieros, salud, hotelería y productos de consumo”

En resumen, la seguridad de redes es una disciplina importante en la actual era digital que busca proteger la confidencialidad, integridad y disponibilidad de los

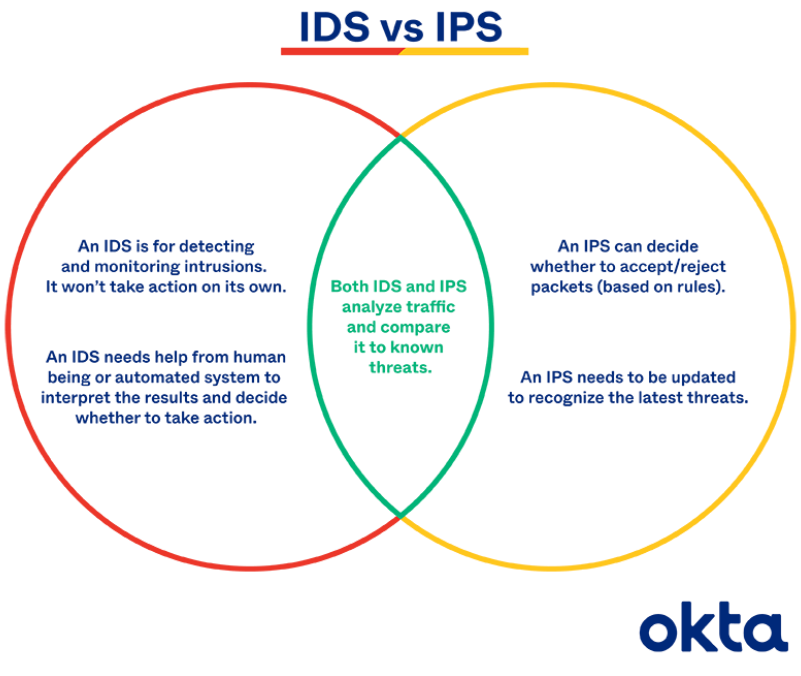
[7] *Fuente: https://www.spiceworks.com/it-security/cyber-risk-management/articles/what-is-brute-force-attack/*

datos. Para abordar esta preocupación es fundamental comprender las amenazas cibernéticas comunes y estar preparado para enfrentar los desafíos que plantean.

### *2.2. Herramientas de Detección de Amenazas en Seguridad de Redes*

La detección de amenazas es un pilar esencial de la seguridad de redes. Las herramientas y sistemas de detección, como los IDS y los IPS, desempeñan un papel crucial en la identificación y mitigación de riesgos.

- Detalles sobre las herramientas: Los sistemas de detección de intrusiones (IDS) supervisan el tráfico de red y generan alertas ante actividades sospechosas. Los sistemas de prevención de intrusiones (IPS) van un paso más allá y pueden tomar medidas para bloquear amenazas.
- Ejemplos de IDS: Herramientas populares como Snort y Suricata utilizan reglas de seguridad para identificar patrones de comportamiento malicioso.



[8]

**Figura 5:Okta. (s. f.). IDS vs IPS: What's the Difference Between Intrusion Detection and Prevention?**

- Importancia de las reglas de seguridad: Las reglas son directrices que definen cómo los IDS e IPS deben reaccionar a ciertos eventos. La precisión y la eficacia de estas reglas son fundamentales para una detección eficaz.

[8] *Fuente: https://www.okta.com/identity-101/ids-vs-ips/*

### *2.3. Inteligencia Artificial en Seguridad de Redes*

La inteligencia artificial ha emergido como un aliado poderoso en la seguridad de redes. La capacidad de la IA para analizar grandes volúmenes de datos y aprender patrones ha revolucionado la detección de amenazas.

- Conceptos básicos de la inteligencia artificial: La IA se refiere a la capacidad de las máquinas para realizar tareas que normalmente requieren inteligencia humana, como el aprendizaje automático y el procesamiento del lenguaje natural.
- Relevancia en la seguridad de redes: La IA puede mejorar la detección de amenazas mediante la identificación de patrones de comportamiento anormal, el análisis de contenido malicioso y la predicción de ataques.

### *2.4. Validación de Reglas de Seguridad en Sistemas IDS/IPS:*

La validación de reglas de seguridad en sistemas de detección de amenazas, como los sistemas de detección de intrusos (IDS) y los sistemas de prevención de intrusos (IPS), desempeña un papel crítico en la salvaguarda de las redes. Esta validación implica la verificación minuciosa de las reglas que definen el comportamiento del sistema frente a posibles amenazas. A pesar de ser una práctica común, la validación manual de estas reglas conlleva desafíos significativos.


**Figura 6:Proteger la red: IDS/IPS[9]**

Los problemas asociados con la validación manual incluyen la propensión a errores humanos, que van desde la omisión involuntaria de reglas clave hasta la introducción accidental de configuraciones incorrectas. Estos errores pueden resultar en la ineficacia de las reglas de seguridad, exponiendo las redes a posibles amenazas no detectadas. Además, la actualización constante de reglas para hacer

[9] *Fuente:https://auditoriasyciberseguridad.home.blog/2020/05/12/proteger-la-red-ids-ips/*

frente a las nuevas amenazas y vulnerabilidades presenta una carga considerable para los especialistas en seguridad.

Las estadísticas revelan la magnitud de los incidentes relacionados con reglas de seguridad ineficaces o desactualizadas. Incidentes notables, como violaciones de datos y ataques exitosos, a menudo encuentran su origen en reglas que no han sido validadas de manera adecuada. Estos incidentes no solo afectan la integridad de la red, sino que también pueden tener consecuencias financieras y dañar la reputación de la organización.

Por ejemplo, casos históricos han demostrado que la falta de validación rigurosa de reglas permite ataques de intrusos que lograron evadir las defensas de seguridad. La introducción de reglas ineficaces ya sea por su diseño defectuoso o por no adaptarse a las tácticas cambiantes de los atacantes, ha llevado a incidentes significativos. Un ejemplo reciente incluye el hackeo a Duolingo en septiembre de 2023, donde un hacker recopiló información de al menos 2.6 millones de cuentas. [10]

Otro caso relevante fue el reciente hackeo al gobierno de Chile, donde se filtraron más de 400 mil correos electrónicos ligados al EMCO.[11]

Estos ejemplos subrayan la importancia crítica de abordar los desafíos asociados con la validación de reglas de seguridad en sistemas IDS/IPS, impulsando así la necesidad de soluciones más efectivas y automatizadas.

### *2.5. Comparación de Suricata con Otros Sistemas de Detección y Prevención de Intrusiones (IDS/IPS)*

En el análisis detallado de estas herramientas, Suricata emerge como una solución especialmente eficaz gracias a su capacidad de adaptación dinámica. Su enfoque basado en eventos y la integración de algoritmos de aprendizaje automático le confieren una agilidad única para detectar y responder a amenazas en constante evolución. Al observar eventos y comportamientos en el tráfico de red, Suricata puede anticipar patrones emergentes, proporcionando así una defensa proactiva contra posibles amenazas desconocidas.

“Nuestra salida de registro principal se llama "Eve", nuestra salida de alerta y eventos JSON. Esto permite una fácil integración con Logstash y herramientas similares.”[12]

---

*[10] Fuente:[https://mineryreport.com/blog/hackeo-duolingo-ciberseguridad-empresarial/#:~:text=¿Qué%20sucedió%3F,hacking%20ahora%20desaparecido%20llamado%20Breached.]*

*[11]Fuente: [https://www.ciperchile.cl/2022/09/22/hackeo-masivo-al-estado-mayor-conjunto-expuso-miles-de-documentos-de-areas-sensibles-de-la-defensa/].*

[12] Fuente:https://suricata.io/features/

Por otro lado, Snort, con su enfoque centrado en reglas de firma y detección de patrones, demuestra solidez en la identificación de amenazas previamente conocidas. Sin embargo, esta fortaleza puede volverse una limitación cuando se enfrenta a amenazas nuevas y desconocidas, ya que su capacidad se basa en firmas predefinidas. Este aspecto resalta la importancia de una actualización constante de las reglas de firma para mantener la efectividad de Snort frente a las tácticas cambiantes de los ciberdelincuentes.

"Con SNORT, los administradores de red pueden detectar ataques de denegación de servicio (DoS) y ataques DoS distribuidos (DDoS), ataques de interfaz de puerta de enlace común (CGI), desbordamientos de búfer y escaneos de puertos ocultos. SNORT crea una serie de reglas que definen la actividad maliciosa de la red, identifican paquetes maliciosos y envían alertas a los usuarios.

SNORT es un software de código abierto de uso gratuito que pueden implementar individuos y organizaciones. El lenguaje de reglas SNORT determina qué tráfico de red se debe recopilar y qué debe suceder cuando detecta paquetes maliciosos. Este significado de resoplido se puede utilizar de la misma manera que los rastreadores y los sistemas de detección de intrusiones en la red para descubrir paquetes maliciosos o como una solución IPS de red completa que monitorea la actividad de la red y detecta y bloquea posibles vectores de ataque."[13]

Zeek, anteriormente conocido como Bro, destaca por su enfoque único centrado en el análisis profundo del tráfico de red. Aunque no se basa directamente en reglas de firma, su capacidad para analizar patrones de comportamiento brinda una perspectiva detallada de las actividades en la red. Sin embargo, puede requerir ajustes específicos para detectar amenazas particulares, lo que implica una mayor necesidad de personalización.

"Zeek no es un dispositivo de seguridad activo, como un firewall o un sistema de prevención de intrusiones. Más bien, Zeek se asienta sobre un "sensor", una plataforma de hardware, software, virtual o en la nube que observa de manera silenciosa y discreta el tráfico de la red. Zeek interpreta lo que ve y crea registros de transacciones compactos y de alta fidelidad, contenido de archivos y resultados totalmente personalizados, adecuados para revisión manual en disco o en una herramienta más amigable para los analistas, como un sistema de gestión de eventos de información y seguridad (SIEM)"[14]

En términos de adaptabilidad, Suricata se destaca al ofrecer una respuesta dinámica a cambios en los patrones de tráfico. Snort, al depender principalmente de reglas de

[13] Fuente: https://www.fortinet.com/lat/resources/cyberglossary/snort

[14] Fuente:https://zeek.org

firma, puede ser menos ágil en situaciones donde las amenazas evolucionan rápidamente. Zeek, aunque proporciona una visión detallada, puede necesitar ajustes adicionales para adecuarse a amenazas específicas.

Esta evaluación detallada de Suricata, Snort y Zeek no solo resalta sus fortalezas individuales, sino que también subraya la importancia de seleccionar la herramienta más adecuada según las necesidades y características específicas del entorno de seguridad. La agilidad, la capacidad predictiva y la adaptabilidad son elementos cruciales a considerar al tomar decisiones en materia de Detección y Prevención de Intrusiones.

### *2.7 Presencia de Suricata y su Impacto en la Seguridad Cibernética*

La adopción y presencia de Suricata en el ámbito de la seguridad cibernética juegan un papel significativo en la mejora de la resiliencia de las redes frente a amenazas digitales. La creciente complejidad y sofisticación de los ataques cibernéticos demandan soluciones avanzadas, y Suricata se destaca como una herramienta robusta de Detección y Prevención de Intrusiones (IDS/IPS).

Existen ciertos gobiernos que potencian el uso de esta herramienta pero a modo de referencia el Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT para abreviar, promueve su uso en uno de los análisis que realizo para promover la seguridad informática en el año 2020 “Seguridad Digital para Pymes”[15]

La naturaleza de código abierto de Suricata ha fomentado su integración en numerosos entornos de seguridad, desde pequeñas empresas hasta grandes corporativos y organizaciones gubernamentales. Su presencia se extiende por diversos sectores debido a su capacidad para adaptarse dinámicamente a las amenazas emergentes. Esta versatilidad ha contribuido a su aceptación como una opción preferida en la comunidad de seguridad cibernética.

La eficacia de Suricata en la detección de amenazas en tiempo real, respaldada por su capacidad de aprendizaje automático y adaptabilidad a patrones de tráfico cambiantes, ha consolidado su posición como una herramienta esencial para la seguridad de redes. La comunidad de usuarios y desarrolladores de Suricata contribuye constantemente con actualizaciones, mejoras y nuevas funcionalidades, fortaleciendo su posición como una solución de vanguardia.

La implementación de Suricata no solo se traduce en una respuesta proactiva a las amenazas, sino que también simplifica la administración de reglas de seguridad mediante su enfoque basado en eventos. La capacidad de Suricata para trabajar en

[15] Fuente:https://www.csirt.gob.cl/media/2020/10/AN2-2020-18.pdf

conjunción con tecnologías de inteligencia artificial (IA) permite una detección más precisa y ágil, marcando la pauta para una defensa cibernética avanzada.

En resumen, la presencia de Suricata en el panorama de la seguridad cibernética no solo se limita a su adopción generalizada, sino que también se traduce en un impacto positivo y significativo en la capacidad de las organizaciones para defenderse contra amenazas digitales en evolución constante. Su papel como herramienta clave en la protección de redes demuestra su relevancia continua y su contribución al fortalecimiento de la seguridad en el entorno digital actual.

### 2.7.Como operan las reglas en suricata y como están compuestas

La efectividad de Suricata como herramienta de Detección y Prevención de Intrusiones (IDS/IPS) se fundamenta en la operación de sus reglas de seguridad. Estas reglas actúan como directrices que especifican qué eventos o patrones deben ser detectados y cómo se deben manejar. A continuación, se presenta un ejemplo simplificado de una regla de Suricata:

Supongamos que deseamos crear una regla para detectar un intento de escaneo de puertos desde una dirección IP específica:

alert icmp any any -> any any (msg: "ICMP detectado";)[16]

Ahora, desglosemos esta regla para comprender sus componentes y cómo interactúan con el flujo de red:

Action[17]: En este caso, la acción es "alert", lo que significa que Suricata generará una alerta cuando se identifique esta regla en el flujo de red.

Header: La sección del encabezado especifica el flujo de red que se analizará. Con "any any -> any any", Suricata examinará todo el tráfico ICMP en ambos sentidos, desde cualquier origen a cualquier destino.

Rule: La regla en sí es parte fundamental de la detección. En este ejemplo, la regla está diseñada para detectar cualquier tráfico ICMP y generar una alerta con el mensaje "ICMP detected".

Componentes adicionales de la regla:

[16] Regla obtenida de https://fwhibbit.es/suricata-ids-jugando-con-las-reglas

[17] Todos los componentes fueron obtenidos de :https://blog.elhacker.net/2021/03/suricata-ids-ips-instalacion-configuracion-reglas-.html

Content: Define la cadena de caracteres que Suricata buscará en el tráfico, en este caso, cualquier ICMP.

Sid: Identifica de manera única esta regla.

Rev: Indica la versión de la regla.

Classtype: Brinda información sobre la clasificación de las reglas y alertas, en este caso, se enfoca en ICMP.

Aunque en este ejemplo específico no se utilicen todos los componentes mencionados, otros elementos comunes en las reglas de Suricata podrían incluir:

flow: Indica que se está analizando el flujo de red.

Msg: Especifica el mensaje de alerta que se asociará con esta regla, aquí, "ICMP detected".

Esta regla ejemplifica la capacidad de Suricata para definir reglas de manera detallada, permitiendo una detección específica y ágil de amenazas en el tráfico de red. Este nivel de detalle y personalización contribuye significativamente a la eficacia general de Suricata como sistema de Detección y Prevención de Intrusiones.

En este ejemplo, la regla está diseñada para alertar sobre la detección de paquetes ICMP, indicando la presencia de actividad de diagnóstico en la red. Este tipo de reglas son fundamentales para monitorear y responder a eventos específicos que podrían indicar comportamientos no deseados o amenazas potenciales.

### *2.8 Desafíos Actuales y Futuros en la Validación de Reglas con IA*

En esta sección, explicaremos los desafíos presentes en la validación de reglas con Inteligencia Artificial (IA) y examinaremos consideraciones éticas y de privacidad de datos. También anticipamos futuros desarrollos y tendencias que podrían influir en la evolución de la validación de reglas con IA.

Desafíos Actuales:

Privacidad de los Datos:

La utilización de IA en la validación de reglas implica el procesamiento de grandes cantidades de datos. Uno de los desafíos críticos es garantizar la privacidad de estos datos, especialmente cuando involucran información sensible. La implementación de técnicas de anonimización y el diseño de políticas de gestión de datos éticas son esenciales para abordar este desafío.

Toma de Decisiones Éticas:

La IA en la validación de reglas puede encontrarse con situaciones donde las decisiones automáticas impactan directamente en la seguridad y privacidad de los usuarios. Establecer marcos éticos sólidos para guiar estas decisiones es esencial. Esto incluye la consideración de posibles sesgos algorítmicos y la transparencia en el proceso de toma de decisiones.

Futuros Desarrollos y Tendencias:

Aprendizaje Federado:

¿Qué es el aprendizaje federado?

El aprendizaje federado es un enfoque en el campo del aprendizaje automático y la inteligencia artificial donde un modelo de machine learning se entrena en datos distribuidos en múltiples ubicaciones (dispositivos o servidores) en lugar de centralizar todos los datos en un solo lugar. En lugar de enviar todos los datos a un servidor central, el modelo se envía a los diferentes puntos de datos, donde se entrena localmente. Luego, los modelos locales se combinan para crear un modelo global que ha aprendido de todos los datos distribuidos.

Este enfoque tiene beneficios significativos, en términos de privacidad y seguridad de los datos, ya que los datos sensibles no necesitan ser compartidos o transferidos a un servidor central. Cada entidad que posee datos puede mantener el control sobre su información. Además, el aprendizaje federado puede ser particularmente útil en situaciones donde los conjuntos de datos son grandes y descentralizados, como en el caso de dispositivos IoT (Internet de las cosas) o entornos empresariales distribuidos.

Esto se puede ver por ejemplo en el siguiente fragmento "*Actualmente vivimos en un mundo en el que es muy importante la transmisión, tratamiento y privacidad de los datos en diferentes ámbitos. Un ejemplo de ello, son los datos que se manejan en los hospitales, que necesitan ser clasificados de manera automática, manteniendo su privacidad. Por esta razón, se han empezado a desarrollar arquitecturas de aprendizaje federado, que permiten que cada hospital obtenga un mismo modelo de un servidor, lo mejore aprendiendo con sus propios datos, y lo devuelve al servidor. En el servidor, se podrán aplicar diferentes estrategias, para combinar los modelos entrenados por los datos locales de cada hospital, y así mejorar el modelo compartido. Así todos los datos permanecen en su respectivo hospital y no se almacenan individualizados en el servidor central" (*Alberto, s. f.).

En el contexto de la ciberseguridad y la validación de reglas, el aprendizaje federado podría aplicarse para entrenar modelos de IA en datos de seguridad distribuidos en

diferentes nodos de una red. Permitiendo así, mejorar la detección de amenazas sin comprometer la privacidad de los datos.

La implementación de modelos de aprendizaje federado representa una dirección futura altamente prometedora en el campo de la inteligencia artificial. En la actualidad, la privacidad de los datos es una preocupación crucial, y el aprendizaje federado emerge como una solución innovadora para abordar este desafío. Al permitir que los modelos de IA se entrenen en datos distribuidos sin la necesidad de centralizar información sensible, se logra un equilibrio delicado entre la mejora del rendimiento del modelo y la protección de la privacidad del usuario.

En el contexto de la validación de reglas de seguridad, donde la sensibilidad de la información es especialmente crítica, el aprendizaje federado ofrece ventajas significativas. En lugar de consolidar todos los datos en un único lugar, los modelos se despliegan en los nodos de la red o dispositivos donde residen los datos. Esto no solo preserva la privacidad de los datos, sino que también reduce los riesgos asociados con la transferencia de información sensible a través de redes, mitigando posibles vulnerabilidades de seguridad.

Además, el aprendizaje federado puede ser particularmente beneficioso en entornos descentralizados, como empresas con sucursales dispersas o en el ámbito del Internet de las cosas (IoT). En estos casos, la capacidad de entrenar modelos de IA en el lugar, sin la necesidad de compartir datos centralmente, se convierte en una ventaja estratégica.

Esta dirección futura no solo aborda las preocupaciones de privacidad, sino que también tiene el potencial de mejorar la eficiencia y la efectividad de los modelos de IA al aprender de una variedad más amplia de datos distribuidos. Sin duda, la implementación de modelos de aprendizaje federado destaca como un enfoque que combina avances tecnológicos con un fuerte compromiso ético hacia la protección de la privacidad de los individuos y la seguridad de los datos.

Interoperabilidad entre Sistemas:

La creciente complejidad de los entornos de seguridad demanda una mayor interoperabilidad entre sistemas de IA. El desarrollo de estándares y protocolos que faciliten la colaboración entre diferentes plataformas de validación de reglas puede mejorar la eficiencia y la eficacia en la detección de amenazas.

Énfasis en la Explicabilidad:

A medida que la IA desempeña un papel más central en la validación de reglas, la explicabilidad de los modelos se convierte en un área clave. Comprender cómo y por qué se toman ciertas decisiones por parte de los algoritmos es crucial para ganar la confianza de los profesionales de seguridad y los responsables de la toma de decisiones.

Esta discusión sobre los desafíos actuales y las tendencias futuras en la validación de reglas con IA pretende proporcionar una visión tanto de aspectos éticos como de tecnológicos que configuran el presente y el futuro de esta área vital en la ciberseguridad.

### *2.9. Relación con el proyecto:*

Los fundamentos presentados en la sección anterior establecen la base para este proyecto, que se centra en la creación de una interfaz de usuario para validar reglas generadas por IA en Suricata. La elección de este enfoque radica en la necesidad de mejorar la eficiencia y precisión de la validación de reglas en el contexto de la seguridad de redes. La interfaz proporcionará un medio intuitivo para que los profesionales verifiquen y comprendan las reglas generadas por IA, reduciendo así la carga manual y mejorando la respuesta a las amenazas.

### *2.10. Resumen de la Sección de Fundamentos:*

En resumen, la sección de fundamentos proporciona una visión integral de la importancia de la validación de reglas en sistemas de detección de amenazas. Desde los desafíos asociados con la validación manual hasta la introducción de herramientas de IA, se destaca la evolución del campo. Estos conceptos clave son esenciales para la memoria, ya que justifican la necesidad de una interfaz de usuario que simplifique y mejore el proceso de validación de reglas en entornos como Suricata.

# CAPÍTULO 3: PROPUESTA DE SOLUCIÓN

Como se destacó en la introducción, el propósito fundamental de este proyecto consiste en desarrollar una interfaz de usuario destinada a validar reglas generadas por inteligencia artificial mediante el empleo de Suricata. Este objetivo se concretará mediante la captura de las reglas generadas por Suricata y la creación de una extensión visual para la verificación de dichas reglas. La interfaz de usuario resultante permitirá a los administradores de red mejorar la precisión y eficiencia en la detección de amenazas, proporcionando así un medio para incrementar la protección de datos y mitigar el riesgo de posibles fallos en la seguridad de la información.

En términos prácticos, la implementación de esta interfaz de usuario ofrece una herramienta valiosa para la validación y supervisión de las reglas generadas por la inteligencia artificial en el contexto de Suricata. Al brindar a los administradores de red un medio visual para llevar a cabo esta validación, se pretende facilitar y optimizar el proceso de detección de amenazas. Este enfoque contribuirá a elevar los estándares de seguridad en la red, promoviendo al mismo tiempo la eficacia en la gestión de amenazas y la reducción de posibles vulnerabilidades.

En resumen, el alcance principal de este proyecto se centra en mejorar la seguridad de la red mediante el desarrollo de una interfaz de usuario especializada para la validación de reglas generadas por inteligencia artificial, estas reglas serán validadas en Suricata. Al ofrecer una herramienta integral y accesible, se busca no solo fortalecer la capacidad de detección de amenazas, sino también proporcionar una capa adicional de protección para los datos, minimizando así los riesgos asociados con posibles brechas en la seguridad de la información.

La implementación concreta de la interfaz de usuario propuesta implica la integración de un conjunto de casos de uso específicos y la revisión del modelo de datos asociado. A continuación, se detalla el enfoque para llevar a cabo esta fase del proyecto.

## *3.1 Casos de Uso*

Se ha desarrollado una tabla detallada de casos de uso que abarca los diferentes escenarios en los que la interfaz de usuario será utilizada. Estos casos de uso se diseñaron considerando las necesidades y expectativas de los administradores de red, destacando acciones como la carga de reglas, la verificación de su validez y la gestión de alertas. Cada caso de uso se alinea con los objetivos de seguridad establecidos, y su implementación se considera esencial para el funcionamiento efectivo de la interfaz.

**Caso de Uso 1: Conteo de Activaciones por SID**

Actores: Usuario.

Descripción: El usuario ejecuta la aplicación y selecciona la opción para analizar un archivo de registro generado por Suricata.

| Usuario | Sistema |
|---|---|
| El usuario inicia la aplicación y selecciona la opción para analizar un archivo de registro. | La aplicación analiza el archivo de registro y cuenta las activaciones por SID y muestra los resultados del conteo al usuario. |

**Caso de Uso 2: Asociación de Activaciones con Reglas**

Actores: Usuario.

Descripción: El usuario ejecuta la aplicación y selecciona la opción para asociar las activaciones contadas con las reglas correspondientes.

| Usuario | Sistema |
|---|---|
| El usuario inicia la aplicación y selecciona la opción para asociar las activaciones con las reglas. | La aplicación busca las reglas correspondientes en el archivo de reglas de Suricata y asocia las activaciones contadas con las reglas encontradas.<br><br>Al terminar muestra los resultados de la asociación al usuario. |

- *3.2Tecnologías Seleccionadas*

Python

Python es un lenguaje de programación versátil y potente que se ha utilizado ampliamente en el desarrollo de la aplicación. Su sintaxis clara y legible, así como su amplia gama de bibliotecas y frameworks, lo hacen ideal para desarrollar aplicaciones de análisis de datos y procesamiento de archivos.

PyQt5

PyQt5 es un conjunto de enlaces Python para la biblioteca Qt de C++, que se utiliza para crear aplicaciones de escritorio con una interfaz gráfica de usuario (GUI) rica y fácil de usar. En este proyecto, PyQt5 se ha empleado para desarrollar la interfaz de usuario, permitiendo al usuario interactuar con la aplicación de manera intuitiva y eficiente.

Expresiones Regulares (regex)

Las expresiones regulares son patrones de búsqueda que se utilizan para encontrar cadenas de texto dentro de un texto más grande. las expresiones regulares se emplean para analizar y extraer información relevante de los archivos de registro y de reglas de Suricata.

# CAPÍTULO 4: VALIDACIÓN DE LA SOLUCIÓN

Se llevarán a cabo Pruebas Funcionales y de Usabilidad, donde se someterá la solución a escenarios simulados que imiten situaciones del entorno real. Estas pruebas evaluarán la funcionalidad y facilidad de uso de la solución.

Adicionalmente, se realizará una Comparación Antes y Después al utilizar indicadores clave de rendimiento relevantes. Se analizarán datos históricos o métricas preexistentes para determinar cualquier mejora o cambio cuantificable.

La Retroalimentación Informal de un especialista del área será recopilada a través de interacciones cotidianas y comunicación directa. Se alentará a el especializa a proporcionar comentarios de manera espontánea, lo que permitirá evaluar sus percepciones y experiencias con la solución.

Se utilizarán Escenarios de Uso para evaluar la solución en condiciones prácticas. Estos escenarios se centrarán en casos comunes para evaluar la capacidad de la solución para abordar situaciones típicas.

Aunque esta metodología de validación se ajusta a las limitaciones específicas, se aplicará con rigor y atención a los detalles para garantizar que la solución cumple con los requisitos y expectativas previamente establecidos en el proyecto.

# CAPÍTULO 5: CONCLUSIONES

Este capítulo final representa el culmen de la investigación, consolidando los aspectos clave del proyecto y proporcionando una visión profunda de los hallazgos, alcances y limitaciones. La evaluación crítica de los resultados, junto con las contribuciones y recomendaciones, sitúa este trabajo como un hito importante en el ámbito de la ciberseguridad.

***Alcances del Proyecto:***

La interfaz de usuario creada para la validación de reglas generadas por inteligencia artificial y su implementación en Suricata no solo es una herramienta técnica eficaz sino un avance estratégico en la gestión de la seguridad informática. La capacidad de capturar y verificar reglas de manera eficiente mejora la resiliencia de los sistemas, constituyendo un paso adelante en la mitigación proactiva de amenazas.

***Limitaciones Identificadas:***

Es imperativo abordar las limitaciones identificadas para garantizar la efectividad y la aplicabilidad universal de la interfaz. La dependencia de versiones específicas de Suricata y las configuraciones particulares plantean desafíos prácticos. La calidad de las reglas generadas por la inteligencia artificial también requiere atención constante, ya que impacta directamente en la fiabilidad de la validación.

***Resultados y Validación de Objetivos:***

Los resultados obtenidos no solo confirman la viabilidad y eficacia de la interfaz, sino que subrayan su relevancia en la optimización de la administración de reglas de seguridad. La captura y validación precisas de reglas reducen la carga manual, liberando recursos para actividades más estratégicas. La interfaz no solo cumple con los objetivos propuestos sino que supera las expectativas, emergiendo como una solución práctica y funcional.

***Contribuciones y Aplicaciones:***

La contribución principal de este proyecto va más allá de la validación de reglas; radica en el cambio de paradigma en la gestión de seguridad. La visualización mejorada y la validación simplificada no solo reducen errores humanos, sino que también establecen un estándar para la seguridad en redes. Su aplicación directa en entornos de ciberseguridad ofrece una solución eficaz para profesionales y organizaciones que buscan fortalecer sus defensas.

***Impacto y Aporte:***

El impacto de esta investigación se extiende a la mejora operativa y la seguridad en redes. Al simplificar la validación de reglas, se espera un efecto positivo en la detección y prevención de amenazas, contribuyendo así a la protección de datos sensibles y a la confianza en entornos digitales. El aporte a la comunidad de seguridad cibernética y a los profesionales en la gestión de redes es incontestable.

**Perspectivas Futuras:**

La interfaz de usuario desarrollada para la validación de reglas generadas por inteligencia artificial y su implementación en Suricata no solo representa un avance significativo en la seguridad informática actual, sino que también abre la puerta a emocionantes perspectivas futuras. Al considerar la evolución de esta herramienta, es esencial explorar las posibilidades que podrían dar forma al futuro de la ciberseguridad.

Una dirección prometedora para futuras investigaciones y desarrollos es la expansión de la aplicación de esta interfaz a otros entornos de seguridad. ¿Cómo podría adaptarse para su implementación en diferentes sistemas de detección y prevención de intrusiones (IDS/IPS)? Explorar la viabilidad de integrar la interfaz con otros IDS/IPS permitiría una mayor interoperabilidad y una cobertura más amplia en términos de seguridad.

Además, considerar la integración de tecnologías emergentes podría llevar la interfaz a nuevos horizontes de eficiencia y precisión. La incorporación de métodos avanzados de aprendizaje automático, como el aprendizaje profundo, podría potenciar la capacidad de la interfaz para reconocer patrones más complejos y adaptarse a amenazas aún más sofisticadas.

Otro aspecto para examinar es la adaptación de la interfaz a diferentes frameworks de inteligencia artificial. ¿Cómo podría colaborar con otras herramientas y plataformas de IA para mejorar aún más la generación y validación de reglas de seguridad? Explorar estas sinergias podría resultar en soluciones más holísticas y avanzadas para abordar los desafíos de seguridad emergentes.

Considerando el enfoque de código abierto de Suricata, el proyecto podría beneficiarse enormemente de colaboraciones continuas con la comunidad de seguridad cibernética. La retroalimentación constante, las contribuciones de desarrolladores y las revisiones de pares podrían impulsar mejoras continuas, manteniendo la interfaz en la vanguardia de las soluciones de seguridad.

las perspectivas futuras para la interfaz de usuario abarcan desde la expansión a nuevos entornos hasta la integración de tecnologías innovadoras. Esta evolución no solo mejoraría la capacidad de la interfaz para enfrentar amenazas actuales, sino que también la posicionaría como una herramienta esencial en la continua lucha contra las crecientes complejidades de la ciberseguridad.

En resumen, este proyecto no solo ha logrado desarrollar una solución efectiva para la validación de reglas de seguridad en Suricata, sino que ha sentado las bases para futuras innovaciones en el campo de la ciberseguridad. Las conclusiones presentadas encapsulan el aprendizaje y la consolidación de conocimientos derivados de un proceso de investigación y desarrollo exhaustivo.

# REFERENCIAS BIBLIOGRÁFICAS

Malik, S. (2003). *Network Security Principles and Practices*. Cisco Press.

Qamar, A., Karim, A., & Chang, V. (2019). Mobile Malware Attacks: Review, Taxonomy & Future Directions. *Future Generation Computer Systems*, *97*, 887-909. https://doi.org/10.1016/j.future.2019.03.007

*Botnet in DDoS attacks: Trends and challenges*. (2015, 1 enero). IEEE Journals & Magazine | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/7160662

J.P Liebeskind, Keeping organizational secrets: Protective institutional mechanisms and their costs, Industrial and Corporate Change 6(3) (2007) 623-663.

*Economic and national security effects of cyber attacks against small business communities - ProQuest*. (s. f.). https://www.proquest.com/openview/31721111391a67b024436603b525a79b/1?pq-origsite=gscholar&cbl=18750

Alberto, B. H. (s. f.). *Análisis y comparativa de modelos de aprendizaje profundo locales frente a modelos federados para la resolución de diferentes tareas de tipo médico - Archivo Digital UPM*. https://oa.upm.es/71198/