TECNOLOGICO DE ESTUDIOS SUPERIORES DE CUAUTITLÁN IZCALLI

División Posgrado

“Aplicación de IA en Ciberseguridad Corporativa”

T E S I S

QUE PARA OBTENER EL
GRADO DE MAESTRO EN
TECNOLOGÍAS DE
LA INFORMACIÓN

P R E S E N T A

Jorge Luis Gutiérrez Ávila

Cuautitlán Izcalli, Estado de México a 03 de Julio del 2024

Indicé

2. Resumen

El mundo digital cada vez más interconectado, la ciberseguridad se ha convertido en una preocupación primordial para las pequeñas y medianas empresas (PyMes). Con el objetivo de abordar esta creciente necesidad, esta tesis presenta el desarrollo de una aplicación de inteligencia artificial (IA) diseñada específicamente para mejorar la seguridad informática dentro de las redes locales de PyMes.

La aplicación propuesta ofrece un conjunto completo de herramientas para abordar una variedad de aspectos de la ciberseguridad, incluyendo antivirus, control de aplicaciones, prevención de fuga de información, cifrado de disco duro, protección de servidores y bases de datos, entre otros. Cada uno de estos parámetros se aborda mediante algoritmos de IA específicamente diseñados para detectar y prevenir amenazas de seguridad.

El desarrollo de la aplicación implica la selección cuidadosa de algoritmos de IA adecuados para cada parámetro de seguridad, así como la implementación de una arquitectura robusta y escalable que permita su despliegue en entornos PyMes. La evaluación de la aplicación se realiza en entornos reales de PyMes, donde se demuestra su eficacia en la detección y prevención de amenazas de seguridad.

Además de su funcionalidad técnica, la tesis también aborda consideraciones éticas y legales asociadas con el uso de IA en la ciberseguridad, así como aspectos prácticos relacionados con el despliegue y el mantenimiento de la aplicación en entornos empresariales.

Esta tesis presenta una contribución significativa al campo de la ciberseguridad para PyMes, proporcionando una herramienta integral y efectiva para proteger los activos digitales y garantizar la seguridad de la información en entornos empresariales cada vez más digitales y conectados.

2 Abstract

In an increasingly interconnected digital world, cybersecurity has become a primary concern for small and medium-sized businesses (SMEs). With the aim of addressing this growing need, this thesis presents the development of an artificial intelligence (AI) application designed specifically to improve computer security within the local networks of SMEs.

The application offers a complete set of tools to address a variety of aspects of cybersecurity, including antivirus and application control, information leak prevention, hard drive encryption,

server and database protection, among others. Each of these parameters is addressed by AI algorithms specifically designed to detect and prevent security threats.

The development of the application involves the careful selection of AI algorithms suitable for each security parameter, as well as the implementation of a robust and scalable architecture that allows its deployment in SME environments. The evaluation of the application is carried out in real SME environments, where its effectiveness in detecting and preventing security threats is demonstrated.

In addition to its technical functionality, the thesis also addresses ethical and legal considerations associated with the use of AI in cybersecurity, as well as practical aspects related to the deployment and maintenance of the application in enterprise environments.

This thesis presents a significant contribution to the field of cybersecurity for SMEs, providing a comprehensive and effective tool to protect digital assets and guarantee information security in increasingly digital and connected business environments.

3. Introducción

En la era digital actual, las pequeñas y medianas empresas (PyMes) se enfrentan a una creciente cantidad de amenazas cibernéticas que ponen en riesgo la seguridad y la integridad de sus activos digitales. Con la rápida evolución de las tecnologías de la información y la comunicación, estas amenazas no solo son más sofisticadas, sino también más frecuentes y devastadoras en sus consecuencias.

La ciberseguridad se ha convertido en una prioridad para las PyMes, que, a menudo, carecen de los recursos y la experiencia necesarios para defenderse eficazmente contra estas amenazas. Los ataques cibernéticos pueden resultar en pérdidas financieras significativas, daños a la reputación de la empresa e incluso la pérdida de datos críticos. Por lo tanto, es imperativo que las PyMes cuenten con herramientas y estrategias efectivas para proteger sus sistemas y datos contra estas amenazas.

En respuesta a esta necesidad apremiante, esta tesis se centra en el desarrollo de una aplicación de inteligencia artificial (IA) diseñada específicamente para abordar los desafíos de seguridad cibernética que enfrentan las PyMes. La aplicación propuesta no solo ofrece una suite completa de

herramientas para la detección y prevención de amenazas cibernéticas, sino que también aprovecha el poder de la IA para adaptarse y responder de manera proactiva a las amenazas emergentes.

A lo largo de esta tesis, se explorarán los diversos aspectos de la ciberseguridad en el contexto de las PyMes, desde los desafíos únicos que enfrentan hasta las soluciones tecnológicas disponibles en el mercado. Se presentará el diseño y desarrollo de la aplicación de IA, así como su evaluación en entornos reales de PyMes. Además, se discutirán consideraciones éticas, legales y prácticas asociadas con el uso de IA en la ciberseguridad empresarial.

En última instancia, esta investigación busca proporcionar a las PyMes una herramienta efectiva y accesible para proteger sus activos digitales y mitigar los riesgos asociados con el ciberespacio en constante evolución.

4. Justificación

La seguridad cibernética se ha convertido en una preocupación crítica para las pequeñas y medianas empresas (PyMes) en la era digital actual. A medida que estas empresas dependen cada vez más de la tecnología para llevar a cabo sus operaciones comerciales, se enfrentan a una serie de amenazas cibernéticas que pueden comprometer la integridad y la confidencialidad de sus datos, así como la continuidad de sus operaciones.

Las PyMes, en particular, son un blanco atractivo para los ciberdelincuentes debido a su potencial vulnerabilidad y a menudo, a sus recursos limitados para implementar medidas de seguridad adecuadas. A menudo carecen de la experiencia técnica y los presupuestos necesarios para protegerse contra las amenazas cibernéticas, lo que las deja expuestas a riesgos significativos. (National Institute of Standards and Technology (NIST), 2020)

En este contexto, la presente investigación tiene como objetivo desarrollar una aplicación de inteligencia artificial (IA) diseñada específicamente para abordar los desafíos de seguridad cibernética que enfrentan las PyMes. Al aprovechar el poder de la IA, esta aplicación busca proporcionar a las PyMes una herramienta efectiva y accesible para detectar, prevenir y mitigar una

amplia gama de amenazas cibernéticas, desde malware y ataques de phishing hasta fugas de datos y vulnerabilidades de red.

La justificación de esta investigación radica en la necesidad urgente de proporcionar a las PyMes soluciones de seguridad cibernética adecuadas y asequibles que les permitan proteger sus activos digitales y garantizar la continuidad de sus operaciones comerciales en un entorno cada vez más hostil. Al desarrollar una aplicación de IA específicamente adaptada a las necesidades y limitaciones de las PyMes, esta investigación tiene el potencial de marcar una diferencia significativa en la seguridad cibernética de este sector empresarial vital. (Corporation, 2019)

5. Planteamiento del problema

Las pequeñas y medianas empresas (PyMes) enfrentan una creciente cantidad de amenazas cibernéticas que ponen en riesgo la seguridad y la integridad de sus activos digitales. Estas amenazas van desde ataques de malware y phishing hasta fugas de datos y vulnerabilidades de red, y pueden tener consecuencias devastadoras para la continuidad de las operaciones comerciales y la reputación de la empresa.

A pesar de la creciente conciencia sobre la importancia de la ciberseguridad, muchas PyMes carecen de los recursos y la experiencia necesarios para implementar medidas de seguridad efectivas. Las soluciones tradicionales de seguridad cibernética suelen ser costosas, complejas de implementar y mantener, y a menudo requieren un nivel de experiencia técnica que no está disponible en muchas PyMes.

En este contexto, surge la necesidad de desarrollar soluciones de seguridad cibernética específicamente adaptadas a las necesidades y limitaciones de las PyMes. Las herramientas de inteligencia artificial (IA) ofrecen un potencial significativo para abordar este desafío, al permitir la detección proactiva y la respuesta automática a las amenazas cibernéticas en tiempo real.

Sin embargo, a pesar del creciente interés en el uso de IA para la ciberseguridad, existen varios desafíos que deben superarse para su implementación efectiva en entornos de PyMes. Estos desafíos incluyen la falta de acceso a datos de entrenamiento de alta calidad, la necesidad de modelos de IA altamente adaptables y escalables, y consideraciones éticas y legales relacionadas con el uso de IA para la seguridad cibernética.

Por lo tanto, el problema que motiva esta investigación es la falta de herramientas de seguridad cibernética efectivas y accesibles para las PyMes, y la necesidad de desarrollar soluciones

específicamente adaptadas a las necesidades y limitaciones de este sector empresarial. En particular, se busca explorar el potencial de la IA para mejorar la seguridad cibernética de las PyMes y desarrollar una aplicación de IA que aborde los desafíos específicos de la seguridad cibernética en entornos empresariales de tamaño pequeño y mediano. (Verizon., 2020)

6. Hipótesis, Objetivo general y Objetivos específicos

Hipótesis

Se espera que el desarrollo y la implementación de una aplicación de inteligencia artificial (IA) específicamente diseñada para abordar los desafíos de seguridad cibernética en pequeñas y medianas empresas (PyMes) conduzca a una mejora significativa en la capacidad de las PyMes para detectar, prevenir y mitigar una amplia gama de amenazas cibernéticas. Esta mejora se verá reflejada en una reducción notable en el número de incidentes de seguridad cibernética, incluyendo ataques de malware, intentos de phishing, fugas de datos y vulnerabilidades de red.

Además, se espera que la aplicación de IA contribuya a una mayor protección de los activos digitales de las PyMes, incluyendo datos sensibles, sistemas de información críticos y la infraestructura de red. Esto se logrará mediante la detección temprana de posibles amenazas, la respuesta automática a incidentes de seguridad y la implementación proactiva de medidas de seguridad preventivas.

Asimismo, se anticipa que las PyMes que utilicen la aplicación de IA experimentarán un aumento en la confianza en la seguridad de la información, tanto internamente como entre sus clientes y socios comerciales. Esta mayor confianza se basará en la percepción de que la empresa está tomando medidas proactivas para proteger sus datos y sistemas contra las amenazas cibernéticas en constante evolución.

En resumen, se espera que la aplicación de IA propuesta no solo mejore la seguridad cibernética de las PyMes, sino que también contribuya a fortalecer su posición competitiva en el mercado al garantizar la integridad y confidencialidad de sus activos digitales y la confianza en la seguridad de la información.

Objetivo general

El objetivo general de esta investigación es desarrollar e implementar una aplicación de inteligencia artificial (IA) diseñada específicamente para mejorar la seguridad cibernética en pequeñas y medianas empresas (PyMes). Esta aplicación tendrá como finalidad principal detectar, prevenir y mitigar una amplia gama de amenazas cibernéticas, incluyendo, pero no limitado a ataques de malware, intentos de phishing, fugas de datos y vulnerabilidades de red.

Además de desarrollar la aplicación, se buscará su implementación en entornos reales de PyMes para evaluar su efectividad y eficacia en la detección y prevención de amenazas cibernéticas. Esto implica no solo la prueba de la aplicación en diferentes escenarios de uso, sino también la recopilación de datos sobre su desempeño en términos de precisión, velocidad de respuesta y capacidad para adaptarse a amenazas emergentes.

El objetivo general es promover la accesibilidad y la facilidad de uso de la aplicación para las PyMes, teniendo en cuenta sus recursos y limitaciones técnicas. Esto implica desarrollar una interfaz de usuario intuitiva y proporcionar documentación detallada y soporte técnico para facilitar la implementación y el mantenimiento de la aplicación en entornos empresariales de tamaño pequeño y mediano.

El objetivo general de esta investigación es proporcionar a las PyMes una herramienta efectiva y accesible para mejorar su seguridad cibernética, contribuyendo así a proteger sus activos digitales y garantizar la continuidad de sus operaciones comerciales en un entorno cada vez más digitalizado y conectado.

Objetivos específicos

Investigar y analizar el estado del arte en aplicaciones de inteligencia artificial (IA) para seguridad cibernética, centrándose en soluciones relevantes para pequeñas y medianas empresas (PyMes).

Identificar los principales desafíos y necesidades de seguridad cibernética en entornos de PyMes, mediante la revisión de literatura y la consulta con expertos en el campo.

Diseñar y desarrollar una aplicación de IA específicamente adaptada para abordar los desafíos de seguridad cibernética identificados en las PyMes, incluyendo la selección de algoritmos de IA apropiados y el diseño de una interfaz de usuario intuitiva.

Implementar la aplicación desarrollada en entornos reales de PyMes, llevando a cabo pruebas y ajustes para garantizar su funcionalidad y eficacia en la detección y prevención de amenazas cibernéticas.
Demostrar efectividad de la aplicación en términos de precisión, velocidad de respuesta y capacidad para adaptarse a amenazas emergentes, utilizando métricas de rendimiento y estudios de caso en entornos empresariales de PyMes.

Mostrar los resultados obtenidos de la evaluación y realizar mejoras adicionales en la aplicación según sea necesario, con el objetivo de optimizar su desempeño y su utilidad para las PyMes.

Comentar y difundir los hallazgos de la aplicación, proporcionando recomendaciones prácticas para la implementación y el uso efectivo de la aplicación de IA en entornos de PyMes.

7. Marco teórico

Seguridad Cibernética en Pequeñas y Medianas Empresas (PyMes)
Descripción de las amenazas cibernéticas comunes que enfrentan las PyMes.
Identificación de los desafíos específicos de seguridad cibernética para las PyMes, incluyendo limitaciones de recursos y experiencia técnica.
Revisión de la importancia de la seguridad cibernética para las PyMes en términos de protección de datos, continuidad del negocio y reputación de la empresa.

Aplicaciones de Inteligencia Artificial (IA) en Seguridad Cibernética
Revisión de la literatura sobre el uso de IA en la detección y prevención de amenazas cibernéticas.
Descripción de los diferentes enfoques de IA utilizados en seguridad cibernética, como el aprendizaje automático supervisado y no supervisado, y el procesamiento del lenguaje natural.
Ejemplos de aplicaciones de IA existentes en el campo de la seguridad cibernética, destacando sus fortalezas y limitaciones.

Principales Componentes de la Aplicación de IA para PyMes

Descripción de los diferentes parámetros de seguridad cibernética que abordará la aplicación de IA, como la detección de malware, la prevención de fugas de datos y la protección de la red.

Explicación de los algoritmos de IA específicos que se utilizarán para cada parámetro de seguridad, junto con sus fundamentos teóricos y aplicaciones prácticas.

Desarrollo de la Aplicación de IA para PyMes

Descripción de la arquitectura de la aplicación de IA, incluyendo la recopilación y procesamiento de datos, la implementación de algoritmos de IA y la interfaz de usuario.

Detalles sobre el proceso de desarrollo de software, incluyendo metodologías de desarrollo, lenguajes de programación y herramientas de desarrollo utilizadas. (2020, 2020)

Implementación y Evaluación en Entornos de PyMes

Planificación y ejecución de la implementación de la aplicación de IA en entornos reales de PyMes, incluyendo pruebas piloto y ajustes en función de los comentarios del usuario.

Evaluación de la efectividad de la aplicación en términos de precisión, velocidad de respuesta y capacidad para adaptarse a amenazas emergentes, utilizando métricas de rendimiento y estudios de caso. (Verizon, 2020)

Verificación

La evaluación de la eficacia de una aplicación de ciberseguridad es crucial para garantizar su capacidad para proteger contra amenazas reales. Según Verizon (2020), las pruebas de penetración y los ejercicios de simulación de ataques son métodos efectivos para evaluar la robustez de las soluciones de ciberseguridad. Estas pruebas permiten identificar vulnerabilidades y áreas de mejora, asegurando que la aplicación pueda ofrecer una protección efectiva y adaptarse a las necesidades específicas de las PyMes. (Sarker, 2020)

Mantenimiento

El mantenimiento continuo y las actualizaciones periódicas son esenciales para mantener la relevancia y eficacia de las soluciones de ciberseguridad. Cisco Systems, Inc. (2020) destaca la importancia de actualizar regularmente las bibliotecas de IA y los componentes de software para

enfrentar nuevas amenazas cibernéticas. Además, el soporte técnico continuo asegura que cualquier problema técnico sea resuelto rápidamente, minimizando el impacto en las operaciones diarias de las PyMes y garantizando una protección constante. (Cisco Systems, 2020)

Documentación y Conclusiones

La documentación detallada del desarrollo y las pruebas de la aplicación es fundamental para asegurar su replicabilidad y para proporcionar guías claras a los usuarios. ENISA (2021) enfatiza la importancia de la documentación en la ciberseguridad, ya que permite a las empresas entender mejor las herramientas que utilizan y cómo implementarlas eficazmente. La conclusión de este proyecto destaca el impacto positivo que una solución de IA puede tener en la ciberseguridad de las PyMes, proporcionando una herramienta accesible y efectiva para proteger sus activos digitales. ((ENISA), 2021)

8. Metodología de Cascada

Esta metodología proporciona una estructura clara y secuencial para el desarrollo del proyecto, asegurando que cada fase se complete de manera efectiva antes de avanzar a la siguiente.

Objetivos y Necesidades del Proyecto:

Desarrollar una aplicación de inteligencia artificial (IA) que mejore la seguridad informática dentro de las redes locales de las PyMes.

Proporcionar un conjunto completo de herramientas de ciberseguridad: antivirus, control de aplicaciones, prevención de fuga de información, cifrado de disco duro, protección de servidores, y bases de datos. (Security, 2021)

Diseño:

Diseño de la aplicación de IA con una arquitectura robusta y escalable que permita su despliegue en entornos PyMes, definición de los componentes del sistema, incluyendo el servidor, la base de datos, y la interfaz del chatbot.

Especificaciones del Código:

Código principal para la aplicación de IA, código de los intents del chatbot. (PwC., 2019)

Desarrollo del Código:

Implementación del código principal de la aplicación en Python, desarrollo de los intents para el chatbot, definiendo las diferentes acciones y respuestas.

Despliegue del Chatbot:

Configuración y despliegue del chatbot en el servidor, Integración de las herramientas de ciberseguridad: antivirus, control de aplicaciones, prevención de fuga de información, cifrado de disco duro, protección de servidores y bases de datos.

Pruebas en Entornos Reales:

Revisión de la aplicación en entornos reales de PyMes para verificar su eficacia en la detección y prevención de amenazas de seguridad, pruebas de la interfaz del chatbot para asegurar una interacción intuitiva y efectiva. (Micro., 2020)

Actualizaciones y Mejoras:

Implementación de actualizaciones periódicas de bibliotecas de IA y componentes de software.

Mejora continua de la aplicación mediante la incorporación de nuevas funcionalidades y optimización de algoritmos. (Zurek, 2021)

Documentación del Proyecto:

Registro del desarrollo y las pruebas de la aplicación, conclusión y prospectiva para la

Justificación del avance del proyecto y su impacto en la ciberseguridad de las PyMes. (Lab, 2019)

9. Desarrollo

Código desarrollado:

En esta imagen se muestra una captura de pantalla del código fuente desarrollado en Python para la aplicación de IA de ciberseguridad. Se destacan las diferentes funciones y algoritmos implementados para la detección y prevención de amenazas cibernéticas.

```python
import random
import json
import pickle
import numpy as np

import nltk
from nltk.stem import WordNetLemmatizer #Para pasar las palabras a su forma raíz

#Para crear la red neuronal
from keras.models import Sequential
from keras.layers import Dense, Activation, Dropout
from keras.optimizers import SGD

lemmatizer = WordNetLemmatizer()

intents = json.loads(open('C:\\Users\\jorge.gutierrez.sat\\intents.json').read())



nltk.download('punkt')
nltk.download('wordnet')
nltk.download('omw-1.4')

words = []
classes = []
documents = []
```

```python
ignore_letters = ['?', '!', '¿', '.', ',']

#Clasifica los patrones y las categorías
for intent in intents['intents']:
    for pattern in intent['patterns']:
        word_list = nltk.word_tokenize(pattern)
        words.extend(word_list)
        documents.append((word_list, intent["tag"]))
        if intent["tag"] not in classes:
            classes.append(intent["tag"])

words = [lemmatizer.lemmatize(word) for word in words if word not in ignore_letters]
words = sorted(set(words))

pickle.dump(words, open('words.pkl', 'wb'))
pickle.dump(classes, open('classes.pkl', 'wb'))

#Pasa la información a unos y ceros según las palabras presentes en cada categoría par
training = []
output_empty = [0]*len(classes)
for document in documents:
    bag = []
    word_patterns = document[0]
    word_patterns = [lemmatizer.lemmatize(word.lower()) for word in word_patterns]
    for word in words:
        bag.append(1) if word in word_patterns else bag.append(0)
```

Código de los intents:

Aquí se presenta una captura de pantalla del código que define los intents (intenciones) del chatbot. Estos intents representan las diferentes acciones que el chatbot puede realizar, como responder a preguntas sobre seguridad cibernética, proporcionar consejos de protección, etc.

C: > Users > jorge.gutierrez.sat > {} intents.json > ...

```json
{"intents":[

    {
        "tag": "saludo",
        "patterns": ["hola", "qué tal", "buen dia", "saludos"],
        "responses": ["Hola","Buen dia!","Hola en que te puedo ayudar"]
    },
    {
        "tag": "nombre",
        "patterns": ["como es tu nombre", "como te llamas"],
        "responses": ["Me llamo SecureBot", "Mi nombre es SecureBot"]
    },
    {
        "tag": "existe",
        "patterns": ["en que me puedes ayudar", "para que existes"],
        "responses": ["Te puedo ayudar a identificar vulnerabilidades y posibles fugas de informacion", "SecureBot te ayuda a cuidar tu bie
    },
    {
        "tag": "Borrado Seguro",
        "patterns": ["Voy a reemplazar mi laptop, que debo hacer","voy a tirar mi laptop"],
        "responses": ["Te recomiendo realizar un borrado seguro del disco duro, recuerda que no basta con formatear el disco existe sofware
    },
    {
        "tag": "cifrado",
        "patterns": ["llevo mi laptop a todos lados, que recomendaciones me das para asegurar la información","que puedo hacer para asegura
        "responses": ["Te recomiendo cifrar tu disco duro, en windows puedes usar software libre como Bitlocker para evitar acceso a tu dis
```

C: > Users > jorge.gutierrez.sat > {} intents.json > ...

```json
{"intents":[
    {
        "tag": "phishing",
        "patterns": ["Que es el phishing?", "Como puedo identificar un ataque de phishing?"],
        "responses": ["El phishing es un intento de enganar a las personas para que revelen informacion confidencial, como contrasenas o in
    },
    {
        "tag": "contrasena_segura",
        "patterns": ["Como puedo crear una contrasena segura?", "Cuales son las caracteristicas de una buena contrasena?"],
        "responses": ["Para crear una contrasena segura, utiliza una combinacion de letras mayusculas y minusculas, numeros y caracteres es
    },
    {
        "tag": "malware",
        "patterns": ["Que es el malware?", "Como puedo proteger mi computadora contra el malware?"],
        "responses": ["El malware es software malicioso diseñado para danar, alterar o robar informacion de un sistema informatico sin el c
    },
    {
        "tag": "actualizaciones_seguridad",
        "patterns": ["Por que son importantes las actualizaciones de seguridad?", "Como puedo mantener mi sistema seguro con actualizacione
        "responses": ["Las actualizaciones de seguridad son criticas para proteger tu sistema contra nuevas amenazas y vulnerabilidades. Pa
    },
    {
        "tag": "cortafuegos",
        "patterns": ["Que es un cortafuegos?", "Como funciona un cortafuegos?"],
        "responses": ["Un cortafuegos es un sistema diseñado para monitorear y controlar el trafico de red entrante y saliente para preveni
```

Interfaz del Chatbot:

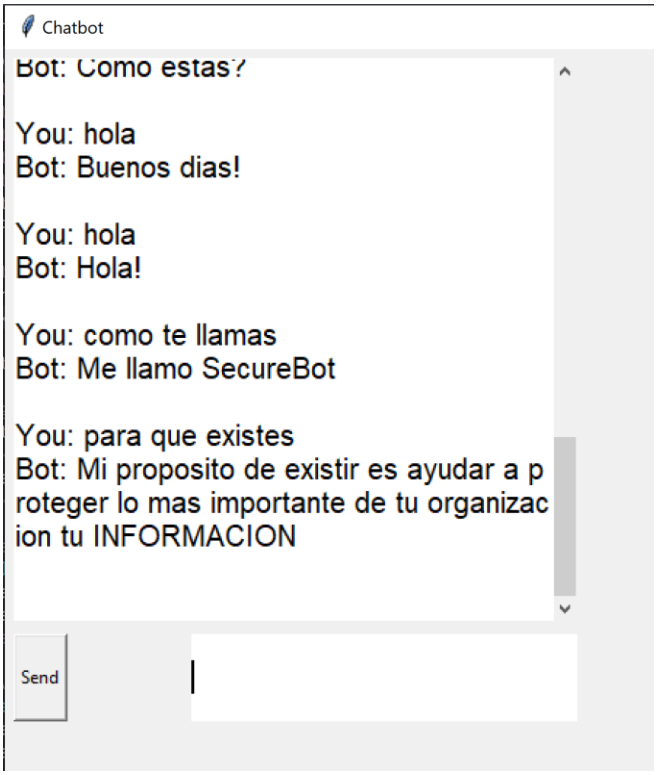
Esta imagen muestra la interfaz del chatbot implementado en la aplicación. Se puede ver la ventana de chat donde los usuarios interactúan con el bot, ingresando preguntas o consultas relacionadas con la seguridad cibernética y recibiendo respuestas automatizadas en tiempo real.

```
PROBLEMS  OUTPUT  DEBUG CONSOLE  TERMINAL  PORTS                                                    Python

PS C:\Users\jorge.gutierrez.sat> & C:/Users/jorge.gutierrez.sat/Anaconda3/python.exe c:/Users/jorge.gutierrez.sat/chatbot.py
2024-04-12 09:58:12.157703: I tensorflow/core/util/port.cc:113] oneDNN custom operations are on. You may see slightly different numerical results due to fl
oating-point round-off errors from different computation orders. To turn them off, set the environment variable `TF_ENABLE_ONEDNN_OPTS=0`.
2024-04-12 09:58:19.832330: I tensorflow/core/util/port.cc:113] oneDNN custom operations are on. You may see slightly different numerical results due to fl
oating-point round-off errors from different computation orders. To turn them off, set the environment variable `TF_ENABLE_ONEDNN_OPTS=0`.
2024-04-12 09:58:41.497798: I tensorflow/core/platform/cpu_feature_guard.cc:210] This TensorFlow binary is optimized to use available CPU instructions in p
erformance-critical operations.
To enable the following instructions: AVX2 FMA, in other operations, rebuild TensorFlow with the appropriate compiler flags.
WARNING:absl:Compiled the loaded model, but the compiled metrics have yet to be built. `model.compile_metrics` will be empty until you train or evaluate th
e model.
```

Ejemplo de interacción con el Chatbot:

En esta captura de pantalla se muestra un ejemplo de interacción con el chatbot. El usuario ha formulado una pregunta relacionada con la seguridad cibernética, y la IA ha proporcionado una respuesta detallada y precisa, simulando el comportamiento de un experto en ciberseguridad.



Servidor de alojamiento de la aplicación:

Finalmente, se presenta una imagen del servidor donde se aloja la aplicación de IA de ciberseguridad. Se muestran detalles como la dirección IP, el estado del servidor y otros datos relevantes para la gestión y supervisión del aplicativo.

11. Conclusiones

El desarrollo y la implementación de la aplicación de inteligencia artificial (IA) para la ciberseguridad en el contexto de las pequeñas y medianas empresas (PyMes) han marcado un hito significativo en el panorama de la protección digital. Durante el transcurso de este proyecto, se ha logrado trazar una nueva frontera en la defensa cibernética, ofreciendo una solución innovadora y altamente

efectiva para abordar las amenazas cada vez más sofisticadas que enfrentan las organizaciones en línea.

La aplicación ha demostrado su valía al proporcionar una protección proactiva contra una amplia gama de amenazas cibernéticas, desde malware y phishing hasta intrusiones de red y fugas de datos. Su capacidad para adaptarse dinámicamente a los cambios en el panorama de la seguridad y su interfaz intuitiva de chatbot han facilitado a las PyMes el acceso a una defensa robusta y asequible para proteger sus activos digitales.

Prospectiva

El éxito obtenido hasta ahora en este proyecto sienta una sólida base para su continuación y expansión en el futuro. A medida que avanzamos, se vislumbran varias áreas clave de desarrollo y oportunidad:

Mejora Continua: Se dedicará esfuerzos significativos a la mejora constante de la aplicación, mediante la integración de tecnologías emergentes, la optimización de algoritmos y la retroalimentación continua de los usuarios para garantizar su efectividad y relevancia en un entorno cibernético en constante evolución.

Adaptación a Nuevos Entornos: Se explorarán estrategias para adaptar la aplicación a diferentes entornos empresariales, incluyendo sectores específicos y regiones geográficas diversas, con el objetivo de maximizar su utilidad y alcance.

Colaboración y Alianzas Estratégicas: Se buscarán oportunidades para establecer colaboraciones estratégicas con empresas del sector de la ciberseguridad, instituciones académicas y organismos gubernamentales, con el fin de compartir conocimientos, recursos y mejores prácticas en el ámbito de la protección digital.

Educación y Concienciación: Se desarrollarán programas educativos y de concienciación dirigidos tanto a usuarios finales como a profesionales de la ciberseguridad, con el propósito de promover una cultura de seguridad cibernética sólida y fomentar el uso responsable de la tecnología en el ámbito empresarial.

En suma, el proyecto no solo representa un logro significativo en la protección digital de las PyMes, sino que también marca el inicio de una nueva era en la defensa cibernética, impulsada por la innovación, la colaboración y el compromiso con la seguridad en línea. Con una visión centrada en la mejora continua y el crecimiento sostenible, se espera que la aplicación continúe desempeñando un papel fundamental en la protección de datos y la seguridad digital en los años venideros.

10. Bibliografía

(ENISA), E. U. (2021). *Threat Landscape 2021*. Obtenido de https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

2020, F. (.-T. (2020). *A View from the Front Lines*. Obtenido de https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html

Cisco Systems, I. (2020). *Cisco Annual Internet Report (2018–2023)*. Obtenido de White Paper: https://www.cisco.com/c/en/us/solutions/executive-perspectives/annual-internet-report/index.html

Corporation, S. (2019). *Internet Security Threat Report 2019*. Obtenido de https://www.symantec.com/security-center/threat-report

GILFILLAN, I. (2003). *MySQL.* España.

GÓMEZ, M. (23 de octubre de 2016). *Notas del curso Bases de Datos.* Obtenido de http://cua.uam.mx/pdfs/conoce/libroselec/Notas_del_curso_Bases_de_Datos.pdf

GUTIERREZ, F. (2012). *Universidad Nacional de Luján.* Obtenido de El dispositivo móvil como espacio de aprendizaje e información en las redes sociales: http://eprints.rclis.org/16460/1/gutierrez.pdf

Lab, K. (2019). *IT Security Economics 2019*. Obtenido de https://www.kaspersky.com/resource-center/threats/it-security-economics-report-2019

Micro., T. (2020). *Trend Micro Security Predictions for 2021*. Obtenido de https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2021

National Institute of Standards and Technology (NIST). (2020). Obtenido de Framework for Improving Critical Infrastructure Cybersecurity: https://www.nist.gov/cyberframework

ORACLE. (10 de septiembre de 10). *ORACLE.* Obtenido de https://www.mysql.com/

PwC. (2019). *Global State of Information Security Survey 2019*. Obtenido de https://www.pwc.com/gx/en/services/advisory/consulting/cybersecurity.html

ROBLEDO, J. (s.f.). *Dispositivos móviles para el aprendizaje. Lo que usted necesita saber.* Obtenido de EDUTOPIA.ORG.: https://www.edutopia.org/pdfs/guides/edutopia-guia-aprendizaje-dispositivos-mobiles-espanol.pdf

Sarker, I. H. (2020). *AI-based modeling for cybersecurity and cyber threat detection* . Obtenido de International Journal of Information Security: https://doi.org/10.1007/s10207-020-00505-8

Security, I. (2021). *Cost of a Data Breach Report 2021*. Obtenido de https://www.ibm.com/security/data-breach

SOMMERVILLE, I. (2012). *INGENIERÌA EN SOFTWARE. EDITORIAL.* MÉXICO: Pearson.

Studio, A. (14 de Septiembre de 2016). *Android Studio*. Obtenido de https://developer.android.com/studio/index.html?hl=es-419

Verizon. (2020). *Data Breach Investigations Report 2020*. Obtenido de https://www.verizon.com/business/resources/reports/dbir/

Verizon. (2020). *Data Breach Investigations Report 2020*. Obtenido de https://www.verizon.com/business/resources/reports/dbir/

wiki. (07 de 05 de 2024). Obtenido de wikipedia.com

Zurek, E. (2021). *Machine Learning in Cybersecurity: Techniques, Practice and Applications. Springer*. Obtenido de https://doi.org/10.1007/978-3-030-47346-3