UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

TÍTULO

Desarrollo de un marco de ciberseguridad para Unidad Educativa Virtual Zúrich Science

AUTORA

Torres Lindao, Valeria Dayanna

TRABAJO DE TITULACIÓN

Previo a la obtención del grado académico en
MAGÍSTER EN CIBERSEGURIDAD

TUTOR

Zambrano Martínez, Jorge Luis

Santa Elena, Ecuador

2025

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

TRIBUNAL DE SUSTENTACIÓN

Firmado electrónicamente por:
ALICIA GERMANIA ANDRADE VERA

Ing. Alicia Andrade Vera, Mgtr
COORDINADORA DEL PROGRAMA

Firmado electrónicamente por:
JORGE LUIS ZAMBRANO MARTINEZ

Ing. Jorge Zambrano Martínez, Ph.D.
TUTOR

Firmado electrónicamente por:
JESENNIA DEL PILAR CARDENAS COBO

Lic. Jessenia Cárdenas Cobo, Ph.D.
DOCENTE ESPECIALISTA

Firmado electrónicamente por:
SANG GUUN YOO .

Ing. Sang Guun Yoo, Ph.D.
DOCENTE ESPECIALISTA

Firmado electrónicamente por:
MARIA MARGARITA RIVERA GONZALEZ

Abg. María Rivera González, Mgtr.
SECRETARIA GENERAL UPSE

UNIVERSIDAD ESTATAL PENÍNSULA
DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

CERTIFICACIÓN

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos, razón por el cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por VALERIA DAYANNA TORRES LINDAO, como requerimiento para la obtención del título de Magíster en Ciberseguridad.

TUTOR

Firmado electrónicamente por:
JORGE LUIS ZAMBRANO MARTINEZ

Ing. Jorge Luis Zambrano Martínez, Ph.D.

Santa Elena, 13 de diciembre de 2024

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

DECLARACIÓN DE RESPONSABILIDAD

Yo, **VALERIA DAYANNA TORRES LINDAO**

DECLARO QUE:

El trabajo de Titulación, Desarrollo de un marco de ciberseguridad para Unidad educativa Virtual Zúrich Science previo a la obtención del título en Magíster en Ciberseguridad, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Santa Elena, 13 de diciembre de 2024

Firmado electrónicamente por:
VALERIA DAYANNA TORRES LINDAO

Valeria Dayanna Torres Lindao

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE CIENCIAS DE LA INGENIERÍA
INSTITUTO DE POSTGRADO

CERTIFICACIÓN DE ANTIPLAGIO

Certifico que después de revisar el documento final del trabajo de titulación denominado Desarrollo de un marco de ciberseguridad para Unidad Educativa Virtual Zúrich Science, presentado por la estudiante, VALERIA DAYANNA TORRES LINDAO fue enviado al Sistema Antiplagio COMPILATIO, presentando un porcentaje de similitud correspondiente al 9%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.

TUTOR

Firmado electrónicamente por:
JORGE LUIS ZAMBRANO MARTINEZ

Ing. Jorge Luis Zambrano Martínez, Ph.D.

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

AUTORIZACIÓN

Yo, **VALERIA DAYANNA TORRES LINDAO**

Autorizo a la Universidad Estatal Península de Santa Elena, para que haga de este trabajo de titulación o parte de él, un documento disponible para su lectura consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos en línea patrimoniales de mi propuesta metodológica y tecnológica avanzada con fines de difusión pública, además apruebo la reproducción de esta propuesta metodológica y tecnológica avanzada dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor

Santa Elena, 13 de diciembre de 2024

LA AUTORA

Firmado electrónicamente por:
VALERIA DAYANNA TORRES LINDAO

Valeria Dayanna Torres Lindao

AGRADECIMIENTO

En primer lugar, quiero agradecer a Dios por su guía y bendiciones en este camino. A mis padres, Pablo Torres y Jessica Lindao, quienes siempre me han brindado su apoyo constante para poder llegar hasta aquí. A mis hermanos, quienes con su compañía y palabras de aliento me motivaron a dar lo mejor de mí.

También, quiero agradecer a mi tutor, Ing. Jorge Luis Zambrano Martínez Ph.D, por su guía y aportes que fueron fundamentales en cada etapa de este proyecto.

Finalmente, quiero agradecer a mis amigos y familiares quienes con su apoyo emocional y constante motivación me animaron a superar los obstáculos que encontré en el camino.

Valeria Dayanna, Torres Lindao

DEDICATORIA

Dedico este trabajo a mis padres, cuyo amor, sacrificio y apoyo incondicional han sido el pilar fundamental en mi vida. A ellos, que siempre han creído en mí, incluso en los momentos más desafiantes, les ofrezco este logro como un testimonio de su esfuerzo y dedicación.

A mis hermanos, cuya compañía y palabras de ánimo han sido una fuente constante de inspiración y fortaleza, y con quienes comparto la alegría de este logro. Finalmente, dedico este proyecto a todas aquellas personas que me han apoyado incondicionalmente, desde amigos hasta compañeros de camino, cuya presencia me ha motivado a seguir adelante. Este trabajo representa no solo mi esfuerzo, sino también la suma del amor y las enseñanzas que he recibido a lo largo de mi vida.

Valeria Dayanna, Torres Lindao

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El presente trabajo aborda el desarrollo de un marco de ciberseguridad para la Unidad Educativa Virtual Zúrich Science, con el propósito de proteger los activos tecnológicos, garantizar la continuidad operativa y fortalecer la confianza de los usuarios en los entornos educativos digitales. A través de un enfoque experimental y cuantitativo, se diseñó un sistema de detección de intrusiones utilizando inteligencia artificial y análisis de comportamiento. El método incluyó la simulación de ataques cibernéticos, análisis del tráfico de red y evaluación de vulnerabilidades mediante herramientas como Snort, Nmap y algoritmos de machine learning. Los resultados evidenciaron una mejora en la detección temprana de amenazas, con una precisión superior al 95%, y una reducción significativa de falsos positivos. El marco propuesto en esta tesis demostró ser efectivo para mitigar riesgos y ataques cibernéticos, consolidando la seguridad de los sistemas educativos y promoviendo un entorno virtual más confiable y resiliente.

Palabras claves: Ciberseguridad, Educación virtual, Detección de amenazas

ABSTRACT

This research delves into developing a cybersecurity framework tailored for the Zürich Science Virtual Educational Institution to safeguard technological assets, ensure operational continuity, and bolster user confidence in digital learning environments. An experimental and quantitative approach engineered an intrusion detection system, leveraging artificial intelligence and behavioral analysis. The methodology encompassed the simulation of cyberattacks, network traffic analysis, and vulnerability assessment using tools such as Snort, Nmap, and machine learning algorithms. The findings demonstrated a significant enhancement in the early detection of threats, achieving an accuracy exceeding 95% and substantially reducing false positives. The framework proposed in this thesis has proven effective in mitigating risks and cyberattacks, solidifying the security of educational systems, and fostering a more reliable and resilient virtual environment.

Keywords: Cybersecurity, Virtual Education, Threat Detection

INTRODUCCIÓN

Con la evolución tecnológica a nivel mundial, las instituciones educativas tanto tradicionales como virtuales dependen en su mayoría de los sistemas informáticos para llevar a cabo sus actividades administrativas y académicas. Debido a esto las instituciones se vuelven dependientes al uso de diferentes plataformas virtuales ya sea para impartir clases, gestionar datos o interactuar entre el docente y los estudiantes, lo cual las vuelve un objeto de ataque atractivo para los ciberdelincuentes, por lo que se vuelven vulnerables a ciberataques (Johanna et al., 2019).

Las instituciones educativas son objeto de ataque para los ciberdelincuentes ya que estas almacenan grandes cantidades de datos sensibles como: información personal y académica tanto de estudiantes como de empleados (Sun y Wu, 2019). Por este motivo la falta de un marco de ciberseguridad en mayor parte en instituciones educativas en línea como lo es la Unidad Educativa Zúrich Science, las expone a posibles amenazas cibernéticas, y no considera la creación de guías para implementar controles o herramientas para proteger los elementos tecnológicos de estas (Pronchev et al., 2023). Por lo tanto, esta falta de marco plantea la pregunta sobre cómo mejorar la ciberseguridad en estos entornos y cómo diseñar un marco que se adapte a las necesidades de estas instituciones educativas virtuales (Pillajo Garcia y Avila Pesantez, 2023).

La implementación de un marco de ciberseguridad adaptado a las Unidad Educativa Virtual Zúrich Science reducirá los riesgos y vulnerabilidades de seguridad (Fernando y Sumalave, 2023). El diseño de este marco de ciberseguridad abarca un análisis exhaustivo de la infraestructura tecnológica actual de la institución, la identificación y evaluación de las principales vulnerabilidades, la implementación de una herramienta de detección de intrusos con inteligencia artificial y la evaluación de la efectividad y eficiencia del marco de ciberseguridad mediante pruebas de penetración y simulaciones de ataques. Esto con el fin de que la institución educativa pueda adoptar prácticas de seguridad eficientes y responder de manera efectiva a incidentes de seguridad.

El desarrollo de esta propuesta es relevante tanto para proteger la información confidencial como los activos tecnológicos de estas instituciones, donde la ciberseguridad se convierte en una competencia requerida (Pillajo Garcia y Avila Pesantez, 2023). Un marco de ciberseguridad aplicado a las instituciones educativas virtuales no solo

mejoraría la seguridad de los datos de los sistemas, sino que también fortalecería la confianza de los usuarios en la seguridad de estas instituciones, promoviendo la presencia de un ambiente seguro y confiable en la educación en línea.(Taherdoost, 2022).

Planteamiento de la investigación (Fundamentación de la investigación)

La ciberseguridad en las instituciones educativas en línea es importante en la actualidad, debido al incremento de la complejidad en la educación y los desafíos que las instituciones enfrentan por el uso significativo de plataformas en línea y recursos digitales, ya que esto ha llevado a que las instituciones educativas sean más propensas a sufrir ataques cibernéticos y ha creado nuevas formas en las que estos ataques pueden ocurrir.

Los incidentes de ciberseguridad en las instituciones educativas virtuales, puede afectar al ecosistema tecnológico, incluso puede conllevar a la pérdida de datos sensibles como la información privada de alumnos y trabajadores. Es por esto que es de vital importancia abordar la ciberseguridad de manera precisas y efectiva en el ámbito educativo virtual.

Aunque existen algunas investigaciones relacionadas a la ciberseguridad en plataformas educativas, aún hacen falta estudios centrados en las necesidades particulares de las instituciones educativas virtuales. Debido a esto se presenta la posibilidad de realizar una aportación a la comunidad educativa en línea por medio del desarrollo de un marco de ciberseguridad que permita principalmente identificar amenazas y vulnerabilidades claves como la propuesta de recomendaciones prácticas para establecer e implementar un marco efectivo de ciberseguridad.

Formulación del problema de investigación

¿Cómo se puede desarrollar un marco de ciberseguridad para la Unidad Educativa Virtual Zúrich Science que permita mejorar la protección de datos y optimizar la detección de amenazas de sus activos digitales?

Objetivo General:

Desarrollar un marco de ciberseguridad para la Unidad Educativa Virtual Zúrich Science por medio de medidas tecnológicas y normativas para garantizar la seguridad de los activos digitales y la continuidad operativa de la institución.

Objetivos Específicos:

1. Analizar el entorno tecnológico para identificar vulnerabilidades y riesgos potenciales en cuanto a la protección de datos y la seguridad informática.
2. Implementar un sistema de detección de intrusos que utilice técnicas de inteligencia artificial para identificar patrones de actividad maliciosa en los activos de la institución.
3. Evaluar la efectividad y eficiencia del modelo de detección de mediante pruebas de penetración, simulaciones de ataques y análisis de incidentes.

Planteamiento hipotético

En la actualidad la ciberseguridad ha tomado fuerza en las instituciones educativas en línea debido al incremento de la complejidad en la educación y los desafíos que las instituciones enfrentan por el uso significativo de plataformas en línea y recursos digitales, ya que esto ha llevado a que las instituciones educativas sean más propensas a sufrir ataques cibernéticos y ha creado nuevas formas en las que estos ataques pueden ocurrir.

Los ataques cibernéticos a las instituciones educativas virtuales, puede afectar al ecosistema tecnológico, incluso puede conllevar a la pérdida de datos sensibles como la información privada de alumnos y trabajadores. Por este motivo es importante abordar la ciberseguridad de manera efectiva en el ámbito educativo en línea.

A pesar de que la información e investigaciones existentes sobre ciberseguridad en educación, aún hace falta un conocimiento que requiere estudios más detallados y específicos centrados en las necesidades particulares de las instituciones educativas en línea. Se presenta una oportunidad de contribuir significativamente a la comunidad educativa mediante el desarrollo de un marco de ciberseguridad que permita la identificación de amenazas y vulnerabilidades clave, así como la propuesta de recomendaciones prácticas para implementar marcos efectivos de ciberseguridad.

CAPÍTULO 1. MARCO TEÓRICO REFERENCIAL

1.1. Revisión de literatura

En la actualidad la digitalización de las instituciones educativas ha traído beneficios significativos, pero también ha incrementado la exposición a amenazas cibernéticas. Por este motivo la implementación de un marco de ciberseguridad sólido se vuelve imprescindible para asegurar la protección de los activos tecnológicos y la continuidad de las operaciones académicas y administrativas. La revisión de literatura realizada en esta sección se basó en la investigación de estudios recientes sobre ciberseguridad en entornos educativos.

Según menciona Farid et al. (2018), los sistemas de e-learning de las instituciones educativas enfrentan riesgos cibernéticos como: accesos no autorizados, ataques de denegación de servicio (DDoS) e inyecciones de Lenguaje de Consulta Estructurada (SQL). Estas amenazas provocan problemas de integridad, confidencialidad y disponibilidad de los sistemas educativos en línea, lo cual crea la necesidad de implementar medidas de ciberseguridad para evitar estas afectaciones a los sistemas.

Taherdoost (2022) enfoca la necesidad de verificar el cumplimiento de normas como las ISO/IEC 27001, ya que estas permiten identificar riesgos, implementar controles y monitorear la efectividad de las medidas de seguridad informáticas aplicadas. Adicional, menciona que la aplicación de estas normas mejora la confianza de estudiantes y personal en el uso de los sistemas de gestión educativas.

El estudio de Dioubate et al. (2022) implementa un marco de gestión de riesgo de ciberseguridad en las universidades públicas de Malasia, permitiendo identificar las prácticas que manejan estas universidades sobre la gestión de riesgos de ciberseguridad. Mediante la aplicación de entrevistas concluyó que es importante establecer estándares específicos para la gestión de riesgos y mejorar la capacitación en ciberseguridad de los usuarios pertenecientes a la institución. Además, destaca la importancia de aplicar una gestión efectiva para proteger a las instituciones educativas de amenazas cibernéticas.

Por otro lado, Syafrizal et al. (2020) se enfoca en la aplicación de aprendizaje automático con sistemas de detección de intrusiones (IDS) mediante el uso de algoritmos como Random forest para detectar las actividades maliciosas en las redes de las

instituciones. Los resultados muestran una reducción en los falsos positivos y un incremento en la precisión del sistema mejorando la capacidad de identificación de amenazas en tiempo real.

En el artículo de Wang et al. (2022), presenta un sistema llamado AI@NTDS para la detección de amenazas de red impulsado por inteligencia artifical que utiliza características de comportamiento y técnicas de inteligencia artificial para lograr una alta precisión en la detección de ataques de red. Este artículo se realizó bajo la siguiente metodología:

Recopilación y etiquetado de datos. Se obtuvo información de interacción del sistema Linux a través del honeypot Cowrie, la cual fue etiquetada según el marco MITRE ATT&CK para asegurar la credibilidad del conjunto de datos.

Extracción y evaluación. Para la extracción y evaluación de características este estudio extrajo cincuenta y dos características relevantes, las cuales incluyeron: mensajes, host y datos geográficos. Estas características fueron recabadas con la finalidad de detectar diferentes niveles de amenaza en la red.

Desarrollo y evaluación. En esta etapa de desarrollo se aplicaron algoritmos de inteligencia artificial como LightGBM, Random Forest y K-nearest neighbors (K-NN). Estos fueron utilizados para validar la precisión para la identificación de características y desarrollar un modelo de detección óptimo.

Evaluación de desempeño. El sistema AI@NTDS obtuvo los siguientes resultados: precisión del 99,20% y una puntuación F1 del 99,80%. Estos valores representaron una mejora del 4% en la precisión y del 1% en la puntuación F1 comparado con otros mecanismos de detección disponibles en la actualidad.

1.2. Desarrollo teórico y conceptual

1.2.1. Amenazas cibernéticas

Las amenazas cibernéticas son un reto actual para los desarrollares, debido a que estos se deben asegurar no solo de que los sistemas informáticos funcionen correctamente sino también de que estos sean seguros. Estas amenazas pueden provenir tanto de fuentes internas como externas, incluyendo ataques técnicos, naturales o humanos. Por este motivo es importante que las organizaciones identifiquen y evalúen estas amenazas para

comprender su impacto potencial y, así, implementar medidas de prevención efectivas que protejan los datos y sistemas ante posibles ataques (Humpiri Flores et al., 2023).

Con el avance de la tecnología, en la actualidad el crimen cibernético se ha incrementado en América Latina. Esto resalta la importancia de proteger los sistemas de información de las amenazas cibernéticas más comunes como lo son: los ataques, daños o accesos no autorizado (Quirumbay Yagual et al., 2022).

1.2.2. Vulnerabilidades

Las debilidades, fallos y configuraciones incorrectas en el hardware, software y redes informáticas hacen que los sistemas de información sean propensos a ataques, los cuales suelen ser aprovechados por piratas informáticos. Las vulnerabilidades en el software, la falta de protocolos de red y la falta de conocimientos de los usuarios sobre tecnología y sistemas de información contribuyen a los ciberataques debido a que dejan los sistemas desprotegidos (Aslan et al., 2023).

Las causas de las fallas de los sistemas se dividen en tres categorías: ataques causados por errores de hardware, ataques causados por errores de software y ataques causados por vulnerabilidades de red informática. Según Zare et al. (2018),las vulnerabilidades más comunes son las siguientes:

Desbordamiento de búfer (Buffer Overrun): Se refiere a la sobreescritura de posiciones en memoria debido a una mala validación de los tipos de datos y longitudes de los campos esperados en la capa de lógica del negocio o en la pasarela que conecta al acceso a datos. Esta vulnerabilidad es aprovechada por ataques de inyección y de denegación de servicio, donde los hackers pueden manipular los datos en el buffer para ejecutar código malicioso o causar la interrupción del servicio (Castellanos Bernal, 2017).

Entorno operativo (Operating Environment): Estas vulnerabilidades pueden incluir archivos del sistema, sistemas operativos, servicios proporcionados por el sistema operativo, cuentas de usuario, datos, aplicaciones y otros elementos del entorno. Es necesario primero clasificar los activos y verificar cuáles están vinculados este entorno (Torres Valero et al., 2020).

Agotamiento de recursos (Resource Exhaustion): Cuando se tienen un excedente al límite de los recursos a los que se puede acceder, esta vulnerabilidad genera una colisión y una asignación de recursos equivocada (Esteban y Jaramillo, 2020).

Actualización de software pospuesta (Postponing the Update of Software): La falta de actualizaciones puede dejar a los sistemas vulnerables, ya que, la ausencia de estas puede no contener parches importantes o puede no tener restricción privilegios de usuarios administrativos (Zare et al., 2018).

Falta de respaldo para activos y servicios críticos (Lack of Backup for Critical Assets and Services): Es importante contar con respaldos, debido a que por medio de un ataque malicioso o por medio de accesos no autorizados se podría perder información de manera irrecuperable generando pérdidas para la organización (Serna Ramírez et al., 2022).

Falta de protección para activos y servicios portátiles (Lack of Protection for Portable Assets and Services): Los activos en una organización deben de estar protegidos para de esta manera poder evitar pérdida o hurto de información y de esta manera poder mantener los datos de mayor relevancia lo más seguro posibles (Zare et al., 2018).

Personal no autorizado y ataques internos (Unauthorized Staff and Attacks from Inside): Los usuarios con acceso o con información de acceso internos al sistema y seguridad pueden perpetuar las políticas de seguridad de la organización, los cuales pueden llevar a la destrucción, divulgación, modificación de datos y negación del servicio. Por lo que es necesario restringir los recursos críticos según el nivel de accesibilidad para cada miembro de la organización (Alines Villegas, 2021).

Seguridad físico-cibernética insuficiente para sistemas de monitoreo remoto (Insufficient Physical-Cyber Security for Remotely Monitoring Systems): Los sistemas de monitoreo remoto, como los sistemas de electricidad y seguridad, presentan vulnerabilidades a diferentes tipos de ataques maliciosos. Es necesario proteger estos sistemas con controles de seguridad y evaluar los riesgos y vulnerabilidades tanto físicas como en las redes (Zare et al., 2018).

1.2.3. Medidas de seguridad

La implementación de medidas de seguridad debe ser cuidadosamente planeada y basada en la lógica, evitando gastar esfuerzos y recursos en áreas que no lo necesitan.

Para que estas medidas y mecanismos de protección sean efectivos, deben formar parte de un sistema más grande de gestión de la seguridad de la información. Es importante asegurarse que cada elemento del sistema pueda garantizar la protección adecuada de los datos y la información (Édison et al., 2017).

Diversos estudios han destacado la importancia de las medidas de seguridad en los sistemas de información.(Blanco Rodríguez et al., 2018) y (Herrera Olivares et al., 2020) destacan la necesidad de materiales prácticos y de un marco de gestión, respectivamente, para garantizar la seguridad de los sistemas de información. De manera similar, (Arévalo-Cordovilla et al., 2020) mencionan las vulnerabilidades que pueden presentar los sistemas de información y el impacto que estas pueden generar tanto en las organizaciones como en los usuarios, concluyendo que la implementación de medidas de seguridad es importante en estos sistemas.

1.2.4. Normativas y Estándares de ciberseguridad

Las normativas y estándares de ciberseguridad son fundamentales para garantizar la protección de los sistemas digitales y la información confidencial. El cumplimiento de estas normas puede lograrse de diversas maneras, adaptándose a la tecnología utilizada y a las necesidades específicas de cada empresa. Estas normativas suelen establecer un conjunto mínimo de medidas de seguridad que las organizaciones debería de aplicar para proteger sus activos tecnológicos de manera efectiva (Srinivas et al., 2019).

Los estándares de ciberseguridad cubren desde algoritmos de cifrado hasta la integridad de aplicaciones como navegadores web y de la seguridad de la información. Es importante que estas normas sean prácticas, económicas y adaptables a las limitaciones técnicas y de recursos de los usuarios que las utilizan. Además, deben cumplir requisitos de verificación para permitir a los usuarios autoevaluar la calidad y solidez de la seguridad, incluida su compatibilidad con otras actividades de verificación de seguridad (Syafrizal et al., 2020).

Las normas de ciberseguridad se clasifican generalmente en dos categorías principales: normas de seguridad de la información y normas de gobernanza de la seguridad de la información. Las normas y marcos de seguridad de la información se centran en cuestiones de seguridad, como la serie ISO 27001, ISF SOGP, la serie NIST 800, SOX y Risk IT (Taherdoost, 2022).

La norma ISO/IEC 27001 establece requisitos para establecer, implementar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI) dentro del contexto de los riesgos generales de la organización (Taherdoost, 2022).

1.2.5. Marco de ciberseguridad

La ciberseguridad es esencial para proteger los datos de una organización, debido a que las amenazas evolucionan día a día adaptándose a las defensas cibernéticas. Por este motivo es crucial contar con soluciones actualizadas que mantengan la confidencialidad, disponibilidad e integridad de la información, actualizando regularmente las políticas de ciberseguridad y la capacitación de los empleados. Los marcos de ciberseguridad ofrecen una estructura basada en fases para garantizar la protección de activos, planificación de respuestas y enseñanza de prácticas recomendadas referente a la ciberseguridad. Estos marcos permiten facilitar la gestión de riesgos cibernéticos y asegurar el cumplimiento de normativas dentro de las instituciones(Toussaint et al., 2024).

Un marco de ciberseguridad es fundamental para garantizar una protección efectiva frente a amenazas cibernéticas, ya que abarcan la definición del alcance, la implementación y los procesos de evaluación necesarios para proteger activos digitales críticos. Las organizaciones pueden utilizar estos marcos como guías para implementar normas de ciberseguridad de manera exitosa, mejorando así su capacidad para identificar, detectar y responder a ciberataques de manera más eficiente (Taherdoost, 2022).

Así mismo, un marco de ciberseguridad incluye normas voluntarias y mejores prácticas consensuadas, buscando armonizar enfoques políticos, empresariales y tecnológicos en la gestión de la ciberseguridad. Un ejemplo de esto es el Marco de Ciberseguridad del NIST, el cual está compuesto de tres elementos principales: el marco básico, el nivel de implementación y el perfil del marco. Dentro de este marco incluye funciones esenciales como: identificar, proteger, detectar, responder y recuperar. De esta manera proporciona a las organizaciones una guía detallada para mejorar sus medidas de seguridad cibernética (Syafrizal et al., 2020).

1.2.6. Amenazas y vulnerabilidades en instituciones educativas en línea

Los usuarios que usan las plataformas en línea para el ámbito de educación pueden llegar a tener varios riesgos, ataques o amenazas. Tanto como a docentes, los alumnos, y

el administrador sus datos residen en ubicaciones físicas y lógicas dispersas e Internet ya que este es el único medio de su conectividad, lo que dificulta difícil aplicar el mecanismo de seguridad de la información. Según Farid et al. (2017) con el uso de estas plataformas, redes o servidores podemos tener las siguientes vulnerabilidades:

Vulnerabilidades de autenticación: Las plataformas de aprendizaje en línea pueden ser vulnerables a ataques de fuerza bruta, donde un atacante intenta adivinar o descifrar las credenciales de inicio de sesión de los usuarios. También pueden ser vulnerables a ataques de suplantación de identidad, donde un atacante se hace pasar por un usuario legítimo (Farid et al., 2017).

Acceso no autorizado. Los sistemas pueden presentar errores que facilitan a los atacantes acceder a información sin autorización.

Protección de datos. Debido a que estos sistemas manejan una gran cantidad de datos personales y académicos, los sistemas necesitan implementar medidas que eviten filtraciones de datos o violaciones de privacidad. La falta de estas medidas puede poner en riesgo la integridad de los sistemas y de los usuarios (Farid et al., 2017).

Comunicación. Cuando las plataformas permiten comunicarse entre usuarios sin una correcta implementación de medidas de seguridad los sistemas se vuelven vulnerables a ataques de ingeniería social.

Infraestructura subyacente. Los activos de mayor vulnerabilidad a ataques cibernéticos son los activos tecnológicos como: servidores, redes y sistemas operativos, ya que si no se encuentran protegidos pueden ser objeto de ataques como malware, ataques de denegación de servicio (DDoS) o accesos no autorizados (Farid et al., 2017).

1.2.7. Técnicas para detección de vulnerabilidades

(Laura y Saucedo, 2015) resume varias técnicas para la detección de vulnerabilidades las cuales se muestran a continuación:

Black-box. Esta técnica se utiliza comúnmente para identificar en aplicaciones web, mediante simulaciones de posibles escenarios (Laura & Saucedo, 2015).

White-box. Permite tener acceso a la información del servidor para realizar un análisis completo de las posibles fallas que puedan ocurrir desde el lado del servidor (Laura & Saucedo, 2015).

Análisis estático de código. Este método realiza un análisis directo al código fuente, lo cual permite determinar fallas de seguridad.

Análisis dinámico de código. Para identificar vulnerabilidades se comunica por medio del frontend con la aplicación web para identificar vulnerabilidades y debilidades de la aplicación web.

Pruebas de penetración. Consisten en simular ataques realizados por actores externos no autorizados y personas internas con acceso legítimo al sistema. Este proceso implica un análisis activo para identificar vulnerabilidades potenciales que puedan surgir debido a configuraciones incorrectas, fallos en el hardware o software (conocidos o desconocidos), o errores operativos en los procesos o en la implementación de contramedidas técnicas (Carolina et al., 2021).

Pruebas pasivas: Las pruebas pasivas son utilizadas en el tráfico de telecomunicaciones, lo cual permite detectar fallas y defectos de seguridad mediante el examen de paquetes capturados.

Pruebas activas: Para el desarrollo de las pruebas activas el encargado desarrolla subprocesos para verificar si las advertencias realizadas por un análisis predictivo son precisas.

Fuzz testing (pruebas de caja negra): Consiste en estimular el sistema bajo prueba, utilizando datos aleatorios o mutados queridos, con el fin de detectar comportamientos no deseados como violación de confidencialidad (Laura & Saucedo, 2015).

1.2.8. Técnicas para detección de vulnerabilidades

La detección de vulnerabilidades en los sistemas de información es una acción importante para garantizar la seguridad informática de las organizaciones. Sin embargo, aunque se implementen controles de seguridad, aún existe la posibilidad de que existan vulnerabilidades que comprometan la protección de aplicaciones, redes, o servidores (Marsal Giménes y Monges Olmedo, 2019). Estas brechas de seguridad pueden ser aprovechadas por diversas amenazas como: abusos, errores y robos (Arévalo-Cordovilla et al., 2020). Por lo tanto, es fundamental contar con un enfoque estructurado para gestionar estas vulnerabilidades y posibles incidentes informáticos (Marsal Giménes y Monges Olmedo, 2019).

La gestión de vulnerabilidades se refiere al proceso de identificar, evaluar, mitigar y controlar las vulnerabilidades en sistemas de información, redes y aplicaciones. A continuación, se detalla algunos puntos y técnicas relevantes para la detección de vulnerabilidades:

Identificación de vulnerabilidades. La identificación de vulnerabilidades consiste en identificar las vulnerabilidades y amenazas de las que posteriormente se identificaran los riesgos asociados a los activos de información previamente registrados o inventariados. Para identificarlos se pueden utilizar herramientas de escaneo de vulnerabilidades que buscan debilidades conocidas en el software y la configuración (Camilo et al., 2023).

Evaluación de riesgos. Luego de identificar las vulnerabilidades, se procede a realizar la identificación de los riesgos de los activos de información, análisis del riesgo y la valoración de estos (Camilo et al., 2023).

Priorización de vulnerabilidades. Es importante clasificar las vulnerabilidades ya que no todas van a requerir la misma atención; se deben clasificar según la magnitud de impacto y la relevancia de sistemas afectados (Guevara-Vega et al., 2023).

Mitigación y corrección. Una vez que se determina el nivel de prioridad de las vulnerabilidades, es necesario aplicar medidas que permitan minimizar los riesgos o corregir los problemas identificados en los sistemas de información. Estas correcciones pueden incluir la implementación de parches de software, configuraciones de seguridad, actualizaciones de sistemas, y cambios en políticas y procedimientos (Pargaonkar, 2023).

Monitoreo continuo. Tal como los ataques evolucionan y las vulnerabilidades se hacen presentes es necesario realizar un monitoreo constante para identificar nuevas vulnerabilidades, evaluar riesgos actualizados y tomar medidas correctivas según sea necesario (Pargaonkar, 2023).

1.2.9. Sistemas de detección de intrusiones (IDS)

Los sistemas de detección de intrusiones son sistemas que permiten detectar ataques cibernéticos mediante un tráfico de red comparándolo con ataques cibernéticos conocidos (Caizapanta González, 2022). Estos sistemas pueden clasificarse en diferentes tipos: en función del sistema que monitorea y en función de cómo se implementan, en el caso de los sistemas que monitorea podemos distinguir entre los sistemas que analizan la

actividad en red (NIDS) y los sistemas que monitorizan la actividad de terminales determinados (HIDS) (Bono et al., 2022).

Los sistemas de detección de intrusos (IDS) Open Source contienen una lista de registros de ataques clasificados, algunos de estos se actualizan por Internet. La principal función de estos sistemas es detectar eventos sospechosos en el sistema donde se encuentre configurado en tiempo real, realizando de esta manera un monitoreo en estos sistemas para la detección de intrusos o intento de ataques (Farro Cachay, 2019).

Los sistemas de detección de intrusiones se desarrollan utilizando diferentes enfoques. Los IDS deberían ser capaces de detectar intrusiones, especialmente las cuatro categorías principales de ataques (Denegación de servicio (DoS), de usuario a raíz (U2R), de remoto a usuario (R2L) y sondeo). Los distintos enfoques de detección de intrusiones tienen sus puntos fuertes y sus limitaciones. El enfoque de aprendizaje automático es un proceso automatizado que casi no requiere intervención humana lo cual lo vuelve más eficaz (Aludhilu, 2020).

1.2.10. Snort

Snort, desarrollado en 2010 por la fundación estadounidense Open Information Security Forum (OISF), introdujo un diseño multihilo con el propósito de optimizar el análisis del tráfico de red y superar las limitaciones de rendimiento asociadas a las arquitecturas de un solo hilo (Abd et al., 2023).

Snort es un sistema de código abierto que permite describir la actividad de la red reflejando la actividad maliciosa por medio de una secuencia de reglas o políticas definidas por los usuarios (Jain y Anubha, 2021). Estas reglas de detección de Snort son el núcleo del proceso de captura. Snort verifica en tiempo real si los paquetes recibidos tienen características similares a las de alguna regla determinada y activa una alarma si esta coincide (Shuai y Li, 2021).

1.2.11. Graphical Network Simulator-3 (GNS-3)

GNS-3 es un emulador de software para redes complejas, lanzado en 2008 (Guimarães et al., 2020). GNS-3 es una herramienta que permite probar configuraciones, simular escenarios diversos y prever posibles fallas antes de la implementación real (Chillagana et al., 2023). También permite la integración con dispositivos físicos y máquinas

virtuales, lo que facilita la creación de una red troncal simulada. Su principal ventaja radica en su capacidad de extensibilidad (Han, 2021).

CAPÍTULO 2. METODOLOGÍA

2.1. Contexto de la investigación

Este trabajo de investigación aborda la necesidad de proteger los datos del entorno tecnológico de las instituciones educativas virtuales. Principalmente esta investigación se centra en la Unidad Educativa Zúrich Science, ubicada en Quevedo, Ecuador. Esta necesidad surge ya que la institución presenta desafíos en el área de seguridad informática como: falta de protección de datos, prevención de ataques y continuidad operativa.

Debido a lo mencionado en el párrafo anterior, la Unidad Educativa Virtual Zúrich Science debe proteger sus activos tecnológicos frente a ataques cibernéticos por medio de un marco de ciberseguridad que permita identificar, evaluar y gestionar los riesgos cibernéticos de manera óptima y efectiva. Dado que la institución maneja gran cantidad de información, la falta de medidas de seguridad puede comprometer la integridad, confidencialidad y disponibilidad de sus activos y datos.

Actualmente la Unidad Educativa Zúrich Science no posee de un marco de ciberseguridad que principalmente permita la detección avanzada de amenazas. El crecimiento de las amenazas cibernéticas hace que sea esencial contar con sistemas que no solo pueda identificar y responder a ataques, sino que permita prevenir ataques mediante la identificación de patrones de comportamiento malicioso. Esto puede lograrse mediante la implementación de un sistema de detección de amenazas basados en inteligencia artificial.

El objetivo de esta propuesta es diseñar, implementar y evaluar un marco de ciberseguridad para la Unidad Educativa Zúrich Science utilizando principalmente una herramienta de detección de intrusiones combinada con un modelo de inteligencia artificial. Con el fin de proteger, garantizar y mejorar la capacidad de la institución para detectar amenazas de seguridad informática en un entorno digital.

Este proyecto se lleva a cabo en un entorno simulado replicando las configuraciones y elementos que se manejan en la institución. Este entorno este compuesto de redes, servidores y dispositivos. Se propone el uso de una herramienta de detección de ataques basado en inteligencia artificial y se evalúa su efectividad por medio de ataques simulados

que son calificados bajo métricas como: intentos de intrusión, tiempos de intrusión, tiempo medio entre fallos y tiempo medio de contención.

Los elementos principales del entorno simulado son:

- Red Local: Compuesta por máquinas que representan a los diferentes departamentos, conectadas por un switch y un router central, simulando el tráfico de datos dentro de la unidad.
- Servidor Central: Donde se almacenan y procesan datos críticos de la institución.
- Conectividad Wi-Fi: Usada por los dispositivos dedicados a la enseñanza y el acceso a las tecnologías de la información.
- Máquina Kali Linux: Actuando como atacante para ejecutar simulaciones de ataques y pruebas de penetración.
- Herramientas de Monitoreo y Detección: Snort3 con un modelo Machine Learning.
- Computadores.
- Plataformas educativas basadas en WordPress y Moodle: los cuales pueden comprometer la seguridad de los datos sensibles.

2.2. Diseño y alcance de la investigación

El diseño de esta investigación se basa en un enfoque experimental y cuantitativo, ya que se desarrollaron actividades prácticas con el fin de diseñar e implementar medidas de seguridad informática. Estas medidas se diseñaron mediante la evaluación del impacto en la protección de la información y la continuidad de las operaciones. Además, se analizó la efectividad de un sistema de detección de amenazas compuesto de una herramienta de detección de intrusos (IDS) y un modelo de inteligencia artificial, mediante un análisis estadístico para evaluar su desempeño.

El desarrollo del marco de ciberseguridad para la Unidad Educativa Virtual Zúrich Science incluye aspectos claves como: la identificación de activos digitales en la institución, abarcando hardware, software y redes. Luego, se realiza una simulación de ataque implementando un sistema de detección de amenazas con Inteligencia artificial y por último este se debe evaluar para obtener su nivel de efectividad. Estos pasos son

fundamentales para garantizar la protección de los activos digitales y la seguridad de la información en la Unidad Educativa Virtual Zúrich Science.

2.3. Tipo y métodos de investigación

El tipo de investigación para el desarrollo de un marco de ciberseguridad para la Unidad Educativa Virtual Zúrich Science es mixto, ya que combina enfoques cuantitativos y cualitativos. Este enfoque mixto se debe a la complejidad que requiere implementar medidas de ciberseguridad, donde es necesario emplear datos cuantitativos para evaluar los riesgos y medir la efectividad de las medidas implementadas, y datos cualitativos que permitan entender el contexto e impresiones de los usuarios involucrados.

Para el método de investigación se aplica el método hipotético-deductivo y el método analítico. El método hipotético-deductivo se aplica en la etapa de diseño del marco de ciberseguridad, permitiendo plantear hipótesis sobre las medidas más efectivas para identificar riesgos y probarlas en un entorno controlado. El método analítico se emplea para analizar las amenazas y vulnerabilidades específicas de la unidad educativa, así como para evaluar la efectividad de las medidas propuestas.

Además, se utilizarían otros métodos como la revisión bibliográfica y la consulta a expertos en ciberseguridad para obtener información relevante y actualizada sobre mejores prácticas y tendencias en este campo.

2.4. Población y muestra

Tomando en cuenta que esta investigación se llevará a cabo una parte en la Unidad Educativa Virtual Zúrich Science y otra parte de esta en un entorno simulado el cual replica la infraestructura tecnológica de la Unidad Educativa Virtual Zúrich Science, este apartado está enfocado a los elementos tecnológicos y humanos que conforman la institución.

2.4.1. Tamaño de la población

La población en este contexto comprende actores humanos y tecnológicos que son parte fundamental de la Unidad Educativa Zurich Science.

Para los actores humanos como población tenemos: 21 estudiantes, 12 profesores, y 5 personas en el personal administrativo. De esta manera la población total de actores

humanos corresponde a 38 personas, las cuales interactúan regularmente con la infraestructura tecnológica y sistemas de la institución.

Para la parte de la población correspondiente a los elementos tecnológicos se tomaron en cuenta los servidores, dispositivos y sistemas, los cuales se detallan a continuación:

Servidor principal. Este servidor fue identificado con la IP 192.168.226.x, tiene como función almacenar y gestionar la información de la institución como: registros académicos, información personal de los estudiantes, y sistemas de gestión educativa.

Dispositivos de Red. Los dispositivos de red incluyeron routers y switches, los cuales son los que permiten la conexión de dispositivos de los departamentos de la institución incluidos (Docentes, Secretaría, Administración).

Máquinas de usuarios. Representan a los departamentos de Docentes (192.168.30.x), Secretaría (192.168.30.x), y Administración (192.168.30.x), estos simulan las estaciones de trabajo que acceden a los recursos educativos y administrativos en la red de la unidad educativa.

2.4.2. Muestra de estudio

En este caso la muestra incluye tanto actores humanos como escenarios simulados de ciberataques a el servidor principal el cual almacena los datos principales de la Unidad Educativa con el fin de evaluar la capacidad de detección del sistema propuesto.

Para el cálculo de la muestra de los actores humanos se utilizó la siguiente fórmula:

$$n_h = \frac{n \times N_h}{N}$$

Donde:

n_h es el tamaño de la muestra en el estrato h.

n es el tamaño total de la muestra que se desea seleccionar (10 estudiantes).

N_h es el tamaño total del estrato h en la población (número de estudiantes en cada nivel).

N es el tamaño de la población.

Entonces:

Para secundaria: $n_{secundaria} = \frac{10 \times 4}{38} = 1{,}05$, se redondea este resultado a 1 estudiante.

Para bachillerato: $n_{bachillerato} = \frac{10 \times 17}{38} = 4{,}74$, se redondea este resultado 5 estudiantes.

Para profesores: $n_{profesores} = \frac{10 \times 12}{38} = 3{,}16$, se redondea este resultado a 3 profesores.

Para personal administrativo: $n_{administrativo} = \frac{10 \times 5}{38} = 1{,}32$, se redondea este resultado a 1 personal administrativo.

Para las simulaciones de los diferentes escenarios se ejecutaron varios ciberataques al servidor en un entorno controlado. Estos ataques correspondieron a las categorías que se detallan a continuación:

Exploits de Vulnerabilidades. Se llevaron a cabo diferentes pruebas de penetración utilizando Kali Linux para explotar vulnerabilidades en los sistemas de red y servidores.

Ataques de Denegación de Servicio (DDoS). Se simularon ataques que intentan sobrecargar los servidores o dispositivos de red para hacerlos inoperantes.

Ataques de Fuerza Bruta. Se realizaron ataques de fuerza bruta para detector usuarios y contraseñas para poder acceder al servidor.

2.5. Técnicas e instrumentos de recolección de datos

Se utilizó una técnica mixta de recolección de datos, integrando métodos cuantitativos y cualitativos, lo cual permitió obtener una visión clara tanto desde los aspectos técnicos como humanos de la Unidad Educativa Virtual Zúrich Science.

2.5.1. Técnicas cuantitativas

Pruebas técnicas en el entorno simulado. Se desarrollaron simulaciones en un entorno que replicó la infraestructura tecnológica de la Unidad Educativa Zurich Science. Dichas pruebas facilitaron la evaluación de la efectividad del marco de ciberseguridad planteado. En la Tabla 1 se detalla las técnicas utilizadas:

Tabla 1 Técnicas de análisis de seguridad

Técnica	Descripción	Instrumento	Métricas por evaluar
Pruebas de Penetración (Penetration Testing)	Simulación de ataques a la red para identificar vulnerabilidades y explotarlas.	Nmap	Intentos de intrusión, tiempos de intrusión, vulnerabilidades explotadas.
Simulaciones de Ataques (Attack Simulations)	Simulaciones de ataques como DDoS, inyección SQL y fuerza bruta.	Hydra, SqlMap	Tiempos de respuesta, amenazas detectadas, tiempo medio de contención (MTTC).
Análisis de Tráfico de Red	Análisis de tráfico en la red para detectar patrones sospechosos.	Snort3, Machine Learning	Tiempos de intrusión, porcentaje de falsos positivos.
Análisis Post-Incidente	Evaluación de los incidentes tras las simulaciones ejecutadas.	Reportes de incidentes generados	Tiempo medio de contención (MTTC).
Evaluación Comparativa	Comparación de la efectividad del marco de ciberseguridad en diferentes tipos de ataques.	Reportes generados tras las simulaciones	Comparación entre tiempos de intrusión, tiempo medio entre fallos (MTBF), tiempos de mitigación.

Encuestas cuantitativas. Se desarrolló un cuestionario estructurado para recopilar datos cuantitativos sobre las prácticas y experiencias de los usuarios en relación con la ciberseguridad. Las secciones incluidas en el cuestionario fueron: Conocimientos y conciencia sobre ciberseguridad, prácticas de seguridad en línea, percepción de amenazas

cibernéticas, experiencias con incidentes de seguridad, colaboración y educación en ciberseguridad.

2.5.2. Técnicas cualitativas

Entrevistas semiestructuradas. Para complementar los datos cuantitativos, se llevó a cabo entrevistas cualitativas dirigidas principalmente a profesores y personal administrativo. Dichas entrevistas se enfocaron en explorar aspectos como: percepción de riesgos y amenazas cibernéticas, cultura de ciberseguridad y conciencia de la institución, desafíos y barreras para la implementación de medidas de seguridad, experiencia y mejores prácticas en el uso de herramientas y protocolos de seguridad. Estas entrevistas proporcionaron un enfoque más profundo sobre las actitudes y comportamientos de los usuarios frente a las amenazas de ciberseguridad.

2.5.3. Simulación y generación de datos

Además de la información obtenida por medio de encuestas y entrevistas, se generaron datos técnicos para entrenar y evaluar un modelo de detección de intrusiones con aprendizaje automático. A continuación, se detallan las fases llevadas a cabo para la simulación y generación de datos.

Recolección de Datos para el entrenamiento del modelo. En este apartado se muestra el proceso para recopilar los datos necesarios para posteriormente evaluar y validar el modelo de machine learning implementado. Para el desarrollo del modelo de machine learning se utilizaron diferentes herramientas para generar y capturar datos precisos, los cuales se presentan en los siguientes apartados.

Para la recolección de datos, se empleó Snort 3 para detectar intrusiones y generar alertas en tiempo real. Hydra se utilizó para simular ataques de fuerza bruta y evaluar la resiliencia del sistema de autenticación. Nmap permitió identificar servicios abiertos y vulnerabilidades específicas en los servidores de prueba. En la Figura 1 se representa este proceso.

Figura 1. Generación y recolección de datos

Técnica de simulación de tráfico. Para generar datos relevantes de escenarios reales en la red simulada de la Unidad Educativa Zúrich Science se utilizó la simulación de tráfico de red, al aplicar esta técnica se pudo producir tráfico maligno y benigno para poder entrenar y evaluar el modelo de detección desarrollado.

Para el tráfico benigno se utilizó herramientas manuales que simulan actividades comunes en entornos educativos como: navegación web y transferencia de archivos. Estas herramientas se detallan en la Tabla 2.

Tabla 2. Simulación de tráfico benigno

Herramienta	Descripción	Escenario
Ping	Simuló solicitudes ICMP para diagnosticar conectividad.	Verificar la disponibilidad de servidores en la red.
Curl	Realizó solicitudes HTTP y HTTPS a servidores locales y remotos.	Simulación de acceso a plataformas educativas y servidores web.

En contraste para simular ciberataques y generar tráfico malicioso se utilizaron herramientas diseñadas para simular actividades maliciosas y detección de vulnerabilidades para generar ataques como se detalla en la Tabla 3.

Tabla 3. Simulación de tráfico maligno

Herramienta	Descripción	Escenario
Hydra	Ataques de fuerza bruta contra servicios como SSH y HTTP.	Intentos no autorizados de acceso a sistemas críticos.
Slowloris	Ataques DoS (Denegación de Servicio) mediante conexiones HTTP lentas.	Saturación del servidor web de la institución.
Nmap	Escaneo de puertos y detección de vulnerabilidades.	Identificación de servicios y puntos débiles en servidores.
Sqlmap	Inyección SQL para acceder y manipular bases de datos.	Explotación de un servidor WordPress simulado.
Hping3	Simuló ataques DoS mediante paquetes TCP/UDP anómalos.	Sobrecarga de recursos en la red.

Registro de datos: Snort3. El sistema de detección de intrusiones (IDS) Snort 3 fue configurado para registrar eventos en tiempo real y generar datos en formato JSON. Estos datos sirvieron como base para entrenar y evaluar el modelo de detección.

Para la generación de estos datos se seleccionaron campos los siguientes campos: src_port, dst_port, proto, msg, timestamp, pkt_num pkt_len, src_addr, sservice, rule, priority, class, action, b64_data. Esta configuración se llevó a cabo dentro del archivo

snort.lua del servidor como se muestra en la Figura 2. La salida que se generó en el archivo .txt se muestra en el Anexo 1.

```
alert_json = {
    file = true,
    fields = 'src_port dst_port proto msg timestamp pkt_num \
    pkt_len src_addr service rule priority \
    class action b64_data',
    limit = 50
}
```

Figura 2. Registro de datos

Procesamiento y etiquetado de datos. Los datos recopilados en el servidor por Snort3 se transformaron y etiquetaron por para construir el conjunto de datos para entrenar y evaluar el modelo de aprendizaje automático como se refleja en la Figura 3.

Para procesar el archivo con los datos recopilados por Snort3 se utilizó un script de Python mostrado en el Anexo 2, por medio de este de generó un archivo CSV estructurado con las columnas src_port, dst_port, protocol, label. En la columna label(etiqueta) se usó un editor de archivos en el servidor para etiquetar el tráfico normal (1) y el tráfico malicioso (-1) de manera manual.

Figura 3 Procesamiento y etiquetado de datos

2.6. Procesamiento de la evaluación: Validez y confiabilidad de los instrumentos aplicados para el levantamiento de información.

2.6.1. Validación de los Instrumentos

Antes de proceder con la ejecución de las simulaciones y pruebas, es fundamental validar los instrumentos y técnicas para asegurar que los resultados sean fiables y

precisos. Esto implica verificar que las herramientas utilizadas (como Kali Linux, Snort, Servidor Ubuntu) funcionen correctamente en el entorno simulado y que las simulaciones representen fielmente amenazas reales.

Pruebas Piloto: Se realizaron pruebas piloto para verificar que los instrumentos y herramientas funcionan de acuerdo con lo esperado. Estas pruebas ayudaron a identificar posibles errores o ajustes necesarios en el entorno simulado antes de realizar las simulaciones de ataques más complejas.

Para el desarrollo de estas pruebas una vez realizada las respectivas conexiones y configuraciones en el entorno simulado, desde la máquina atacante se realizó la comunicación a los distintos dispositivos conectados a la red, para comprobar que el entorno simulado funcionaba correctamente, en la Figura 4 se representa este proceso.

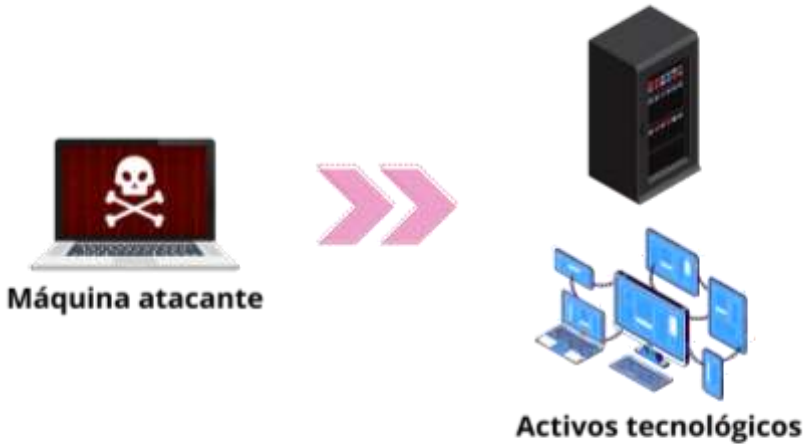


Figura 4 Pruebas Piloto

Revisión por Expertos: Se llevó a cabo una revisión por expertos en ciberseguridad para evaluar la pertinencia de las herramientas y métodos empleados en la investigación, asegurando que sean adecuados para el tipo de pruebas y simulaciones a realizar.

2.6.2. Análisis de los Datos

Una vez que se haya recopiló la información a través de las simulaciones, se realizó el análisis de los datos patrones de actividad maliciosa, evaluar el desempeño del sistema de detección de amenazas y medir la eficacia general del modelo.

Análisis Cuantitativo: Se aplicaron técnicas estadísticas para analizar los datos generados en las simulaciones como: tiempos de intrusión, amenazas detectadas y tiempos de respuesta. Este análisis permitió evaluar la eficiencia del modelo de detección de amenazas desarrollado.

Análisis Post-Incidente: Los ataques generados durante la fase de simulaciones fueron analizados para identificar qué tan rápido y preciso el sistema respondió a cada uno de estos.

2.6.3. Confiabilidad de los Resultados

La confiabilidad de los resultados obtenidos fue verificada por medio de pruebas estadísticas que permitieron verificar la consistencia de los datos obtenidos en las simulaciones. Se utilizaron diferentes métricas para evaluar que las mediciones reflejaran el comportamiento del sistema bajo condiciones reales de ataque.

2.6.4. Interpretación de Resultados

Finalmente, los datos fueron interpretados en el contexto del marco de ciberseguridad implementado. Se evaluó la eficacia del sistema en términos de detección, contención y mitigación de amenazas.

Identificación de Fortalezas y Debilidades: A partir de los resultados obtenidos, se identificaron los puntos fuertes del sistema y las áreas que requieren mejoras. En la Tabla 4 se detallan los aspectos evaluados, resultados, fortalezas, debilidades, y sugerencias de mejora.

Tabla 4 Interpretación de resultados

Aspecto Evaluado	Resultados	Fortalezas Identificadas	Debilidades Detectadas	Sugerencias de Mejora
Detección de Amenazas	96% de precisión en la detección de amenazas como fuerza bruta e	Algoritmo para identificar patrones maliciosos. Alta	Los Falsos positivos generan alertas innecesarias.	Ajustar el modelo para reducir falsos positivos.

	inyecciones SQL. Falsos positivos en el 3% de los casos.	sensibilidad en detección.		
Mitigación de Impactos	Disponibilidad del 98% en sistemas críticos durante simulaciones de ataque.	Continuidad operativa. Estructura robusta frente a interrupciones críticas.	Falta de redundancia en algunos componentes críticos. Dependencia de hardware con limitada capacidad de carga.	Invertir en infraestructura redundante para sistemas críticos. Mejorar la capacidad de los componentes existentes mediante actualizaciones tecnológicas.
Capacitación del Personal	Personal con poco o nada de conocimientos básicos de ciberseguridad. Respuesta limitada a incidentes complejos.	Concienciación inicial sobre seguridad informática presente.	Falta de conocimiento especializado en manejo de incidentes avanzados. Dependencia de equipos externos para soporte en casos críticos.	Implementar programas regulares de capacitación en ciberseguridad. Realizar simulacros periódicos de incidentes para entrenar al personal.

Infraestructura Tecnológica	Sistemas operativos y aplicaciones actualizados parcialmente. Ausencia de redundancia en hardware crítico.	Infraestructura básica funcional. Sistemas clave operativos en la mayoría de los casos.	Riesgo de interrupciones debido a falta de respaldo. Uso limitado de herramientas avanzadas como firewalls de última generación.	Implementar redundancia en hardware crítico. Incorporar tecnologías avanzadas como firewalls de próxima generación y autenticación multifactor.

CAPÍTULO 3. RESULTADOS Y DISCUSIÓN

3.1.Análisis del entorno tecnológico y la infraestructura de la Unidad Educativa Virtual Zúrich Science

Para identificar y evaluar los activos tecnológicos de la Unidad Educativa Virtual Zúrich Science, se llevó a cabo un inventario de los activos tecnológicos principales. Posteriormente se clasificó los activos que pueden ser afectados directamente a la confidencialidad, integridad y disponibilidad de la información, conforme a las normas ISO 27001.

3.1.1. Inventario de Activos Tecnológicos:

En este apartado se registraron todos los activos tecnológicos, incluidos servidores, redes, dispositivos de almacenamiento y aplicaciones de la Unidad Educativa Virtual Zúrich Science. En la Figura 5 se muestra una visión general de los elementos tecnológicos de la Unidad Educativa Virtual Zúrich Science. Por otro lado, en la Tabla 5 se detallan estos activos tecnológicos mecionados con su respectiva información.

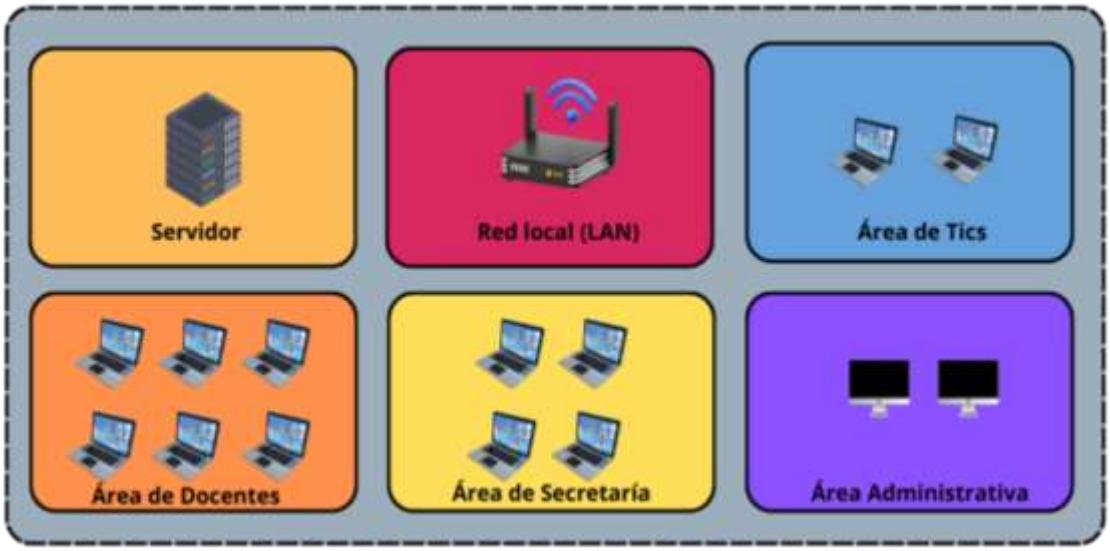


Figura 5 Elementos tecnológicos

Tabla 5 Inventario de activos tecnológicos

ID del Activo	Categoría	Descripción	Marca/ Modelo	Número de Serie	Dirección IP/MAC	Ubicación Física/Virtual	Fecha de Adquisición	Estado	Responsable
001	Red	Router Principal	Cisco ISR 4331	XYZ987654321	IP: 192.168.1.1 / MAC: 01:2B:3C:4D:5E:6F	Sala de Comunicaciones	2021-11-20	Operativo	Departamento de TI
002	Almacenamiento	Servidor	Synology DS920+	NAS567890123	IP: 192.168.226.x / MAC: 02:3C:4D:5E:6F:7A	Sala de Servidores	2023-03-01	Operativo	Departamento de TI

003	Software	Sistema de Gestión Académica	Moodle	-	N/A	https://campus.zurichscience.com/	2023-02-01	Activo	Departamento de TI
004	Software	Antivirus Corporativo	Kaspersky Endpoint Security	-	N/A	Instalado en todos los equipos	2022-07-01	Operativo	Departamento de TI
005	Hardware	Computador de escritorio	HP	EWS123456789	MAC: 00:4D:3C:2B:1A:0E	Oficina Administrativa	2023-02-15	Operativo	Departamento Administrativo
006	Software	SGA	PHP/MySQL (en Hostinger)			www.zurichscience.edu/notas	2023-03-01	Activo	Departamento de TI

007	Software	Página Principal	Word Press (en Hostinger)	https://zurichscience.com/	2023-02-01	Activo	Departamento de TI
008	Hardware	Laptop	HP ProBook 450 G7	Core i7, 16GB RAM, 512GB SSD	Sala de Profesores	2023-03-05	Activo	Docentes
009	Hardware	Laptop	HP ProBook 450 G7	Core i7, 16GB RAM, 512GB SSD	Sala de Profesores	2023-03-05	Activo	Docentes
010	Hardware	Laptop	HP ProBook 450 G7	Core i7, 16GB RAM,	Sala de Profesores	2023-03-05	Activo	Docentes

				512GB SSD			
011	Hardware	Laptop	HP ProBook 450 G7	Core i7, 16GB RAM, 512GB SSD	Sala de Profesores	2023-03-05	Activo	Docentes
012	Hardware	Laptop	HP ProBook 450 G7	Core i7, 16GB RAM, 512GB SSD	Sala de Profesores	2023-03-05	Activo	Docentes
013	Hardware	Laptop	HP ProBook 450 G7	Core i7, 16GB RAM, 512GB SSD	Sala de Profesores	2023-03-05	Activo	Docentes

014	Hardware	Computador de escritorio	HP	EWS123456789	MAC: 00:4D:3C:2B:1A:0E	Oficina Administrativa	2023-02-15	Operativo	Departamento Administrativo
015	Hardware	Laptop	HP ProBook 450 G7	Core i7, 16GB RAM, 512GB SSD		Secretaría	2023-03-05	Activo	Docentes
016	Hardware	Laptop	HP ProBook 450 G7	Core i7, 16GB RAM, 512GB SSD		Secretaría	2023-03-05	Activo	Docentes

3.1.2. Activos Tecnológicos críticos

La infraestructura tecnológica de la Unidad Educativa Virtual Zúrich Science está compuesta por diversos activos, en este apartado se clasifican estos activos en categorías críticas para garantizar la seguridad de la información, la continuidad operativa y el cumplimiento de los estándares ISO 27001. En la Tabla 6 se detalla cada activo con su categoría prioridad y relación con el Anexo A de las normas ISO 27001.

Tabla 6 Activos tecnológicos críticos

ID del Activo	Categoría	Descripción	Justificación (ISO 27001)	Prioridad	Control del Anexo A
001	Red	Router Principal	Punto central para garantizar la disponibilidad de la red y la continuidad operativa.	Alta	A.13.1.1 (Controles de Red)
002	Almacenamiento	Servidor NAS	Almacena información sensible y copias de seguridad, impactando la confidencialidad, integridad y disponibilidad.	Alta	A.12.3.1 (Copia de Seguridad)
003	Software	Sistema de Gestión Académica (Moodle)	Gestiona procesos educativos críticos. Impacta la disponibilidad y	Alta	A.14.1.1 (Seguridad en Sistemas de Información)

			confidencialidad de datos académicos.		
006	Software	SGA (PHP/MySQL)	Gestiona calificaciones y datos administrativos. Impacta en la integridad y confidencialidad.	Alta	A.14.2.5 (Pruebas de Sistemas)
007	Software	Página Principal (WordPress)	Interfaz pública para comunicación institucional. Su protección impacta en la integridad y disponibilidad.	Media	A.14.1.3 (Transacciones Seguras)

3.1.3. Diseño de la Infraestructura de Red:

En la herramienta GNS3 se simuló la topología de red, aquí se detallaron los puntos de acceso, se realizó la configuración de red y se configuró en IDS en este caso Snort que es al que se le implementará el modelo Machine Learning para detectar y clasificar los ataques. En la Figura 6 se muestra la topología final.

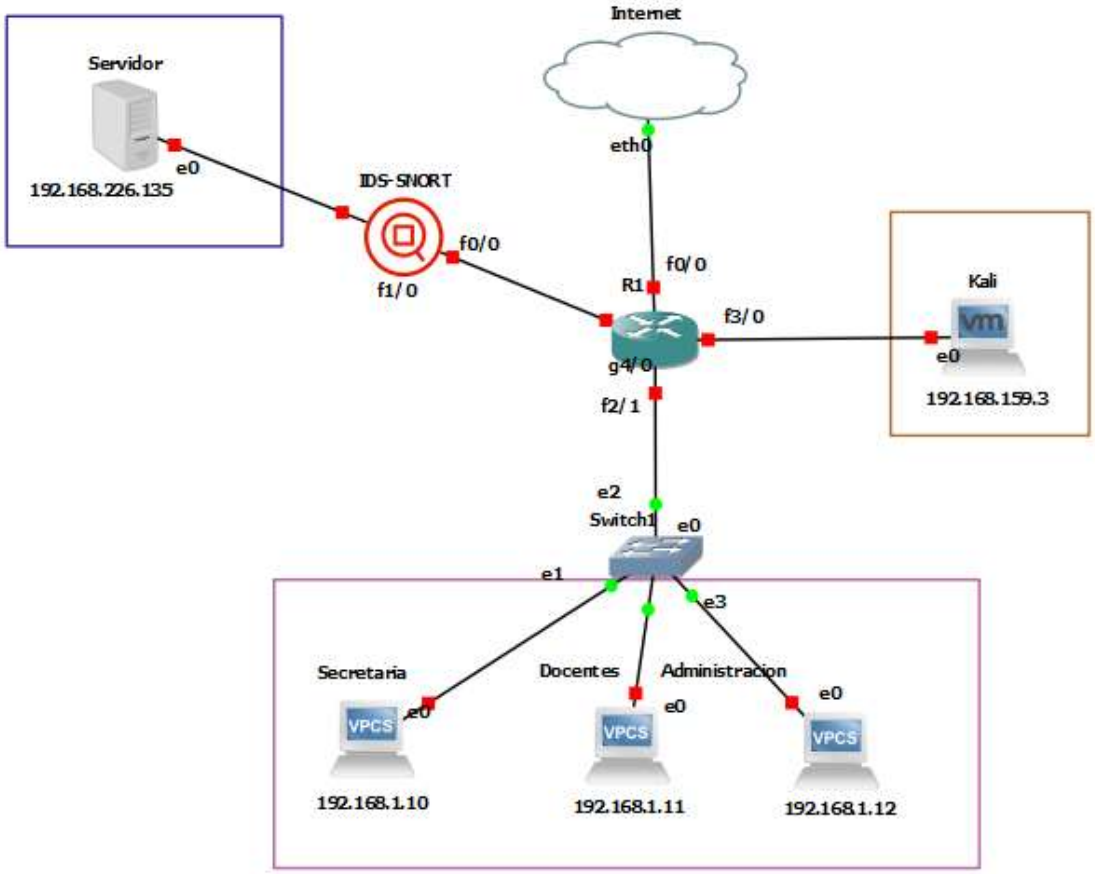


Figura 6. Mapeo de red

3.1.4. Detección de Vulnerabilidades

Para identificar las vulnerabilidades presentes en los activos críticos, se han utilizado herramientas avanzadas de análisis de vulnerabilidades como Nmap. El resultado del escaneo con Nmap muestra los siguientes aspectos clave de las vulnerabilidades y servicios detectados en el servidor, el cual demoró 4 minutos 4 segundos:

Servicios Detectados. Después de realizar el análisis de vulnerabilidades como se muestra en la Figura 7, se obtuvieron cuatro vulnerabilidades claves, que fueron en el Secure Shell (SSH), Hypertext Transfer Protocol (HTTP), Common Vulnerabilities and Exposures (CVE) y Cross-Site Request Forgery (CSRF). A continuación, se detallan cada una de las vulnerabilidades detectadas:

SSH (Puerto 22): Se detectaron varias vulnerabilidades asociadas con este puerto como: **CVE-2023-38408** y **CVE-2020-15778**.

HTTP (Puerto 80): Las vulnerabilidades encontradas en este puerto fue la siguiente:

- **CSRF (Cross-Site Request Forgery)**: Se encontraron ulnerabilidades de CSRF en la página de inicio (`/index.php/comments/feed/1`).

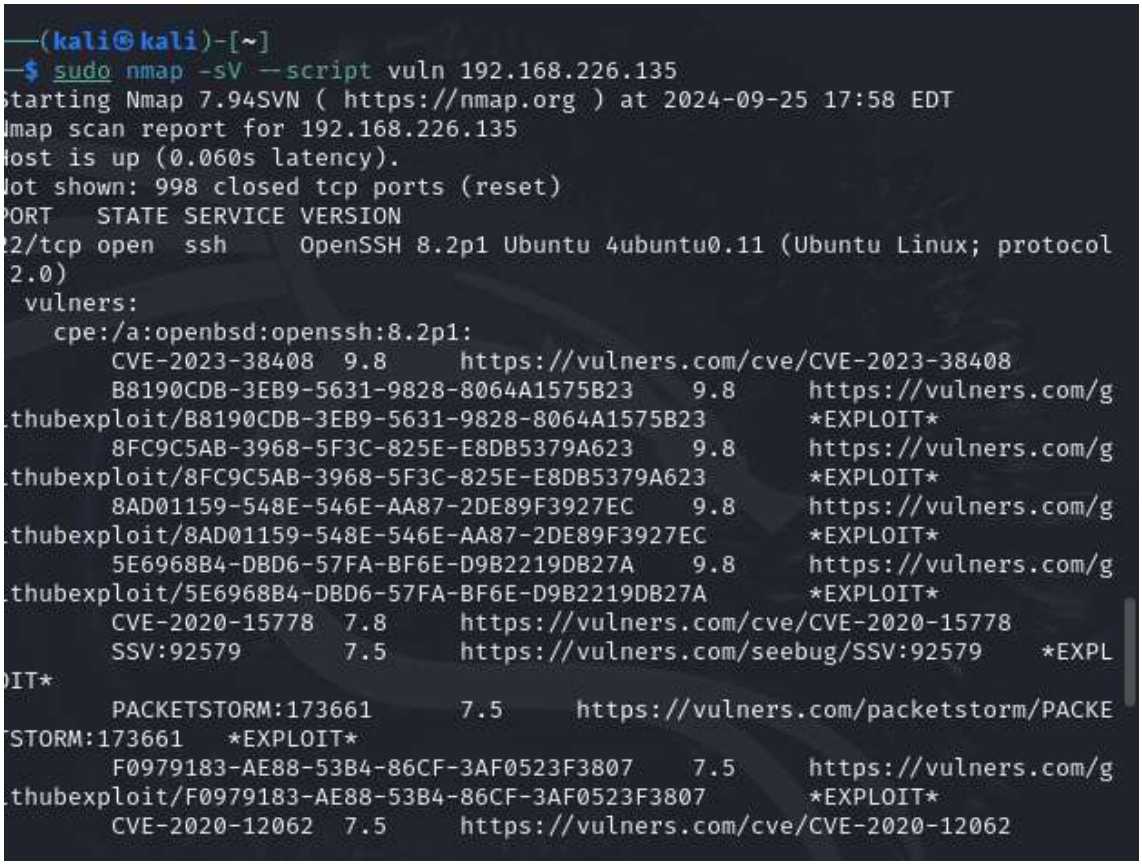


Figura 7 Detección de vulnerabilidades

A continuación, en la Tabla 7 se presentan los resultados de la detección de las vulnerabilidades detectadas en relación con los activos de la Unidad Educativa Zúrich Science.

Tabla 7 Relación de vulnerabilidades con los activos

Activo	Vulnerabilidades Detectadas	Nivel de Riesgo	Medida Propuesta
Servidor Central	Puertos abiertos (22, 80).	Alto	Configurar el firewall para restringir accesos no autorizados.

Router Principal	Configuración débil de Secure Shell (SSH).	Alto	Fortalecer contraseñas y configurar la autenticación basada en claves públicas.
Sistema Moodle	Cross-Site Request Forgery (CSRF)	Medio	Implementar un token CSRF.
Página Principal	Sin validación Protocolo de Transferencia de Hipertexto Seguro (HTTPS).	Medio	Configurar certificados SSL para garantizar la seguridad de las conexiones.

En el contexto de una institución educativa virtual como Zúrich Science, la seguridad de los activos tecnológicos es esencial para garantizar lo siguiente:

- **Confidencialidad**: Protegiendo los datos personales y académicos de estudiantes y docentes.
- **Integridad**: Asegurando la fiabilidad de los sistemas académicos y administrativos.
- **Disponibilidad**: Evitando interrupciones en los servicios educativos esenciales.

3.2.Análisis de incidentes pasados

A continuación, se presentan los resultados obtenidos a partir de los instrumentos aplicados para la recolección de datos en la investigación que en este caso fueron: encuestas y entrevistas. Estos instrumentos permitieron recopilar información relevante sobre las percepciones, prácticas y conocimientos en torno a la ciberseguridad dentro de la Unidad Educativa Virtual Zúrich Science.

3.2.1. Resultados de la encuesta

Pregunta 1: ¿Cuál es tu rol en la Unidad Educativa Virtual Zúrich Science?

Tomando en cuenta el resultado de la muestra se encuestó a 3 profesores, 6 estudiantes (1 de educación básica y 5 de bachillerato) y a 1 personal administrativo. En la Tabla 8 se muestran los resultados de la pregunta 1.

Tabla 8 Resultado pregunta uno de la encuesta

Rol	Cantidad de Respuestas	Porcentaje
Profesor	3	30%
Estudiante	6	60%
Personal Administrativo	1	10%
Total	10	100%

Pregunta 2: ¿Cuánto tiempo llevas utilizando los sistemas digitales de la institución?

En la Tabla 9 muestra que el 90% de los encuestados tienen entre 1 y 3 años de experiencia utilizando los sistemas digitales de la institución. Esto sugiere que la mayoría tiene un conocimiento básico del entorno tecnológico de la institución.

Tabla 9 Resultado pregunta dos de la encuesta

Tiempo de Uso	Cantidad de Respuestas	Porcentaje
Menos de 1 año	1	10%
Entre 1 y 3 años	9	90%
Total	10	100%

Pregunta 3: ¿Conoces los conceptos básicos de ciberseguridad?

Los resultados mostrados en la Tabla 10 detalla que 60% de los encuestados desconocen los conceptos básicos de ciberseguridad, lo que evidencia una necesidad de capacitación en este ámbito para mejorar la seguridad institucional.

Tabla 10 Resultado pregunta tres de la encuesta

Respuesta	Cantidad de Respuestas	Porcentaje
Sí	4	40%
No	6	60%
Total	10	100%

Pregunta 4: ¿Conoces las políticas de ciberseguridad implementadas en la institución?

Como resultado en la pregunta cuatro mostrados en la Tabla 11 nos da que solo el 10% de los encuestados conoce las políticas de ciberseguridad de la institución, lo que indica una falta de difusión y concienciación sobre las mismas.

Tabla 11 Resultado pregunta cuatro de la encuesta

Respuesta	Cantidad de Respuestas	Porcentaje
Sí	1	10%
No	9	90%
Total	10	100%

Pregunta 5: ¿Con qué frecuencia cambias tus contraseñas en los sistemas informáticos de la institución?

Los resultados de la Tabla 12 presenta que el 70% de los encuestados nunca cambian sus contraseñas, lo cual es una práctica nada segura que puede ser de alto riesgo para la protección de las cuentas de los usuarios.

Tabla 12 Resultado pregunta cinco de la encuesta

Frecuencia	Respuestas	Porcentaje
Nunca	7	70%
Periódicamente	2	20%
A veces	1	10%
Total	10	100%

Pregunta 6: ¿Usas contraseñas diferentes para cada sistema informático de la institución?

En la Tabla 13 muestra que el 70% de los encuestados no utilizan contraseñas diferentes para cada sistema, lo cual diferentes ciberataques.

Tabla 13 Resultado pregunta seis de la encuesta

Respuesta	Cantidad de Respuestas	Porcentaje
Siempre	2	20%
A veces	1	10%
Nunca	7	70%
Total	10	100%

Pregunta 7: ¿Utilizas herramientas de verificación en dos pasos (2FA)?

Los resultados de la Tabla 14 muestran que ningún encuestado utiliza herramientas de verificación en dos pasos (2FA), lo cual es una grave deficiencia en las prácticas de seguridad digital.

Tabla 14 Resultado pregunta siete de la encuesta

Respuesta	Cantidad de Respuestas	Porcentaje
Sí	0	0%
No	10	100%
Total	10	100%

Pregunta 8: ¿Consideras que la institución está protegida frente a las amenazas cibernéticas?

El 60% de los encuestados percibe que la institución está poco protegida, mientras que un 30% la considera moderadamente protegida. Esto refleja una percepción negativa sobre las medidas de seguridad existentes en los sistemas de la institución. En la Tabla 15 muestra a detalle estos resultados.

Tabla 15 Resultado pregunta ocho de la encuesta

Opciones	Respuestas	Porcentaje
Poco protegida	6	60%
Moderadamente protegida	3	30%
Muy protegida	1	10%
Total	10	100%

Pregunta 9: ¿Qué nivel de riesgo percibes en el uso de las plataformas educativas de la institución?

En la Tabla 16 muestra que el 50% de los encuestados percibe un nivel alto de riesgo de que las plataformas educativas de la institución sean objeto de ciberataques. Lo que refleja la necesidad de mejorar la seguridad informática de estos.

Tabla 16 Resultado pregunta nueve de la encuesta

Opciones	Respuestas	Porcentaje
Bajo	1	10%
Medio	4	4%
Alto	5	50%
Total	10	100%

Pregunta 10: ¿Has experimentado o presenciado algún incidente de seguridad informática en el uso de las plataformas educativas de la institución?

Los resultados que se muestran en la Tabla 17 refleja que el 60% de los encuestados han experimentado algún incidente de seguridad informática, por lo que se puede considerar que sus plataformas son altamente propensas a ataques.

Tabla 17 Resultado pregunta diez de la encuesta

Opciones	Cantidad de Respuestas	Porcentaje
Sí	6	60%
No	4	40%
Total	10	100%

Pregunta 11: Si respondiste "Sí", ¿de qué tipo fue el incidente informático?

Gran parte de los incidentes informáticos experimentados por los usuarios encuestados como se muestra en la Tabla 18 están relacionados con el acceso no autorizado a datos, lo cual indica la relevancia de implementar controles de acceso en las diferentes plataformas.

Tabla 18 Resultado pregunta once de la encuesta

Opciones	Respuestas	Porcentaje
Acceso no autorizado a datos	4	67%
Phishing o intento de suplantación	1	17%
Malware	1	17%
Total	6	100%

Pregunta 12: ¿Consideras que recibes suficiente capacitación en ciberseguridad?

Todos los encuestados como se detalla en la Tabla 19 consideran que no reciben suficiente capacitación en ciberseguridad, lo que evidencia una necesidad urgente de formación en este ámbito.

Tabla 19 Resultado pregunta doce de la encuesta

Respuesta	Cantidad de Respuestas	Porcentaje
Sí	0	0%
No	10	100%
Total	10	100%

Pregunta 13: ¿Participarías en talleres o cursos sobre ciberseguridad si fueran ofrecidos?

La Tabla 20 muestra que el 80% de los encuestados estarían dispuestos a participar en talleres o cursos sobre ciberseguridad, lo que muestra un interés significativo en mejorar sus conocimientos en esta área.

Tabla 20 Resultado pregunta trece de la encuesta

Opciones	Respuestas	Porcentaje
Sí	8	80%
No	2	20%
Total	10	100%

3.2.2. Resultados de la entrevista

La Tabla 21 presenta un resumen de las respuestas recopiladas por medio de las entrevistas aplicadas a profesores y personal administrativo de la Unidad Educativa Zúrich Science. Dichas entrevistas brindaron información relevante sobre las percepciones, prácticas y desafíos vinculados a la aplicación de medidas de ciberseguridad dentro de la institución.

Tabla 21 Resultado de la entrevista

Pregunta	**Respuestas**	**Análisis**
1. En su opinión, ¿qué tan vulnerable considera que son las plataformas de la institución frente a amenazas cibernéticas?	- Muy vulnerable, especialmente frente a accesos no autorizados. - Algo vulnerable, pero no he tenido incidentes mayores.	La mayoría de los entrevistados consideran que las plataformas de la institución como muy vulnerables.
2. ¿Qué tan frecuente cree que son los intentos de acceso no autorizado u otros incidentes de seguridad informática en las	-Ocasionales. - Muy raros.	Los intentos ocasionales sugieren la necesidad de monitoreo para identificar constantemente las amenazas.

plataformas de la institución?		
3. ¿Cuáles considera que son las principales amenazas cibernéticas que enfrentan las plataformas de la institución educativa en la actualidad?	- Phishing e intentos de accesos no autorizados. - Intentos de acceso no autorizados	Las principales amenazas identificadas por los entrevistados son: el phishing y los accesos no autorizados.
4. ¿Cómo describiría la cultura de ciberseguridad dentro de la institución?	- Inexistente, no considero que tengan políticas claras. - Básica, creo que los usuarios no están lo suficientemente capacitados.	La cultura de ciberseguridad es clasificada como débil o inexistente.
5. ¿Considera que los usuarios están conscientes de la importancia de la ciberseguridad? ¿Por qué?	- No, la mayoría de los usuarios no comprenden los riesgos informáticos. -Algunos sí, pero la mayoría desconoce su importancia.	La mayoría de los usuarios no están conscientes de la importancia de la ciberseguridad.
6. ¿Existe algún tipo de programa en la institución para fomentar la conciencia sobre ciberseguridad en los usuarios? Si no existen, ¿Cuáles considera que serían útiles?	-No existen programas, pero considero que serían de gran utilidad. -No, pero sería importante y de gran	Existe una ausencia de programas de concienciación, a lo que los entrevistados consideran que impartir capacitaciones a los usuarios sería útil.

	utilidad capacitaciones a los usuarios.	
7. ¿Qué obstáculos cree que existen en la institución para implementar medidas de ciberseguridad en sus plataformas?	- Falta de presupuesto y recursos. - Desconocimiento del área.	Los principales obstáculos para implementar medidas de ciberseguridad son la falta de presupuesto y el desconocimiento.
8. ¿Ha enfrentado algún incidente cibernético en la institución? En caso de que la respuesta sea sí, ¿cómo se manejó y qué se aprendió de esa experiencia?	- Sí, experimenté un acceso no autorizado a una de las plataformas educativas. - Creo que no he experimentado ningún incidente cibernético.	Los incidentes de acceso no autorizado son los más mencionados por los entrevistados, pero algunos desconocen si han ocurrido.
9. ¿Qué herramientas o utiliza para protegerse de amenazas cibernéticas en su día a día?	- Cambiar contraseñas regularmente. - Ninguna	Las medidas de seguridad son básicas, lo cual da como resultado una falta de herramientas avanzadas como lo es la autenticación multifactorial.
10. ¿Qué estrategias o prácticas recomendaría para mejorar la seguridad informática dentro de la institución?	- No conozco ninguna práctica - Capacitar regularmente a los usuarios.	Las recomendaciones solo incluyen capacitar a los usuarios, el resto de entrevistados desconoce de estrategias.

3.2.3. Acciones Recomendadas

En la Tabla 22 se da a conocer las acciones propuestas clasificadas en cuatro secciones importantes como: mitigación de riesgos, fortalecimiento de infraestructura, monitoreo continuo y capacitación a usuarios.

Tabla 22 Acciones recomendadas

Categoría	Acción
Mitigación de Riesgos	Configurar los respectivos certificados SSL en las plataformas para cifrar las conexiones HTTP.
Fortalecimiento de Infraestructura	Implementar un firewall actualizado para proteger el servidor de accesos no autorizados. Habilitar cifrado SSL/TLS en el servidor para garantizar la seguridad.
Monitoreo Continuo	Configurar sistemas de detección de intrusos (IDS) como Snort con Machine Learning para alertar sobre intentos de ataques a los activos tecnológicos. Realizar escaneos periódicos para garantizar una gestión efectiva de vulnerabilidades.
Capacitación del Personal	Entrenar a los administradores, profesores y estudiantes en la implementación de controles de seguridad de las plataformas educativas que utilicen en la institución.

3.3. Implementación de un sistema de detección avanzada de amenazas que utilice técnicas de inteligencia artificial

3.2.1. Implementación del Sistema de Detección de Amenazas

El sistema de detección de amenazas integró Snort 3 con un modelo de aprendizaje automático (Random Forest), utilizando datos generados a partir de los logs de Snort 3.

En el Anexo 1 se muestra uno de los datos generados después de la configuración de Snort 3.

Entrenamiento del modelo Machine Learning. Una vez que los logs fueron extraídos, se utilizó el código en Python que se muestra en el Anexo 2 para extraer las columnas importantes y posteriormente etiquetar cada uno con -1 para el tráfico maligno y 1 para el tráfico benigno. Esto nos dio como resultado el formato que se muestra en la Figura 8.

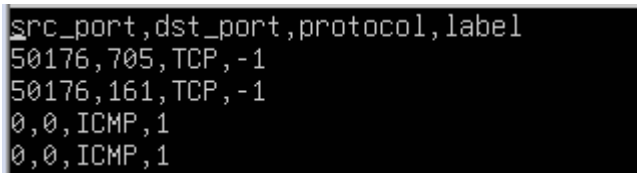


Figura 8 Datos extraídos

El modelo de aprendizaje automático desarrollado fue entrenado utilizando datos generados y etiquetados a partir de los documentos de registros de Snort y del tráfico de red del servidor. El conjunto de datos final tuvo como resultado 903 registros divididos entre tráfico normal y tráfico malicioso. Para el tráfico normal, se generaron datos a través de herramientas como ping y curl, por otro lado, para el tráfico malicioso fue simulado con herramientas como Hydra, SQLmap, y Nmap.

Entrenamiento y validación del modelo. Se desarrolló un modelo basado en Random Forest, el cual fue entrenado y evaluado utilizando el conjunto anteriormente mencionado. Para evaluar el modelo se llevó a cabo el proceso que se detalla en la Tabla 23.

Tabla 23 Entrenamiento y validación del modelo

Etapa	Descripción	Detalles
Conjunto de Datos	Combinación de datos etiquetados manualmente.	Registros anómalos y normales.
División	División del conjunto de datos en entrenamiento y prueba.	70% entrenamiento (633 registros). 30% prueba (270 registros).

Modelo	Algoritmo de clasificación utilizado.	Modelo: Random Forest Classifier. Número de árboles: 100. Profundidad máxima: Sin límite.
Balanceo de Clases	Aplicación de SMOTE para balancear la representación de las clases minoritarias.	Aumentó la representación de tráfico normal para evitar sesgos.
Entrenamiento	Entrenamiento del modelo con los datos procesados y balanceados.	Duración: 2 minutos. Características utilizadas: `src_port`, `dst_port`, `protocol`.
Evaluación	Evaluación del modelo utilizando métricas de clasificación.	Métricas calculadas: Precisión, Recall, F1-Score, y Matriz de Confusión.
Resultados	Reporte de clasificación del modelo en conjunto de prueba.	Precisión general: 96%. Recall para clase normal: 100%. Recall para clase anómala: 93%.
Validación Cruzada	Validación cruzada para garantizar la generalización del modelo.	K-Folds utilizados: 5. Precisión promedio en validación cruzada: 95%.

En la Tabla 24 se detalla los resultados obtenidos del modelo Random Forest destacan por su efectividad en la clasificación de tráfico de red. Para la clase de anomalía tuvo una precisión de 100% y para la clase normal de un 93%. El modelo tiene una precisión global del 96% como de detalla en la Tabla 24.

La matriz de confusión mostrada en la Tabla 25 detalla que el modelo clasificó correctamente 68 de los 68 registros de tráfico normal y 55 de los 60 registros de tráfico malicioso. Solo se presentaron 5 falsos positivos y 0 falsos negativos en el caso del tráfico normal. En el Anexo 3 Código Random Forest se encuentra el código utilizado para el entrenamiento del modelo.

Tabla 24 Resultados obtenidos del modelo

Clase	Precisión	Recall	F1-Score	Support
Anomalía	1.00	0.92	0.96	60
Tráfico normal	0.93	1.00	0.96	68
Accuracy	0.96			128
Macro Avg	0.97	0.96	0.96	128
Weighted Avg	0.96	0.96	0.96	128

Tabla 25 Matriz de confusión

Predicción/Realidad	Anomalía	Normal
Anomalía	55	5
Normal	0	68

3.3. Evaluación de la efectividad y eficiencia del modelo

3.3.1. Simulaciones de Ataques

Se realizaron simulaciones en el entorno replicado en la herramienta GNS3 con máquinas virtuales. Para simular los ataques se utilizaron diferentes herramientas proporcionadas por Kali, las cuales incluyeron lo siguiente:

Ataques de Fuerza Bruta: Para los ataques de fuerza bruta se usó la herramienta Hydra, el cual permitió generar múltiples intentos de accesos en diferentes servicios como: SSH y HTTP. Esto permitió replicar escenarios reales de ataques al servidor.

Ataques de Escaneo y Explotación de Vulnerabilidades: Se utilizó Nmap con scripts de vulnerabilidades mediante la instrucción nmap -sV –script vuln, para identificar las vulnerabilidades de los sistemas.

Tráfico Generado Manualmente: Para generar tráfico de manera manual se utilizó hping3 y ping para simular tráfico normal y malicioso.

Pruebas de penetración. En la fase de pruebas de penetración se simularon varios tipos de ataques a la red para detectar y explotar vulnerabilidades como se detalla a continuación:

a. Escaneo de puertos

Se utilizó la herramienta Nmap de Kali Linux para encontrar puertos abiertos y servicios disponibles en los servidores y dispositivos. En la Figura 9 tenemos el resultado del escaneo en este caso al servidor Ubuntu de mi topología. Obtuvimos dos puertos abiertos, el puerto 22 y el puerto 82, y 998 puertos cerrados.

El puerto 22 (TCP) es el que está asociado al servicio SSH del servidor el cual permite al servidor tener conexiones SSH (Secure Shell). El puerto 80 (TCP) está asociado al servicio HTTP que es el servidor web en ejecución en este caso Apache.

En conclusión, tenemos dos puertos abiertos: el SSH que es un posible punto de entrada para un ataque de fuerza bruta y el HTTP al que podemos explotar vulnerabilidades web que es un sqlmap o un ataque DoS.

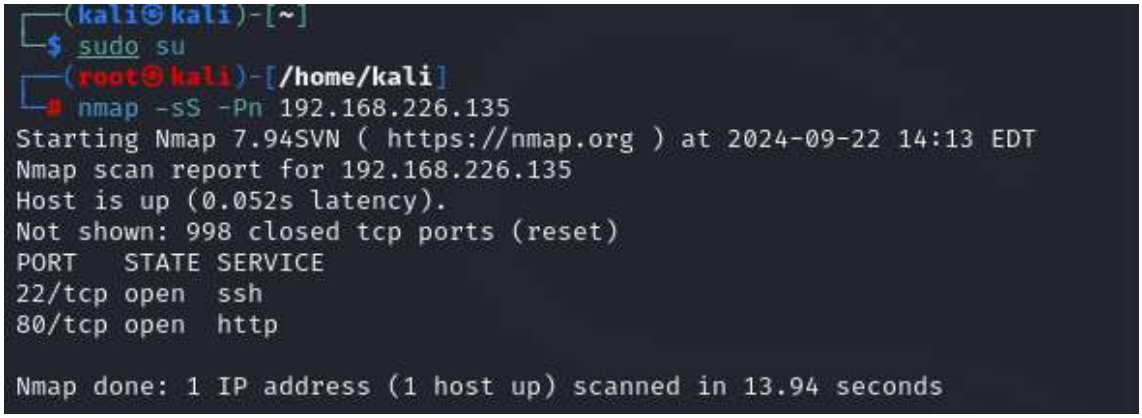


Figura 9 Mapeo de puertos abiertos

b. Ataques de fuerza bruta

Se utilizó Hydra para intentar una intrusión por fuerza bruta en servicios como SSH como se muestra en la Figura 10. Esto nos dio como resultado los datos de acceso al servidor como se observa en la Figura 11.

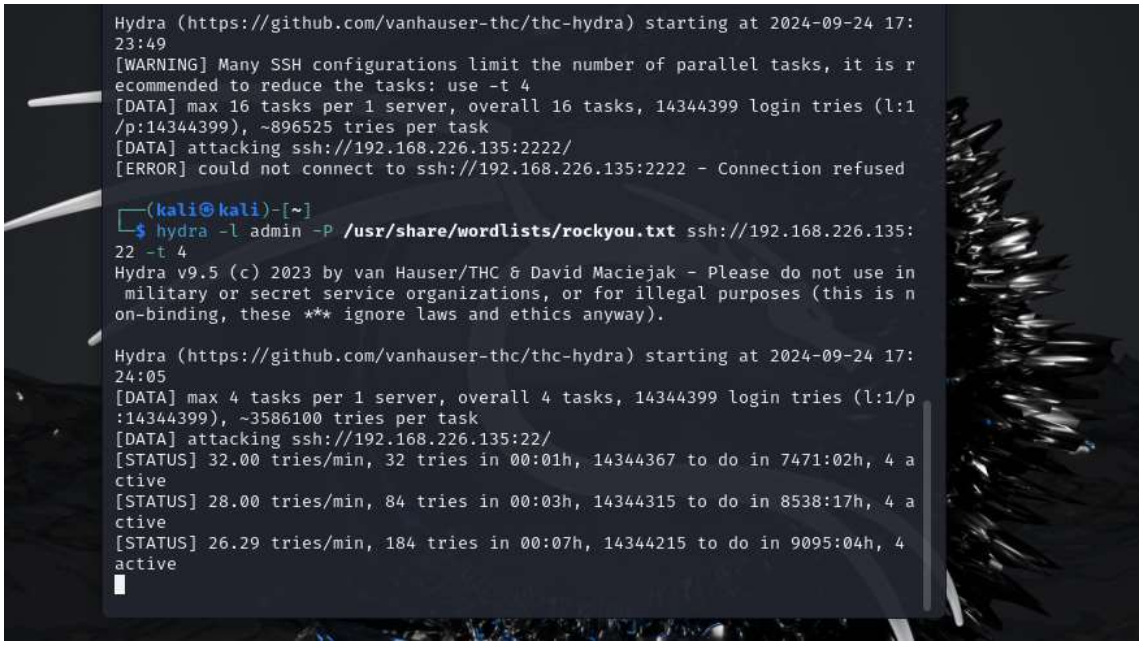


Figura 10 Intentos de intrusión

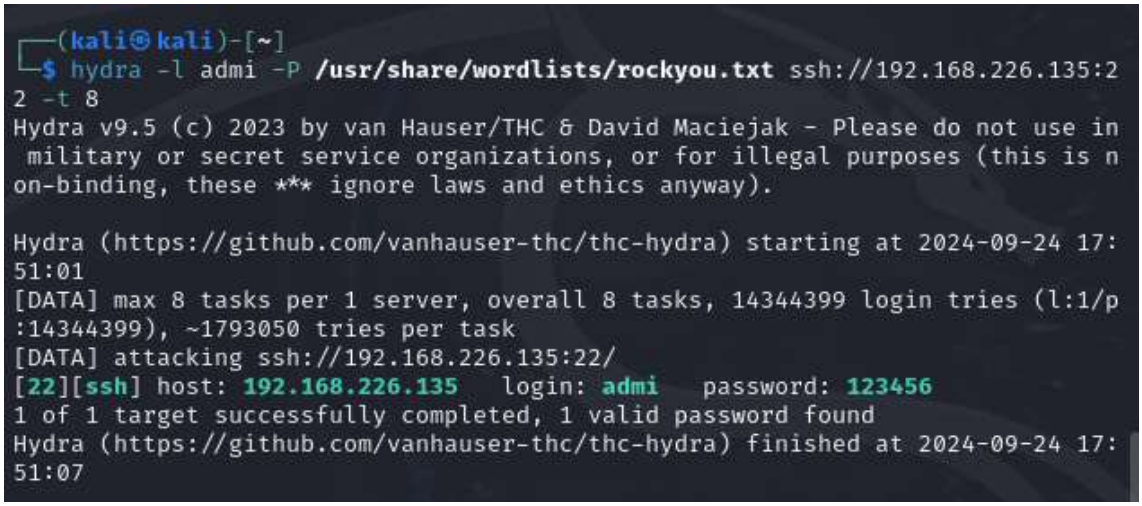


Figura 11 Resultado de ataque de fuerza bruta

3.3.2. Evaluación del modelo

Métricas claves de simulación. En las simulaciones realizadas se analizaron intentos y tipo de intrusión de los cuales se obtuvieron los resultados mostrados en la Tabla 26.

Tabla 26 Métricas de simulación

Métrica	Resultado
Intentos de intrusión	Se registraron un total de 505 intentos maliciosos.

Resultados del Análisis Post-Incidente. Los resultados obtenidos de las simulaciones que se muestran en la Tabla 27 donde refleja que el sistema está expuesto a ataques, sin embargo, las amenazas fueron neutralizadas en un promedio de diez segundos.

Tabla 27 Análisis Post-Incidentes

Métrica	Descripción	Tiempo
Tiempo medio entre fallos (MTBF)	Se registraron 505 intentos maliciosos.	7 días
Tiempo medio de contención (MTTC)	Una vez detectado un intento de intrusión, el sistema respondió a la	10 segundos

	amenaza en un promedio de 10 segundos, mostrando una capacidad de respuesta rápida.

El análisis de los resultados muestra que el marco de ciberseguridad diseñado tiene una alta capacidad para detectar y mitigar amenazas en tiempo real. La integración de Snort 3 con Machine Learning mejora la efectividad en comparación con sistemas tradicionales, al identificar patrones maliciosos en los logs generados.

3.3.3. Comparación Estadística de Snort con Snort y Snort con el modelo Machine Learning

A continuación, se presenta una comparación detallada entre el desempeño de Snort en su configuración tradicional y su integración con Machine Learning (ML). La evaluación incluye métricas clave como precisión, recall, F1-score y exactitud, acompañadas de un análisis detallado para cada una.

Para el cálculo de las métricas para el modelo de ML se utilizó el código mostrado en el Anexo 7. En contraste se utilizaron los siguientes cálculos para el snort tradicional, los datos para los respectivos cálculos se obtuvieron de los logs proporcionados por Snort 3 mediante un Código en Python como se muestra en el Anexo 1.

Cálculo de Métricas para Snort Tradicional. Para el cálculo de las métricas para Snort Tradicional se utilizaron las siguientes formulas, donde predominan: True Positives (TP), True Negatives (TN), False Positives (FP), y False Negatives (FN).

$$Precisión = \frac{TP}{TP + FP}$$

$$Recall = \frac{TP}{TP + FN}$$

$$F1 = 2 \text{ x } \frac{\text{Precisión x Recall}}{\text{Precisión} + \text{Recall}}$$

La precisión de Snort en su configuración tradicional es del 75%, lo que indica que tres de cada cuatro detecciones positivas fueron correctas. Sin embargo, esta cifra varía en función de la calidad y cobertura de las reglas configuradas. Mientras que, la precisión del modelo Random Forest integrado con Snort alcanza un 97%, gracias a su capacidad para aprender patrones complejos a partir de los datos de entrenamiento etiquetados.

El resultado del recall para Snort tradicional es del 68%, lo cual indica que hay amenazas que pasan desapercibidas si no se tienen especificada reglas para detectarlas. Mientras que el modelo ML tiene un recall del 96%, el modelo de ML detecta en gran parte las amenazas que se obtuvieron en los datos de prueba, incluso aquellas que no coinciden con patrones previamente observados.

El F1-score para Snort tradicional es del 71%, lo cual indica que su desempeño tiene limitaciones de detección. Por otro lado, el modelo ML tiene un 96% logrando un equilibrio óptimo entre la precisión y el recall.

Representación Gráfica. En la Figura 12 se visualiza la comparación de las métricas de desempeño entre Snort Tradicional y Snort mejorado con Machine Learning, de las cuales se puede verificar las diferencias en términos de precisión, recall y F1-Score. Estas métricas permiten evaluar la capacidad de los sistemas para identificar amenazas de seguridad en una red, considerando tanto los casos maliciosos como benignos.

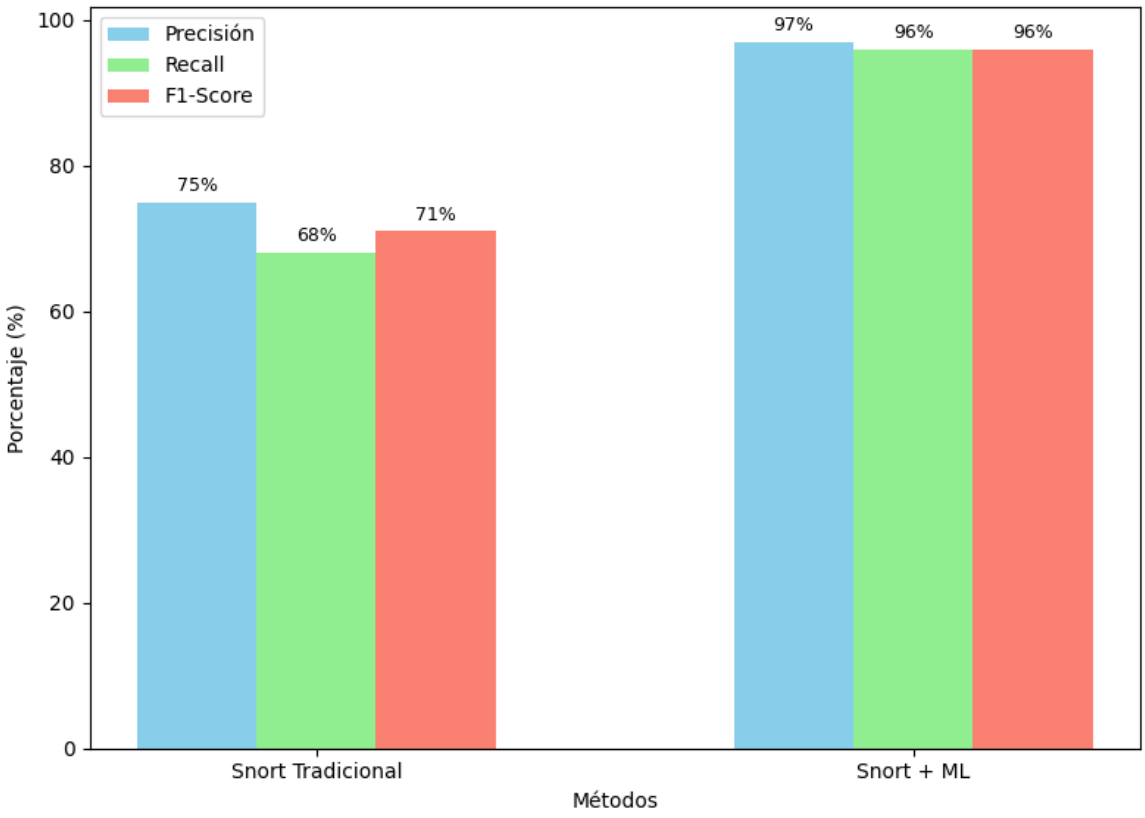


Figura 12 Comparación de desempeño

La Figura 13 presenta la curva Receiver Operating Characteristic (ROC) correspondiente a la evaluación del sistema Snort con Machine Learning. Esta curva grafica la relación entre: Verdaderos Positivos (TPR) y la Tasa de Falsos Positivos (FPR) a diferentes umbrales de decisión.

La curva resalta que el sistema es capaz de detectar con alta precisión el tráfico malicioso, manteniendo una baja tasa de falsos positivos, lo que lo posiciona como una mejora significativa respecto al enfoque de Snort tradicional. Este análisis confirma la robustez del modelo basado en aprendizaje automático para proteger redes contra amenazas avanzadas.

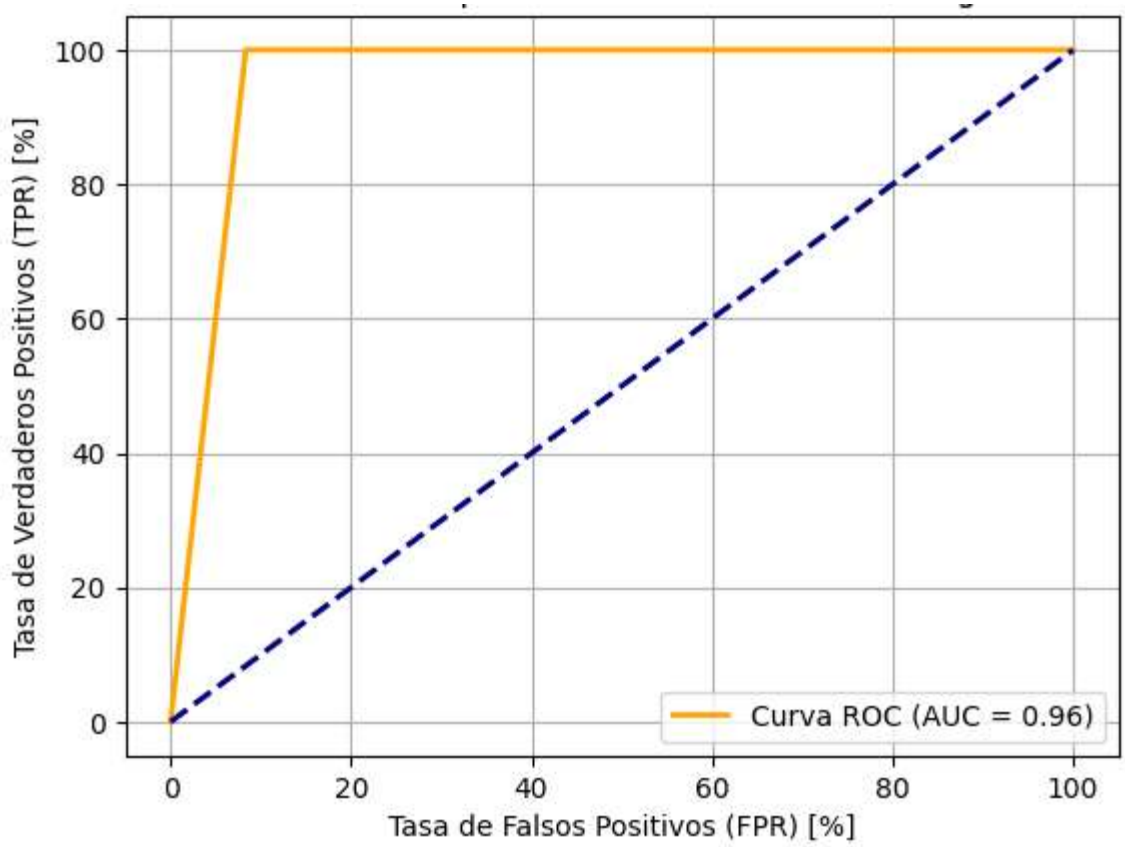


Figura 13 Curva ROC

3.4. Propuesta

3.4.1. Objetivo general de la propuesta

Diseñar e implementar un marco de ciberseguridad que permita proteger la confidencialidad, integridad y disponibilidad de los activos tecnológicos y datos sensibles de la Unidad Educativa Virtual Zúrich Science.

3.4.2. Objetivos específicos de la propuesta

- Realizar un análisis detallado de la infraestructura tecnológica de la institución para identificar vulnerabilidades y riesgos.
- Implementar soluciones para monitorear y detectar mediante la integración de inteligencia artificial.
- Evaluar la efectividad del modelo de detección mediante simulaciones de ataques, pruebas de penetración y análisis post-incidente.

- Diseñar un plan de capacitación para promover prácticas óptimas de ciberseguridad a los usuarios de la institución.

3.4.3. Plan de Acción

Evaluación del Entorno Tecnológico

Inventario de Activos:

- Documentar servidores, redes, aplicaciones y demás elementos tecnológicos.
- Priorizar activos según su criticidad siguiendo ISO 27001 (Anexo A.8.1).

Detección de Vulnerabilidades:

- Usar herramientas de escaneo como Nmap para identificar vulnerabilidades técnicas.

Implementación de Herramientas de Seguridad

Sistema de Detección de Intrusiones:

- Configurar Snort3 e integrarlo con modelos de Machine Learning para la detección de tráfico malicioso.
- Entrenar el modelo con datos generados en simulación es controladas.

Firewall y Cifrado:

- Establecer reglas específicas para puertos y protocolos.
- Implementar cifrado SSL/TLS.

Control de Accesos:

- Activar autenticación multifactor (MFA) en las plataformas educativas de la institución.

Pruebas de Seguridad y Evaluación

Simulaciones de Ataques:

- Ejecutar pruebas de fuerza bruta, DDoS e inyección SQL utilizando herramientas como Hydra, Slowloris Sqlmap.
- Evaluar diferentes métricas como: tiempos de intrusión, intentos detectados y respuesta del sistema.

Pruebas de Penetración:

- Replicar escenarios reales de ataques para verificar la resistencia del marco.
- Validar la efectividad de las contramedidas implementadas.

Métricas Evaluadas:

- Intentos de intrusión detectados.
- Tiempos promedio de intrusión y contención (MTTC).
- Porcentaje de falsos positivos y negativos en la detección de amenazas.

Capacitación y Sensibilización

Capacitación Técnica:

- Entrenar al personal técnico en herramientas de seguridad y simulaciones de amenazas.

Concientización General:

- Realizar talleres sobre mejores prácticas de ciberseguridad para el personal docente y administrativo.
- Realizar campañas de sensibilización para estudiantes sobre la importancia de la ciberseguridad.

CONCLUSIONES

El desarrollo del marco de ciberseguridad para la Unidad Educativa Virtual Zúrich Science permitió fortalecer la protección de datos y mejorar la detección de amenazas por medio de implementación de políticas y herramientas tecnológicas para detección de anomalías. Una vez realizado el análisis de la Unidad Educativa Virtual Zúrich Science infraestructura se identificó vulnerabilidades críticas, como configuraciones débiles y la ausencia de protección en las plataformas educativas de la institución.

La integración de Snort con el modelo Random Forest permitió identificar patrones maliciosos con alta precisión. La integración de este modelo redujo falsos positivos, demostrando una alta capacidad para adaptarse frente a amenazas cibernéticas que puedan presentarse en el entorno real.

Para finalizar, la evaluación del modelo mostró resultados efectivos dando como resultado lo siguiente: la precisión del modelo alcanzó un 97%, frente a Snort tradicional que solo obtuvo el 75%. El recall mejoró con un 96% detectando incluso amenazas que no se encontraban previamente configuradas. Asimismo, el F1-score pasó del 71% al 96% por lo que se evidencia la efectividad del modelo.

RECOMENDACIONES

Es esencial establecer un plan de mantenimiento y actualización continua del marco de ciberseguridad para garantizar que las medidas implementadas sigan proporcionando eficacia frente a diferentes amenazas. Además, se recomienda incorporar este marco como modelo para otras instituciones educativas virtuales con características similares.

Se recomienda implementar controles adicionales como: firewalls y autenticación multifactor y aplicar políticas para la gestión de vulnerabilidades que contemple la actualización periódica de sistemas y el cifrado de la transferencia de datos sensibles.

Es necesario ajustar los modelos de inteligencia artificial para reducir el número de falsos positivos. También, se sugiere mejorar el modelo de detección con el fin de incluir amenazas más avanzadas, como ataques de persistencia y vulnerabilidades zero-day.

Por último, se recomienda realizar pruebas de penetración y simulación de ataques de manera periódica con el fin de evaluar la capacidad del modelo y poderlo adecuar a nuevos escenarios. Adicional, se recomienda también establecer un programa de capacitación en ciberseguridad para docentes, estudiantes y personal administrativo.

REFERENCIAS

Abd, A., Boukebous, E., Fettache, M. I., Bendiab, G., & Shiaeles, S. (2023). A Comparative Analysis of Snort 3 and Suricata. *2023 IEEE IAS Global Conference on Emerging Technologies (GlobConET)*, 1–6. https://doi.org/10.1109/GlobConET56651.2023.10150141

Alines Villegas, M. A. (2021). *Modelo de ciberseguridad para la prevención de ataques cibernéticos en la oficina de seguros de la Diris Lima Norte*. https://repositorio.upn.edu.pe/bitstream/handle/11537/29301/Alvines%20Villegas%20Maylen%20Alida.pdf?sequence=1&isAllowed=y

Aludhilu, H. (2020). *A Systematic Literature Review on Intrusion Detection Approaches Una revisión sistemática de la literatura sobre los enfoques de detección de intrusiones*. *14*(1). http://rcci.uci.cuPág.58-78Editorial"EdicionesFuturo"http://rcci.uci.cuPág.58-78

Arévalo-Cordovilla, F. E., Ordoñez-Sigcho, I. B., Peñaherrera-Larenas, M. F., & Suárez-Matamoros, V. J. (2020). Importancia de la seguridad de los sistemas de información frente el abuso, error y hurto de información. *Revista Científica Dominio de Las Ciencias*, *6*, 835–8446. https://doi.org/http://dx.doi.org/10.23857/dc.v6i2.1197

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. In *Electronics (Switzerland)* (Vol. 12, Issue 6). MDPI. https://doi.org/10.3390/electronics12061333

Blanco Rodríguez, F. J., Curto Diego, B., Moreno Rodilla, V., & Polo Martín, M. J. (2018). *Diseño de materiales prácticos para la asignatura Seguridad en Sistemas Informáticos del grado en Ingenieria Informática*. https://gredos.usal.es/bitstream/handle/10366/138254/MID_17_029.pdf?sequence=1&isAllowed=y

Bono, A. S., Pere, A., & Deyà, I. (2022). *Implementación de un sistema de detección de intrusos IDS mediante la inspección del tráfico a través de la red*.

Caizapanta González, A. E. (2022). Análisis comparativo de Sistemas de Detección de Intrusos (IDS) en entornos universitarios. *Revista Tecnológica - ESPOL*, *34*(3), 118–138. https://doi.org/10.37815/rte.v34n3.955

Camilo, J., Mejía, G., Vargas Agudelo, F. A., Rivas, M. M., & Delgado, I. A. (2023). Método para Gestionar la Seguridad de activos de Información. *Revista Ibérica de Sistemas e Tecnologias de Informação*, 252–266.

Carolina, J., Castro, M., Mercedes Ortiz Hernández, M., Antonio, E., & Lino, M. (2021). Análisis de las herramientas y técnicas utilizadas en prueba de penetración para la detección de vulnerabilidades en aplicaciones web. *UNESUM-Ciencias: Revista Científica Multidisciplinaria* , *5*(1), 135–144. https://revistas.unesum.edu.ec/index.php/unesumciencias/article/view/316/298

Castellanos Bernal, M. F. (2017). Asegurar Web Servicces no es cuestión de costos. *Revista Ciencia, Innovación y Tecnología (RCIYT)*, *III*. https://doi.org/https://doi.org/10.38017/2390058X.79

Chillagana, J., Simbaña, J., & Suntaxi, K. (2023). *Design and Deployment of a WAN/LAN/WLAN Network Infrastruc-ture with Security using FortiGate in GNS-3*. *VIII*(3), 68–76. https://doi.org/10.24133/RCSD.VOL08.N03.2023.05

Dioubate, B. M., Daud, W., & Norhayate, W. (2022). Cyber Security Risk Management Frameworks Implementation in Malaysian Higher Education Institutions. *International Journal of Academic Research in Business and Social Sciences*, *12*(4). https://doi.org/10.6007/ijarbss/v12-i4/12300

Édison, D., Vergara, F., Camilo, F., Riveros, C., Castillo, R. A., Víctor, E., Gil Vera, D., Carlos, J., & Vera, G. (2017). Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas Informatic organizational security: a simulation model based on systems dynamic. *Scientia et Technica Año XXII*, *22*(2).

Esteban, J., & Jaramillo, O. (2020). Desafíos de seguridad en las redes WBAN para Soluciones IoT Security challenges in WBAN networks for IoT Solutions. *Tecnológico de Antioquia, Institución Universitaria.* https://dspace.tdea.edu.co/handle/tdea/922

Farid, S., Itmazi, J., & Qaisar, G. (2017). *Security Threats and Measures in E-learning in Pakistan: A Review Mujahid Alam*. https://www.researchgate.net/publication/330663167

Farid, S., Qadir, M., Uddin Ahmed, M., & Daud Khattak, M. (2018). Critical Success Factors of E-Learning Systems: A Quality Perspective. In *Pakistan Journal of Distance & Online Learning*.

Farro Cachay, M. J. (2019). *Análisis y técnicas de seguridad en redes informáticas basado en Open Source, una revisión de la literatura científica en los últimos 5 años.* https://repositorio.upn.edu.pe/bitstream/handle/11537/24156/Farro%20Cachay%2c%20Mario%20Jes%c3%bas.pdf?sequence=1&isAllowed=y

Fernando, D., & Sumalave, G. (2023). *Modelo de gestión de ciberseguridad para resolver incidentes en instituciones de educación superior*. Universidad Francisco de Paula Santander Ocaña.

Guevara-Vega, E. M. D., Delgado-Deza, J. R., & Mendoza-de-los-Santos, A. C. (2023). Vulnerabilidades y amenazas en los activos de información. *Revista Científica de Sistemas e Informática*, *3*(1), e461. https://doi.org/10.51252/rcsi.v3i1.461

Guimarães, A. P., Rodrigues, D., & Nogueira, B. C. E. S. (2020). Performability evaluation of voice services in converged networks. *Revista de Informatica Teorica e Aplicada*, *27*(4), 11–19. https://doi.org/10.22456/2175-2745.94016

Han, M. P. (2021). *Hybrid GNS3 and Mininet-WiFi emulator for survivable SDN Hybrid GNS3 and Mininet-WiFi emulator for survivable SDN backbone network supporting wireless IoT traffic backbone network supporting wireless IoT traffic* [Chulalongkorn University]. https://digital.car.chula.ac.th/chulaetd

Herrera Olivares, M. S., Rada Martínez, A. J., & Palacio Salcedo, I. E. (2020). *Framework gestión de la seguridad de la información para universidades*. http://hdl.handle.net/10584/8868

Humpiri Flores, M. E., Figeroa Donayre, E. M., Guillen Guevara, M. L., Cabel Moscoso, D. J., Humpiri Flores, R., & Huanca Marín, J. C. (2023). Revisión sistemática: vulnerabilidades de seguridad cibernética en los activos digitales. *Ñawparisun* -

Revista de Investigación Científica, *2*(Vol. 4, Num. 2), 93–100. https://doi.org/10.47190/nric.v4i2.250

Jain, G., & Anubha. (2021). Application of SNORT and Wireshark in Network Traffic Analysis. *IOP Conference Series: Materials Science and Engineering*, *1119*(1), 012007. https://doi.org/10.1088/1757-899x/1119/1/012007

Johanna, J., Carrillo, M., Zambrano, N. A., Simón, J., Cantos, M., & Bravo, M. Z. (2019). *Ciberseguridad y su aplicación en las Instituciones de Educación*.

Laura, A., & Saucedo, H. (2015). Guía de ataques, vulnerabilidades, técnicas y herramientas para aplicaciones web. *ReCIBE, Revista Electrónica De Computación, Informática, Biomédica Y Electrónica*, *4*(1). https://doi.org/https://doi.org/10.32870/recibe.v4i1.43

Marsal Giménes, M. M. del R., & Monges Olmedo, M. R. (2019). Modelo teórico de gestión de incidentes de seguridad de la información, para entidades financieras, basado en ISO 27035:2011. *Revista Científica Estudios e Investigaciones*, *7*, 152. https://doi.org/10.26885/rcei.foro.2018.152

Pargaonkar, S. (2023). Advancements in Security Testing: A Comprehensive Review of Methodologies and Emerging Trends in Software Quality Engineering. *International Journal of Science and Research (IJSR)*, *12*(9), 61–66. https://doi.org/10.21275/sr23829090815

Pillajo Garcia, P. A., & Avila Pesantez, D. (2023). Análisis de ciberseguridad en plataformas e-learning: revisión sistemática de la literatura. *Revista Perspectivas*, *5*(1), 19–29. https://doi.org/10.47187/perspectivas.5.1.179

Pronchev, G. B., Goncharova, I. V, Lyubimov, A. P., & Mikhailov, A. P. (2023). Information Security and Online Education During the COVID-19 Pandemic. *Journal of Higher Education Theory and Practice*, *23*(2), 219.

Quirumbay Yagual, D. I., Castillo Yagual, C., & Coronel Suárez, I. (2022). Una revisión del Aprendizaje profundo aplicado a la ciberseguridad. *Revista Científica y Tecnológica UPSE*, *9*(1), 57–65. https://doi.org/10.26423/rctu.v9i1.671

Serna Ramírez, S., Montoya Londoño, Á., Quintero Barco, Y. A., Henao Villa, C. F., & Castro Ramírez, F. D. J. (2022). Desarrollo de un sistema de seguridad informática

a partir de una auditoría sobre una red empresarial. *INGENIERÍA: Ciencia, Tecnología e Innovación*, *9*(2), 135–151. https://doi.org/10.26495/icti.v9i2.2267

Shuai, L., & Li, S. (2021). Performance optimization of Snort based on DPDK and Hyperscan. *Procedia Computer Science*, *183*, 837–843. https://doi.org/10.1016/j.procs.2021.03.007

Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems*, *92*, 178–188. https://doi.org/10.1016/j.future.2018.09.063

Sun, W., & Wu, L. (2019). Research on network and information security in Colleges and Universities. *Proceedings - 2019 International Conference on Information Technology and Computer Application, ITCA 2019*, 292–295. https://doi.org/10.1109/ITCA49981.2019.00071

Syafrizal, M., Selamat, S. R., & Zakaria, N. A. (2020). Analysis of Cybersecurity Standard and Framework Components. In *International Journal of Communication Networks and Information Security (IJCNIS* (Vol. 12, Issue 3). https://doi.org/https://doi.org/10.17762/ijcnis.v12i3.4817

Taherdoost, H. (2022). Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview. In *Electronics (Switzerland)* (Vol. 11, Issue 14). MDPI. https://doi.org/10.3390/electronics11142181

Torres Valero, R. A., Medina Becerra, F. A., & Mendoza Moreno, M. Á. (2020). Propuesta metodológica para la auditoría de ciberseguridad aplicada a un sistema SCADA. *Ingenierías USBMed*, *11*(2), 62–70. https://doi.org/10.21500/20275846.4307

Toussaint, M., Krima, S., & Panetto, H. (2024). Industry 4.0 data security: A cybersecurity frameworks review. In *Journal of Industrial Information Integration* (Vol. 39). Elsevier B.V. https://doi.org/10.1016/j.jii.2024.100604

Wang, B. X., Chen, J. L., & Yu, C. L. (2022). An AI-Powered Network Threat Detection System. *IEEE Access*, *10*, 54029–54037. https://doi.org/10.1109/ACCESS.2022.3175886

Zare, H., Zare, M. J., & Azadi, M. (2018). Cybersecurity Vulnerabilities Assessment (A Systematic Review Approach). *Advances in Intelligent Systems and Computing*, *738*, 61–68. https://doi.org/10.1007/978-3-319-77028-4_10

ANEXOS


```
{
    "timestamp": "10/22-05:26:13.593169",
    "msg": "PROTOCOL-SNMP AgentX/tcp request",
    "pkt_num": 1324,
    "proto": "TCP",
    "pkt_gen": "raw",
    "pkt_len": 44,
    "dir": "C2S",
    "src_addr": "192.168.159.3",
    "src_port": 61054,
    "dst_port": 705,
    "service": "unknown",
    "rule": "1:1421:19",
    "priority": 2,
    "class": "Attempted Information Leak",
    "action": "allow"
}
```


Anexo 1 Salida del archivo de registros

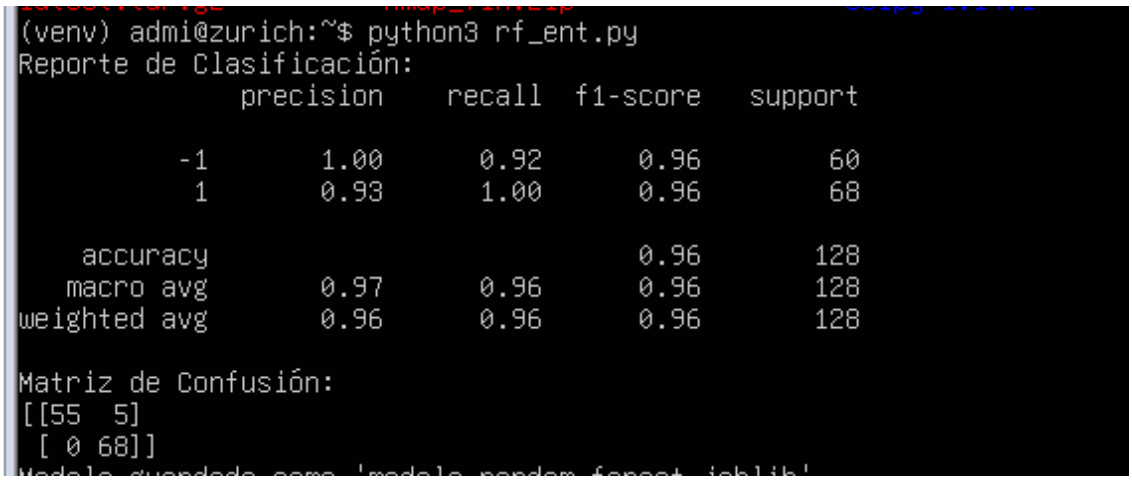
```
import json
import csv

log_file = "var/log/snort/alert_json.txt"

csv_file = 'etiquetados.csv'

with open (csv_file, mode='w', newline='') as file:
    writer = csv. writer(file)
    writer. writerrow ['src_port', dst_port', 'protocol',
'label'])

    with open (log_file, 'r') as log:
      for line in log:
         try:
             entry = json. loads (line. strip ())
             src_port = entry.get ('src_port', 0)
             dst_port = entry.get ('dst_port', 0)
             protocol = entry.get('proto',"")

             writer.writerow ([src_port, dst_port,
protocol, -1])
         except json. JSONDecodeError:
             continue
print ("Datos extraidos")
```

Anexo 2 Código de extración de datos para entrenamiento

```
import csv
from sklearn. ensemble import RandomForestClassifier
from sklearn. model_selection import train_test_split
from sklearn. metrics import classification_report,
confusion_matrix
from imblearn. over_sampling import SMOTE
import joblib

# 1. Leer el Conjunto de Datos desde el Archivo CSV
input_file = 'etiquetados_dos.csv’ # Cambia por el nombre
correcto de tu archivo
data = []
labels = []

with open (input_file, 'r') as file:
    reader = csv. reader(file)
    next(reader) # Saltar el encabezado

    for row in reader:
        # Convertir protocolo a valores numéricos
        protocol_map = {'TCP': 0, 'UDP': 1, 'ICMP': 2}
        protocol = protocol_map [row [2]] # Columna
'protocol'

        # Agregar características y etiqueta
        data. append ([float (row [0]), float (row [1]),
protocol])  # src_port, dst_port, protocol
        labels. apenad (int (row [3])) # Etiqueta: 1 para
tráfico normal, -1 para malicioso

# 2. Balancear las Clases con SMOTE
smote = SMOTE (random_state=42)
data_resampled, labels_resampled = smote.fit_resample
(data, labels)

# 3. Dividir los Datos en Entrenamiento y Prueba
X_train, X_test, y_train, y_test = train_test_split
(data_resampled, labels_resampled, test_size=0.3,
random_state=42)

# 4. Entrenar el Modelo Random Forest
model = RandomForestClassifier (n_estimators=100,
random_state=42)
model.fit (X_train, y_train)

# 5. Evaluar el Modelo
y_pred = model. predica(X_test)

print ("Reporte de Clasificación:")
```

```
print (classification_report (y_test, y_pred))

print ("Matriz de Confusión:")
print (confusion_matrix (y_test, y_pred))

# 6. Guardar el Modelo Entrenado
joblib. duma (model, 'modelo_random_forest. joblib')
print ("Modelo guardado como 'modelo_random_forest.
joblib'")
```

Anexo 3 Código Random Forest

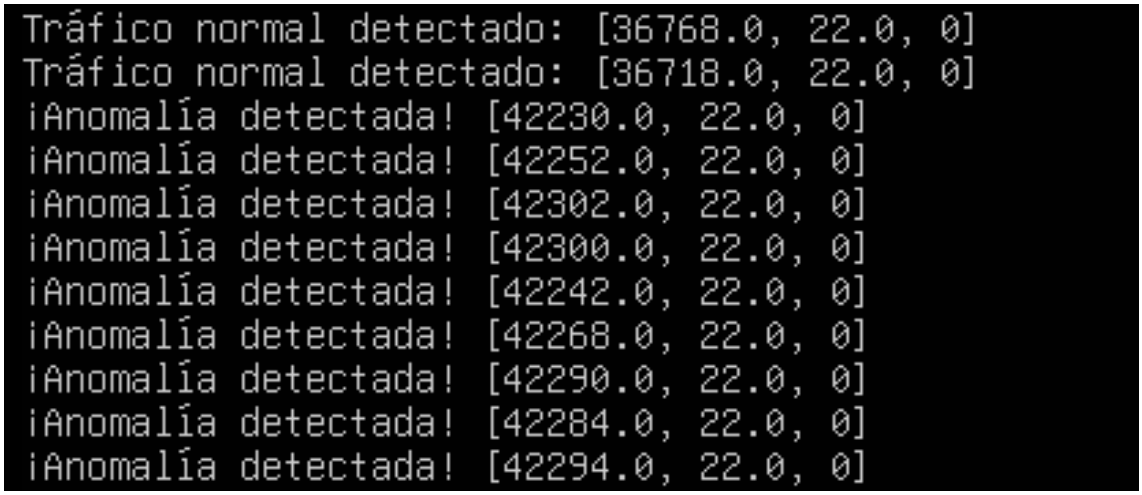


Anexo 4 Resultado del modelo

```
import json
import joblib

# Cargar el modelo entrenado
model = joblib. load ('modelo_random_forest. joblib')

# Mapeo para convertir texto a números (como en el
entrenamiento)
protocol_map = {'TCP': 0, 'UDP': 1, 'ICMP': 2}

# Ruta al archivo de logs en tiempo real
log_file_path = '/var/log/snort/alert_json.txt'

def parse_log_line(line):
    """
    Convierte una línea de log en un formato que el
modelo pueda interpretar.
    """
    try:
```

```
        entry = json. loads (line. strip ()) # Leer el
JSON
        src_port = float (entry.get ("src_port", 0))
        dst_port = float (entry.get ("dst_port", 0))
        protocol = protocol_map.get (entry.get ("proto",
"TCP"), 0)
        return [src_port, dst_port, protocol]
    except json. JSONDecodeError:
        return None

def monitor_logs ():
    """
    Monitorea el archivo de logs y clasifica nuevas
líneas en tiempo real.
    """
    print ("Monitoreando el tráfico...")
    with open (log_file_path, 'r') as log_file:
        log_file. seek (0, 2) # Ir al final del archivo
        while True:
            line = log_file. readline ()
            if line:
                data_point = parse_log_line(line)
                if data_point:
                    prediction = model.
predict([data_point]) [0]
                    if prediction == 1:
                        print ("Tráfico normal
detectado:", data_point)
                    else:
                        print ("¡Anomalía detectada!",
data_point)

if __name__ == "__main__":
    monitor_logs ()
```

Anexo 5 Código de monitoreo en tiempo real



Anexo 6 Resultados de la detección de anomalías en tiempo real

```
import pandas as pd
from sklearn. metrics import confusion_matrix,
precision_score, recall_score, accuracy_score, f1_score

# Cargar los logs procesados
df_logs = pd. read_csv('datos.csv')

# Definir categorías maliciosas
malicious_classes = [
    "Executable code was detected",
    "Web Application Attack",
    "Attempted Information Leak",
    "Access to a potentially vulnerable web application"
]

# Generar predicciones de Snort tradicional
df_logs['snort_prediction'] = df_logs['class']. apply (
    lambda x: -1 if x in malicious_classes else 1
)

# Comparar etiquetas reales con predicciones
y_true = df_logs['label']
y_pred = df_logs['snort_prediction']

# Calcular métricas
conf_matrix = confusion_matrix (y_true, y_pred)
precision = precision_score (y_true, y_pred, pos_label=-
1)
recall = recall_score (y_true, y_pred, pos_label=-1)
accuracy = accuracy_score (y_true, y_pred)
f1 = f1_score (y_true, y_pred, pos_label=-1)
```

```
print ("Matriz de Confusión:", conf_matrix)
print ("Precisión:", precision)
print ("Recall:", recall)
print ("Exactitud:", accuracy)
print ("F1-Score:", f1)
```

Anexo 7 Cálculo de metricas de Snort tradicional

Nombres y apellidos:

Fecha de la entrevista: **Hora de la entrevista:**

Tema: "Desarrollo de un marco de ciberseguridad para la Unidad Educativa Zúrich Science"

Cuestionario de la entrevista:

Percepción de Riesgos y Amenazas Cibernéticas

1. En su opinión, ¿qué tan vulnerable considera que está la institución frente a amenazas cibernéticas como phishing, malware o ataques de denegación de servicio?

   ……
   ……

2. ¿Qué tan frecuente cree que son los intentos de acceso no autorizado o los incidentes de seguridad en la institución?

   ……
   ……

3. ¿Cuáles considera que son las principales amenazas cibernéticas que enfrenta la institución actualmente?

   ……
   ……

Cultura de Ciberseguridad y Conciencia Institucional

4. ¿Cómo describiría la cultura de ciberseguridad dentro de la institución?

   ……
   ……

5. ¿Cree que los usuarios (profesores, estudiantes y personal administrativo) están conscientes de la importancia de la ciberseguridad? ¿Por qué?

   ……
   ……

6. ¿Existen iniciativas o programas en la institución para fomentar la conciencia sobre ciberseguridad? Si no existen, ¿considera que serían útiles?

   ……
   ……

Desafíos y Barreras

7. ¿Qué obstáculos cree que existen para implementar medidas de ciberseguridad en la institución?

   ……
   ……

Experiencia y Mejores Prácticas

9. ¿Ha enfrentado algún incidente cibernético en la institución? Si es así, ¿cómo se manejó y qué se aprendió de esa experiencia?

   ……
   ……

10. ¿Qué herramientas o protocolos utiliza para protegerse de amenazas cibernéticas en su día a día?

    ……
    ……

11. ¿Qué estrategias o prácticas recomendaría para mejorar la seguridad informática dentro de la institución?

……
……

Anexo 8 Formato de entrevista a Profesores y administrativos

Tema: "Desarrollo de un marco de ciberseguridad para la Unidad Educativa Zúrich Science"

A continuación, encontrarás un cuestionario dividido en varias secciones. Marca la respuesta que mejor refleje tu opinión o experiencia. Todas las respuestas serán tratadas de forma confidencial y solo se utilizarán con fines de investigación.

Sección 1: Perfil del Encuestado

1. ¿Cuál es tu rol en la Unidad Educativa Virtual Zúrich Science?

    a) Profesor

    b) Estudiante

    c) Personal Administrativo

2. ¿Cuánto tiempo llevas utilizando los sistemas digitales de la institución?

    a) Menos de 1 año

    b) Entre 1 y 3 años

    c) Más de 3 años

Sección 2: Conocimientos y Prácticas de Ciberseguridad

3. ¿Conoces los conceptos básicos de ciberseguridad (por ejemplo, protección de contraseñas, phishing, etc.)?

a) Sí

b) No

4. ¿Conoces las políticas de ciberseguridad implementadas en la institución?

   a) Sí

   b) No

5. ¿Con qué frecuencia cambias tus contraseñas en los sistemas de la institución?

   a) Nunca

   b) Cada 6 meses

   c) Cada 3 meses o menos

6. ¿Usas contraseñas diferentes para cada sistema digital que utilizas?

   a) Siempre

   b) A veces

   c) Nunca

7. ¿Utilizas herramientas de verificación en dos pasos (2FA) en los sistemas de la institución?

   a) Sí

   b) No

Sección 3: Percepción de la Seguridad Institucional

8. ¿Consideras que la institución está protegida frente a las amenazas cibernéticas?

   a) Muy protegida

   b) Moderadamente protegida

   c) Poco protegida

9. ¿Qué nivel de riesgo percibes en el uso de las plataformas educativas?

   a) Bajo

   b) Medio

c) Alto

Sección 4: Experiencias e Interés

10. ¿Has experimentado o presenciado algún incidente de seguridad informática en la institución?

    a) Sí

    b) No

11. Si respondiste "Sí", ¿de qué tipo fue el incidente? (Puedes seleccionar más de una opción)

    a) Acceso no autorizado a datos

    b) Phishing o intento de suplantación de identidad

    c) Malware

    d) Otro (especificar): _____

12. ¿Consideras que recibes suficiente capacitación en ciberseguridad por parte de la institución?

    a) Sí

    b) No

13. ¿Participarías en talleres o cursos sobre ciberseguridad si fueran ofrecidos?

    a) Sí

    b) No

Anexo 9 Formato de encuesta a estudiantes, profesores y administrativos