Escuela de Ingenierías

IUSH Institución Universitaria SALAZAR Y HERRERA

SER PERSONA DESDE EL SABER Y EL HACER

EXE-RAY

Isabela López Cardona
Simón Zapata Flórez
Simón Vélez Gutiérrez
Sebastian Zapata Zapata

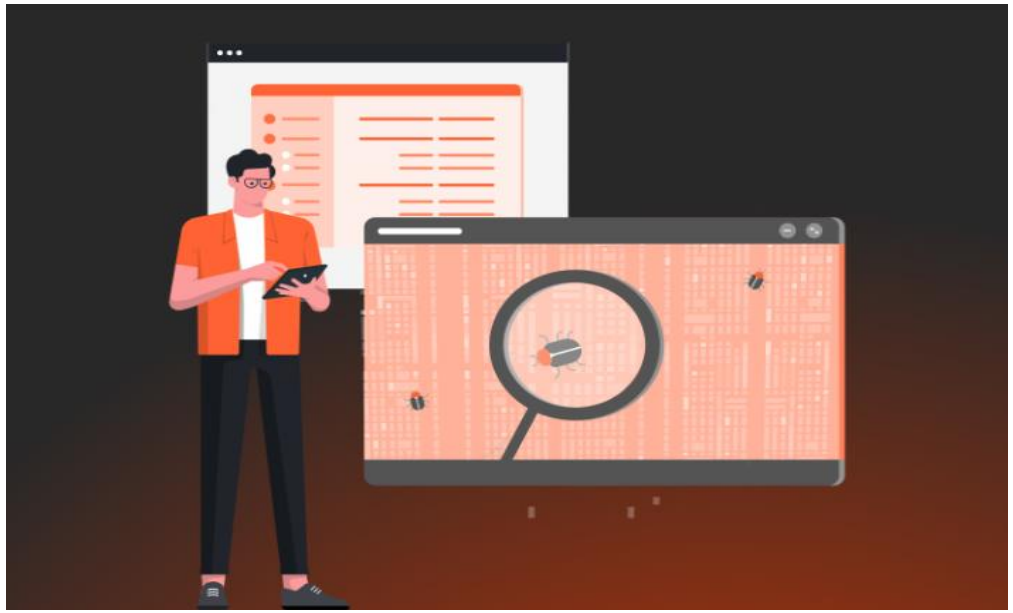
Escuela de Ingenierías
IUSH Institución Universitaria SALAZAR Y HERRERA
SER PERSONA DESDE EL SABER Y EL HACER

PREGUNTA

¿Cómo pueden las técnicas de Inteligencia Artificial mejorarse y aplicarse eficazmente para la detección y mitigación de malware, teniendo en cuenta la evolución constante de las amenazas cibernéticas y los desafíos asociados?

CONTEXTO

América Latina y el Caribe sufrieron más de 63 mil millones de intentos de ciberataques, Colombia (5 mil millones)



Escuela de Ingenierías
IUSH Institución Universitaria SALAZAR Y HERRERA
SER PERSONA DESDE EL SABER Y EL HACER

CROWDSTRIKE

TREND MICRO™

SOPHOS

Escuela de Ingenierías

IUSH Institución Universitaria SALAZAR Y HERRERA

SER PERSONA DESDE EL SABER Y EL HACER

HITOS

- **Investigación preliminar y análisis de amenazas**
  - Revisión bibliográfica sobre malware en medianas empresas.
  - Identificación de los tipos de malware más comunes.
  - Análisis de las familias de malware relevantes.
- **Definición de la técnica de IA**
  - Estudio de técnicas de Machine Learning y Deep Learning aplicadas a ciberseguridad.
  - Selección de CNN como enfoque principal para la detección.

HITOS

- **Recopilación y preparación de datos**
  - Obtención de una base de datos de archivos .exe (maliciosos y benignos).
  - Conversión de archivos .exe en imágenes binarias para el análisis con CNN.
  - Etiquetado y preprocesamiento de datos.
- **Diseño de la arquitectura del modelo**
  - Selección del framework de IA (TensorFlow, PyTorch, etc.).
  - Definición de la estructura de la red neuronal convolucional (capas, funciones de activación, etc.).

HITOS

- **Entrenamiento del modelo de IA**
  - Dividir los datos en conjuntos de entrenamiento, validación y prueba.
  - Entrenar la CNN con distintas configuraciones de hiperparámetros.
  - Evaluar la precisión y ajustar el modelo según los resultados.
- **Pruebas y validación del modelo**
  - Realizar pruebas con muestras desconocidas.
  - Evaluar métricas de desempeño como precisión, recall y F1-score.
  - Comparación con otros métodos tradicionales de detección de malware.

HITOS

- **Desarrollo de la interfaz de usuario**
  - Diseño de la GUI para facilitar la carga de archivos y visualización de resultados.
  - Integración con el modelo entrenado para predicciones en tiempo real.
- **Optimización y mejora del modelo**
  - Refinamiento del modelo para mejorar la detección de malware y su clasificación por familias.
  - Reducción de falsos positivos y falsos negativos.

HITOS

- **Implementación y despliegue**
  - Integración del sistema en la infraestructura de ciberseguridad de medianas empresas.
  - Pruebas en entornos reales y ajustes finales.
- **Documentación y presentación de resultados**
- Elaboración de informes técnicos y documentación del modelo.
- Presentación de resultados y recomendaciones para su implementación en seguridad informática.

METODOLOGÍA

3. Implementar la técnica basada en IA para la prevención de malware.
   A. Recopilación de datos para el entrenamiento de IA.
   B. Entrenamiento de técnica de IA

Tab.3 Malware Dataset of 25 Families

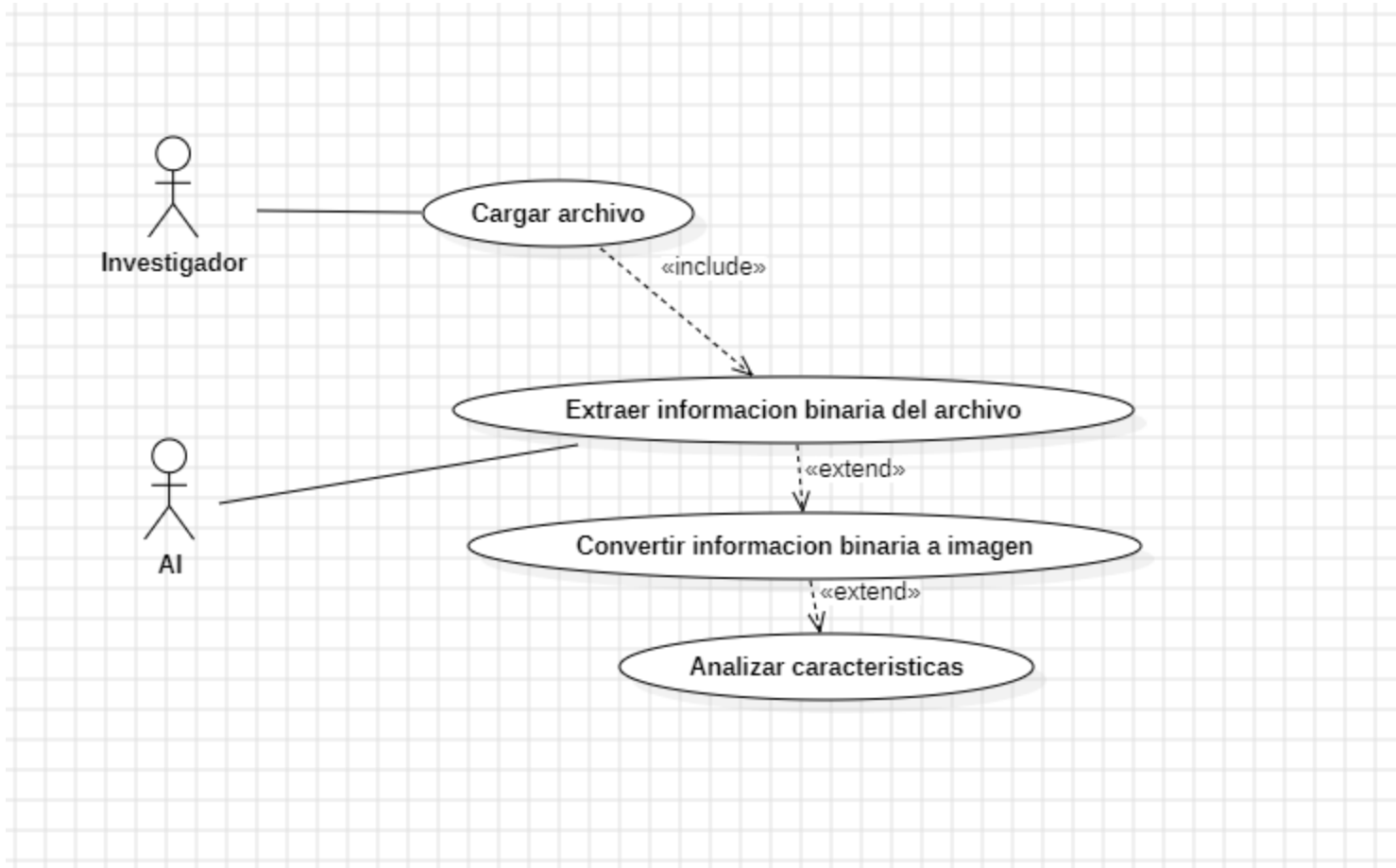
#	Class	Family	#
1.	Worm	Allaple.L	1591
2.	Worm	Allaple.A	2949
3.	Worm	Yuner.A	800
4.	PWS	Lolyda.AA 1	213
5.	PWS	Lolyda.AA 2	184
6.	PWS	Lolyda.AA 3	123
7.	Trojan	C2Lop.P	146
8.	Trojan	C2Lop.gen!g	200
9.	Dialer	Instantaccess	431
10.	TDownloader	Swizzot.gen!I	132
11.	TDownloader	Swizzor.gen!E	128
12.	Worm	VB.AT	408
13.	Rogue	Fakerean	381
14.	Trojan	Alueron.gen!J	198
15.	Trojan	Malex.gen!J	136
16.	PWS	Lolyda.AT	159
17.	Dialer	Adialer.C	125
18.	TDownloader	Wintrim.BX	97
19.	Dialer	Dialplatform.B	177
20.	TDownloader	Dontovo.A	162
21.	TDownloader	Obfuscator.AD	142
22.	Backdoor	Agent.FYI	116
23.	Worm:AutoIT	Autorun.K	106
24.	Backdoor	Rbot!gen	158
25.	Trojan	Skintrim.N	80

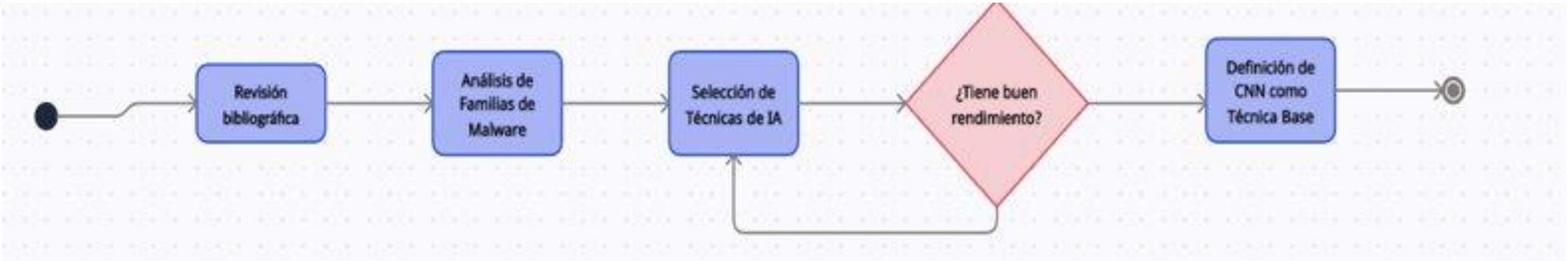
Escuela de Ingenierías
IUSH Institución Universitaria SALAZAR Y HERRERA
SER PERSONA DESDE EL SABER Y EL HACER

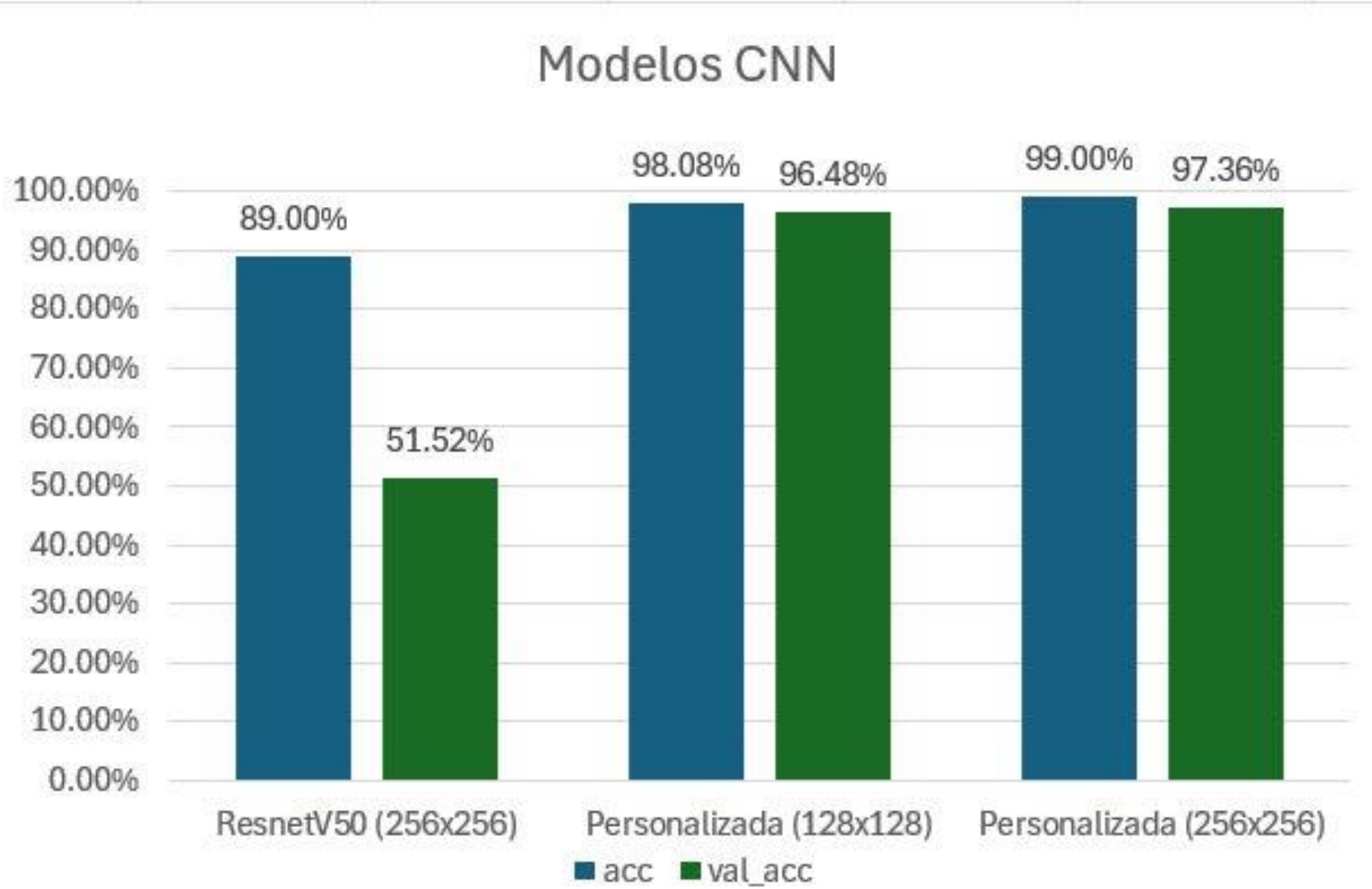
METODOLOGÍA

4. Desarrollar el modelo de IA.
   A. Diseño de la GUI.
   B. Elección del lenguaje/framework de programación.
   C. Desarrollo de la interfaz.
   D. Implementación del modelo entrenado de IA

Escuela de Ingenierías
IUSH Institución Universitaria SALAZAR Y HERRERA
SER PERSONA DESDE EL SABER Y EL HACER


Investigador
Cargar archivo
«include»
Extraer informacion binaria del archivo
AI
«extend»
Convertir informacion binaria a imagen
«extend»
Analizar caracteristicas


Revisión bibliográfica
Análisis de Familias de Malware
Selección de Técnicas de IA
¿Tiene buen rendimiento?
Definición de CNN como Técnica Base



Escuela de Ingenierías

IUSH Institución Universitaria SALAZAR Y HERRERA

SER PERSONA DESDE EL SABER Y EL HACER

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

Escuela de Ingenierías

IUSH Institución Universitaria SALAZAR Y HERRERA

SER PERSONA DESDE EL SABER Y EL HACER