ANTEPROYECTO TRABAJO DE GRADO DE INVESTIGACIÓN
Centro de Investigación, Innovación y Desarrollo Empresarial (CIIDE)
Revisión 2021

Nombre proyecto:	**Análisis de malware con Inteligencia Artificial**		
Grupo de investigación:	INGENIUSH		
Línea de investigación:	Sistemas		
Periodo académico:	2	Año:	2023

Estudiante: Isabela López Cardona **Código:202110434**
Correo electrónico: **Cédula:1027660036**
isabela.lopezc@comunidad.iush.edu.co **Celular:3004693192**
Programa: Ingeniería de sistemas

Estudiante: Simón Zapata Florez **Código:202110146**
Correo electrónico: **Cédula:1055830554**
simon.zapataf@comunidad.iush.edu.co **Celular:3135884284**
Programa: Ingeniería de sistemas

Estudiante: Sebastian Zapata Zapata **Código:202110003**
Correo electrónico: **Cédula:1000759790**
sebastian.zapataz@comunidad.iush.edu.co **Celular:3016349525**
Programa: Ingeniería de sistemas

Asesor: John Byron Buitrago Paniagua
Correo electrónico: **Cédula:**
john.buitrago@salazaryherrera.edu.co **Cargo:**

GLOSARIO

IA: Campo de la informática que se enfoca en crear sistemas que puedan realizar tareas que normalmente requieren inteligencia humana, como el aprendizaje, el razonamiento y la percepción.
Malware: Cualquier tipo de software malicioso diseñado para dañar o explotar cualquier dispositivo, servicio o red programable.
Software: Conjunto de reglas o programas que dan instrucciones a un ordenador para que realice tareas específicas.
Ciberseguridad: Es la práctica de proteger equipos, redes, aplicaciones de software, sistemas críticos y datos de posibles amenazas digitales.
Machine Learning: Es la ciencia de desarrollo de algoritmos y modelos estadísticos que utilizan los sistemas de computación con el fin de llevar a cabo tareas sin instrucciones explícitas, en vez de basarse en patrones e inferencias (AWS, amazon, s.f.).

1. TEMA DEL PROYECTO

Software basado en IA para la detección de malware

Área	Porcentaje (%)
IA	30
Ciberseguridad	30
Programación	40
Total	100

2. PLANTEAMIENTO DEL PROBLEMA

Los ciberataques, según IBM, son aquellos que de manera no deseada intentan “robar, exponer, alterar, deshabilitar o destruir información” (IBM, 2020). Se llega a entender, que los ciberataques son incidentes provocados con afectaciones de índole malicioso a empresas o individuos. Estos hechos son una creciente amenaza en la actual era digital, donde el crecimiento económico y poblacional de un país va ligado indirecta y directamente al flujo de información que se registra en internet (Robledo, 2012). El crecimiento exponencial de la interconexión digital ha creado un entorno propicio para la proliferación de amenazas cibernéticas en la actualidad, donde las empresas se ven obligadas a protegerse de manera preventiva de estos incidentes. Por su parte, los

atacantes utilizan diversas técnicas y herramientas de exploración, para analizar a su objetivo y posteriormente encontrar y/o generar algún tipo de vulnerabilidad dentro del ecosistema (infraestructura) del afectado, las cuales se puede generar de una forma física, pormedio de ataques de ingeniería social, tales como *baiting* y *quid pro quo*, o de manera digital, como por ejemplo malwares, spywares, troyanos, scareware, etc (IBM, 2021). Esta diversidad creciente de técnicas dificulta la prevención y detección de los ataques.

Las intenciones de los atacantes pueden variar en cada caso, y estos podrían ser desde espionaje, sabotaje y extorsión. En este contexto, es esencial comprender a rasgos básicos la naturaleza de los ciberataques, sus tendencias actuales y las consecuencias potenciales que surgen si no se abordan de manera correcta, además, se debe considerar el impacto económico y social de estos incidentes, así como la necesidad de desarrollar estrategias de ciberseguridad sólidas, para proteger la información sensible y la infraestructura digital. Según el periódico El Tiempo, las cifras mostradas por la empresa de ciberseguridad Fortinet, "América Latina y el Caribe sufrieron más de 63 mil millones de intentos de ciberataques, Brasil recibió la mayor cantidad de intentos de ataques (23 mil millones), seguido por México (14 mil millones), Venezuela (10 mil millones), Colombia (5 mil millones) y Chile (4 mil millones)" (Díaz, 2023), si bien ha tenido una reducción a comparación el año 2022, con un registro de 6 mil millones de ataques, gracias a la adopción de *ransomware* como servicio (RaaS) (Barbosa, 2022), estos ataques se han vuelto más específicos, dirigiéndose principalmente a empresas en los sectores de tecnología, manufactura, gobierno, telecomunicaciones y salud. A partir de la información anterior, surge la siguiente incógnita, ¿es posible identificar y adaptar técnicas de entrenamiento de IA adecuadas y eficaces para el contexto local, teniendo en cuenta el ámbito económico y poblacional en Medellín? En esta creciente amenaza cibernética, esta investigación no solo tiene como objetivo determinar la técnica de entrenamiento de IA más eficaz, sino también proporcionar recomendaciones prácticas y estratégicas para su implementación efectiva en empresas ubicadas en la ciudad de Medellín. Este trabajo busca fortalecer las defensas cibernéticas de las ciudad, permitiendo proteger la información sensible, y fomentando un entorno seguro y propicio para el crecimiento económico y social.

3. ESTADO DEL ARTE Y/O MARCO TEÓRICO

Los ataques informáticos mediante malware representan una de las principales amenazas para la seguridad cibernética. Este tipo de software malicioso puede causar daños graves, como la pérdida de datos, la interrupción de los servicios y el robo de información confidencial. En este estado del arte, se examinará el análisis de programas malignos mediante el uso de técnicas de *machine*

learning, destacando la eficacia mostrada en la detección de nuevas y desconocidas amenazas cibernéticas (Navarro, 2022).

Estos ataques o malwares son usualmente propagados a través de internet, y se dividen en diversas categorías según las intenciones de los atacantes. Estas categorías incluyen infecciones por ransomware, troyanos o spyware (García, 2022). Estos softwares maliciosos pueden afectar tanto a individuos como a organizaciones completas, causando daños significativos que van desde la filtración de información confidencial hasta la pérdida de datos críticos y cuantiosas pérdidas económicas. Según estadísticas de Cybersecurity Ventures (Morgan, 2019), el costo anual de estos ataques ha ido en aumento, superando los 325 millones de dólares en 2015, 5.000 millones en 2017 y 11.500 millones en 2019 en la ciudad de Nueva York.

Para que un ciberataque tenga éxito, se requiere la ejecución de un programa capaz de dañar y modificar el comportamiento habitual de los sistemas informáticos de la víctima (Navarro, 2022). Esto a menudo involucra engañar al usuario para explotar vulnerabilidades en el sistema operativo. Los atacantes utilizan diversas técnicas de ingeniería social, como el phishing, para persuadir a las víctimas de descargar e instalar el malware.

AVTEST (AVTEST, 2023) ha informado que en los últimos años se han detectado más de 1302 millones de piezas de malware, con más de 173 millones de nuevas variantes. Este aumento exponencial en la cantidad de archivos maliciosos plantea un desafío significativo para la comunidad de la seguridad cibernética. Esto subraya la urgente necesidad de soluciones más avanzadas y efectivas, como el uso de *Machine Learning (ML)*. Al exponer constantemente al machine learning a las últimas variantes de malware, la inteligencia artificial mejora su capacidad de detección y adaptabilidad, proporcionando una defensa más robusta contra esta creciente ola de amenazas cibernéticas.

El análisis de malware mediante machine learning utiliza algoritmos de aprendizaje automático para clasificar e identificar software malicioso (García, 2022). Este analisis se divide en dos enfoques principales:

1. Basado en Características: Este enfoque utiliza características estáticas o dinámicas del malware para su identificación. Las características estáticas pueden extraerse del malware sin necesidad de ejecutarlo, como el código fuente, la estructura de archivos o las firmas de código. Las características dinámicas se obtienen al ejecutar el malware y observar su comportamiento, incluyendo patrones y llamadas a funciones.
2. Basado en Aprendizaje Automático: Este enfoque utiliza algoritmos de aprendizaje automático para identificar el malware. Estos algoritmos se entrenan en un conjunto de datos de malware conocidos para aprender a distinguir si un archivo es malicioso o no (gopinath & Chakkaravarthy, 2022).

La aplicabilidad de la inteligencia artificial en el análisis de malwares requiere enfoques de aprendizajes versátiles para lidiar con la complejidad de las decisiones autónomas frente a ataques en tiempo real. Se propone la utilización del método DQEAF (Fang, Wang, & Li, 2019) para el entrenamiento de la IA. Con un rendimiento de hasta un 75%, este método supera a las metodologías de aprendizaje supervisado, que se basan en características estáticas y son susceptibles a ataques basados en información sensible o gradiente (Anderson, Kharka, & Filar, 2017).

En este trabajo, se ha explorado y analizado un mecanismo de protección que utiliza diversos algoritmos de machine learning para la detección de malware. Se encontró que, en comparación con otros clasificadores, DT (árboles de decisión) (99%), CNN (redes neuronales convencionales) (98,76%) y SVM (Máquinas de Soporte Vectorial) (96,41%) tuvieron una mayor precisión en la detección de software malicioso cuando se combinaron con una preselección de datos específicos.

En resumen, la inteligencia artificial se ha convertido en una herramienta esencial en la ciberseguridad, especialmente debido al crecimiento exponencial de los datos generados diariamente (GRUPO BIT, 2021). La automatización de tareas se vuelve crucial, ya que resulta imposible supervisar cada proceso de manera manual. Los sistemas de inteligencia artificial pueden adaptarse y aprender de su entorno, lo que los hace óptimos para la defensa corporativa. Además, la inclusión de la nube como una capa adicional de seguridad permite el aislamiento de áreas comprometidas durante los ataques.

Este estado del arte proporciona una visión integral de cómo el machine learning y la inteligencia artificial están revolucionando la detección y prevención de amenazas cibernéticas, destacando la necesidad de una defensa cibernética cada vez más avanzada y adaptable.

4. JUSTIFICACIÓN

El crecimiento exponencial de los ciberataques y la creciente amenaza cibernética plantean un problema crítico en la actual era digital, afectando tanto a grandes empresas como a pequeñas, por ello, la implementación de una técnica basada en IA fortalecerá la capacidad de detección de malware en las empresas pequeñas, ayudando a mejorar el entorno de seguridad de los servicios que estas ofrecen.

5. OBJETIVOS

5.1. Objetivo general:

Implementar una aplicación de seguridad basada en IA para la detección y mitigación de malware en pequeñas empresas.

5.2. Objetivos específicos:

- Identificar los tipos de malware con mayor impacto que afectan a las pequeñas empresas.
- Proponer una técnica basada en IA para la prevención de malware
- Implementar la técnica basada en IA para la prevención de malware
- Medir precisión de la técnica implementada y su velocidad de respuesta.

6. METODOLOGÍA

Se realiza un estudio bibliográfico de malwares existentes para construir una sólida base de conocimientos. A continuación, se crea una tabla de resumen del estudio bibliográfico para organizar la información de manera clara y concisa. Se hace un análisis de los tipos de malware más comunes para comprender las amenazas predominantes en las pequeñas empresas.

Luego, realizamos una investigación de técnicas de machine learning para abordar la detección de malware, Basado en esto, elegimos la técnica de machine learning más integrada para desarrollarse. Procedemos con la recopilación de datos para el entrenamiento de IA para alimentar el modelo.

Iniciamos el entrenamiento de la técnica de IA utilizando los datos recopilados, Posteriormente, definimos las métricas de precisión que serán fundamentales para evaluar el rendimiento del modelo. Finalmente, llevamos a cabo la observación y medición de las métricas, para evaluar la efectividad de la técnica de IA en la detección de malware.

7. PRODUCTOS ESPERADOS

Comenzamos generando un reporte con una tabla comparativa de los tipos de malware existentes para proporcionar una visión general. Luego, exploramos una técnica basada en IA para la prevención de malware, destacando su aplicación y beneficios potenciales.

Investigamos y consideramos la implementación de software de detección de malware con IA para el fortalecimiento de las medidas preventivas, para así, presentar un informe de resultados que resuma la eficacia de la técnica basada en IA y del software de detección en la prevención de malware, incorporando datos y análisis pertinentes.

8. PRESUPUESTO

RECURSOS PRESUPUESTADOS	PARTICIPACIÓN (MILES DE PESOS)				IMPLICA DESEMBOLSO	
	EMPRESA	**ESTUDIANTE**	**IUSH**	**DONACIONES**	**SI** (nuevo)	**NO** (existente)
GASTOS DE PERSONAL						
Horas trabajo asesor temático. ($/h)						
Horas asesor metodológico($/h)						
Estímulo a estudiantes auxiliares						
GASTOS DE OPERACIÓN - ADQUISICIÓN DE BIENES						
Fotocopias y papelería						
Material bibliográfico						
Servicio de computador. ($/h)						
Internet y llamadas						
Materiales y herramientas						
Software especializado						

Equipos						
ADQUISICIÓN DE SERVICIOS						
Viáticos y gastos de viajes						
Servicios de terceros						
Procesos externos						
Imprevistos						
Mantenimiento de equipos						
Impresos y publicaciones						
Totales						
TOTAL GENERAL:						

Este ítem se diligencia cuando el proyecto es financiado por alguna entidad en particular o por la misma Universidad, de lo contrario puede omitirse del formato.

9. CRONOGRAMA DE ACTIVIDADES

Es un plan de trabajo o un plan de actividades, que muestra en un orden lógico y secuencial la duración del proceso investigativo, en una forma gráfica o de tabla. Proyectar los tiempos que cada

una de las fases previstas de la investigación se podrá demorar. No perder de vista los tiempos establecidos por la Universidad de acuerdo con cada asignatura de investigación.

Fase	Actividad	TIEMPO (Meses)											
		M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12
	Estudio bibliográfico de malwares existentes												
O.E.1	Construcción tabla de resumen de estudio bibliografico												
	Análisis de tipos de malware más comunes												
	Investigación de técnicas de machine learning												
O.E.2	Elección de técnica de Machine Learning más integrada												
	Recopilación de datos para el entrenamiento de IA												
O.E.3	Entrenamiento de técnica de IA												
	Definición de métricas de precisión												
O.E.4	Observación y medición de las métricas												
	Construcción de documento final												

10. CONFIDENCIALIDAD

Si existe necesidad de guardar reserva sobre alguna información confidencial en el proyecto debe declararse aquí.

La obligación de confidencialidad incluye la reserva, el secreto y/o privilegio, adicionalmente obliga a las partes a utilizar la información a la que se tiene acceso sólo para los fines específicos para los cuales fue solicitada, todo dentro del marco jurídico desarrollado por el artículo 15 de la Constitución Política de Colombia, la ley 1266 de 2008, la ley 1581 de 2012, los decretos reglamentarios 1727 de 2009 y 2952 de 2010, el Decreto Reglamentario 1377 de 2013 y las demás normas complementarias que regulen el tema.

11. PROPIEDAD INTELECTUAL

Los derechos morales de autor corresponden a los estudiantes, al director y a toda persona que haga aportes originales intelectuales en los avances y en el resultado final del proyecto. En cualquier tipo de divulgación se dará crédito a los autores y la Institución Universitaria Salazar y Herrera. Por su parte, los derechos sobre los resultados derivados del presente trabajo de grado se rigen por el Reglamento de Propiedad Intelectual de la institución.

REFERENCIAS

Es fundamental hacer uso del acervo bibliográfico que se encuentra en las bases de datos de la IUSH, así como tener bibliografía de referencia tanto en lo temático propio del tema de investigación, como en lo metodológico. Artículos en revistas indexadas, bibliografía y cibergrafía. Mantener sistema de referenciación APA.

Bibliografía

AWS. (s.f.). *amazon*. Obtenido de https://aws.amazon.com/es/what-is/machine-learning/

AWS. (s.f.). *Amazon*. Obtenido de https://aws.amazon.com/es/what-is/cybersecurity/#:~:text=La%20ciberseguridad%20es%20la%20práctica,cliente%20y%20cumplir%20la%20normativa.

España, G. d. (19 de abril de 2023). *planderecuperacion*. Obtenido de https://planderecuperacion.gob.es/noticias/que-es-inteligencia-artificial-ia-

prtr#:~:text=La%20inteligencia%20artificial%20(IA)%20es,el%20razonamiento%20y%20la%20percepción.

Mcafee. (2020). *mcafee*. Obtenido de https://www.mcafee.com/es-co/antivirus/malware.html#:~:text=Malware%20es%20un%20término%20que,dispositivo%2C%20servicio%20o%20red%20programable.

Barbosa, D. C. (23 de Febrero de 2022). Welivesecurity. Obtenido de https://www.welivesecurity.com/la-es/2022/02/23/ransomware-as-a-service-raas-quees-como-funciona/

Díaz, L. L. (15 de Agosto de 2023). EL TIEMPO. Obtenido de https://www.eltiempo.com/tecnosfera/novedades-tecnologia/colombia-tuvo-mas-de5-000-intentos-de-ciberataques-al-inicio-del-2023-796252

IBM. (2020). IBM. Obtenido de https://www.ibm.com/es-es/topics/cyber-attack

IBM. (2021). Obtenido de https://www.ibm.com/es-es/topics/social-engineering

Robledo, J. C. (2012). Impacto de las Patentes sobre el Crecimiento Económico: Un Modelo Panel Cointegrado. Bogotá: Hal Open Science

Todos los partícipes de este proyecto de trabajo de grado declaran conocer el Reglamento de Propiedad Intelectual de la Institución Universitaria Salazar y Herrera, así como el Reglamento de trabajos de grado estipulado por el Centro de Investigación, Innovación y Desarrollo Empresarial (CIIDE).

Para constancia se firma en Medellín, el _____

_____
ASESOR PROYECTO
Nombre:
Cédula:

_____
ESTUDIANTE
Nombre:
Cédula:
Código:

_____
COORDINADOR DEL PROGRAMA

ANTEPROYECTO TRABAJO DE GRADO DE INVESTIGACIÓN
Centro de Investigación, Innovación y Desarrollo Empresarial (CIIDE)
Revisión 2021

Nombre:
Cédula: