UNIVERSIDAD NACIONAL DE CHIMBORAZO
FACULTAD DE INGENIERÍA
CARRERA DE INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

Modelo Zero Trust Access para la protección contra bots en Azure utilizando Redes Neuronales Recurrentes

Trabajo de titulación para optar al título de
Ingeniera en Tecnologías de la Información

Autor:
Cristina Angelica Suarez Oñate

Tutor:
Ing. José Luis Jinez Tapia

Riobamba, Ecuador. ***2025***

DECLARATORIA DE AUTORÍA

Yo, Cristina Angelica Suarez Oñate, con cédula de ciudadanía 0954153391, autora del trabajo de investigación titulado: MODELO ZERO TRUST ACCESS PARA LA PROTECCIÓN CONTRA BOTS EN AZURE UTILIZANDO REDES NEURONALES RECURRENTES, certifico que la producción, ideas, opiniones, criterios, contenidos y conclusiones expuestas son de mi exclusiva responsabilidad.

Asimismo, cedo a la Universidad Nacional de Chimborazo, en forma no exclusiva, los derechos para su uso, comunicación pública, distribución, divulgación y/o reproducción total o parcial, por medio físico o digital; en esta cesión se entiende que el cesionario no podrá obtener beneficios económicos. La posible reclamación de terceros respecto de los derechos de autora de la obra referida será de mi entera responsabilidad; librando a la Universidad Nacional de Chimborazo de posibles obligaciones.

En Riobamba, 1 de octubre de 2024

Cristina Angelica Suarez Oñate
C.I.: 0954153391

DICTAMEN FAVORABLE DEL PROFESOR TUTOR

Quien suscribe, José Luis Jinez Tapia catedrático adscrito a la Facultad de Ingeniería, por medio del presente documento certifico haber asesorado y revisado el desarrollo del trabajo de investigación titulado: Modelo Zero Trust Access para la protección contra bots en Azure utilizando Redes Neuronales Recurrentes, bajo la autoría de Cristina Angelica Suarez Oñate; por lo que se autoriza ejecutar los trámites legales para su sustentación.

Es todo cuanto informar en honor a la verdad; en Riobamba, a los 08 dias del mes de octubre de 2024

José Luis Jinez Tapia

C.I: 0602899007

CERTIFICADO DE LOS MIEMBROS DEL TRIBUNAL

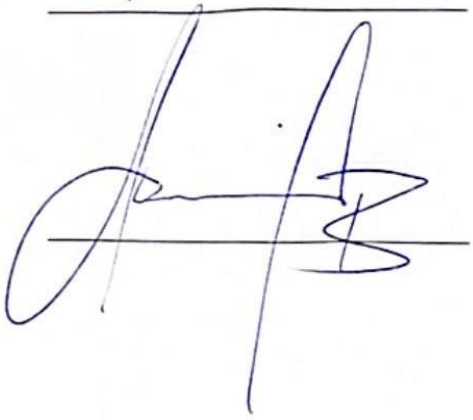
Quienes suscribimos, catedráticos designados Miembros del Tribunal de Grado para la evaluación del trabajo de investigación Modelo Zero Trust Access para la protección contra bots en Azure utilizando Redes Neuronales Recurrentes por Cristina Angelica Suarez Oñate, con cédula de identidad número 0954153391, bajo la tutoría del Ing. José Luis Jinez Tapia certificamos que recomendamos la APROBACIÓN de este con fines de titulación. Previamente, se ha evaluado el trabajo de investigación y escuchada la sustentación por parte de su autor; no teniendo más nada que observar.

De conformidad a la normativa aplicable, firmamos en Riobamba a los 16 días del mes de diciembre del 2024.

PhD. Lorena Paulina Molina Valdiviezo
PRESIDENTE DEL TRIBUNAL DE GRADO

PhD. Fernando Tiverio Molina Granja
MIEMBRO DEL TRIBUNAL DE GRADO

Mgs. Andres Santiago Cisneros Barahona
MIEMBRO DEL TRIBUNAL DE GRADO



C E R T I F I C A C I Ó N

Que, **SUAREZ OÑATE CRISTINA ANGELICA** con CC: **0954153391**, estudiante de la Carrera de **Tecnologías de la Información**, Facultad de **INGENIERÍA**; ha trabajado bajo mi tutoría el trabajo de investigación titulado "**MODELO ZERO TRUST ACCESS PARA LA PROTECCIÓN CONTRA BOTS EN AZURE UTILIZANDO REDES NEURONALES RECURRENTES**", cumple con el 4%, de acuerdo al reporte del sistema Anti plagio **TURNITIN**, porcentaje aceptado de acuerdo a la reglamentación institucional, por consiguiente autorizo continuar con el proceso.

Riobamba, 26 de noviembre de 2024

Firmado electrónicamente por:
JOSE LUIS JINEZ TAPIA

Mgs. José Luis Jinez Tapia
TUTOR

DEDICATORIA

A mi querida Juanita, mi perrita adorada, quien siempre fue el apoyo que necesitaba en mis momentos de tristeza y soledad. Tu sonrisa inigualable, cada vez que llegaba a casa, llenaba mi corazón de alegría. Gracias por tu cariño constante. Siempre estarás en mi corazón, de aquí hasta el cielo. Te quiero con todo mi ser.

Quiero dedicarme también a mí, por la perseverancia, el esfuerzo y la dedicación que he puesto en cada paso de este camino. Este logro es el resultado de muchas horas de trabajo y sacrificio, y me siento orgullosa de haber llegado hasta aquí.

Cristina Angelica Suarez Oñate

AGRADECIMIENTO

A mi familia, por su amor, paciencia y comprensión. Su apoyo incondicional me ha dado la fuerza y la motivación necesarias para superar los desafíos y alcanzar mis metas.

Especialmente, un profundo agradecimiento a mi hermano (Alex), así como a sus padres y hermanos, por el gran apoyo incondicional que me han brindado durante todos estos años.

A mis amigos, por su constante aliento y por hacer de este viaje una experiencia inolvidable. Vuestra amistad y apoyo han sido una fuente inagotable de motivación y alegría.

Finalmente, a todos aquellos que, de una u otra manera, han estado presentes en este camino, ofreciéndome su apoyo y amistad. Gracias por creer en mí y en mi capacidad para lograr este objetivo.

Cristina Angelica Suarez Oñate

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

Los bots maliciosos son una amenaza creciente en el entorno digital, especialmente para la seguridad de los recursos en línea. Este estudio aborda el problema de detección de bots maliciosos en el sitio web de la Universidad Nacional de Chimborazo. La motivación de esta investigación es mejorar la protección de los recursos digitales en entornos académicos. Se propone un modelo basado en una red neuronal recurrente para detectar estos bots y se evalúa en términos de precisión, recall y F1- score. Los resultados muestran una precisión del 100 %, un recall de 0,9998 y un F1- score de 0,9999, lo que indica que el modelo es muy eficaz para detectar bots maliciosos. Estos resultados pueden ayudar a implementar medidas de seguridad en línea más efectivas en instituciones académicas, proporcionando una herramienta eficaz para la detección temprana de amenazas.

Palabras claves: Bots maliciosos, Azure, Denegación de servicio, Zero Trust Access, Redes Neuronales Recurrentes.

ABSTRACT

Malicious bots are a growing threat in the digital environment, especially for the security of online resources. This study addresses the problem of detecting malicious bots on the National University of Chimborazo website. This research aims to improve the protection of digital resources in academic environments. A model based on a recurrent neural network is proposed to detect these bots and is evaluated in terms of precision, recall, and F1 score. The results show a precision of 100%, a recall of 0.9998, and an F1-score of 0.9999, indicating that the model effectively detects malicious bots. These results can help implement more effective online security measures in academic institutions, providing an effective tool for early threat detection.

Keywords: Malicious bots, Azure, Denial of service, Zero Trust Access, Recurrent Neural Networks.

Reviewed by:
Ms.C. Ana Maldonado León
ENGLISH PROFESSOR
C.I.0601975980

CAPÍTULO I. INTRODUCCIÓN

En el entorno digital actual, los bots maliciosos representan una amenaza creciente para la seguridad cibernética de empresas e instituciones. Estos bots son utilizados para actividades como espionaje, piratería, propagación de malware, ataques de denegación de servicio (DoS) y manipulación de datos en redes sociales [1]. Su capacidad para automatizar estas acciones a gran escala compromete la integridad de los sistemas informáticos, afectando tanto la seguridad de la información como la reputación de las entidades afectadas. En la Universidad Nacional de Chimborazo, el uso de estos bots ha comenzado a comprometer la seguridad de sus plataformas educativas.

A medida que los bots maliciosos se vuelven más sofisticados, los métodos tradicionales de detección, como el análisis de comportamiento y las huellas digitales, se muestran insuficientes para identificar estas amenazas de manera efectiva. En el contexto de la UNACH, la plataforma web que sustenta gran parte de la actividad académica se ha vuelto vulnerable a la infiltración de estos bots, lo que genera preocupaciones sobre la seguridad de los datos de estudiantes y docentes, así como sobre la disponibilidad de los servicios educativos.

La importancia de este problema radica en la necesidad urgente de proteger los recursos digitales y la información confidencial de la UNACH. La detección temprana y efectiva de bots maliciosos es clave para prevenir ataques que puedan interrumpir los servicios educativos y comprometer datos sensibles. Además, garantizar la seguridad de estas plataformas es esencial para mantener la confianza de los usuarios y proteger la reputación de la institución.

En los últimos años, varios estudios han investigado el uso de técnicas avanzadas de inteligencia artificial (IA) para la detección de bots maliciosos. Las redes neuronales recurrentes (RNN) han demostrado ser efectivas en la identificación de patrones anómalos en secuencias de datos, lo que las convierte en una herramienta ideal para detectar comportamientos sospechosos asociados a bots. Asimismo, el modelo de Zero Trust Access (ZTA) ha emergido como un enfoque innovador en ciberseguridad, al eliminar la confianza implícita en las conexiones, exigiendo autenticación constante y monitoreo continuo de los usuarios.

La motivación principal de esta investigación radica en la necesidad de abordar las limitaciones de los métodos tradicionales de detección de bots maliciosos en el entorno digital de la UNACH. La integración de tecnologías como las RNN y ZTA ofrece una solución más robusta y adaptativa frente a las amenazas avanzadas, permitiendo proteger los datos críticos y garantizar la continuidad operativa de la plataforma educativa.

El objetivo de esta investigación es implementar un modelo basado en Redes Neuronales Recurrentes (RNN) para la detección de bots maliciosos en la plataforma web de la UNACH. Este modelo se complementa con el enfoque de Zero Trust Access (ZTA) en Azure para mejorar la seguridad general, previniendo accesos no autorizados y minimizando el riesgo de ataques cibernéticos.

La propuesta combina las capacidades de las RNN para identificar patrones de tráfico anómalos con las características de seguridad del modelo ZTA en un entorno Azure. El modelo de detección de bots se entrena con datos reales de tráfico de la web de la UNACH, utilizando técnicas de inteligencia artificial que mejoran la precisión y la detección de bots maliciosos. A través de este enfoque, se logra una mejora significativa en la protección de los recursos digitales de la universidad.

La presente investigación está organizada de la siguiente manera: en la sección de metodología, se describe el diseño e implementación del modelo RNN y la integración con ZTA. La sección de resultados presenta el rendimiento del modelo basado en métricas de precisión, recall y F1-score. En la discusión, se comparan estos resultados con otros estudios previos y se analizan las implicaciones del modelo en el entorno de la UNACH. Finalmente, en la conclusión, se destacan las contribuciones del estudio y las posibles direcciones futuras para la investigación.

1.1 Planteamiento del problema

Los bots maliciosos son una amenaza creciente para las empresas que operan en entornos en línea. Estos bots pueden acceder a información confidencial, realizar ataques de denegación de servicio (DoS) y dañar gravemente la experiencia del usuario. Las soluciones tradicionales de seguridad perimetral se ven abrumadas por esta amenaza, ya que los bots pueden imitar el comportamiento humano y eludir las medidas de seguridad establecidas.

Este problema se extiende incluso a sitios web de instituciones educativas, como la Universidad Nacional de Chimborazo, donde los datos y recursos en línea también están en riesgo de ser comprometidos por actividades maliciosas de bots.

Con el objetivo de dar solución a la actividad maliciosa de los bots, surge la necesidad de desarrollar estrategias más sofisticadas y adaptables que permitan detectar estos ataques de manera eficiente.

Se propone el uso de redes neuronales recurrentes (RNN) como una estrategia avanzada que cumple con estas características de sofisticación y adaptabilidad. Las RNN son capaces de aprender patrones complejos en el tráfico de red y adaptarse a nuevos comportamientos maliciosos, lo que las convierte en una herramienta confiable para detectar ataques de DoS y proteger los recursos en línea de la Universidad Nacional de Chimborazo.

Este enfoque permite implementar un sistema que responde de manera dinámica y precisa a las amenazas emergentes.

1.2 Justificación

Aunque existen diversos estudios sobre la detección de ataques de denegación de servicio (DoS) y el uso de redes neuronales recurrentes (RNN), la aplicación específica de las RNN para detectar bots maliciosos en entornos educativos sigue siendo limitada. Esta área representa una oportunidad para profundizar en cómo las RNN pueden aplicarse eficazmente para fortalecer la seguridad en instituciones educativas, como la Universidad Nacional de Chimborazo. Al explorar este enfoque, la presente investigación busca aportar una contribución significativa al campo, ofreciendo un análisis más completo y adaptado a las necesidades de este entorno particular.

Además, la relevancia práctica de esta investigación es innegable. En un contexto donde la ciberseguridad es una prioridad crítica, la protección contra bots es de suma importancia, especialmente en plataformas que gestionan datos y recursos educativos sensibles. Al desarrollar un modelo de RNN enfocado en la detección de bots maliciosos.
La necesidad de innovación tecnológica también respalda esta investigación. Las redes neuronales recurrentes representan un avance significativo en la detección de comportamientos maliciosos, ya que son capaces de analizar secuencias de datos y aprender patrones complejos a lo largo del tiempo. Este enfoque podría lograr una identificación más precisa y oportuna de actividades sospechosas en los sistemas de la UNACH, mejorando así la postura de seguridad general de la institución.

Por último, los beneficios potenciales que esta investigación podría aportar a la comunidad educativa y a la sociedad en general son notables. Los resultados obtenidos podrían traducirse en soluciones prácticas y aplicables para instituciones educativas que buscan proteger sus recursos en línea. Un modelo mejorado de detección de bots podría ayudar a prevenir la fuga de datos, la interrupción de servicios educativos y otros tipos de ataques cibernéticos, lo que a su vez fortalecería la confianza en la infraestructura tecnológica de las instituciones educativas y la reputación de estas.

1.3 Formulación del problema

¿Qué tan confiables son las redes neuronales recurrentes (RNN) en la detección de bots maliciosos para proteger la página web de la Universidad Nacional de Chimborazo (UNACH) contra ataques de denegación de servicio (DoS)?

1.4 Objetivos

Objetivo general

Adaptar el modelo de Zero Trust Access (ZTA) para la protección contra bots en Azure utilizando Redes Neuronales Recurrentes (RNN).

Objetivos específicos

- Investigar la arquitectura de ZTA y los criterios de seguridad para detectar bots en Azure.
- Integrar las RNN y el modelo ZTA en un entorno de prueba en Azure con una réplica simple de la página web de la UNACH.
- Evaluar la confiabilidad de las RNN de bots maliciosos utilizando la herramienta TensorFlow.

CAPÍTULO II. MARCO TEÓRICO

2.1 Seguridad en la era digital

En la era digital actual, la información personal y confidencial es un activo extremadamente valioso y es cada vez más importante protegerlo. El uso de Internet y la tecnología para almacenar y procesar datos se ha generalizado, tanto que la seguridad informática se ha convertido en una preocupación importante para empresas, organizaciones y usuarios individuales. La seguridad de la información incluye un conjunto de medidas, herramientas y técnicas diseñadas para proteger la confidencialidad, integridad y disponibilidad de los datos y la información gestionados por los sistemas informáticos. Los ataques cibernéticos y las amenazas informáticas, como virus, malware y piratas informáticos, pueden comprometer la seguridad de estos sistemas, provocando pérdidas financieras, daños a la reputación y riesgos para la privacidad del usuario [2].

La seguridad se vuelve un aspecto importante debido a la gran cantidad de datos personales en circulación y la conexión constante entre dispositivos y sistemas. Para garantizar la protección de la información es necesario implementar medidas de seguridad como el cifrado de datos, restringir el acceso a información sensible y actualizar constantemente los sistemas de protección. Además, los gobiernos y las organizaciones deben acelerar el desarrollo de regulaciones apropiadas para las nuevas tecnologías y garantizar la seguridad jurídica y práctica en el uso de la inteligencia artificial y los macrodatos. Los usuarios también desempeñan un papel importante en la adopción de medidas de seguridad, como limitar el intercambio de información en línea, utilizar contraseñas seguras y leer atentamente los términos y condiciones de las plataformas digitales para garantizar que sus datos personales estén protegidos [2].

2.2 Bots

2.2.1 Definición

Los bots están automatizados, lo que significa que se ejecutan según sus instrucciones sin la necesidad de que los usuarios humanos los inicien manualmente cada vez. Los bots suelen imitar o reemplazar el comportamiento humano. A menudo realizan tareas repetitivas y pueden completarlas más rápido que los humanos [3].

2.2.2 Tipos de bots maliciosos

Cualquier acción automatizada realizada por un bot que viole la intención del propietario del sitio, los términos de servicio del sitio o las reglas bots.txt del sitio con respecto al comportamiento del bot puede considerarse maliciosa. Los bots que intentan cometer delitos cibernéticos, como el robo de identidad o la apropiación de cuentas, también son bots “malos”. Aunque algunas de estas actividades son ilegales, los bots no tienen que infringir ninguna ley para ser considerados maliciosos [3].

Además, el tráfico excesivo de bots puede sobrecargar los recursos de un servidor web, ralentizando o deteniendo el servicio para usuarios humanos legítimos que intentan utilizar el sitio web o la aplicación. En ocasiones, esta práctica es intencionada y toma la forma de un ataque DoS o DDoS [3].

La actividad de los bots maliciosos incluye:

- Relleno de credenciales
- Scraping web/de contenido
- Ataques DoS o DDoS
- Descifrado de contraseñas mediante ataques de fuerza bruta
- Inventory hoarding (secuestro de inventarios)
- Contenido spam
- Recolección de direcciones de correo
- Fraude de clics

Para realizar estos ataques y ocultar la fuente del tráfico de ataque, los bots se pueden distribuir en botnet. Esto significa que otras copias del bot se ejecutan en varios dispositivos, a menudo sin el conocimiento de sus propietarios. Dado que cada dispositivo tiene su propia dirección IP, el tráfico de la botnet proviene de muchas direcciones IP diferentes, lo que dificulta identificar y bloquear su fuente [3].

2.3 Seguridad Cibernética y Riesgos Asociados

2.3.1 Definición de seguridad cibernética

La seguridad cibernética (ciberseguridad) es una colección de técnicas y procesos de diseñados para proteger computadoras, redes, programas y datos contra actividades maliciosas, ataques, destrucción o acceso no permitido [4].

2.3.2 Amenazas y riesgos asociados con los bots maliciosos

Los bots maliciosos representan una amenaza multifacética en ciberseguridad, con el potencial de desencadenar una variedad de actividades dañinas. Estos programas automatizados pueden propagar malware, realizar ataques de denegación de servicio, cometer fraude publicitario, robar información personal, manipular las redes sociales y la opinión pública, falsificar identidades, atacar la infraestructura de IoT y realizar actividades de minería de criptomonedas. Su capacidad para operar de forma autónoma y coordinada hace que sean difíciles de detectar, lo que destaca la importancia de implementar fuertes medidas de seguridad y estrategias de defensa proactivas para protegerse contra estas amenazas emergentes en el entorno digital.

2.3.3 Impacto potencial de los ataques de bots en la seguridad y la privacidad de los datos

Los ataques de bots tienen muchas consecuencias para la seguridad y la privacidad de los datos. En primer lugar, estos ataques pueden dañar la integridad y confidencialidad de los datos al facilitar la distribución de malware, lo que podría resultar en la exfiltración de datos sensibles o la corrupción de datos críticos. Además, los bots maliciosos pueden aprovechar fallas en sistemas y redes para robar información personal como nombres de usuario, contraseñas y números de tarjetas de crédito, lo que podría llevar a robos de identidad, fraude financiero y violaciones graves de la privacidad. Los ataques de bots también pueden tener un impacto en la disponibilidad de servicios en línea mediante ataques de denegación de servicio, que impiden el acceso legítimo a los servicios.

2.4 Modelos de seguridad tradicionales

Durante décadas, los modelos de seguridad tradicionales, como antivirus, firewalls y autenticación de usuarios, han desempeñado un papel importante en la protección de los sistemas contra amenazas conocidas. Sin embargo, su eficacia se ve cuestionada por la rápida evolución de las tácticas cibercriminales y la creciente complejidad del entorno tecnológico moderno. Estos sistemas suelen operar de forma estática y adoptar un enfoque ad hoc, lo que limita su capacidad para adaptarse y responder de forma proactiva a amenazas emergentes y ataques sofisticados [5].

2.5 Model Zero Trust Access (ZTA)

2.5.1 Principios y fundamentos del modelo Zero Trust

Zero Trust es un cambio de paradigma esencialmente, propone eliminar la existencia de zonas seguras dentro de las redes corporativas, sugiriendo que cada red y cada dispositivo es vulnerable por defecto y, por lo tanto, no deben considerarse zonas, equipos o dispositivos completamente seguros y usuarios completamente confiables. Es importante señalar que esta propuesta no debe implementarse de una manera completamente radical, aumentando los controles de seguridad de manera indefinida y eliminando por completo las llamadas zonas de seguridad ocultas, sino reduciendo al máximo esta zona segura y elevándola al máximo cuanto más cerca esté de la propiedad que desea proteger, mejor [6].

Es importante aclarar esto porque a veces tendemos a pensar que la confianza cero lo proporciona elimine las brechas de seguridad y convierta a todos, estén autenticados o no aquellos que no lo hacen, como usuarios iguales, este no es el caso los usuarios autenticados deberían inspirar más confianza [6].

2.5.2 Componentes de ZTA y diferencias con los enfoques tradicionales de seguridad perimetral

El enfoque Zero Trust Architecture (ZTA) se centra en proteger los activos y el acceso a los recursos en lugar de depender únicamente de la seguridad del perímetro de la red.
Los componentes clave de ZTA incluyen:

Identidad y acceso: se basa en la autenticación continua de usuarios y dispositivos antes de otorgar acceso a los recursos de la red, utilizando técnicas como la autenticación multifactor y la autorización basada en políticas [7].

Segmentación: divide la red en partes más pequeñas y seguras, limitando el movimiento lateral de las amenazas y reduciendo la superficie de ataque en caso de brecha [7].

Visibilidad y análisis de comportamiento: supervise continuamente el tráfico de la red y el comportamiento de los usuarios y dispositivos para detectar anomalías y amenazas potenciales [7].

Seguridad a nivel de aplicación: céntrese en la seguridad a nivel de aplicación, protegiendo aplicaciones y servicios individuales con medidas como el cifrado de datos y la gestión de identidad y acceso [7].

2.5.3 Del perímetro de seguridad al Zero Trust

En la figura 1 se muestra el paso de la seguridad tradicional al modelo de seguridad de la actualidad, el enfoque tradicional del control de acceso a TI se basa en restringir el acceso a la red de una empresa y luego agregar controles adicionales según corresponda. Este modelo limita todos los recursos a la conexión a la red propiedad de la empresa y se ha vuelto demasiado limitado para satisfacer las necesidades comerciales dinámicas [7].

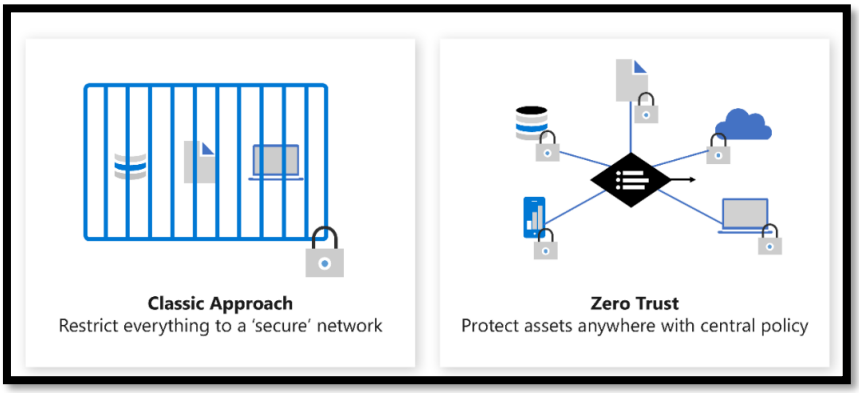


Figura 1: Del perímetro de seguridad al Zero Trust [8]

Las organizaciones deben adoptar un enfoque de confianza cero para el control de acceso a medida que adoptan el trabajo remoto y utilizan la tecnología de la nube para transformar digitalmente sus modelos de negocio y de participación del cliente, su modelo de participación de los empleados y su modelo de habilitación [7].

Zero Trust ayuda a crear y mejorar continuamente las medidas de seguridad, manteniendo al mismo tiempo la flexibilidad necesaria para seguir el ritmo de este nuevo mundo. La mayoría de los caminos de Zero Trust comienzan con el control de acceso y se centran en la identidad como control principal y prioridad, y continúan adoptando la tecnología de ciberseguridad como elemento central. La tecnología de redes y las tácticas de perímetro de seguridad todavía están presentes en el paradigma moderno de control de acceso, pero no son el enfoque dominante y preferido en una estrategia integral de control de acceso [7].

2.5.4 Arquitectura de confianza cero

El enfoque Zero Trust abarca todo el dominio digital y sirve como una filosofía de seguridad integrada y una estrategia general.

La figura 2 proporciona una representación de los elementos principales que contribuyen al Zero Trust.

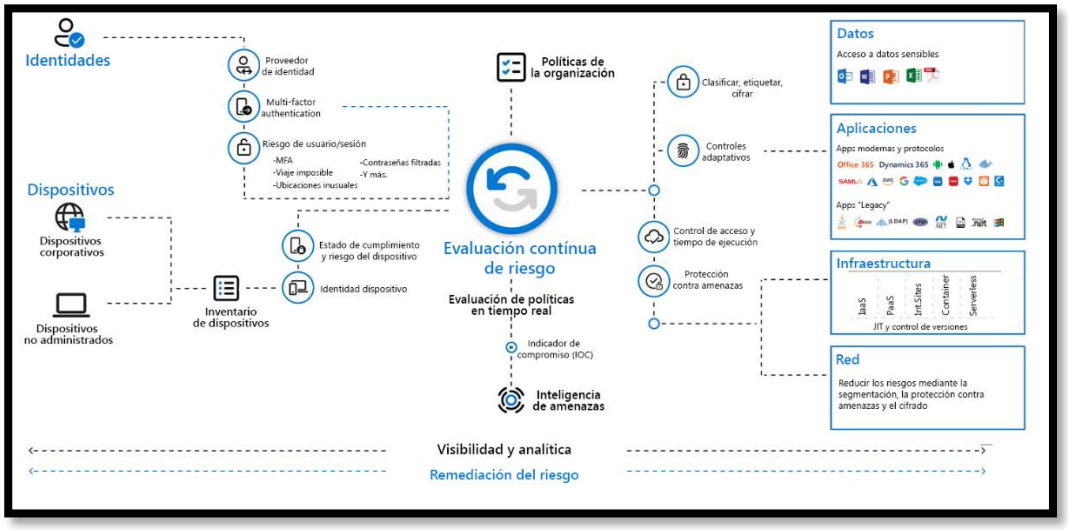


Figura 2: Elementos clave que contribuyen a Zero Trust [8]

Las organizaciones deben adoptar un enfoque de confianza cero para el control de acceso a medida que adoptan el trabajo remoto y utilizan la tecnología de la nube para transformar digitalmente sus modelos de negocio y de participación del cliente, su modelo de participación de los empleados y su modelo de habilitación [7].

Zero Trust ayuda a crear y mejorar continuamente las medidas de seguridad, manteniendo al mismo tiempo la flexibilidad necesaria para seguir el ritmo de este nuevo mundo.
La mayoría de los caminos de Zero Trust comienzan con el control de acceso y se centran en la identidad como control principal y prioridad, y continúan adoptando la tecnología de ciberseguridad como elemento central. La tecnología de redes y las tácticas de perímetro de seguridad todavía están presentes en el paradigma moderno de control de acceso, pero no son el enfoque dominante y preferido en una estrategia integral de control de acceso [7].

2.6 Redes Neuronales Recurrentes (RNN)

2.6.1 Fundamentos de las redes neuronales recurrentes

Redes Neuronales Recurrentes (RNN) es un curso de aprendizaje profundo basado en el trabajo de 1986 de David Rumelhart. Los RNN son conocidos por su capacidad para procesar secuencias de datos y extraer información. Por lo tanto, el análisis de vídeo, el procesamiento de imágenes, el procesamiento del lenguaje natural (NLP) y el análisis de música dependen de las capacidades de las redes neuronales. A diferencia de las redes neuronales artificiales vistas anteriormente que son independientes entre las entradas, los RNN capturan sus propiedades espaciales y espaciales [9].

En las redes neuronales vistas hasta ahora, la activación es en una dirección, por lo que no es recursiva, excepto en el método de retro propagación, donde se cambian los pesos para reducir el error. Por el contrario, los RNN contienen conexiones de retroalimentación que permiten a las neuronas recibir entradas del momento actual y salidas del momento anterior simultáneamente. Además, pueden analizar secuencias, lo que resulta especialmente útil si el material contiene tiempo o si su orden es importante [10].

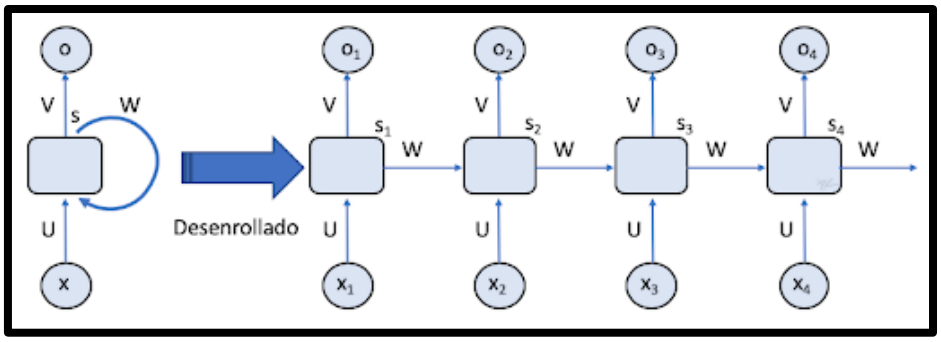


Figura 3: Esquema de una red recurrente [11]

En la figura 3 muestra el diseño y funcionamiento de redes neuronales recurrentes (RNN), lo que demuestra su capacidad para procesar datos con respuestas pasadas como entrada actual. Sin embargo, señala un problema fundamental: la pérdida de información a largo plazo debido al desvanecimiento o explosión del gradiente. Este problema se soluciona mediante dos diseños específicos: LSTM y GRU, que combinan técnicas de integración para controlar el flujo de información y mantener la memoria a largo plazo. Aunque LSTM es más complejo y requiere más parámetros que GRU, ambos resuelven el problema de la memoria corta en RNN. Además, se propone un método de inversión de tiempo para entrenar RNN, que implica descomponer una red de retroalimentación en una red de retroalimentación utilizando un método de inversión [10].

2.6.2 Arquitecturas comunes de RNN como LSTM y GRU

a) Celda LSTM

La figura 4 muestra la estructura básica de una celda LSTM (Long Short-Term Memory), destacando sus entradas y salidas. En contraste con una red recurrente básica, una celda LSTM tiene una entrada y una salida adicionales, que representan la memoria de la celda o el canal de memoria. Este canal de memoria es fundamental para mantener y gestionar la información a largo plazo, lo que ayuda a resolver el problema de la pérdida de memoria a largo plazo en las redes recurrentes tradicionales. Además, se señala que una red LSTM puede aprender dependencias tanto a corto como a largo plazo gracias a la presencia del canal de memoria y al control del flujo de información, que se logra mediante tres compuertas: la compuerta de entrada, la compuerta de olvido y la compuerta de

salida. Estas compuertas funcionan como válvulas que permiten o bloquean el paso de información, dependiendo de su estado, lo que facilita el aprendizaje de dependencias temporales complejas [10].

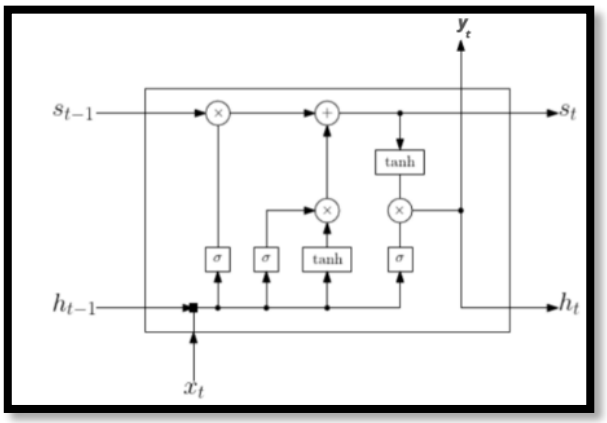


Figura 4: Diagrama de una celda LSTM [10]

b) Celda GRU

Seguidamente, se presentan de una circunstancia más esquemática el cabestrillo y el funcionamiento de las celdas GRU (Gated recurrent unit). Debido al alto rendimiento de las redes LSTM se han investigado diferentes variantes, siendo una de las más útiles, justo a su naturalidad y competencia computacional, siendo una simplificación de las anteriores. Han demostrado pegar rendimientos bastante similares a las LSTM en varios casos, por lo que tonada enormemente recomendable en datos grandes. Esta fue proporcionada por Kyunghyun Cho en 2014, introduciendo una cerca codificadora/descodificador [10].

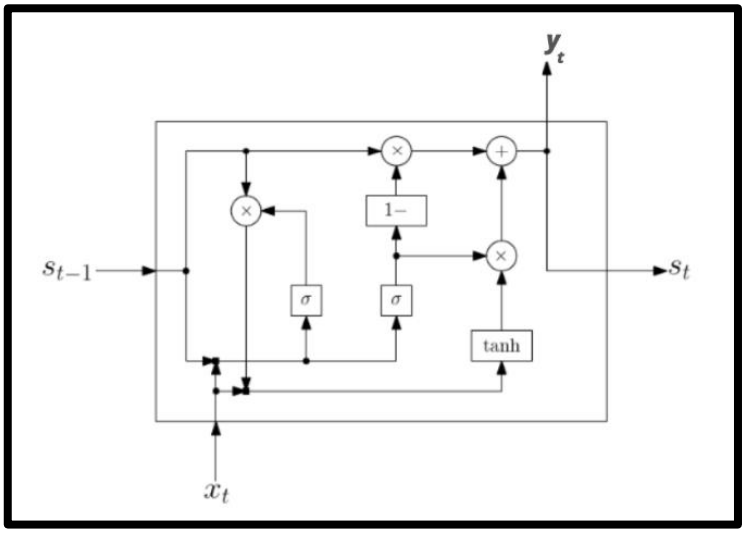


Figura 5: Diagrama de una celda GRU [10]

La figura 5 describe una celda simplificada de una arquitectura GRU (Gated Recurrent Unit), que fusiona los estados de corto y largo plazo en un solo vector *s*. Además, reduce la cantidad de puertas utilizadas a solo la puerta de reset y la

puerta de actualización. La puerta de reset (rt) decide qué información de la memoria debe mantenerse en el paso actual, basándose en el estado anterior de la red $st-1$ y los datos de entrada xt, utilizando una función sigmoide. Luego, la puerta de actualización (zt) calcula un vector que determina cuánta nueva información debe agregarse a la memoria, también utilizando el estado anterior de la red y los datos de entrada. Después, se calcula la información candidata que podría ser agregada a la memoria, utilizando una función tangente hiperbólica. Finalmente, se actualiza el estado de la red combinando el estado anterior con la nueva información, ponderada por el vector de actualización. La salida de la red se calcula de manera similar a la explicación anterior, utilizando el nuevo estado (s) como base. Este enfoque simplificado de GRU permite una gestión eficiente de la información en las redes neuronales recurrentes [10].

2.6.3 Aplicación de las RNN en la ciberseguridad

Las redes neuronales recurrentes (RNN, por sus siglas en inglés) tienen aplicaciones significativas en la ciberseguridad, particularmente en la detección de amenazas y anomalías en la red. Estas aplicaciones se centran en el análisis de patrones en datos secuenciales, lo que es esencial para identificar comportamientos sospechosos en el tráfico de red y proteger los sistemas contra ataques[12].

a. Detección de Anomalías

Las RNN son especialmente útiles para la detección de anomalías debido a su capacidad para procesar y analizar datos secuenciales. En ciberseguridad, estas redes pueden aprender patrones normales de comportamiento en el tráfico de red y detectar desviaciones que podrían indicar actividades maliciosas, como intentos de intrusión o ataques de denegación de servicio (DoS). Al entrenar una RNN con datos de tráfico normal y de ataque, es posible que la red identifique patrones anómalos en tiempo real y emita alertas para una respuesta rápida[13].

b. Detección de Malware

Otra aplicación crucial de las RNN en ciberseguridad es la detección de malware. Las RNN pueden analizar secuencias de bytes en archivos o flujos de red para identificar firmas de malware conocidas y patrones de comportamiento sospechoso. Esto permite a los sistemas de seguridad identificar y bloquear malware antes de que pueda comprometer el sistema[14].

a. Autenticación y Gestión de Acceso

Las RNN también se pueden utilizar para mejorar los sistemas de autenticación y gestión de acceso. Por ejemplo, pueden analizar patrones de uso y comportamiento de los usuarios para detectar accesos no autorizados o intentos de suplantación de identidad. Al aprender los patrones de comportamiento

habituales de los usuarios, las RNN pueden identificar y bloquear accesos que no coinciden con estos patrones[15].

b. Evaluación y Análisis

La implementación de RNN en ciberseguridad requiere una cuidadosa evaluación y análisis para garantizar su efectividad. Es fundamental entrenar las RNN con datos de alta calidad y mantenerlas actualizadas con las últimas firmas y técnicas de ataque. Además, se deben considerar las implicaciones de rendimiento, ya que el análisis en tiempo real de grandes volúmenes de datos puede ser computacionalmente intensivo[13].

2.7 Plataformas

a) Microsoft Azure

La plataforma Azure incluye más de 200 productos y servicios en la nube diseñados para ayudarlo a dar vida a nuevas soluciones para resolver los desafíos actuales y dar forma a los desafíos del mañana. Cree, administre y administre aplicaciones en la nube, en las instalaciones y en el perímetro utilizando las herramientas y marcos de su elección [16].

b) TensorFlow

Ya sea principiante o experto, TensorFlow facilita la creación de sistemas de aprendizaje automático para escritorio, dispositivos móviles, web y la nube [17].

2.8 Métodos de detección de ataques de denegación de servicios (Dos)

Detectar ataques de denegación de servicio (DoS) es fundamental para proteger los sistemas y las redes de interrupciones maliciosas. Hay varias formas de identificar estos ataques. Los métodos basados en firmas utilizan patrones conocidos para detectar ataques y son eficaces contra ataques conocidos, pero no contra ataques nuevos. Los enfoques basados en anomalías pueden identificar comportamientos anómalos en comparación con perfiles de comportamiento normales, lo que permite detectar ataques desconocidos, aunque pueden generar falsos positivos. Los métodos basados en estadísticas que analizan patrones inusuales en el tráfico de la red pueden ayudar a identificar ataques repetidos, pero requieren grandes cantidades de datos para establecer umbrales precisos. Finalmente, los enfoques híbridos combinan múltiples métodos, proporcionando mayor eficiencia y flexibilidad, pero a costa de una mayor complejidad y costos de implementación [18].

Las técnicas de aprendizaje automático mejoran significativamente la detección de ataques DoS. Los algoritmos de clasificación como las máquinas de vectores de soporte (SVM), los árboles de decisión y los bosques aleatorios se utilizan ampliamente debido a su capacidad para procesar datos de alta dimensión y su eficiencia de procesamiento. Las redes neuronales, especialmente las redes neuronales recurrentes (RNN) y las redes neuronales

convolucionales (CNN), son adecuadas para detectar patrones temporales y espaciales en el tráfico de la red. Las técnicas de agrupación como K-means y DBSCAN ayudan a identificar comportamientos anómalos agrupando datos similares. Además, las técnicas de aprendizaje profundo y de conjunto, como los codificadores automáticos y las redes generativas adversarias (GAN), proporcionan mayor precisión y solidez en la detección al combinar múltiples modelos y generar tráfico sintético para el entrenamiento. La implementación de estas técnicas requiere datos de alta calidad y un preprocesamiento adecuado para extraer características relevantes del tráfico de la red [19].

2.9 Matriz de confusión

La matriz de confusión en la tabla 1 muestra las predicciones del modelo en comparación con los valores reales. Para un problema de clasificación binaria, la matriz se presenta de la siguiente manera:

Tabla 1 Matriz de confusión

	Predicción Positiva	Predicción Negativa
Real Positivo	Verdaderos Positivos (TP)	Falsos Negativos (FN)
Real Negativo	Falsos Positivos (FP)	Verdaderos Negativos (TN)

2.9.1 Fórmulas de los parámetros de evaluación

- **Precisión**

La precisión mide la proporción de verdaderos positivos entre el total de positivos predichos. Indica cuántas de las instancias clasificadas como positivas realmente son positivas.

$$\text{Precisión} = \frac{\text{TP}}{\text{TP} + \text{FP}}$$

- **Recall**

El recall mide la proporción de verdaderos positivos entre el total de positivos reales. Indica cuántos de los casos positivos reales han sido identificados por el modelo.

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

- **F1-Score**

El F1-score es la media armónica entre la precisión y el recall. Proporciona un balance entre ambas métricas, especialmente útil en situaciones de clases desbalanceadas.

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

CAPÍTULO III. METODOLOGÍA

3.1 Metodología de investigación

Un enfoque mixto permite obtener una comprensión más completa del fenómeno estudiado, al integrar datos numéricos y análisis interpretativos. En este estudio, los datos cuantitativos, como el tráfico de red capturado y la precisión del modelo de red neuronal recurrente (RNN), se complementan con observaciones cualitativas sobre el comportamiento del sistema bajo diferentes condiciones de ataque y tráfico normal. Esta triangulación de datos asegura la validez y confiabilidad de los resultados.

3.2 Tipo de investigación

Exploratoria, ya que busca indagar en un fenómeno relativamente nuevo en el contexto de la Universidad Nacional de Chimborazo: la detección de bots maliciosos mediante redes neuronales recurrentes. Al tratarse de una problemática emergente en el campo de la seguridad informática, el objetivo principal es generar un entendimiento preliminar y descubrir patrones o tendencias que puedan ser explotados en estudios futuros o en implementaciones prácticas.

3.3 Diseño de la investigación

Cuasi experimental, dado que no se realizó una asignación aleatoria de los participantes o condiciones. En su lugar, se trabajó con un entorno controlado que replicaba las condiciones reales de una red institucional, utilizando equipos de prueba en laboratorios y simulaciones de ataques y tráfico legítimo.

3.4 Datos del estudio

Conjunto de datos sintéticos generados para representar tráfico web en un entorno de red. El conjunto de datos incluyó patrones de tráfico normales, correspondientes a usuarios legítimos, y patrones de tráfico maliciosos, representando ataques DoS. Para asegurar la validez del experimento, se generaron múltiples escenarios de tráfico, variando las intensidades y tipos de ataques para evaluar la capacidad de detección del modelo RNN.

3.5 Técnicas de recolección de datos

Herramientas como Wireshark para capturar el tráfico de red en ambos escenarios (tráfico legítimo y tráfico malicioso). Además, se simularon comportamientos automáticos con scripts de bots. Los datos fueron etiquetados manualmente para diferenciarlos entre benignos y maliciosos, y posteriormente se utilizaron para entrenar y evaluar el modelo de red neuronal recurrente (RNN).

1. Descripción de los datos obtenidos

Los datos recolectados consisten en una serie de atributos obtenidos directamente de los paquetes capturados y los registros del servidor. Entre las características más relevantes se incluyen:

- **Tamaño de los paquetes**: Refleja el volumen de datos enviados en cada transacción.
- **Protocolo de red**: Diferentes tipos de tráfico (TCP, UDP, ICMP) fueron observados y clasificados.
- **Tiempos entre paquetes (timestamps)**: Para medir la frecuencia de las solicitudes.
- **Direcciones IP**: Origen y destino de los paquetes, identificando los posibles atacantes.
- **Número de paquetes por sesión**: Para distinguir el comportamiento normal de un ataque sostenido.

El conjunto de datos final fue dividido en dos categorías principales: tráfico normal y tráfico malicioso. Estos datos fueron luego utilizados para entrenar y evaluar el modelo de red neuronal recurrente (RNN) con el fin de detectar patrones asociados con bots maliciosos.

3.6 Identificación de variables

3.6.1 Variable dependiente

Modelo redes neuronales recurrentes (RNN).

3.6.2 Variable independiente

Confiabilidad del modelo de redes neuronales recurrentes.

3.7 Operacionalización de variables

La tabla 2 muestra la operacionalización de variables para el estudio de investigación que tiene como objetivo evaluar la confiabilidad de las redes neuronales recurrentes (RNN) como un complemento para el modelo Zero Trust Access (ZTA) para la protección contra bots en Azure.

Tabla 2: Operacionalización de variables

PROBLEMA	TEMA	OBJETIVOS	VARIABLES	CONCEPTUALIZACIÓN	DIMENSIÓN	INDICADORES
¿Qué tan confiables son las redes neuronales recurrentes (RNN) en la detección de bots maliciosos para proteger la página web de la Universidad Nacional de Chimborazo (UNACH) contra ataques de denegación de servicio (DoS)?	"Modelo Zero Trust Access para la protección contra bots en Azure utilizando Redes Neuronales Recurrentes"	GENERAL • Adaptar el modelo de Zero Trust Access (ZTA) para la protección contra bots en Azure utilizando redes neuronales recurrentes (RNN). ESPECÍFICOS • Investigar la arquitectura de ZTA y los criterios de seguridad para detectar bots en Azure. • Integrar las RNN y el modelo ZTA en un entorno de prueba en Azure con una réplica simple de la página web de la UNACH. • Evaluar la confiabilidad de las RNN de bots maliciosos utilizando la herramienta TensorFlow.	INDEPENDIENTE Modelo de Redes neuronales recurrentes DEPENDIENTE Confiabilidad del modelo de redes neuronales recurrentes	Las redes neuronales recurrentes (RNN) son un tipo de modelo de aprendizaje profundo que procesa datos secuenciales, como texto o series temporales, utilizando conexiones retroalimentadas para capturar la dependencia temporal Confiabilidad se refiere a la capacidad de una aplicación para funcionar de manera consistente y predecible, sin experimentar fallas o interrupciones inesperadas, incluso bajo condiciones de carga pesada o situaciones adversas.	Redes neuronales Calidad RNN	Independiente • Tiempo de desarrollo • Número de líneas de código • Tamaño de la red • Tipo de datos Dependiente Confiabilidad: • Precisión • Recall • F1-Score

3.8 Metodología de desarrollo

En el enfoque para establecer un acceso de confianza cero, la sólida plataforma de autenticación y autorización de Microsoft fue utilizada como base. Esta solución permitió implementar un modelo de seguridad dinámico y adaptativo, donde cada solicitud de acceso fue evaluada exhaustivamente, independientemente de su origen o ubicación.

Para el desarrollo del sistema de detección de anomalías basado en redes neuronales recurrentes (RNN), se adoptó el enfoque KDD (Descubrimiento de conocimientos en bases de datos). Este enfoque proporcionó una estructura eficaz para extraer conocimiento relevante de grandes conjuntos de datos, lo que facilitó la identificación eficiente y efectiva de patrones y anomalías en el tráfico de la red.

En la figura 6 se presentó el escenario del despliegue de la página web de la UNACH que contiene la seguridad ZTA y en la figura 7 se presentó desarrollado un escenario en VMware para el consumo de las redes neuronales recurrentes para el ataque y monitorio.

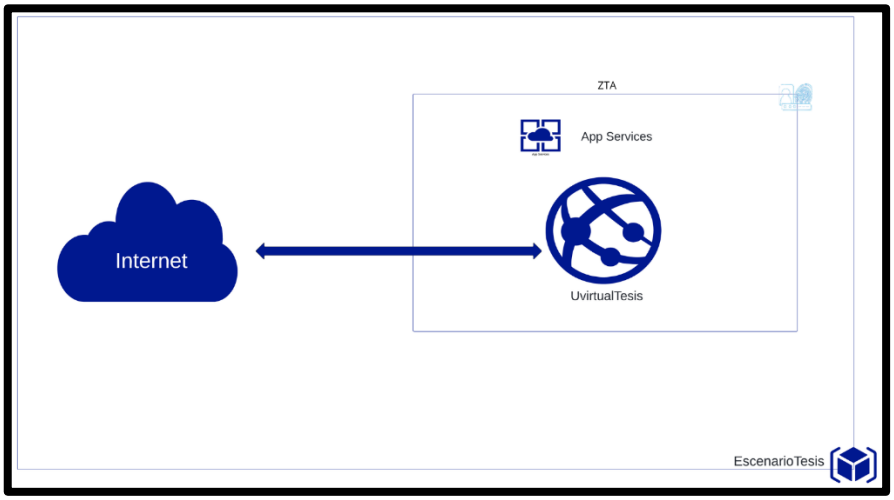


Figura 6: Escenario en Azure

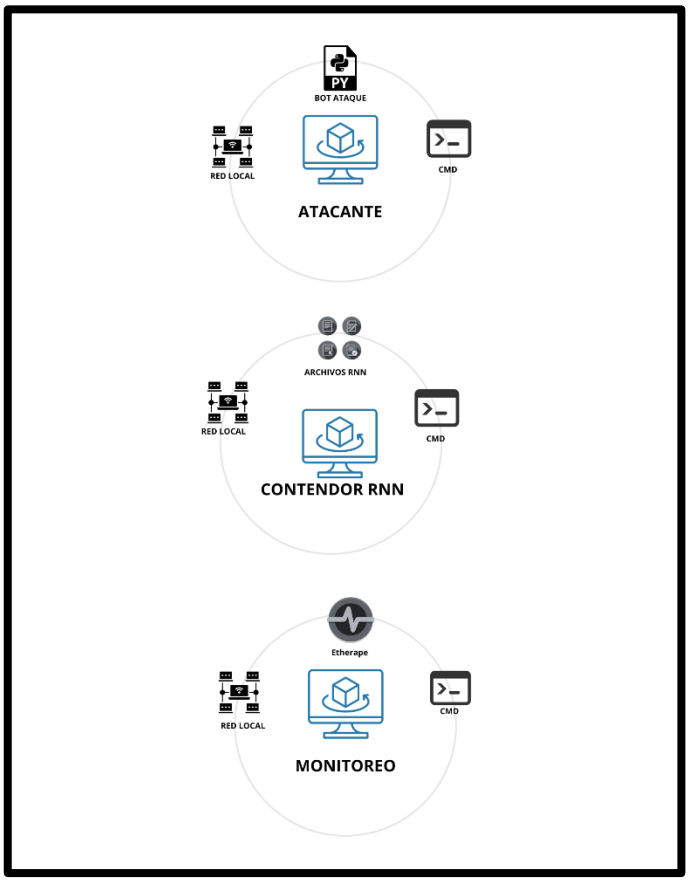


Figura 7: Escenario utilizando VMware Workstation

3.8.1 Implementación de Microsoft para Acceso de Confianza Cero en Azure App Servicie como Proveedor de Identidad

Cuando un usuario intenta acceder a la aplicación web, esta redirige al proveedor de identidades (Microsoft) para autenticarlo, solicitándole su correo electrónico y contraseña asociados. Una vez autenticado, el proveedor genera un token de acceso que contiene información sobre la identidad del usuario y sus permisos, el cual es enviado de vuelta a la aplicación. La aplicación valida este token con el proveedor para asegurar su autenticidad y garantizar que no ha sido manipulado. Si el token es válido, la aplicación web permite al usuario acceder y realizar las acciones autorizadas.

La figura 8 y 9 mostraban cuando un usuario intentaba acceder a la aplicación, solicitándole el correo y la contraseña asociados con la institución para la autenticación.

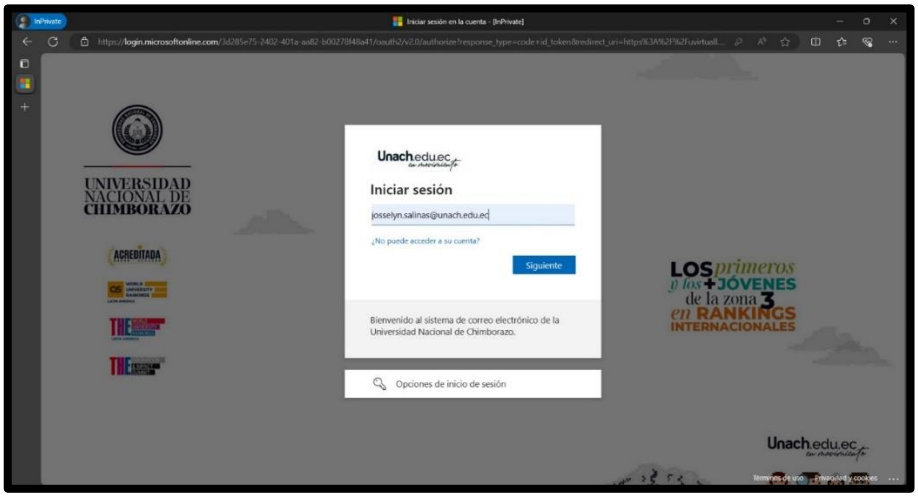


Figura 8: Ingreso de correo electrónico

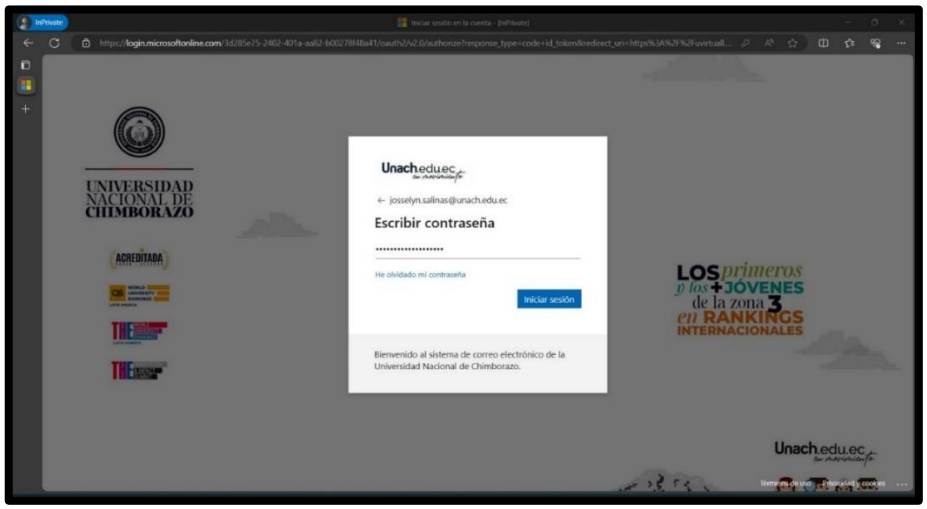


Figura 9: Ingreso de contraseña

Las figuras 10 y 11 mostraban cómo la aplicación web recibía el token de acceso y lo validaba con el proveedor de identidades para asegurarse de que fuera auténtico y no hubiera sido manipulado. Si el token era válido, la aplicación web permitía al usuario acceder y realizar las acciones autorizadas; caso contrario, deniega el acceso.

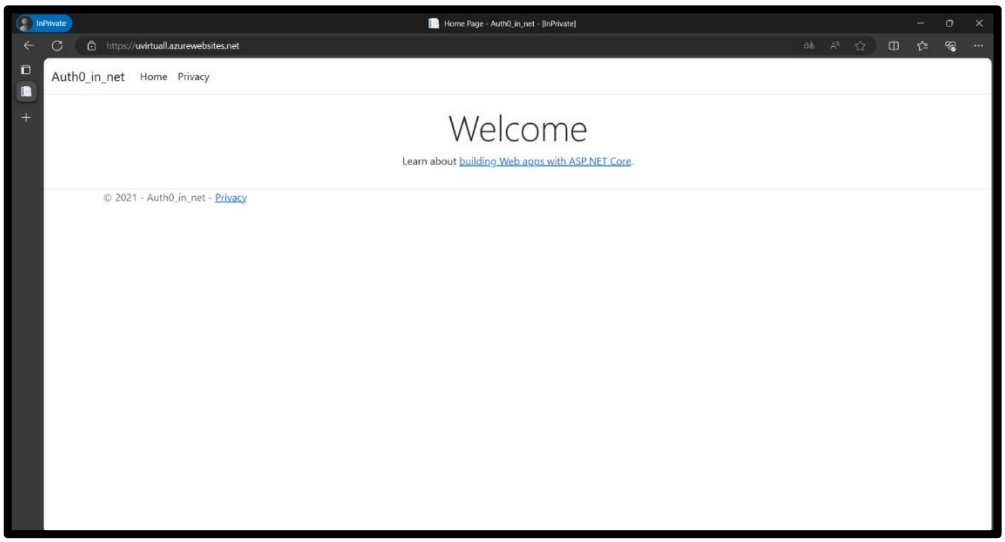


Figura 10: Inicio de la página web

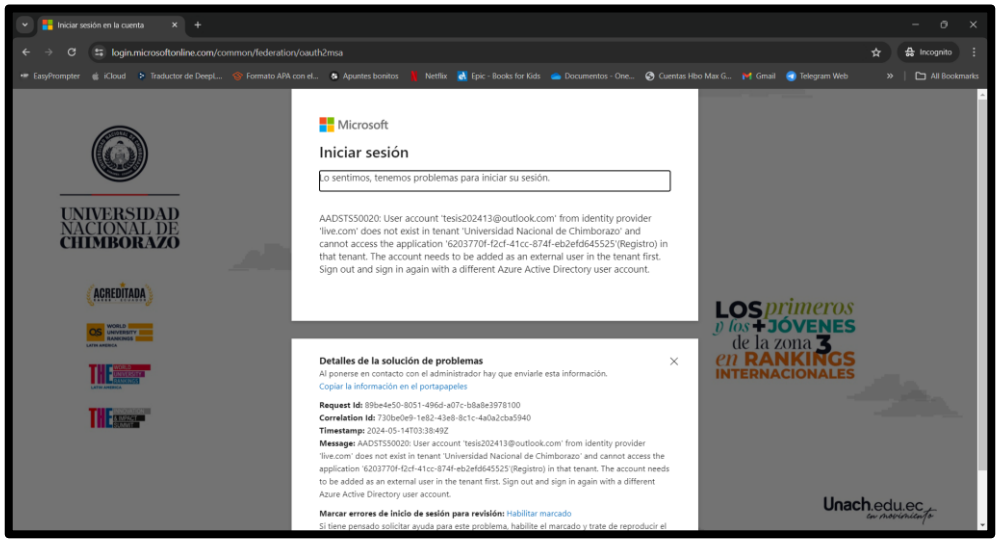


Figura 11: Negación de acceso a la página web

3.8.2 Desarrollo de un sistema de detección de anomalías basado en RNN

Se utilizó el método de ataque de bot de denegación de servicio (DoS) mediante hping3, con los parámetros --icmp --rand-source --flood -d 1400 dirigidos hacia la dirección IP 20.119.16.26. Este ataque fue empleado como parte del estudio representado en la figura 12, que ilustra el proceso KDD para el desarrollo de redes neuronales recurrentes. Este proceso constaba de las siguientes etapas:

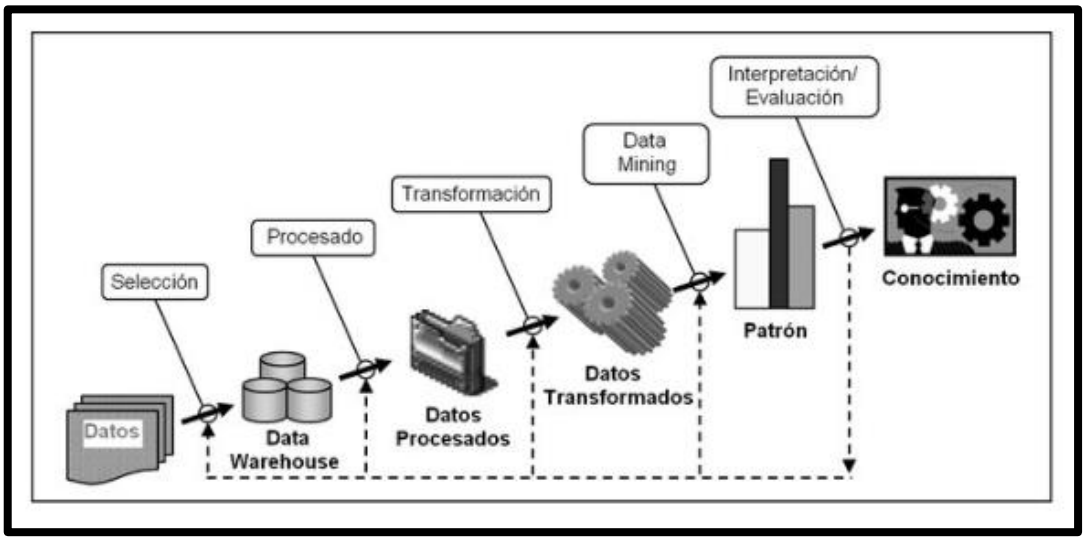


Figura 12: Etapas del proceso de KDD [20]

1. Selección de Datos

Se cargaron los datos de ataques y tráfico normal desde archivos CSV ubicados en Google Drive utilizando Pandas. Los datos se leyeron con la función read_csv (), especificando el separador como punto y coma (';').

```
# Cargar los datos de ataques de tráfico normal
ataque_data = pd. read_csv ('/content/drive/MyDrive/TESIS/ataque.csv', sep=';')
normal_data = pd. read_csv ('/content/drive/MyDrive/TESIS/normal.csv', sep=';')
```

2. Preprocesamiento de Datos

Se añadió una columna de etiqueta ('Etiqueta') a cada DataFrame para distinguir entre ataques (etiqueta 1) y tráfico normal (etiqueta 0). Luego, se combinaron los DataFrames en uno solo. Para facilitar el análisis, se codificaron los valores categóricos del campo 'Protocol' a valores numéricos utilizando LabelEncoder. Se verificó y eliminó cualquier valor nulo o infinito en los datos.

```
# Añadir la columna de etiqueta
ataque_data['Etiqueta'] = 1
normal_data['Etiqueta'] = 0
```

3. Transformación a Secuencias Temporales

Se separaron las características (variables independientes) y las etiquetas (variable dependiente) del DataFrame combinado. Las características seleccionadas fueron 'Protocol' y 'Length'. Posteriormente, se aplicó la normalización a las características utilizando MinMaxScaler para escalarlas al rango [0, 1].

```
 # Separar características y etiquetas
X = data [['Protocol', 'Length']]. values
```

4. División del Conjunto de Datos

Los datos normalizados se dividieron en conjuntos de entrenamiento y prueba utilizando train_test_split de Scikit-learn. Se utilizó un tamaño de prueba del 20% y se estratificó según las etiquetas para mantener la proporción de clases en los conjuntos de entrenamiento y prueba.

```
# Dividir los datos en conjuntos de entrenamiento y prueba
X_train, X_test, y_train, y_test = train_test_split (X_scaled, y, test_size=0.2, random_state=42, stratify=y)
```

5. Modelado

Se construyó un modelo de red neuronal secuencial utilizando Keras con TensorFlow. El modelo constó de capas densas (totalmente conectadas) con funciones de activación 'relu' en las capas ocultas y 'sigmoid' en la capa de salida, adecuada para problemas de clasificación binaria.

```
# Construir el modelo de red neuronal
model = Sequential ()
model.add (Dense (64, input_dim=X_train. shape [1], activation='relu'))
```

6. Entrenamiento del modelo

Se compiló el modelo especificando el optimizador Adam con una tasa de aprendizaje de 0.0001, la función de pérdida 'binary_crossentropy' para problemas de clasificación binaria, y se monitoreó la métrica de precisión ('accuracy'). El modelo se entrenó con los datos de entrenamiento durante 50 épocas, utilizando un tamaño de lote de 32 y reservando el 20% de los datos de entrenamiento para validación.

```
# Compilar el modelo
model. compile(optimizer=Adam(learning_rate=0.0001),
# Entrenar el modelo
history = model.fit (X_train, y_train, epochs=50, batch_size=32, validation_split=0.2)
```

7. Evaluación del modelo

Se evaluó el rendimiento del modelo entrenado utilizando los datos de prueba. Se calcularon la pérdida y la precisión del modelo y se imprimieron en pantalla para su análisis posterior.

```
# Evaluar el modelo con los datos de prueba
loss, accuracy = model. evaluate (X_test, y_test)
```

8. Despliegue de resultados

Predicciones sobre los datos de prueba y se generó un informe detallado de clasificación utilizando classification_report de Scikit-learn como se muestra en la figura 13. Además, el modelo entrenado se guardó como un archivo HDF5 en Google Drive para su posterior

uso. También se guardaron los objetos LabelEncoder y MinMaxScaler utilizando joblib para aplicar transformaciones similares en datos futuros.

```
# Evaluar el modelo con los datos de prueba
loss, accuracy = model. evaluate (X_test, y_test)
```

```
Mounted at /content/drive
17843/17843 [==============================] - 39s 2ms/step
Precision: 1.0000, Recall: 0.9998, F1-Score: 0.9999
Clasificación de Impacto: Alto Impacto
              precision    recall  f1-score   support

           0       1.00      1.00      1.00     69600
           1       1.00      1.00      1.00    501368

    accuracy                           1.00    570968
   macro avg       1.00      1.00      1.00    570968
weighted avg       1.00      1.00      1.00    570968
```

Figura 13: Informe de clasificación

3.8.3 Implementación de las RNN

Para las redes neuronales, se utilizó máquinas como Ubuntu y Kali todas con IP dinámica, como se ve en figura 14, donde se disponía de varios archivos específicos para el proyecto. Entre ellos se encontraba rnn.py, que tenía la función de capturar el tráfico de red de la aplicación web en desarrollo. Además, se contaba con modelo.h5, que representaba el modelo de red neuronal recurrente (RNN) utilizado para llevar a cabo las pruebas y análisis pertinentes durante la fase de implementación del proyecto.

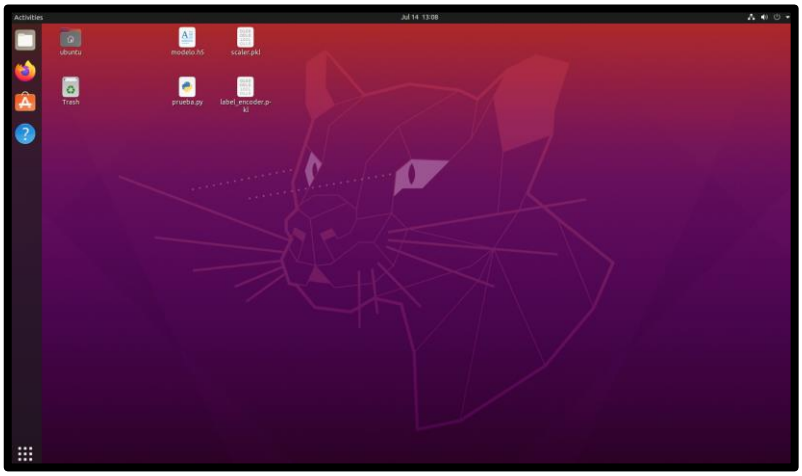


Figura 14: Consumo de RNN

La figura 15 se procedió con la ejecución del archivo que contenía todo lo referente al entrenamiento y la captura del tráfico de red.

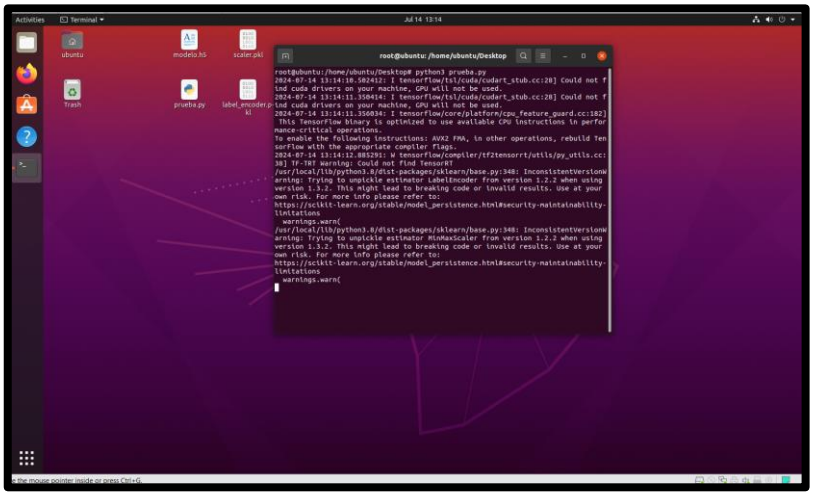


Figura 15: Ejecución de archivo .py

La figura 16 se ejecutó archivo de bot de ataque dirigido a la página web para proceder con la captura y probar el funcionamiento de las RNN (redes neuronales recurrentes).

Figura 16: Ejecución de Bot de ataque

Al momento de ejecutar el archivo **prueb.py**, comenzó la captura del tráfico de red de la aplicación web, mostrando el protocolo y la longitud del tráfico normal, tal como en la figura 17.

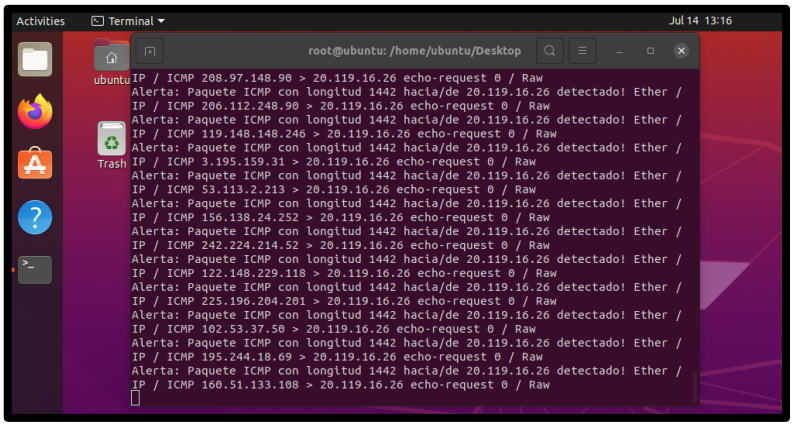


Figura 17: Captura del tráfico normal

Se realizó el ataque a la página web, lo que provocó la aparición de mensajes de alerta y ralentización del sitio, como se vio en la figura 18. Asimismo, se mostró la longitud y el protocolo del tráfico afectado.

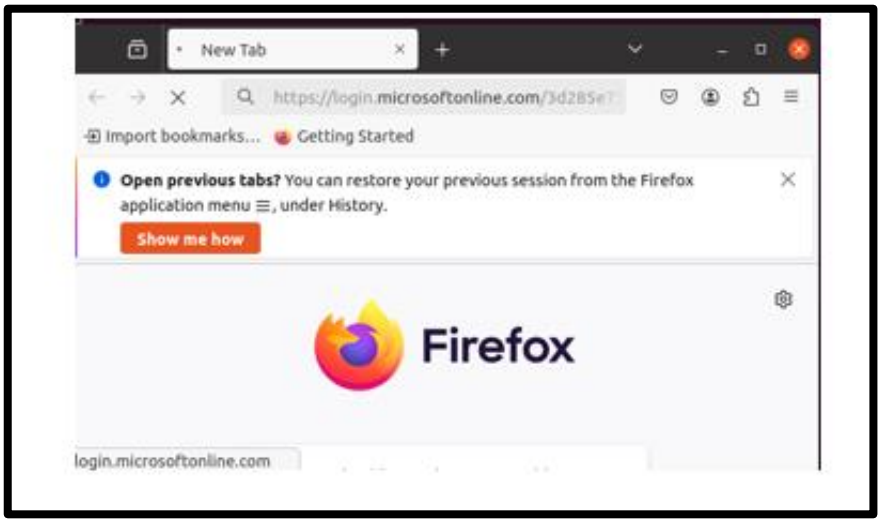


Figura 18: Captura tráfico malicioso

Al finalizar los ataques, tanto el monitoreo de la página web como las gráficas mostraron tanto el impacto de los ataques como el tráfico normal. Se generó una gráfica combinada que presentaba los resultados del análisis de los ataques en tiempo real, similar a como se muestra en la Figura 19.

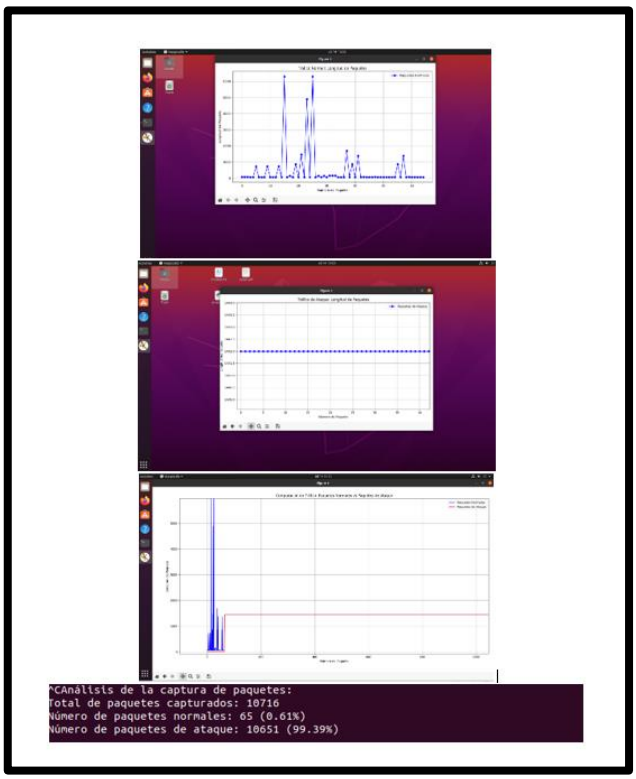


Figura 19: Análisis de captura de paquetes

Con los pasos realizados, se puede afirmar que las RNN estaban funcionando correctamente, ya que se ejecutaron pruebas mediante un ataque a la página web, lo cual generó alertas y ralentización en el sitio, mostrando además la longitud y el protocolo del tráfico afectado.

Además, se realizó el monitoreo de la red utilizando EtherApe, el cual mostró un incremento notable en los paquetes ICMP durante los ataques, y se monitoreó el rendimiento de la máquina virtual Kali Linux, como se ve en la figura 20.

Figura 20: Monitoreo

CAPÍTULO IV. RESULTADOS Y DISCUSIÓN

4.1 Resultados

La tabla 3 presenta un resumen de las características principales del modelo de red neuronal recurrente (RNN) que fue desarrollado para la detección de bots maliciosos en la red.

Tabla 3: Detalles del modelo entrenado

Característica	Descripción
Tiempo de desarrollo	8 semanas
Número de líneas de código	66 líneas de código
Tamaño de la red neuronal	2 capas ocultas con 64 y 32 neuronas, respectivamente
Tipo de datos	Tráfico de red categorizado en protocolos y longitud de paquetes
Datos de ataques	501368
Datos de tráfico normal	69600

4.1.1 Matriz de Confusión

A continuación, se presenta en la figura 22 la matriz de confusión, que es una herramienta utilizada para evaluar el desempeño de un modelo de clasificación. En este caso, la matriz de confusión se utiliza para evaluar un modelo que clasifica el tráfico de red en dos categorías. “Normal” y “Ataque”.
Vamos a desglosar los elementos de esta matriz:

- **Eje horizontal (predicción)**: Representa las predicciones hechas por el modelo. Las categorías son “Normal” y “Ataque”.
- **Eje vertical (valor real)**: Representa las verdaderas categorías de los datos. Las categorías son “Normal” y “Ataque”.

Interpretación de los números en la matriz

- **[0,0] - Verdaderos Negativos (TN)**: 69,600
  El modelo predijo “Normal” y el tráfico era realmente “Normal”. Esto indica que el modelo hizo 69,600 predicciones correctas para el tráfico normal.

- **[0,1] - Falsos Positivos (FP)**: 0
  El modelo predijo “Ataque” pero el tráfico era realmente “Normal”. Esto indica que no hubo falsas alarmas; el modelo no clasificó incorrectamente ningún tráfico normal como ataque.

- **[1,0] - Falsos Negativos (FN)**: 106
  El modelo predijo “Normal” pero el tráfico era realmente “Ataque”. Esto indica que el modelo no detectó 106 ataques, clasificándolos incorrectamente como tráfico normal.

- **[1,1] - Verdaderos Positivos (TP)**: 501,262
  El modelo predijo “Ataque” y el tráfico era realmente “Ataque”. Esto indica que el modelo detectó correctamente 501,262 instancias de ataques.

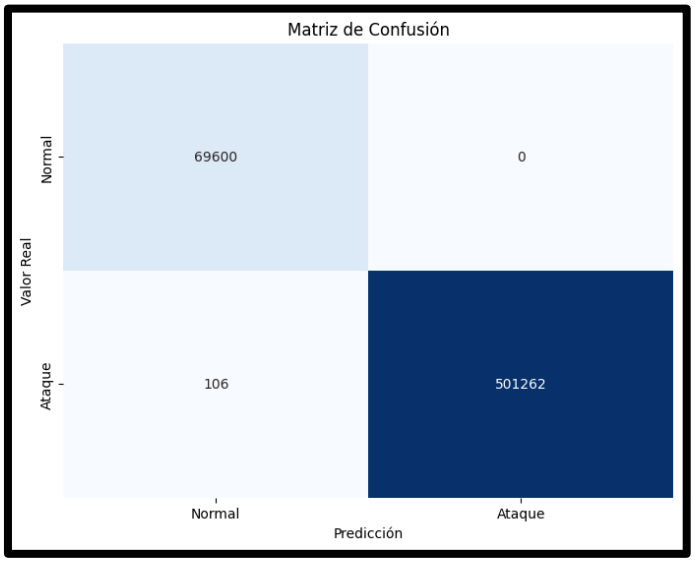


Figura 21: Matriz de confusión

4.1.2 Métricas de Evaluación

Después de entrenar el modelo de Red Neuronal Recurrente (RNN), se realizó una evaluación utilizando el conjunto de datos de prueba. Las métricas obtenidas fueron las siguientes:

Precisión:

$$\textbf{Precisión} = \frac{501{,}262}{501{,}262 + 0} = \frac{501{,}262}{501{,}262} = 1.000$$

Este valor indicó que el modelo fue capaz de identificar correctamente todos los bots maliciosos sin generar falsos positivos, es decir, todos los casos clasificados como bots fueron efectivamente maliciosos. Este resultado demostró que el modelo cumplió con uno de los objetivos principales: garantizar que no se confundiera tráfico legítimo con bots maliciosos, minimizando el riesgo de interrumpir a los usuarios legítimos.

Recall:

$$\textbf{Recall} = \frac{501{,}262}{501{,}262 + 106} = \frac{501{,}262}{501{,}268} \approx 0.9998$$

El valor de recall reflejó la capacidad del modelo para detectar la mayoría de los bots presentes en el tráfico, con un valor cercano al 100%, lo que evidenció una baja tasa de falsos negativos. En términos del objetivo de la investigación, este valor confirmó que el modelo fue altamente efectivo en la detección exhaustiva de amenazas, capturando casi todos los bots maliciosos que intentaron acceder a los recursos de la web de la UNACH.

F1-Score:

$$\textbf{F1} - \textbf{Score} = 2\text{x}\frac{1.0000\text{x}1.0000}{1.0000 + 0.9998} = 2\text{x}\frac{0.9998}{1.9998} \approx 0.9999$$

El F1-Score combinó la precisión y el recall en una sola métrica, lo que confirmó un equilibrio casi perfecto entre ambas métricas. Este valor indicó que el modelo no solo detectó correctamente los bots, sino que lo hizo con un balance óptimo entre precisión y recall, cumpliendo así el objetivo de implementar un sistema de detección eficiente y confiable. Al mantener este equilibrio, se aseguró una respuesta efectiva ante la presencia de bots maliciosos, sin generar falsos positivos ni dejar pasar amenazas inadvertidas.

Estas métricas indican un rendimiento excepcional del modelo, con valores casi perfectos en precisión, recall y F1-score como en la figura 21.

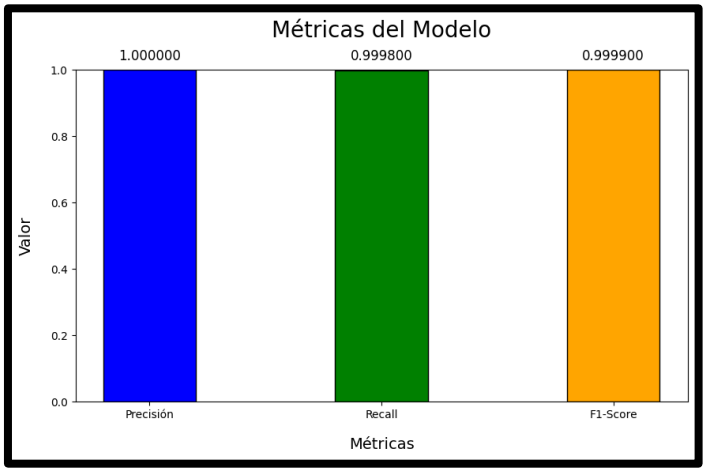


Figura 22: Métricas de evaluación

4.1.3 Gráficos de Evaluación

Los gráficos siguientes muestran las curvas de precisión-recall y ROC del modelo entrenado:

1. **Curva de Precisión-Recall:**
La curva de precisión-recall confirmó el excelente rendimiento del modelo. Mostró que tanto la precisión como el recall fueron elevados en todos los umbrales, indicando que el modelo mantuvo un equilibrio adecuado entre ambas métricas en diferentes puntos de decisión como en la figura 23.

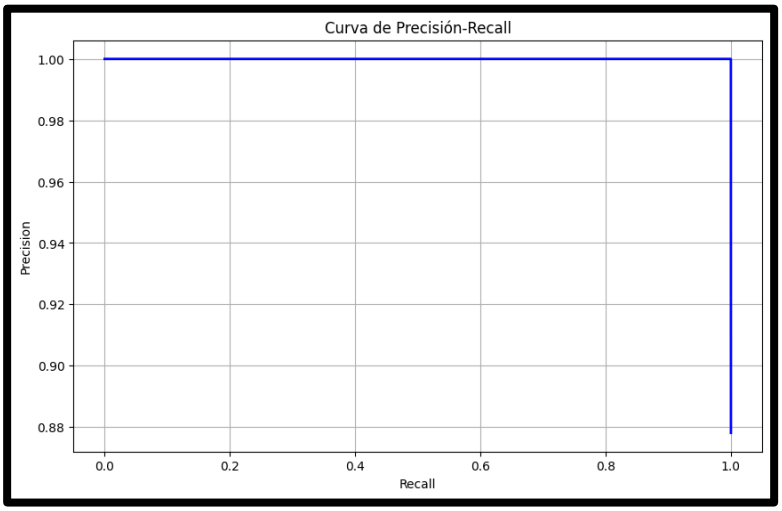


Figura 23: Curva de Precisión-Recall

2. **Curva ROC:**
Estas curvas confirmaron el rendimiento excelente del modelo, como se muestra en la figura 24. La curva ROC, con un área bajo la curva (AUC) de 1.00, indicó un rendimiento perfecto en la clasificación, separando correctamente las clases positivas de las negativas en todos los umbrales.

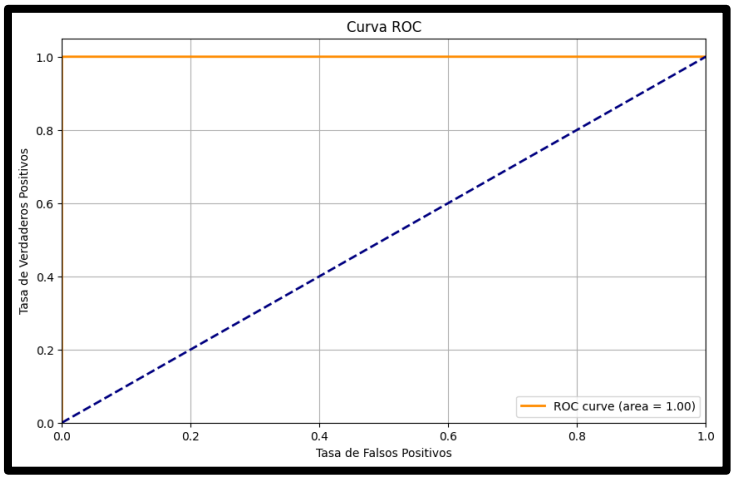


Figura 24: Curva de ROC

Estas curvas confirman el rendimiento excelente del modelo. La curva de precisión-recall muestra que la precisión y el recall son altos para todos los umbrales. La curva ROC, con un área bajo la curva (AUC) de 1.00, indica que el modelo tiene un rendimiento perfecto en la clasificación.

4.1.4 Clasificación de Impacto

El presente documento analiza la clasificación del impacto de las detecciones realizadas por el modelo propuesto. La evaluación se basa en métricas estándar de rendimiento como precisión, recall y F1-score. Según los resultados obtenidos:

- Cuando el F1-score es mayor que 0.8, se clasifica como Alto Impacto.
- Cuando el F1-score está entre 0.5 y 0.8, se clasifica como Impacto Medio.
- Cuando el F1-score es menor o igual a 0.5, se clasifica como Bajo Impacto.

El modelo ha demostrado un rendimiento excepcional en la clasificación de "Alto Impacto", alcanzando un F1-score y una precisión del 100% en esta categoría crítica.

Este análisis proporciona una base sólida para entender la capacidad del modelo en la identificación y priorización de incidentes relevantes, fundamentales para la protección de recursos en línea.

4.2 Discusión

La detección de bots maliciosos en plataformas digitales representa un desafío significativo en el ámbito de la seguridad cibernética. En este contexto, el desarrollo de un modelo de Red Neuronal Recurrente (RNN) para identificar este tipo de amenazas en el tráfico de red puede tener implicaciones importantes para futuras implementaciones.

Entorno sin el aporte del modelo.

En ausencia de un enfoque especializado como el que se propuso en este estudio, las instituciones habrían dependido de métodos tradicionales de detección. Estos métodos demostraron ser menos efectivos ante la creciente sofisticación de los bots maliciosos. Por ejemplo, los sistemas de detección de intrusos (IDS) convencionales, que a menudo se basaron en reglas y patrones estáticos, se encontraron con dificultades para adaptarse al comportamiento dinámico de los bots, lo que resultó en un aumento en los ataques de Denegación de Servicio (DoS) y un mayor riesgo de comprometer la disponibilidad de los servicios en línea.

Además, sin el uso de técnicas avanzadas como las redes neuronales recurrentes, se habrían enfrentado a altas tasas de Falsos Positivos (FP) y Falsos Negativos (FN). Esto no solo habría conducido a una utilización ineficiente de los recursos de seguridad, sino que también habría

generado desconfianza en los sistemas de detección utilizados, resultando en una respuesta a incidentes lenta y reactiva.

Entorno con el aporte del modelo.

Por otro lado, la implementación del modelo RNN en esta investigación mostró un alto potencial en la detección de bots maliciosos. Con resultados preliminares que incluyen una precisión del 100%, un recall de 0.9998 y un F1-score de 0.9999, el modelo demostró una capacidad notable para clasificar correctamente el tráfico de red entre “Normal” y “Ataque”.

Estos resultados sugieren que, de ser implementado en el futuro, este enfoque podría ser una herramienta eficaz para mejorar la detección de amenazas en tiempo real.

La baja tasa de errores, evidenciada por la matriz de confusión, indicó que el modelo tiene un rendimiento prometedor en comparación con las metodologías tradicionales. Al reducir los falsos positivos, se facilitaría la identificación de amenazas reales, lo que permitiría a los equipos de seguridad concentrarse en incidentes críticos y optimizar el uso de recursos.

En resumen, el modelo RNN desarrollado en esta investigación ofrece un enfoque innovador para la detección de bots maliciosos, con resultados que, aunque aún en fase de prueba, abren la puerta a futuras investigaciones y potenciales implementaciones en el ámbito de la seguridad cibernética. Sin este tipo de enfoque, las organizaciones seguirían enfrentando riesgos significativos en su infraestructura, lo que podría comprometer la integridad de sus datos y la confianza de sus usuarios.

CAPÍTULO V. CONCLUSIONES y RECOMENDACIONES

5.1 Conclusiones

El modelo Zero Trust Access (ZTA) y los estándares de seguridad en la plataforma Azure nos permitieron implementar un sistema robusto de control de acceso, asegurando que solo los usuarios autorizados accedan a la plataforma. Este enfoque confirma la eficacia del modelo de seguridad en la nube, al mismo tiempo que abre nuevas oportunidades para fortalecer la seguridad en entornos digitales y establece una base sólida para futuras aplicaciones e innovación.

La exitosa integración de redes neuronales recurrentes (RNN) con el modelo ZTA en un entorno de prueba replicando el sitio de la UNACH demostró la factibilidad de aplicar esta tecnología en la realidad. Los resultados experimentales confirman que el modelo puede detectar y clasificar tráfico malicioso con alta precisión, lo que muestra un amplio potencial en la protección de plataformas web en diversas industrias.

La evaluación de la confiabilidad del RNN utilizando TensorFlow produjo resultados excepcionales, con 100 % de precisión, 99,98 % de recuperación y 99,99 % de puntuación F1. Estas métricas reflejan un rendimiento excepcional en la detección de comportamientos maliciosos, lo que convierte al modelo en una solución sólida y confiable.
Esta clasificación precisa reduce los riesgos y garantiza la seguridad, lo cual es esencial para una protección eficaz en las plataformas digitales.

5.2 Recomendaciones

A futuras implementaciones del modelo ZTA y RNN que se realicen en entornos productivos diversos y complejos para evaluar y asegurar la escalabilidad y adaptación del modelo.

Es importante ajustar y optimizar el modelo en función de las características y necesidades específicas de cada organización, para maximizar su efectividad en la detección de bots.

Realizar programas de capacitación y concientización, enfocándose en el uso y gestión del modelo ZTA con RNN, así como en las mejores prácticas de seguridad en la plataforma Azure.

BIBLIOGRAFÍA

[1] A. Dolores and Z. Rendón, "Impacto de la inteligencia artificial en los ciberataques," *Revista Científica Sinapsis*, vol. 24, no. 1, pp. 2024–2030, Jun. 2024, doi: 10.37117/S.V24I1.895.

[2] M. O. Arango and G. Página, "EL ABC DE LA SEGURIDAD INFORMATICA, GUIA PRACTICA PARA ENTENDER LA SEGURIDAD DIGITAL."

[3] Cloudflare, "¿Qué es un robot? | Definición de robot." Accessed: Apr. 24, 2024. [Online]. Available: https://www.cloudflare.com/es-es/learning/bots/what-is-a-bot/

[4] D. I. Quirumbay Yagual, C. Castillo Yagual, and I. Coronel Suárez, "Una revisión del Aprendizaje profundo aplicado a la ciberseguridad," *Revista Científica y Tecnológica UPSE*, vol. 9, no. 1, pp. 57–65, Jun. 2022, doi: 10.26423/rctu.v9i1.671.

[5] D. I. Quirumbay Yagual, C. A. Castillo Yagual, I. A. Coronel Suárez, D. I. Quirumbay Yagual, C. A. Castillo Yagual, and I. A. Coronel Suárez, "Una revisión del aprendizaje profundo aplicado a la ciberseguridad," *Revista Científica y Tecnológica UPSE (RCTU)*, vol. 9, no. 1, pp. 57–65, Jun. 2022, doi: 10.26423/RCTU.V9I1.671.

[6] G. Pérez Pérez, "Zero Trust como Concepto de Seguridad."

[7] Microsoft, "Zero Trust security." Accessed: Apr. 27, 2024. [Online]. Available: https://learn.microsoft.com/en-us/azure/security/fundamentals/zero-trust

[8] Microsoft, "Seguridad de Confianza cero." Accessed: May 13, 2024. [Online]. Available: https://learn.microsoft.com/es-es/azure/security/fundamentals/zero-trust

[9] D. De Trabajo and C. Arana, "UNIVERSIDAD DEL CEMA Buenos Aires Argentina Serie," 2021. [Online]. Available: www.cema.edu.ar/publicaciones/doc_trabajo.html

[10] Juan López Segura, "Análisis de las Redes Neuronales Recurrentes: Enfoque en las LSTM y GRU para predicción."

[11] Mariano Rivera, "Introducción a Redes Neuronales Recurrentes (RNN)." Accessed: May 13, 2024. [Online]. Available: http://personal.cimat.mx:8181/~mrivera/cursos/aprendizaje_profundo/RNN_LTSM/introduccion_rnn.html

[12] D. I. Quirumbay Yagual, C. A. Castillo Yagual, I. A. Coronel Suárez, D. I. Quirumbay Yagual, C. A. Castillo Yagual, and I. A. Coronel Suárez, "Una revisión del aprendizaje profundo aplicado a la ciberseguridad," *Revista Científica y Tecnológica UPSE (RCTU)*, vol. 9, no. 1, pp. 57–65, Jun. 2022, doi: 10.26423/RCTU.V9I1.671.

[13] U. I. Especial and M. Septiembre, “Anomaly detection algorithms with deep networks. Review for Bank Fraud Detection,” *Revista Cubana de Ciencias Informáticas*, vol. 15, p. 2021, [Online]. Available: http://rcci.uci.cuPág.244-264Editorial"EdicionesFuturo"https://orcid.org/0000-0002-6734-7493OdeynisValdésSuárez1https://orcid.org/0000-0002-5847-1257HéctorGonzálezDiez1https://orcid.org/0000-0002-7601-4201

[14] “GonzalezHerreraDaniel-TFM”.

[15] J. E. Manuel, R. Campos, L. Daniel, and A. Luján, “Sistema de reconocimiento facial para el control de accesos mediante Inteligencia Artificial Facial recognition system for access control through Artificial Intelligence] , Alberto Carlos Mendoza de los Santos 4[0000-0002-0469-915X],” 2023.

[16] Azure, “¿Qué es Azure?” Accessed: Apr. 28, 2024. [Online]. Available: https://azure.microsoft.com/es-es/resources/cloud-computing-dictionary/what-is-azure/?ef_id=_k_CjwKCAjw57exBhAsEiwAaIxaZkk2xZkF_CHXcixgz5CB2xc1Lp6Wtky3PzlyoqkPJBOY_B-hYFC84xoCzb0QAvD_BwE_k_&OCID=AIDcmmvcssag76_SEM__k_CjwKCAjw57exBhAsEiwAaIxaZkk2xZkF_CHXcixgz5CB2xc1Lp6Wtky3PzlyoqkPJBOY_B-hYFC84xoCzb0QAvD_BwE_k_&gad_source=1&gclid=CjwKCAjw57exBhAsEiwAaIxaZkk2xZkF_CHXcixgz5CB2xc1Lp6Wtky3PzlyoqkPJBOY_B-hYFC84xoCzb0QAvD_BwE

[17] TensorFlow, “Introducción a TensorFlow.” Accessed: Apr. 28, 2024. [Online]. Available: https://www.tensorflow.org/learn?hl=es-419

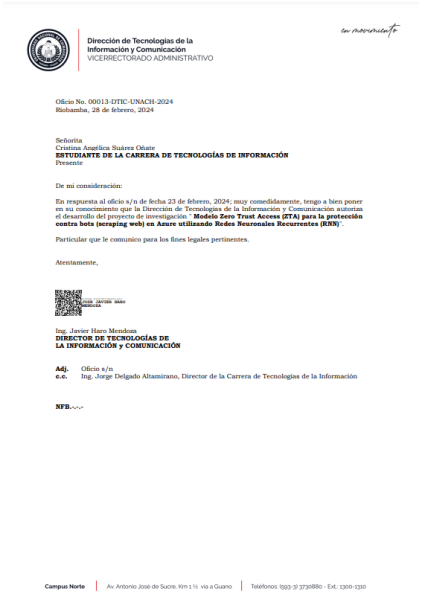
[18] S. Bravo Mullo and Á. H. Moreno, “CARACTERIZACIÓN DE LOS MÉTODOS DE DETECCIÓN DE ATAQUES DISTRIBUIDOS DE DENEGACIÓN DE SERVICIO SOBRE LA CAPA DE APLICACIÓN CHARACTERIZATION OF THE METHODS OF DETECTION OF DISTRIBUTED DENIAL OF SERVICE ATTACKS ON THE APPLICATION LAYER”.

[19] F. De Sistemas, U. De Titulación, J. Orlando, T. Portero, M. Enrique, and B. Palacios, “ESCUELA POLITÉCNICA NACIONAL,” 2023.

[20] Juan A. Lara, “Marco de Descubrimiento de Conocimiento para Datos Estructuralmente Complejos con Énfasis en el Análisis de Eventos en Series Temporales.” Accessed: May 13, 2024. [Online]. Available: https://www.researchgate.net/publication/49911537_Marco_de_Descubrimiento_de_Conocimiento_para_DatosEstructuralmente_Complejos_con_Enfasis_en_el_Analisis_de_Eventos_en_Series_Temporales

ANEXOS

Anexo 1. Autorización para el desarrollo del proyecto de investigación



Dirección de Tecnologías de la Información y Comunicación
VICERRECTORADO ADMINISTRATIVO

en movimiento

Oficio No. 00013-DTIC-UNACH-2024
Riobamba, 28 de febrero, 2024

Señorita
Cristina Angélica Suárez Oñate
ESTUDIANTE DE LA CARRERA DE TECNOLOGÍAS DE INFORMACIÓN
Presente

De mi consideración:

En respuesta al oficio s/n de fecha 23 de febrero, 2024; muy comedidamente, tengo a bien poner en su conocimiento que la Dirección de Tecnologías de la Información y Comunicación autorizas el desarrollo del proyecto de investigación " **Modelo Zero Trust Access (ZTA) para la protección contra bots (scraping web) en Azure utilizando Redes Neuronales Recurrentes (RNN)**".

Particular que le comunico para los fines legales pertinentes.

Atentamente,

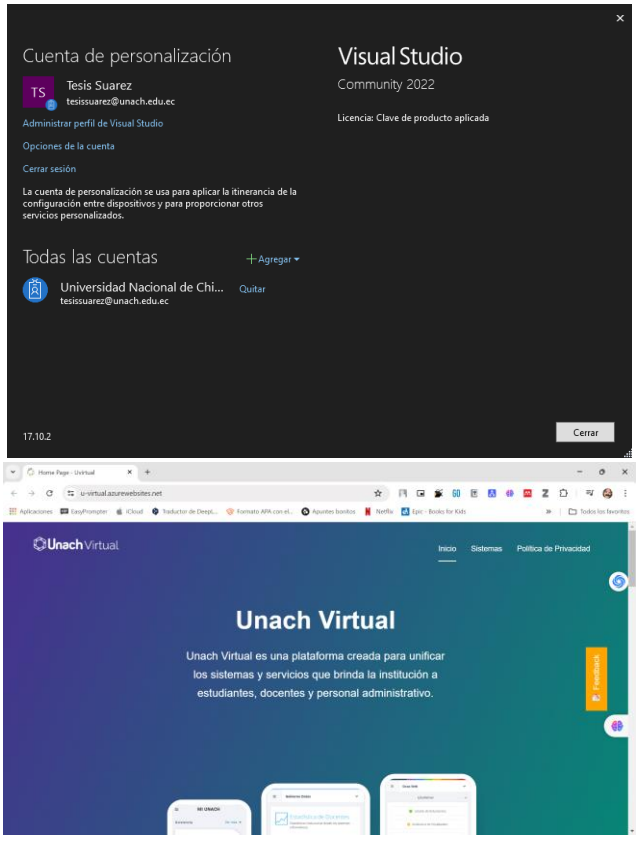
Ing. Javier Haro Mendoza
DIRECTOR DE TECNOLOGÍAS DE LA INFORMACIÓN y COMUNICACIÓN

Adj. Oficio s/n
c.c. Ing. Jorge Delgado Altamirano, Director de la Carrera de Tecnologías de la Información

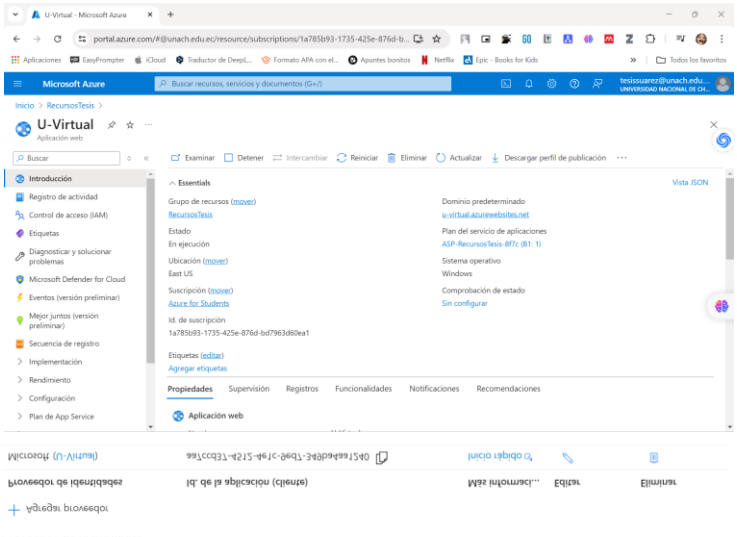
NFB.

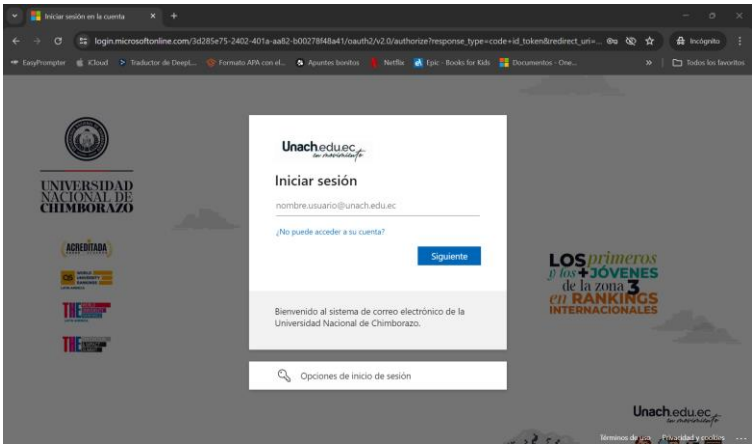
Campus Norte | Av. Antonio José de Sucre. Km 1 ½ vía a Guano | Teléfonos: (593-3) 3730880 - Ext. 1300-1310

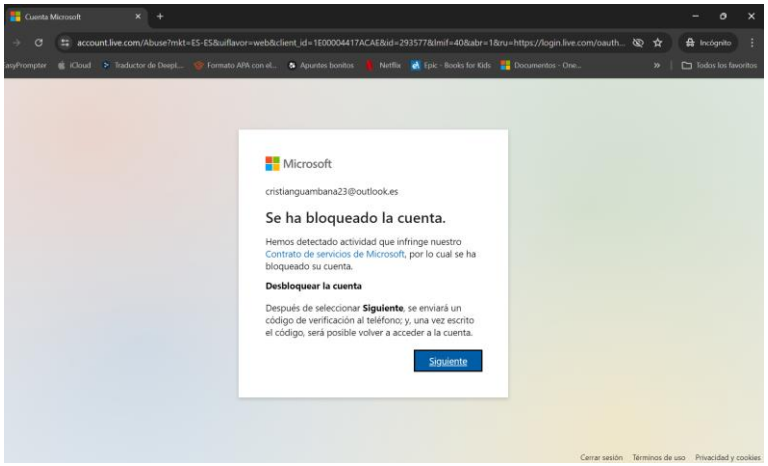
Anexo 2. Publicación de la Página Web



Anexo 3. Creación de App Servicie Azure con Proveedor de Identidades







Anexo 4. Entrenamiento de Redes Neuronales Recurrentes: