Trabajo Fin de Grado
Grado en Ingeniería Electrónica, Robótica Y Mecatrónica

Análisis de Aplicación de Técnicas Basadas en Inteligencia Artificial en la Industria de Defensa y Caso Práctico

Autor: Pedro Vaca Rodríguez
Tutor: Fernando Guerrero López

Dpto. Organización Industrial y Gestión de Empresas I
Escuela Técnica Superior de Ingeniería
Universidad de Sevilla

Sevilla, 2024

Trabajo Fin de Grado
Ingeniería Electrónica, Robótica y Mecatrónica

Análisis de Aplicación de Técnicas Basadas en Inteligencia Artificial en la Industria de Defensa y Caso Práctico

Autor:
Pedro Vaca Rodríguez

Tutor:
Fernando Guerrero López
Profesor titular

Dpto. de Organización Industrial y Gestión de Empresas I
Escuela Técnica Superior de Ingeniería
Universidad de Sevilla
Sevilla, 2024

Trabajo Fin de Grado: Análisis de Aplicación de Técnicas Basadas en Inteligencia Artificial en la Industria de Defensa y Caso Práctico

Autor: Pedro Vaca Rodríguez

Tutor: Fernando Guerrero López

El tribunal nombrado para juzgar el Proyecto arriba indicado, compuesto por los siguientes miembros:

Presidente:

Vocales:

Secretario:

Acuerdan otorgarle la calificación de:

Sevilla, 2024

El Secretario del Tribunal

A mi familia

A mis compañeros

A mis maestros

Agradecimientos

Quiero expresar, en primer lugar, mi más sincero agradecimiento a mi familia por su apoyo incondicional a lo largo de este duro pero gratificante viaje académico. Su amor, comprensión y ánimo constante han sido pilares fundamentales que me han impulsado a alcanzar mis metas. Agradezco profundamente su sacrificio y dedicación, sin los cuales no habría sido posible llegar hasta aquí.

A mis compañeros de estudios y proyectos, les estoy enormemente agradecido por su colaboración, el constante intercambio de ideas, así como la ayuda en situaciones diversas y los momentos de desconexión que me han brindado. Cada momento compartido ha enriquecido mi experiencia y me ha permitido crecer tanto a nivel personal como profesional.

No puedo pasar por alto el invaluable aporte de mis estimados profesores, cuya dedicación y disponibilidad han sido ejemplares. Su guía, consejos y estímulo constante han sido esenciales en mi desarrollo a lo largo de estos años. Agradezco sinceramente su compromiso con mi formación y por poner a mi disposición las herramientas necesarias para alcanzar mis metas.

Pedro Vaca Rodríguez

Sevilla, 2024

Resumen

El presente trabajo de fin de grado se centra en el análisis de la aplicación de técnicas basadas en inteligencia artificial (IA) en la industria de defensa, con un enfoque particular en un caso práctico denominado "Trustworthy AI for Cybersecurity Reinforcement and System Resilience". El objetivo principal es evaluar cómo la IA puede mejorar la ciberseguridad y la resiliencia de los sistemas en el sector defensa.

En primer lugar, se revisa el estado actual de la industria de defensa y la integración de la IA en este ámbito. Se discuten los avances recientes y los desafíos en la ciberseguridad, así como los conceptos fundamentales de la IA aplicados a la defensa.

A continuación, se presenta el estado del arte, destacando los desarrollos más relevantes en técnicas de IA para la ciberseguridad y la resiliencia de sistemas. Se describen dos herramientas principales: AI4FIX, destinada a la corrección de bugs y mejora de la robustez, y AI4VULN, enfocada en la identificación de vulnerabilidades.

La metodología del trabajo incluye la implementación de estas herramientas en un entorno simulado para evaluar su efectividad. AI4FIX utiliza algoritmos avanzados para escanear sistemas en busca de fallos de seguridad y generar parches automáticos, mientras que AI4VULN se especializa en la identificación y priorización de vulnerabilidades mediante análisis de riesgos.

El caso práctico demuestra la capacidad de estas herramientas para mejorar significativamente la detección y corrección de vulnerabilidades en sistemas de defensa. Los resultados de las simulaciones muestran una mejora notable en la seguridad del sistema, subrayando la eficacia de los métodos basados en IA para fortalecer la ciberseguridad.

Finalmente, se presentan las conclusiones y recomendaciones para futuras investigaciones, destacando la necesidad de avanzar en técnicas más sofisticadas de detección de vulnerabilidades y la importancia de considerar aspectos éticos en el uso de IA en ciberseguridad.

Abstract

This final degree project focuses on the analysis of the application of artificial intelligence (AI) techniques in the defense industry, with a particular emphasis on a practical case called "Trustworthy AI for Cybersecurity Reinforcement and System Resilience". The main objective is to assess how AI can enhance cybersecurity and system resilience in the defense sector.

First, the current state of the defense industry and the integration of AI in this field are reviewed. Recent advancements and challenges in cybersecurity are discussed, along with the fundamental concepts of AI applied to defense.

Next, the state of the art is presented, highlighting the most relevant developments in AI techniques for cybersecurity and system resilience. Two main tools are described: AI4FIX, aimed at bug fixing and robustness improvement, and AI4VULN, focused on vulnerability identification.

The methodology of the work includes the implementation of these tools in a simulated environment to evaluate their effectiveness. AI4FIX uses advanced algorithms to scan systems for security flaws and generate automatic patches, while AI4VULN specializes in identifying and prioritizing vulnerabilities through risk analysis.

The practical case demonstrates the ability of these tools to significantly improve the detection and correction of vulnerabilities in defense systems. Simulation results show a notable improvement in system security, underscoring the effectiveness of AI-based methods for strengthening cybersecurity.

Finally, conclusions and recommendations for future research are presented, highlighting the need to advance more sophisticated vulnerability detection techniques and the importance of considering ethical aspects in the use of AI in cybersecurity.

Índice

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

Glosario

ADT	AlphaDogfight Trials
AMI	Advanced Metering Infrastructure
ANN	Artificial Neuronal Networks
ASG	Abstract Semantic Graph
CCN-CERT	Centro Criptológico Nacional – Computer Emergency Response Team
CEMA	Cyber Electromagnetic Activities
CFG	Control Flow Graph
CONVOY	Cloud Intelligent Explosive Detection System
DARPA	Defense Advanced Research Projects Agency
DDoS	Distributed Denia lof Service
DMP	Data Management Plan
EDF	European Defence Fund
EWO	Electronic Warfare Operation
FaRADAI	Frugal and Robust AI for Defense Advance Intelligent
FCAS	Future Combat Air System
GDPR	General Data Protection Regulation
IA	Inteligencia Artificial
IDS	Intrusion Detection Systems
IEEE	Institute of Electrical and Electronics Engineers
IED	Improvised Explosive Devices
IoT	Internet of Things
IP	Internet Protocol
ITM	In the Moment
LGP	Linear Genetic Programs
LLM	Large Language Model
MARS	Multivariate Adaptive Regression using Splines
ML	Machine Learning
NLP	Natural Language Processing
OpenVAS	Open Vulnerability Assessment Scanner
PSO	Project Security Officer
PYME	Pequeñas y Medianas Empresas
RAG	Retrieval-Augmented Generation
RPA	Robotic Process Automation
SBA	Security Advisory Board
SVM	Support Vector Machine
TAI	Trustworthy Artificial Intelligence
UOWM	University of Western Macedonia
VM	Virtual Machine
VPN	Virtual Private Network

1 INTRODUCCIÓN

En un mundo cada vez más dinámico y complejo, la industria de defensa se encuentra en una evolución constante para adaptarse a los desafíos y amenazas que pueden surgir. La unión de tecnología de vanguardia y estrategias innovadoras se ha convertido en un elemento fundamental para mantener la seguridad nacional.

La rápida evolución tecnológica, junto con la creciente complejidad de los conflictos actuales, ha llevado a un aumento en la integración de técnicas basadas en inteligencia artificial en el ámbito de la defensa. Desde sistemas autónomos hasta algoritmos de análisis predictivos, la inteligencia artificial está transformando la forma en que se llevan a cabo operaciones militares.

En este contexto, la ciberseguridad se erige como una preocupación central. Con el incremento de amenazas cibernéticas constantemente y la dependencia cada vez mayor de la tecnología digital en los sistemas de defensa, proteger la confidencialidad de la información y esta misma se ha vuelto algo obligatorio.

Este trabajo se propone explorar algunas técnicas, así como analizar las basadas en inteligencia artificial en casos de defensas, centrándonos en un proyecto de ciberseguridad, para más tarde, realizar un caso práctico en el que veamos lo previamente estudiado. Este nos va a ilustrar la aplicación concreta en el marco en el que vamos a adentrarnos.

1.1. Objetivos del Trabajo

Este trabajo tiene como objetivo principal explorar y analizar las técnicas basadas en Inteligencia Artificial (IA), destacando su creciente relevancia en la industria de la defensa, específicamente en el ámbito de la ciberseguridad y ciberataques. Se busca comprender cómo dichas técnicas pueden contribuir a fortalecer la seguridad de sistemas críticos.

En esta línea, se pretende investigar el estado actual de las técnicas de IA aplicadas a esta industria, además se busca analizar cómo la inteligencia artificial puede jugar un papel crucial en la protección ante ciberataques considerando su capacidad para identificar patrones y anomalías en grandes volúmenes de datos.

Se buscará comprender las directrices y enfoques establecidos por el proyecto europeo “Trustworthy Artificial Intelligence for Cybersecurity Reinforcement and System Resilence” [1], así como ver cómo desarrolla marcos integrales de servicios que usan tecnologías de IA y Big Data.

Además, se diseñará un entorno de desarrollo propio, basado en las tecnologías estudiadas, con el fin de llevar a cabo un caso práctico que demuestre la aplicación efectiva de las técnicas de inteligencia artificial en la mejora de la ciberseguridad. Este caso práctico servirá como una evaluación de la eficacia y viabilidad de estas técnicas en un entorno operativo real.

1.2. Estado de la Industria de Defensa

La industria de la defensa ha experimentado cambios significativos en las últimas décadas, impulsados por diversos factores como son los tecnológicos. A partir de la década 2000, se observa una intensificación de las estrategias exportadoras y tecnológicas como vías para ingresar a nuevos mercados, juntos con la diversificación para reducir la dependencia de los presupuestos de defensa, siendo en muchos países la estrategia dominante el importar armamento de otros que le suministran y se enriquecen a costa de este hecho.

Países	Totales (millones)		Cuotas de mercado (%)	
	1986-2002	2003-2020	1986-2002	2003-2020
Estados Unidos	191463	153470	41,0	32,9
Rusia	40080	108844	8,6	23,3
Unión Soviética	67666	0	14,5	0,0
Francia	30455	33746	6,5	7,2
Alemania	26682	32435	5,7	7,0
Reino Unido	31661	19327	6,8	4,1
China	16623	20936	3,6	4,5
Países Bajos	7791	10274	1,7	2,2
Italia	5843	11193	1,3	2,4
Israel	4552	10991	1,0	2,4
España	2412	12937	0,5	2,8
Ucrania	3975	8182	0,9	1,8
Suecia	5007	6620	1,1	1,4
Suiza	4720	4977	1,0	1,1
Corea del Sur	772	6270	0,2	1,3
Otros	26933	28293	5,8	6,1
Total	466633	468496	100,0	100,0

Tabla 1.1 Top 15 exportadores de armamento 1986-2020 [2].

En cuanto a la situación en la Unión Europea [3], la colaboración se ve impulsada por la fragmentación en los mercados de defensa, sin embargo, la UE aún no alcanza los objetivos establecidos para la colaboración en equipos de defensa y en investigación y tecnología. En otro sentido, se plantea el riesgo de perder el co-liderazgo en el mercado aeronáutico militar en la próxima década si no se avanza con proyectos clave como el FCAS. Dicha preocupación surge en un contexto donde la industria de defensa de Estados Unidos gana peso internacional, siendo vista como referencia incluso por países europeos en situaciones como la actual en Rusia.

La dependencia de la importación de armamento en muchos países europeos resalta la necesidad de abordar estrategias más proactivas para fortalecer la industria nacional de defensa. De esta forma, la colaboración internacional se presenta como una oportunidad para compartir costos, tecnologías y capacidades, pero, diversos factores como el proteccionismo, las diferencias en los requisitos técnicos y los problemas financieros han limitado su efectividad.

Por otro lado, la entrada de las PYME en el mercado de defensa está transformando la industria al modificar las relaciones con los grandes contratistas y los gobiernos. Este cambio se refleja en la adopción de contratos de servicio basados en resultados, que requieren una relación fluida y de co-creación con el cliente [2]. Dicha entrada obliga a las grandes empresas a adaptarse a la nueva dinámica, estimulando la competencia en segmentos específicos.

En general, como se ha descrito, la industria de defensa se encuentra en un período de cambio notable, donde se están gestando tendencias que moldearán el futuro. Una de las principales características que se mantendrá en el tiempo es la dimensión nacional de esta industria, los países continuarán desarrollando y manteniendo sus propias capacidades de defensa, impulsados por la necesidad de autonomía estratégica. Sin embargo, la globalización presenta desafíos a esta autonomía, ya que las interdependencias empresariales, alianzas entre países y acuerdos de colaboración limitan las posibilidades de actuación individual.

Las nuevas demandas para la defensa, basadas en análisis estratégicos profundos, requieren una reorientación de la industria en términos de sistemas y formas de producción [2]. Además, con la entrada de nuevos actores en el mercado global de defensa como China, Brasil, India y Corea del Sur, se están reestructurando los equilibrios industriales, económicos y políticos.

Principales aspectos	Situación hasta ahora	Principales cambios
-Definición de la industria	Heterogénea, perspectivas de oferta y demanda.	Aumento de la heterogeneidad. Mayor movilidad: entradas y salidas. Nuevos sectores.
-Grado de competencia	Monopolios y oligopolios tradicionales y mercados cerrados a la competencia.	Mayor apertura internacional y nuevos competidores: países "new commers" y empresas civiles. Mayor competencia en precios.
-Cadena de suministro	Centradas en servicios y productos. Seguridad de suministro.	Mayor creación de valor. Contrato de servicio basado en resultados. Centrada en el cliente.
-Financiación de la I+D	Créditos blandos y subvenciones. Baja o nula asunción de riesgos por las empresas. Derechos de propiedad generalmente de la empresa.	Co-financiación. Reparto de riesgos entre cliente y contratista. Créditos fiscales. Derechos de propiedad compartidos.
-Performance	Capacidad de trasladar aumentos de costes a precios. La falta de competencia por oligopolios/monopolios genera mayores rentabilidades, pero no mayor performance.	Mayor competencia por entrada de nuevas empresas civiles y de menor tamaño en tecnologías clave. Aumento del valor añadido en cadenas de suministro. Respuesta más ágil de las PYMEs.
-Política industrial	Paliar fallos de mercado. Promover una estructura industrial concreta. Impulsar la innovación.	Paliar fallos de mercado. Promover una estructura industrial concreta. Impulsar la innovación. Impulsar la competencia. Articular políticas (en plural) para las industrias de defensa, dada su heterogeneidad.

Tabla 1.2 Cuadro de la situación actual y los cambios en la Industria de Defensa Mundial [2].

En resumen, la industria de defensa se encuentra en un proceso de transformación impulsado por la globalización, la evolución de la demanda, y la entrada de nuevos actores en el panorama. Esto requerirá cierta adaptabilidad por parte de los países y empresas para mantener la autonomía estratégica y competitividad en un entorno de evolución.

1.3. Integración de la Inteligencia Artificial en Defensa

El campo militar ha experimentado un avance significativo en la integración de la Inteligencia Artificial en diversas áreas, como el análisis de inteligencia, logística, ciberseguridad, ciberoperaciones, sistemas de mando y control, y vehículos autónomos. Sin embargo, la transferencia de tecnologías civiles al ámbito militar plantea desafíos como la desconfianza en el caso de países no alineados que invierten en empresas con tecnologías de IA avanzadas, además, la aplicación de los sistemas de IA en el campo militar no está exenta de riesgos [4].

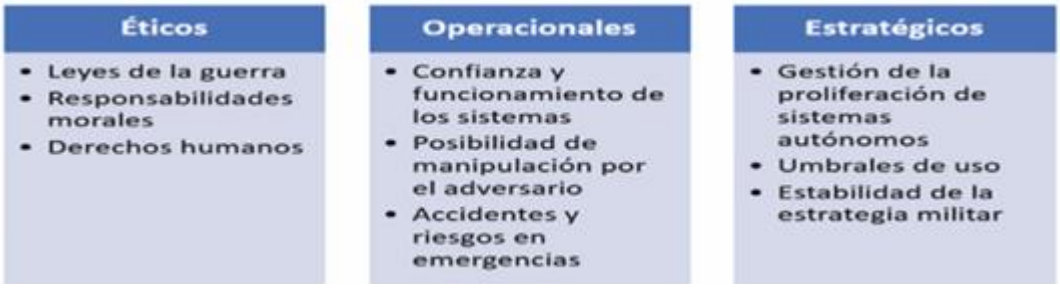

Figura 1.1 Riesgos asociados al uso militar de la IA [4].

La competencia entre países por dominar la IA en la industria de la defensa es intensa con enfoques diferentes en la aplicación de estas tecnologías. Por un lado, China ha avanzado rápidamente en aplicaciones militares con dicha herramienta con un enfoque en el desarrollo de sistemas de armas inteligentes, contramedidas autónomas y capacidades de supercomputación para la guerra moderna. Por otro lado, Rusia prioriza el desarrollo de capacidades de IA para debilitar los sistemas de mando y control del adversario, considerando la guerra de la información como un elemento central de los conflictos contemporáneos [5].

En España, la introducción de la inteligencia artificial en el ámbito de la defensa está siendo impulsada por numerosas empresas, entre las cuales destaca Indra. Esta compañía lidera proyectos innovadores en el campo de la Defensa y la Seguridad, aprovechando tecnologías de IA para abordar desafíos cada vez más complejos. Uno de estos proyectos es FaRADAI, diseñado para mejorar el rendimiento de la Inteligencia Artificial en operaciones militares [5]. Además de este, Indra presentó LANDEF, una suite de combate electrónico terrestre diseñada para misiones de inteligencia y contramedidas electromagnéticas [6].

Figura 1.2 Drones plegables con Inteligencia artificial [7].

Como se puede ver en la Figura 1.2, en Estados Unidos se están desarrollando sistemas que incluyen drones autónomos capaces de realizar misiones de reconocimiento y ataque con mínima intervención humana, así como algoritmos de procesamiento de datos en tiempo real para proporcionar inteligencia táctica en tiempo real a los comandantes en el terreno [7].

En otras regiones como Israel y Reino Unido, se están llevando a cabo investigaciones significativas en el ámbito de la IA aplicada a la defensa con un enfoque particular en la mejora de la seguridad fronteriza, la detección de amenazas y la interoperabilidad de sistemas de armas, así como comenta elDiario.es [8] en el que habla de cómo Israel ha empleado la inteligencia artificial para detectar 37.000 objetivos que eran una amenaza.

Sin duda, la adopción de la Inteligencia Artificial está en marcha en todo el mundo, y se le están asignando cada vez más responsabilidades y metas por cumplir. Para países como España y otros, esto presenta tanto oportunidades como desafíos, ya que necesitan ajustarse rápidamente para mantener su competitividad y seguridad en un mundo geopolítico en constante cambio, puesto que el avance tan veloz de la IA en el ámbito militar podría tener un impacto considerable en cómo se equilibran las potencias entre sí, lo que podría transformar las estrategias de seguridad y las dinámicas internacionales.

1.4. Ciberseguridad en la Actualidad

La ciberseguridad se ha convertido en uno de los pilares fundamentales en el panorama actual de la tecnología y la información. [9] La ciberseguridad se define como la habilidad de proteger y defender las redes o sistemas de los ciberataques, ello abarca un conjunto de prácticas, tecnologías y políticas diseñadas para salvaguardar sistemas, redes y datos contra ataques, intrusiones y cualquier forma de acceso no autorizado.

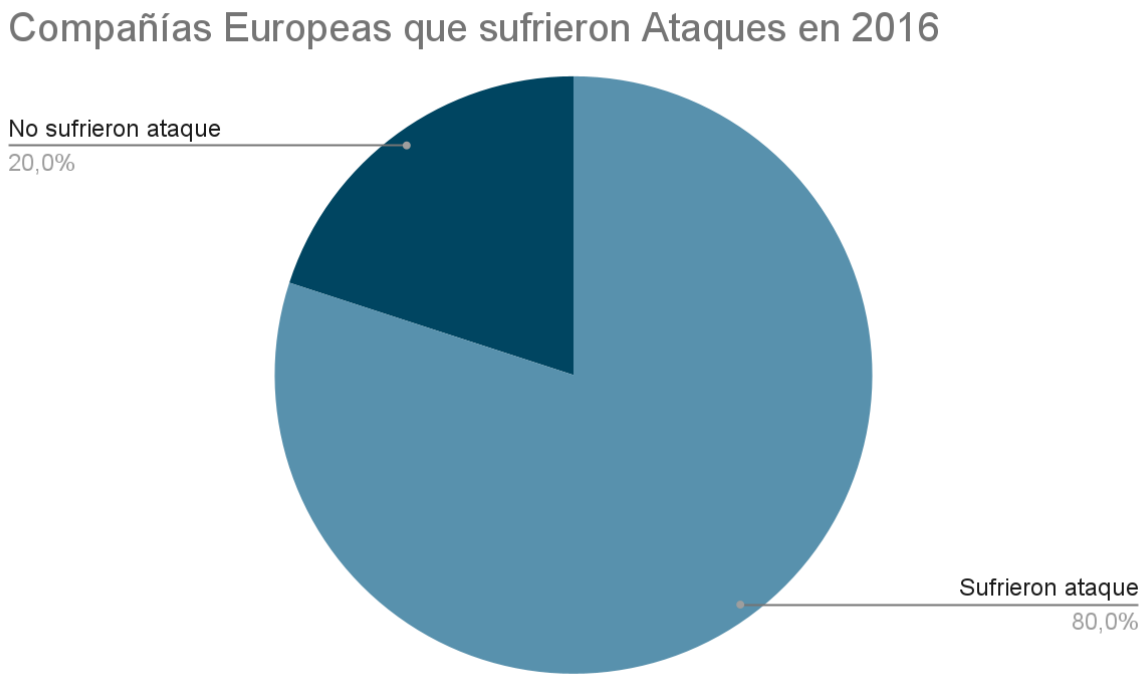

Figura 1.3 Gráfico ilustrativo de la cantidad de ataques recibidos en un año [10].

El incremento de los ciberdelitos se atribuye no solo a la facilidad para llevarlos a cabo con una inversión relativamente baja, sino también a la baja probabilidad de ser castigados, ya que las infracciones penales en este ámbito suelen gozar de alta impunidad. Este gráfico citado señala que en Europa [10], el 80% de las compañías experimentaron al menos un incidente de seguridad en 2016, con un aumento del 38% en los incidentes en el sector industrial respecto al 2015, cifra en la que se aprecia el aumento considerable.

Claramente, desde el malware, software malicioso que se infiltra en sistemas informáticos para causar daño o robar información, hasta el phishing [10], técnica social que utiliza correos electrónicos o mensajes falsos para engañar a las personas y obtener información confidencial, pasando por el ransomware que cifra los archivos de la víctima y exige un rescate económico por ellos, el panorama de amenazas es vasto y en constante evolución, lo que requiere una respuesta igualmente dinámica y sofisticada, en este caso en la ciberseguridad.

En estos días, [11] el Internet de las Cosas (IoT) ha revolucionado nuestra interacción con la tecnología al integrar dispositivos como relojes inteligentes, termostatos conectados y dispositivos de seguridad doméstica en nuestra vida cotidiana. Sin embargo, este crecimiento también ha aumentado los riesgos de seguridad, haciendo imperativo proteger adecuadamente estos dispositivos para evitar su explotación por parte de ciberataques. La ciberseguridad en el IoT se refiere a medidas destinadas a proteger tanto los dispositivos conectados como la red que los une contra posibles ataques. Esto implica garantizar la confidencialidad, integridad y disponibilidad de la información transmitida y almacenada.

Figura 1.4 Ciberseguridad en IoT [11].

Ejemplos sonados de algunos de ataques similares a los comentados pueden ser los Shadow Brokers, y los incidentes WannaCry y Petya, así como hasta el gobierno de los Estados Unidos ha sido vulnerable [4]. Con respecto a esta situación y con la creciente utilización de la Inteligencia Artificial (IA) en el ámbito militar, se presentan oportunidades en materia de ciberseguridad, si bien la IA puede mejorar las capacidades operativas y tácticas.

El Departamento de Defensa de EEUU reconoce la importancia de la IA en la predicción, identificación y respuesta a ciberataques, promoviendo la colaboración público-privada para desarrollar sistemas de ciberseguridad avanzados [4]. Sin embargo, esta tecnología puede ser usada en contra, planteando desafíos adicionales en la protección de los sistemas.

En un contexto donde el ciberespacio se considera un quinto dominio de conflicto, junto con tierra, mar, aire y espacio exterior, la ciberseguridad se convierte en una preocupación estratégica fundamental. La dependencia de sistemas basados en la IA en el ámbito de la ciberseguridad plantea interrogantes sobre la autonomía operativa

y su propia vulnerabilidad. En última instancia, el desarrollo de capacidades propias en ciberseguridad y tecnologías basadas en inteligencia artificial se vuelve crucial para garantizar la soberanía y seguridad.

2 MARCO TEÓRICO

Tratando los aspectos comentados anteriormente se ha mencionado repetidamente en diversas ocasiones el concepto de Inteligencia Artificial cuya definición varía dependiendo de la perspectiva y el enfoque del autor así como dependiendo del organismo que la defina. Alan Turing, pionero en el campo de la computación, establece que es la capacidad de una máquina para imitar la inteligencia humana de manera que un observador no pueda distinguir entre las acciones realizadas por la máquina y las realizadas por un ser humano [4]. Por otro lado, David Pool y Alan Mackworth ofrecen una definición más amplia; un agente computacional actúa inteligentemente si sus acciones son coherentes con sus circunstancias y objetivos, siendo flexible a cambios de su entorno, si aprende de la experiencia y si toma decisiones apropiadas según sus percepciones.

Según la Comisión Europea [12], la Inteligencia Artificial (IA) es un 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. Otra organización que propone otro significado es el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE), que expone que la IA es la capacidad de las computadoras o sistemas informáticos para realizar tareas que normalmente requieren inteligencia humana, como el reconocimiento de voz, el aprendizaje, la planificación y la resolución de problemas [13].

El campo de la Inteligencia Artificial puede entenderse como una disciplina con múltiples ramas especializadas, entre las que destacan el Machine Learning (ML), el deep learning y la inteligencia artificial generativa [14]. El machine learning se centra en el desarrollo de algoritmos y modelos que permiten a las máquinas aprender de datos y realizar tareas específicas sin ser programadas explícitamente, es lo llamado aprendizaje automático.

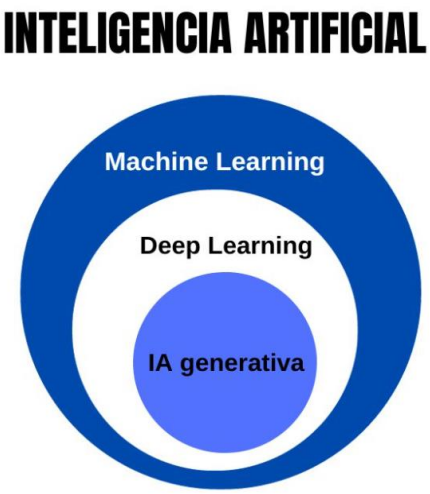

Figura 2.1 Estructura de la Inteligencia Artificial con las ramas más destacadas [14].

Hay una gran cantidad de campos de acción para el ML como la medicina o la educación, puesto que la finalidad que se busca es lograr el aprendizaje autónomo de máquinas o sistemas que nos ayudan, este puede definirse en tres tipos de algoritmos [15]:

- Aprendizaje Supervisado: Etiqueta los conjuntos de datos para que los patrones puedan ser detectados y puedan ser usados para etiquetar nuevos conjuntos de información.

- Aprendizaje no supervisado: Usado cuando algún conjunto de datos no esté etiquetado y por ello el único camino para que sea acomodado es mediante la revisión de similitudes o diferencias que permitan la propia diferenciación.

- Aprendizaje de refuerzo: Los datos del sistema no están etiquetados, pero después de varias acciones el sistema es retroalimentado mediante actualizaciones.

Por otro lado, el deep learning es una subrama del machine learning que utiliza redes neuronales profundas para aprender representaciones jerárquicas de datas, siendo especialmente efectivo en tareas de reconocimiento de patrones y procesamiento de imágenes y sonido [16].

En una red neuronal artificial, las neuronas artificiales se organizan en capas interconectadas. Cada neurona recibe entradas, realiza una operación matemática ponderada por los pesos de esas entradas y un parámetro de sesgo, para luego aplicar una función de activación para producir una salida. Las capas se organizan en tres tipos: capa de entrada, capa de salida y capas ocultas.

La información fluye de la capa de entrada a través de las capas ocultas hasta la capa de salida donde se produce el resultado final. Durante el entrenamiento, la red ajusta sus pesos y sesgos para minimizar todo lo que pueda la discrepancia entre las salidas producidas y las deseadas, usando algoritmos de optimización.

La inteligencia artificial generativa es otra rama importante que se centra en la creación de modelos capaces de generar contenido nuevo y realista, como imágenes, música o texto, mediante el aprendizaje de las características y estructuras subyacentes de los datos de entrenamiento. El desarrollo de la IA generativa ha sido significativo, alcanzando niveles de sofisticación que eran difíciles de imaginar [17].

Desde otra perspectiva se ve como su uso plantea importantes desafíos éticos. Por ejemplo, la seguridad y responsabilidad en su uso son cruciales para evitar la creación y difusión de contenido engañoso. Además, es necesario abordar cuestiones relaciones con la privacidad y los derechos del autor, así como evitar que su implementación contribuya a la discriminación.

Figura 2.2 Ejemplo de IA generativa: Protagonistas de Con la muerte en los talones (1959) insertados en un tren de Virgin Trains (2005), ante la sorpresa de una usuaria moderna [17].

2.1. Descripción del Problema: Aplicaciones de Inteligencia Artificial en Defensa Texto principal

En el ámbito de la defensa, el papel de la tecnología es fundamental para la seguridad y la eficacia militar. Con la rápida evolución de las amenazas se requieren soluciones innovadoras que aprovechen al máximo los nuevos avances, de esta forma surge la inteligencia artificial, ofreciendo una amplia gama de aplicaciones que mejoran las capacidades militares en diversas áreas.

Se exploran las diversas aplicaciones de dicha herramienta en defensa, destacando cómo estas tecnologías están transformando la forma en que las fuerzas armadas abordan los desafíos modernos. Desde la protección cibernética hasta la logística militar, pasando por el reconocimiento de objetivos y la atención médica en entornos hostiles, la IA está revolucionando cada aspecto de las operaciones militares.

Actualmente, el ámbito militar presenta una amplia gama de aplicaciones de inteligencia artificial en constante crecimiento, siendo las principales las siguientes [18]:

1. Ciberseguridad: Se usa la inteligencia artificial para proteger las redes militares, detectar patrones de ciberataques y generar contramedidas para defenderse de ellos, asegurando la integridad de la información clasificada.

2. Sistemas de Combate Militares: La integración de la IA en armas y vehículos militares permite desarrollar sistemas más eficientes capaces de tomar decisiones en tiempo real.

3. Logística y Transporte Militar: La IA optimiza la logística y el transporte al identificar anomalías, prever fallos y optimizar rutas de transporte, agilizando de esta forma las operaciones.

4. Reconocimiento de Objetivos: Los sistemas basados en IA analizan datos para mejorar el reconocimiento de objetivos, prediciendo el comportamiento del enemigo y preparando estrategias para el contraataque.

5. Atención Médica durante Conflictos Armados: Con esta herramienta se proporciona apoyo quirúrgico remoto y ayuda en el propio diagnóstico médico, proporcionando una atención más precisa en entornos hostiles.

6. Monitoreo de Amenazas y Seguridad del Personal Militar: Dispositivos como los drones equipados con la inteligencia artificial monitorean y vigilan las áreas fronterizas, identificando peligros potenciales.

7. Procesamiento de Grandes Volúmenes de Datos [19]: La IA facilita el procesamiento de grandes volúmenes de datos, extrayendo la información crucial. En este sentido, permite la identificación de tendencias y conexiones entre diferentes eventos para la toma de decisiones según la información y datos analizados.

8. Simulación y Entrenamiento de Combate: Este aspecto es crucial al igual que los anteriores, se permite el desarrollo de software de simulación y entrenamiento más avanzado, proporcionando a las tropas una experiencia más realista y efectiva en la capacitación, mejorando el rendimiento de los soldados.

Figura 2.3 Inteligencia Artificial se enfrenta a pilotos de combate [20].

2.2. Evolución de la Ciberseguridad en el Contexto de la Industria de Defensa

La ciberseguridad surge como un factor crucial en una gran cantidad de ámbitos de la vida moderna, siendo uno de los más notorios en la industria de defensa. La conformación del ciberespacio como el quinto dominio ha generado la necesidad de asegurar este entorno.

El ciberespacio tiene repercusiones palpables en el mundo real por la interconexión de múltiples puntos, bases de datos, redes y sistemas. Dicha conectividad masiva, impulsada por el avance tecnológico, ha dado origen a un nuevo escenario de conectividad global en el que la ciberseguridad desempeña un papel fundamental.

En este apartado se establecerá una visión integral de la evolución de la ciberseguridad en el contexto de la defensa para comprender la importancia de esta en el panorama estratégico actual, sentando una base sólida para explorar implicaciones futuras.

El surgimiento de la ciberseguridad desde la evolución tecnológica se puede entender desde el uso de ondas electromagnéticas para entorpecer comunicaciones, o, mejor dicho, para proteger estas. [21] El empleo del espectro electromagnético en fonía y telegrafía dio puerta a la manipulación de emisiones en un entorno de una naciente guerra electrónica, como lo fue en la batalla de Tsushima (1905), en la que un operador telegráfico ruso detectó la emisión de señales de radio por parte de Japón y procedió a generar contramedidas. Con ello comenzó la primera acción documentada como Operación de Guerra Electrónica (EWO).

Durante la Guerra Fría, el uso del espectro electromagnético para fines bélicos marcó hitos en una creciente guerra electrónica. Esta nueva dimensión de conflicto se alineaba con la polarización entre Occidente y la órbita soviética, caracterizada por la competencia tecnológica, conflictos subsidiarios y la carrera armamentística. La guerra electrónica ofrecía una opción estratégica en esta escena, permitiendo acciones de hostigamiento y desequilibrio de poder.

Figura 2.4 Ciberguerra híbrida [22].

Posteriormente, la evolución hacia el ciberespacio introdujo una nueva dimensión, marcando el surgimiento de la ciberguerra. Esta modalidad destacaba por su velocidad, dinamismo y capacidad para generar impacto inmediato en infraestructuras. Las plataformas de conformación CEMA, que abarcan operaciones ciberelectromagnéticas, se convirtieron en elementos esenciales para garantizar la defensa y el ataque en el ciberespacio y el espectro electromagnético [21].

La distinción entre ciberdefensa y ciberseguridad se hace relevante en este contexto. Mientras la ciberdefensa se centra en el desarrollo de capacidades para preservar la seguridad de sistemas e información, la ciberseguridad se enfoca en proteger el ciberespacio contra el uso indebido y asegurar el funcionamiento de las propias redes.

La evolución de las ciberamenazas se ha caracterizado por un crecimiento en la sofisticación y diversificación de los ataques, así como en las motivaciones detrás de ellos. Según el CCN-CERT, en la actualidad, las ciberamenazas pueden clasificarse en varias categorías principales cada una con sus características [9]:

1. Ciberespionaje: Estos ataques están dirigidos a obtener secretos de Estado, propiedad industrial, intelectual, información comercial sensible o datos personales. Son los más complejos y técnicamente avanzados, y su detección requiere herramientas especializadas con un personal con habilidades bastante avanzadas.

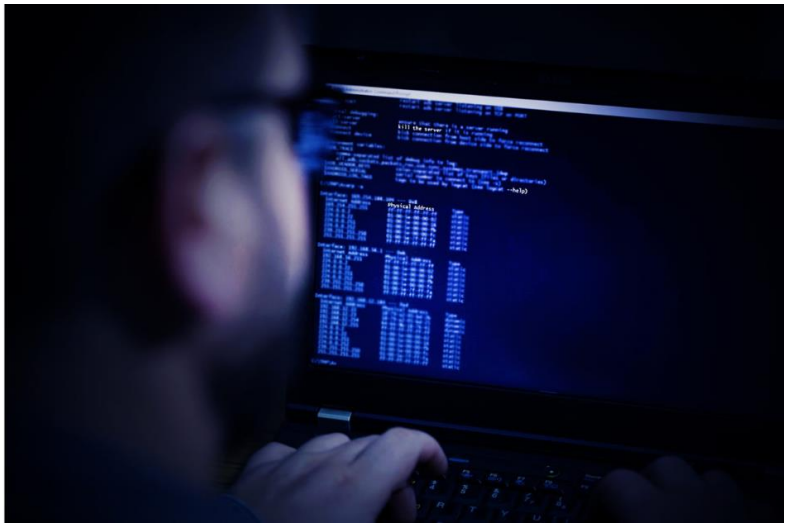

Figura 2.5 Ciberespionaje industrial [23].

2. Ciberactivismo: Activismo digital antisocial, que busca promover una causa o defender un posicionamiento político o social mediante el control de redes o sistemas. Aunque su actividad ha disminuido en comparación con años anteriores, sigue siendo relevante.

3. Ciberterrorismo: Actividades destinadas a causar pánico o catástrofes en las redes y sistemas, o utilizando estas como medio para tales fines. Aunque el volumen de casos detectados es mínimo, el uso de internet por parte de grupos terroristas para comunicación y coordinación ha aumentado.

4. Ciberconflicto/ciberguerra: Operaciones dirigidas por Estados para desestabilizar otros Estados y polarizar a la población civil. Incluye una variedad de herramientas, como ciberataques, acciones de inteligencia, propaganda y desinformación. Estos ataques pueden tener un impacto significativo en infraestructuras críticas y servicios esenciales.

Para concluir esta evolución [9], podemos sacar conclusiones acerca del impacto de la pandemia de COVID-19 en la ciberseguridad, puesto que las medidas de confinamiento aceleraron la adopción de tecnologías de teletrabajo y aumentaron la dependencia de servicio en la nube, VPN y herramientas de colaboración remota, introduciendo numerosas deficiencias de seguridad que los ciberatacantes aprovecharon con un incremento en el número de los ataques dirigidos a estas plataformas, Los ciberdelincuentes encontraron en ellas una forma rentable de acceder a las redes corporativas y organismos públicos.

Viendo estos sucesos se pone en evidencia que muchas de estas tecnologías no han sido sometidas a procesos de certificación adecuados. Además, las redes de control industrial carecen a menudo de las medidas de ciberseguridad necesarias. Por tanto, tenemos un desarrollo muy rápido de ciberamenazas debido a factores como fue la pandemia o el crecimiento propio de las tecnologías, a lo que está respondiendo la ciberseguridad, aunque a veces situándose por detrás de los ataques.

Ante la situación descrita es crucial que las organizaciones implementen medidas de prevención y detección de malware, así como protocolos de gestión de incidentes. Además, es importante que se refuercen las medidas de seguridad en las redes de control industrial y se promueva la conciencia sobre ciberseguridad entre los usuarios domésticos de dispositivos IoT.

2.3. Conceptos Fundamentales de la Inteligencia Artificial aplicada a la Defensa

En este apartado trataremos de ver las bases que se han ido sentado acerca de la Inteligencia Artificial en la Industria de la Defensa, así como veremos de forma general como se ha adaptado a este ámbito.

En Defensa, la adopción de la IA se ha basado en una serie de fundamentos clave que han sentado las bases para su aplicación y desarrollo. Estos fundamentos han sido esenciales para poder adaptar la Inteligencia Artificial a las necesidades específicas y los desafíos únicos que enfrentan las fuerzas armadas y las organizaciones de seguridad.

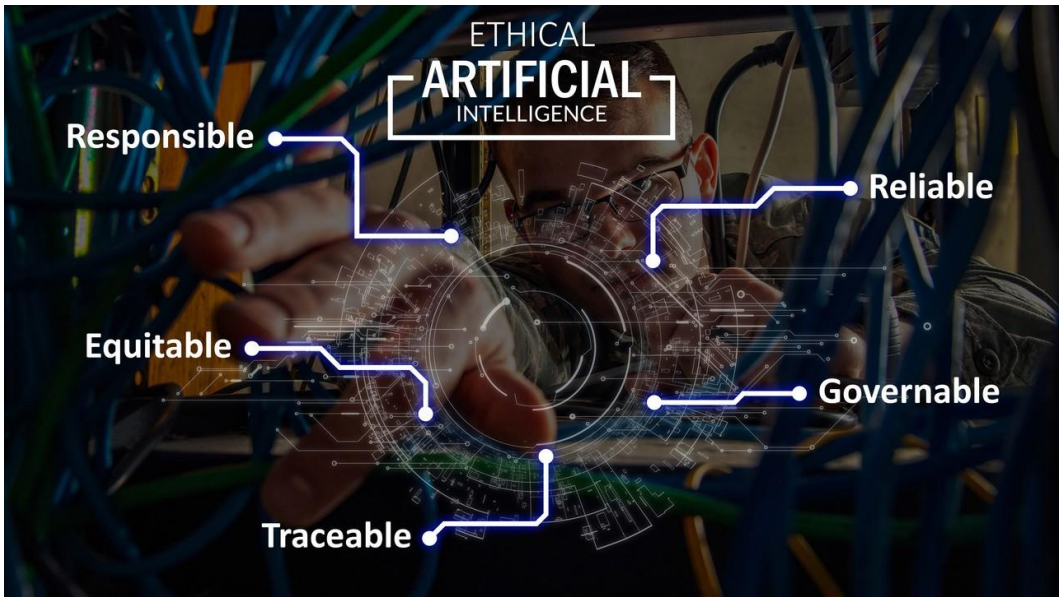

Figura 2.6 Conceptos fundamentales de la IA en Industria Defensa [24].

En primer lugar [24], destaca la necesidad de la innovación, la industria de la defensa está constantemente buscando nuevas tecnologías y enfoques para mejorar sus capacidades y mantenerse a la vanguardia de un entorno cambiante y cada vez más complejo. La IA ofrece oportunidades significativas para la innovación en áreas como la toma de decisiones, la planificación de misiones y la optimización de recursos, siendo una herramienta que explotar.

Para más, tenemos como otro de los aspectos clave la resolución de problemas complejos. Los desafíos en el campo de batalla y en la seguridad nacional son inherentemente complejos y dinámicos, siendo en ocasiones casi imposible encontrar una solución óptima. La IA puede ayudar a enfocar estos problemas al analizar grandes volúmenes de datos, e identificar tendencias, proporcionando información procesable para la toma de decisiones.

Eficiencia operativa es otro de los conceptos fundamentales de la IA, debido a que la automatización y la autonomía impulsadas por la IA pueden mejorar esta eficiencia operativa en una variedad de áreas amplia, desde la lógica y el mantenimiento de equipos hasta la vigilancia y el reconocimiento. En un cuerpo de fuerzas armadas, esto permite optimizar el uso de recursos que puede ser crucial en las misiones, así como mejorar su capacidad para cumplir con ellas.

Viendo desde una perspectiva más variada de funcionalidad, tenemos la adaptabilidad y flexibilidad. La naturaleza adaptable que posee de por sí la herramienta de estudio, permite su aplicación en una gama amplia de escenarios operativos. Dicha flexibilidad es significativa para abordar amenazas y desafíos que enfrentan las organizaciones de seguridad en todo el mundo.

Por otro lado, dos aspectos a tener en cuenta son la seguridad y la confiabilidad, si bien la inteligencia artificial ofrece numerosos beneficios, también plantea desafíos en términos de seguridad y confiabilidad. Pero a su vez, garantizar que los sistemas de IA sean seguros es mediante el uso de técnicas de la propia herramienta, protegiendo de manipulaciones maliciosas.

En cuanto a las ramas de la Inteligencia Artificial, en Defensa son aplicadas todas ellas, partiendo del Machine Learning en los sistemas principales, así como en casi todos, siguiendo con el Deep Learning, y terminando con la IA generativa para disipar conocimiento de los enemigos, y difundir información falsa.

2.4. Trustworthy Artificial Intelligence en el Contexto de la Ciberseguridad y la Resiliencia de Sistemas

El trabajo se va a concentrar en este proyecto entre todas las aplicaciones y técnicas emergentes que están siendo utilizadas en proyectos de defensa, específicamente aquellas basadas en inteligencia artificial. El proyecto es llevado a cabo por la Unión Europea, más concretamente es coordinado por la Fundación Tecnalia Investigación e Innovación, situada en España, San Sebastián.

El proyecto [25], AL4CYBER, tiene como objetivo principal proporcionar un Marco de Ecosistema de próxima generación de servicios de ciberseguridad confiables que aprovechen las tecnologías de Inteligencia Artificial y Big Data para respaldar a los desarrolladores y operadores de sistemas en la gestión efectiva de la robustez, la resiliencia y la respuesta dinámica contra ciberataques impulsados por la IA. Esto es crucial debido a que la IA puede ser usada tanto como una herramienta defensiva para mejorar la preparación del sistema y la respuesta ante incidentes cibernéticos, como un arma formidable para los atacantes.

En términos más específicos, el proyecto se centrará en desarrollar un tipo de servicio de prueba de robustez y seguridad impulsados por la IA que faciliten significativamente el trabajo de los expertos en pruebas mediante una identificación más inteligible de fallas y una automatización de la corrección de código. Para más, se ofrecerán servicios de ciberseguridad para la comprensión, detección y análisis de ataques impulsados por IA para preparar a los sistemas críticos par que sean resilientes.

El apoyo en la respuesta a incidentes por parte de AI4CYBER liberará a los operadores de seguridad de tareas complejas y tediosas, ofreciéndoles mecanismos para optimizar la orquestación de la combinación más adecuada de protecciones de seguridad, y aprender continuamente del estado del sistema y la eficacia de las defensas.

El marco AI4CYBER garantizará los derechos fundamentales y los valores basados en la IA en sus servicios, a través de la integración de capacidades demostrables de explicabilidad, equidad y robustez tecnológica (seguridad) en los componentes de AI4CYBER. El ecosistema se validará en tres escenarios: i) Detección y Mitigación de Ataques Impulsados por IA contra el Sector Energético, ii) Robustez y adaptación autónoma de aplicaciones bancarias para enfrentar ataques impulsados por IA y iii) Servicios hospitalarios resilientes contra ciberataques avanzados y impulsados por IA en el ámbito ciberfísico.

Este enfoque integral y detallado del proyecto AI4CYBER busca abordar tanto los desafíos actuales como emergentes en el campo de la ciberseguridad, con un énfasis particular en sectores críticos como la energía, la banca y los servicios hospitalarios. Al desarrollar y aplicar tecnologías de IA avanzadas, se espera fortalecer la seguridad cibernética y proteger estos sistemas vitales contra las crecientes amenazas cibernéticas.

Figura 2.7 Proyecto AL4CYBER de la Unión Europea [26].

3 ESTADO DEL ARTE

En la actualidad, existen multitud de proyectos en los que se ha implementado la Inteligencia Artificial como herramienta principal. Este apartado se centrará en el análisis de la aplicación de técnicas basadas en IA en la industria de defensa, examinando las diversas formas en que la IA está transformando las operaciones militares.

Uno de los eventos recientes que ha tenido éxito ha sido el evento virtual AlphaDogfight Trials (ADT) organizado por la Agencia de Investigación de Proyectos Avanzados de Defensa (DARPA) [20]. Este, entraría como un sistema de simulación y entrenamiento de combate, puesto que en dicho acontecimiento ocho algoritmos de IA compitieron en combates aéreos simulados contra aviones de combate F-16. Tras la competición, en la fase final del evento, el algoritmo ganador (compañía Heron Systems) se enfrentó a un piloto humano de la Fuerza Aérea de los Estados Unidos, quien pilotaba el F-16 en un simulador. Destaca el resultado en el que el algoritmo de IA emergió victorioso en todos los enfrentamientos, destacando por su habilidad en puntería y agresividad. Lo expuesto es un avance evidente en el entrenamiento y desarrollo de capacidades de los ejércitos, en este caso el aéreo.

Por otro lado, tenemos el Proyecto Maven [27], un programa militar del Departamento de Defensa de Estados Unidos que se inició en 2018, en el que se emplean tecnologías de IA y Machine Learning para el reconocimiento de objetivos y a su vez para el monitoreo de amenazas. Este ha sido implementado de manera exitosa en situaciones de batalla real, como en la respuesta a los ataques de Hamás a Israel en Octubre de 2023, marcando un hito significativo en la adopción de tecnologías de IA. Desde entonces se ha logrado identificar y neutralizar diversas amenazas como cohetes, misiles, drones e instalaciones enemigas utilizando algoritmos de IA.

Figura 3.1 Proyecto Maven con IA en reconocimiento de objetivos [27].

Un proyecto que se encuentra actualmente en desarrollo es el liderado por GMV, Cloud Intelligent Explosive Detection System (CONVOY) [28], respaldado por el programa European Defence Fund (EDF), como una iniciativa en el ámbito de la seguridad del personal militar. Este proyecto se centra en desarrollar un sistema innovador de detección de Artefactos Explosivos Improvisados (IED) y minas terrestres para proteger a las fuerzas europeas. CONVOY se basa en tecnologías de vanguardia, como es la inteligencia artificial, la cual deberá procesar y fusionar la información que le llegue al sistema de todos los tipos de sensores que se integrarán.

Figura 3.2 Proyecto ITM de atención médica militar [29].

Un último ejemplo de proyectos que se están llevando a cabo en la línea de usar la IA en sistemas de defensa es el programa "In the Moment (ITM)" [30], el cual podemos introducir en una aplicación para la atención médica militar durante conflictos armados. Esta idea busca generar un marco de alineación cuantitativa para un tomador de decisiones humano confiable y un algoritmo. Este marco permitirá a los algoritmos incorporar atributos clave de confianza y apoyará el desarrollo de algoritmos que puedan ajustarse para alinearse con humanos específicos y confiables. ITM investigará en el contexto de dos dominios específicos: triaje de unidades pequeñas en entornos austeros en la Fase 1 y triaje de víctimas en masa en la Fase 2.

En los próximos meses y años, la aplicación de la Inteligencia Artificial (IA) en la industria de la defensa seguirá evolucionando y expandiéndose hacia nuevas áreas, impulsando avances a nivel mundial. Algunas tendencias futuras incluyen [31]:

1. Sistemas Autónomos y Swarming: Coordinación en enjambres de sistemas autónomos como drones para llevar a cabo una variedad de misiones.

2. Sistemas de Mando y Control Avanzados: Mejora de sistemas de mando y control mediante la IA, facilitando la coordinación de operaciones militares.

3. Tecnologías de Camuflaje y Contramedidas: Desarrollo de técnicas avanzadas de camuflaje, ocultación y engaño, así como la detección de ellas por parte de sistemas de contramedidas impulsados por la inteligencia artificial.

4. Automatización Robótica de Procesos (RPA): La RPA propulsada por la IA automatizará tareas repetitivas y basadas en reglas, liberando recursos humanos para tareas más estratégicas y críticas en el ámbito militar.

Figura 3.3 Robot Autónomo para almacén en ejército [32].

3.1. Avances en las técnicas basadas en Inteligencia Artificial para Ciberseguridad en la Industria de Defensa

En el ámbito de la industria de la defensa, la ciberseguridad se erige como un bastión vital en la protección frente a las crecientes amenazas cibernéticas, pero, enfrentarse a estas amenazas con enfoques tradicionales se está volviendo cada vez más insuficiente. Para abordar estos nuevos desafíos, la Inteligencia Artificial emerge como un arma poderosa en el arsenal de la ciberdefensa militar.

En este apartado se explorarán los avances en técnicas basadas en la IA que están revolucionando la ciberseguridad en la industria de la defensa, desde la detección proactiva de amenazas hasta la respuesta automatizada en tiempo real. A través de una serie de proyectos y casos de estudio se verán cómo dichas técnicas están siendo implementadas en la práctica para fortalecer las defensas cibernéticas militares.

Algunas de las aplicaciones que tiene la Inteligencia Artificial y, con ella, el Machine Learning en el ámbito de la Ciberseguridad son [33]:

1. Detección Amenazas: La IA y el ML permiten analizar grandes volúmenes de datos en tiempo real para detectar patrones y anomalías que puedan indicar posibles amenazas a nuestro sistema, capacitando a los equipos de seguridad para anticiparse y adoptar medidas preventivas para neutralizar las amenazas antes de que se materialicen.

2. Análisis de vulnerabilidades: A través de diversos análisis, como el comportamiento del usuario, el tráfico de red y la inteligencia de amenazas, podemos identificar y priorizar las vulnerabilidades más críticas. Esto alerta a los equipos y permite implementar medidas para remediarlas.

3. Respuestas a incidentes: Implica la detección, evaluación, y respuesta a amenazas o ciberataques que puedan afectar a nuestros sistemas o datos. Mediante las herramientas mencionadas, podemos tener respuestas automatizadas basadas en patrones de ataques analizados, análisis de vulnerabilidades y análisis de riesgos.

Las aplicaciones de inteligencia artificial en ciberseguridad son muy amplias y en las que se han definido anteriormente se engloban una gran cantidad de ellas. Por otro lado, hay diversas técnicas que se ponen en uso según la aplicación que se de. A continuación, se describen algunas de las técnicas más conocidas de IA aplicadas en Sistemas de Detección de Intrusos (IDS) y otras áreas de ciberseguridad [34]:

1. Máquina de Vectores de Soporte (SVM): Utilizada para la calificación de textos, como en el caso de la detección de correo spam. La SVM emplea algoritmos de aprendizaje automático para categorizar mensajes y realizar un filtrado eficiente de spam.

2. Redes Neuronales Artificiales (ANN): Modelos computacionales inspirados en el funcionamiento del cerebro humano. En ciberseguridad, las ANN son usadas para detectar patrones anómalos en el tráfico de la red, identificando ataques.

3. Regresión Multivariada Adaptativa usando Splines (MARS): Esta técnica se emplea en el análisis de la complejidad en la detección de amenazas. Permite estudiar diversas técnicas funcionales sobre la observación de datos, lo que contribuye a mejorar la precisión en la detección de ataques.

4. Programas Genéticos Lineales (LGP): Los LGP son algoritmos evolutivos que se usan en ciberseguridad para encontrar soluciones óptimas a problemas específicos.

Figura 3.4 Artificial Neural Network [35].

Además de las técnicas mencionadas, es importante destacar cómo la inteligencia artificial está siendo implementada en proyectos prácticos de ciberseguridad, siguiendo la línea de estás técnicas. Por ejemplo, L7 Defense [36], con sede en Luxemburgo, ofrece la mitigación de Denegación de Servicio Distribuida (DDos) para redes inteligentes mediante su herramienta Ammune, como parte del proyecto Energy Shield. Han ampliado su herramienta para considerar botnets de medidores inteligentes y ataques utilizando el Advanced Metering Infrastructure (AMI) como vector. Para más, han desarrollado el modelo analítico FC-DDoS para comprender mejor los parámetros de ataque en el contexto de la red inteligente.

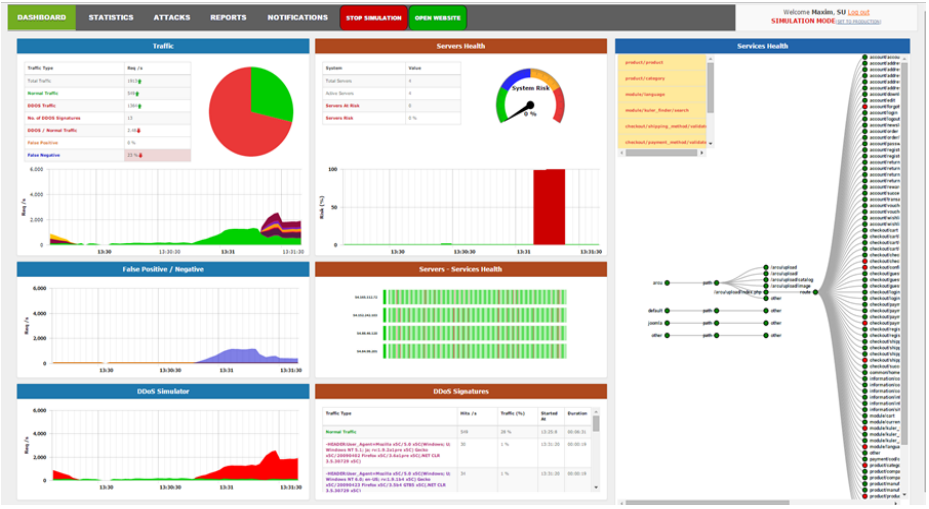

Figura 3.5 Panel de Control de los Clientes de L7 Defense [36].

Para tener una visión global de estas técnicas y proyectos con IA en ciberseguridad en caso de defensa, hay que diferenciar las amenazas y desafíos con los que hay que pelear durante los avances [37]. Uno de los más destacados es la explotación de vulnerabilidades en algoritmos de Inteligencia Artificial; dado que la IA juega un papel cada vez más importante en la industria de la defensa, es fundamental proteger los propios algoritmos basadas en esta herramienta de posibles explotaciones y hacer un sistema con una robustez sólida. La identificación y corrección de vulnerabilidades en estos algoritmos son aspectos clave de la ciberseguridad.

Por otro lado, se encuentran los ataques a la integridad de los datos, lo denominado Data Poisoning; puesto que los sistemas de inteligencia artificial dependen en una gran medida de los datos para su aprendizaje y funcionamiento, es crucial que estos datos sean protegidos contra manipulaciones por parte de adversarios, garantizando la fiabilidad de los sistemas en la industria de la defensa.

Otra de las complicaciones que se plantea es la cuestión de seguridad en la IA autónoma; con el aumento de la autonomía de los sistemas de inteligencia artificial en el ámbito militar, es crucial abordar las posibles amenazas que podrían surgir puesto que la seguridad de los vehículos no tripulados y otros sistemas autónomos es una preocupación creciente que requiere cierto enfoque.

Se ve como unos avances en ciberseguridad vienen de la mano con nuevas dificultades y desafíos, teniendo que ser precavidos en el uso de la IA, puesto que para ello es necesario un sistema robusto y que pueda contemplar todo tipo de vulnerabilidades para que sea capaz de protegerse.

3.2. Desarrollos Relevantes en Trustworthy AI for Cybersecurity Reinforcement and System Resilience

El proyecto Trustworthy AI for Cybersecurity Reinforcement and System Resilience tiene como objetivo desarrollar y aplicar técnicas avanzadas de Inteligencia Artificial para mejorar la seguridad cibernética. Actualmente, este se encuentra en desarrollo, dando pasos a destacar hacia el objetivo principal. Por el momento, se diferencian dos componentes principales en AI4CYBER: Herramienta de Corrección de Bugs y Mejora de Robustez, y un Sistema de Identificación de Vulnerabilidades [38].

3.2.1. Herramienta de Corrección de Bugs y Mejora de Robustez

Dicha herramienta es denominada técnicamente como AL4FIX, esta es una plataforma centrada en la detección y corrección de vulnerabilidades en sistemas informáticos mediante el uso de IA. Sus componentes principales son:

- Módulo Detección de Vulnerabilidades: Este módulo escanea el código y los sistemas para identificar vulnerabilidades tanto conocidas como nuevas. Utiliza algoritmos avanzados para detectar posibles fallos de seguridad que podrían ser explotados.

- Módulo de Corrección Automática: Una vez que se detecta una vulnerabilidad, este módulo genera automáticamente parches o recomendaciones de corrección. Se basa en modelos de IA entrenados en conjuntos de datos de código y parches históricos para proporcionar soluciones efectivas.

- Módulo de Monitoreo y Evaluación: Este componente monitorea continuamente los sistemas para asegurar que las correcciones implementadas no introduzcan nuevas vulnerabilidades ni problemas de rendimiento. Evalúa la efectividad de las soluciones aplicadas y ajusta los modelos de IA según sea necesario.

- Interfaz de Usuario: Proporciona una vista centralizada de todas las vulnerabilidades detectadas, las acciones tomadas y el estado de seguridad general del sistema. Facilita la interacción con los módulos de detección y corrección, permitiendo a los desarrolladores y administradores de sistemas gestionar la seguridad de manera eficiente.

3.2.2. Sistema de Identificación de Vulnerabilidades

Este sistema, nombrado como AI4VULN, se enfoca en la identificación, análisis y priorización de vulnerabilidades en infraestructuras críticas y sistemas de TI. Sus componentes clave incluyen:

- Módulo de Escaneo de Vulnerabilidades: Este módulo realiza escaneos automatizados para identificar vulnerabilidades en aplicaciones, redes y sistemas operativos. Utiliza tanto firmas conocidas de vulnerabilidades como técnicas heurísticas para descubrir nuevas fallas.

- Módulo de Análisis de Riesgo: Evalúa el riesgo asociado a cada vulnerabilidad identificada, basándose en factores como el impacto potencial, la facilidad de explotación y la criticidad del sistema afectado. Utiliza modelos de IA para priorizar las vulnerabilidades que requieren atención inmediata.

- Módulo de Inteligencia de Amenazas: Integra fuentes de inteligencia de amenazas para mantenerse actualizado sobre las últimas tácticas, técnicas y procedimientos utilizados por los atacantes. Esto permite ajustar dinámicamente los modelos de análisis de riesgo y detección de vulnerabilidades.

- Interfaz de Usuario: Ofrece una interfaz intuitiva que permite visualizar todas las vulnerabilidades detectadas, su clasificación de riesgo y las recomendaciones de mitigación. Facilita la toma de decisiones informadas y la planificación de acciones de seguridad.

Estos componentes forman el núcleo de AI4FIX y AI4VULN, construyendo una solución robusta y automatizada, de la que se investigará en la sección 4.1 y la sección 4.2.

4 METODOLOGÍA

El desarrollo del proyecto Trustworthy Artificial Intelligence for Cybersecurity Reinforcement and System Resilience (AI4CYBER) está siendo llevado a cabo desde Septiembre de 2022, estableciendo unos procedimientos y criterios, realizando una división de roles dentro de todos los contribuyentes en dicho proyecto [39].

Gestión de la Seguridad

La gestión de la seguridad en el proyecto Trustworthy Artificial Intelligence for Cybersecurity Reinforcement and System Resilience (AI4CYBER) se centra en la protección de información sensible y en la prevención de problemas de seguridad. Para esta finalidad se han formado dos cuerpos principales: el Oficial de Seguridad del Proyecto (PSO) y la Junta Asesora de Seguridad (SAB).

El PSO, designado en el tercer mes de proyecto, es responsable de monitorear los entregables del proyecto y asegurar la correcta protección y manejo de la información clasificada de la UE (EUCI) cuando sea necesario. La SAB, que apoya al PSO, asiste en el diseño e implementación de medidas relevantes para gestionar, mitigar y responder eficazmente a las preocupaciones de seguridad que surjan. Estos dos grupos se reunirán cada 3 meses para discutir los resultados de las revisiones de seguridad y las actividades del período, identificando posibles riesgos. Además, en estas reuniones se informará a la Junta Ejecutiva, así como al coordinador del proyecto.

Las reuniones entre el PSO y la SAB, así como las reuniones con la Junta Ejecutiva, serán virtuales y estarán presididas por el PSO. Estas reuniones tienen como objetivo identificar anticipadamente posibles problemas de seguridad previstos por los participantes en las tareas de investigación, así como en la producción de entregables y generación de datos.

Plan de Gestión de Datos (DMP)

El DMP del proyecto se establece para asegurar la ética y privacidad en todas las actividades y resultados del proyecto, así como para definir la estrategia de gestión de datos. Este plan incluye un listado de conjuntos de datos de investigación que los socios de AI4CYBER están usando o planean utilizar. Actualmente, se han identificado varios conjuntos de datos que son útiles para la investigación que se está llevando a cabo.

La estructura del DMP se compone de: Recolección de Datos, descripción de los métodos y herramientas utilizadas para la recolección de datos, asegurando que se recopilen de manera ética y conforme a las regulaciones; Almacenamiento de Datos, políticas para el almacenamiento seguro de datos, incluyendo medidas

para proteger contra accesos no autorizados y pérdida de datos; Acceso a los Datos, directrices sobre quién puede acceder a los datos y bajo qué condiciones, garantizando que solo personas autorizadas tengan acceso; Conservación de Datos, estrategias para la conservación a largo plazo de los datos, asegurando que permanezcan accesibles y utilizables en el futuro; y Compartición de Datos, políticas para la compartición de datos entre los socios del proyecto y con el público.

Title	Role	Partner
Project DPO	Revisa los procedimientos de gestión de datos y proporciona orientación.	TECNALIA
Partner DPO	Revisa procedimientos de gestión de datos y apoya al DPO del proyecto en el manejo de aspectos de privacidad.	Todos los socios
Joint Controller	Revisa y sigue el DMP, así como asegura el cumplimiento de las responsabilidades de los socios con respecto al Reglamento General de Protección de Datos (GDPR).	Todos los socios
Quality Assurance Manager	Monitorea la calidad general del proyecto, incluyendo los tipos de datos generados.	TECNALIA
Project Security Officer (PSO)	Monitorea los entregables del proyecto y asegura la protección y manejo de la información clasificada.	University of Western Macedonia (UOWM)
Security Advisory Board Member (SAB)	Asesora al PSO, implementando procedimientos de seguridad y definir medidas para proteger entregables.	Public Power Corporation (PPC), Hospital Do Espirito Santo de Évora (HES), y Caixabank S.A (CXB)

Tabla 4.1 Roles en la Gestión de Datos en AI4CYBER [39].

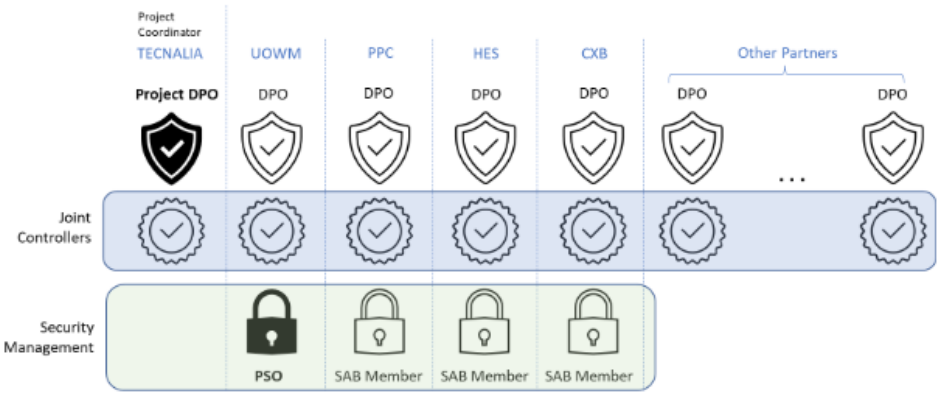

Figura 4.1 Estructura de la Gestión de Datos en AI4CYBER [39].

Publicación y Accesibilidad de Datos

El proyecto promueve una cultura proactiva en la gestión de riesgos, asegurando que los datos generados sean accesibles, interoperables y reutilizables según los principios FAIR (Findable, Accessible, Interoperable, Reusable). Se han adoptado medidas de seguridad y privacidad rigurosas, asegurando que los datos no se refieran a entidades reales en un entorno industrial.

4.1. Herramienta de Corrección de Bugs y Mejora de Robustez (AI4FIX)

4.1.1. Enfoque de Investigación

El principal enfoque de este componente se trata de la corrección automática de debilidades relacionadas con la robustez del software. Dicha perspectiva de investigación incluye mejorar la robustez tal y como se ha indicado, usando modelos de evolución de software para sugerir mejoras propias, y generar pruebas para verificar la corrección de ellas.

El componente emplea técnicas de Procesamiento del Lenguaje Natural (NLP) para aprovechar el conocimiento de modelos construidos según la evolución del software. AI4FIX puede generar, seleccionar y modificar las correcciones propuestas, asegurando que estas sean adecuadas.

AI4FIX está diseñado para leer las salidas de AI4VULN, permitiendo una integración fluida entre la identificación y la corrección de vulnerabilidades. Esto se logra mediante una estructura JSON definida para la comunicación entre ambos componentes.

4.1.2. Contexto del Sistema

AL4FIX utiliza un plugin de UI en VSCode para interactuar con los desarrolladores, permitiendo la selección, aceptación, rechazo y modificación de correcciones generadas, así como la ejecución misma de la herramienta.

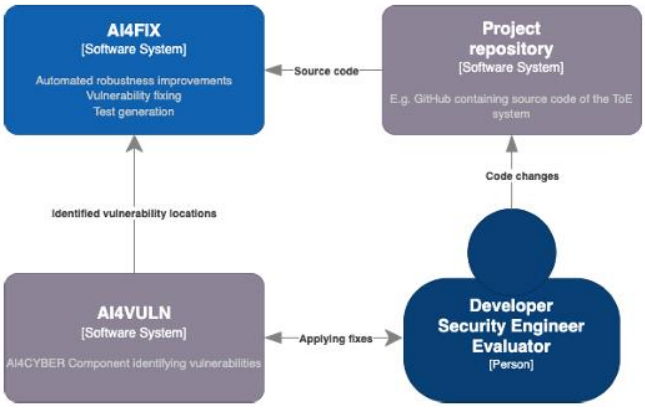

Figura 4.2 Contexto del Sistema de AI4FIX [38].

AI4FIX está diseñado para ser utilizado por desarrolladores y evaluadores de seguridad. El contexto del sistema se ilustra en la Figura 4.2; AI4FIX, principal componente responsable de mejoras automáticas interactuando de forma directa con el código fuente; AI4VULN, sistema secundario que identifica dentro del software y proporciona las ubicaciones a investigar; Repositorio del Proyecto, representado por otro sistema de software como puede ser GitHub, donde reside el código fuente del sistema objetivo, siendo el lugar en el que se aplican los cambios generados; y Roles Humanos, proporcionan retroalimentación y validación necesaria para las correcciones y mejoras realizadas por AI4FIX. La interacción se muestra mediante flechas que indican el flujo de información, como cambios de código y aplicación de correcciones.

4.1.3. Modelo de Contenedor

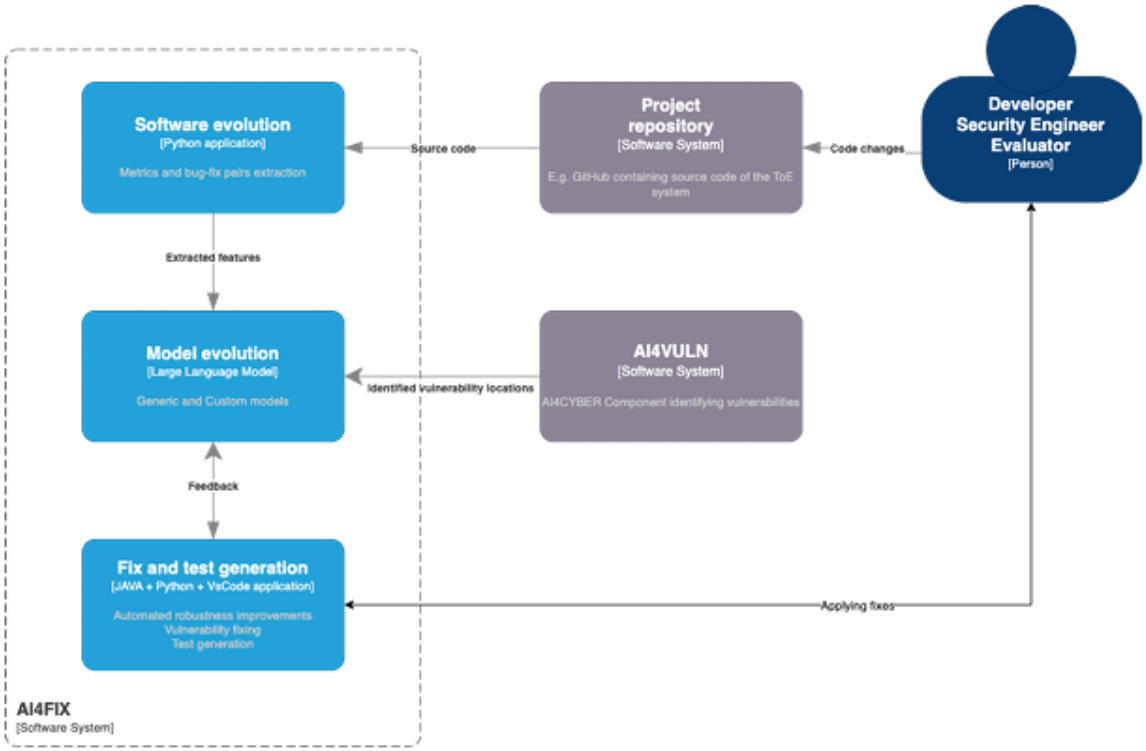

Figura 4.3 Modelo de Contenedor de AI4FIX [38].

En este modelo de contenedor se proporciona una vista del sistema de AI4FIX desglosado en sus principales componentes:

- Software Evolution: Aplicación en Python responsable de la extracción de métricas y pares de corrección de errores del código fuente.

- Model Evolution: Consiste en un Modelo de Lenguaje Grande (LLM), un tipo de modelo de inteligencia artificial que se entrena con grandes cantidades de texto para comprender y generar lenguaje humano de forma coherente. En este caso, usa características extraídas del proceso anterior, incluyendo modelos genéricos y personalizados.

- Fix and Test Generation: Engloba múltiples tecnologías (Java, Python, y aplicación VSCode) y es el responsable de las mejoras automáticas de robustez y las correcciones.

Componentes de Software Evolution

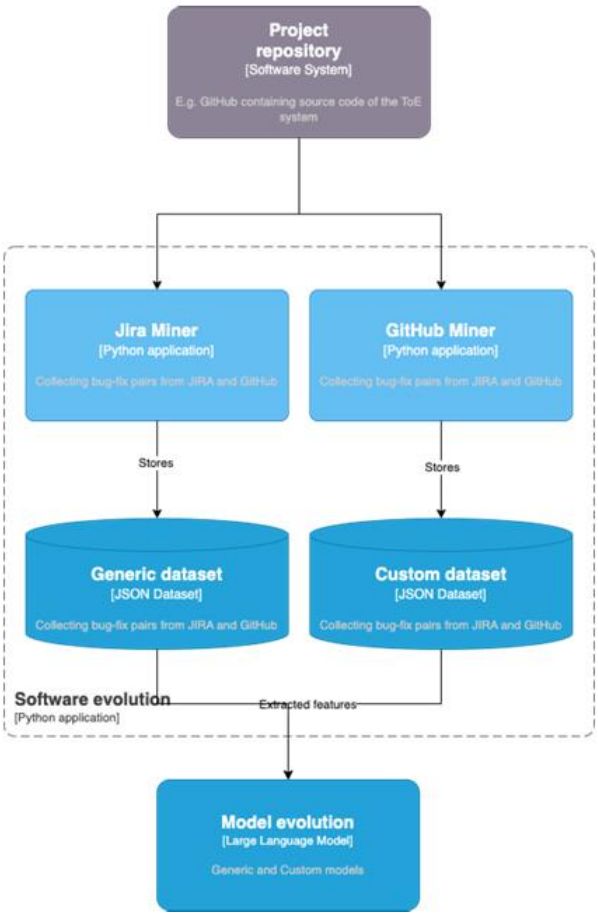

Figura 4.4 Componentes de Software Evolution [38].

Es un componente que proporciona una visión arquitectónica de las partes que componen la aplicación Python dentro del sistemaAI4FIX:

- Jira Miner: Aplicación Python que recopila pares de corrección de errores de JIRA y GitHub.
- GitHub Miner: Aplicación Python que recopila datos directamente de los repositorios de GitHub, relacionados con el historial de commits y las interacciones con herramientas de análisis de seguridad de aplicaciones estáticas.
- Datasets: Generic Dataset que almacena pares de corrección de errores en formato JSON, considerados universales o genéricos; y Custom Dataset, personalizado para proyectos específicos.

Componentes de Model Evolution

Modelo detallado del contenedor Model Evolution, que se centra en el refinamiento del modelo de aprendizaje automático en AI4FIX.

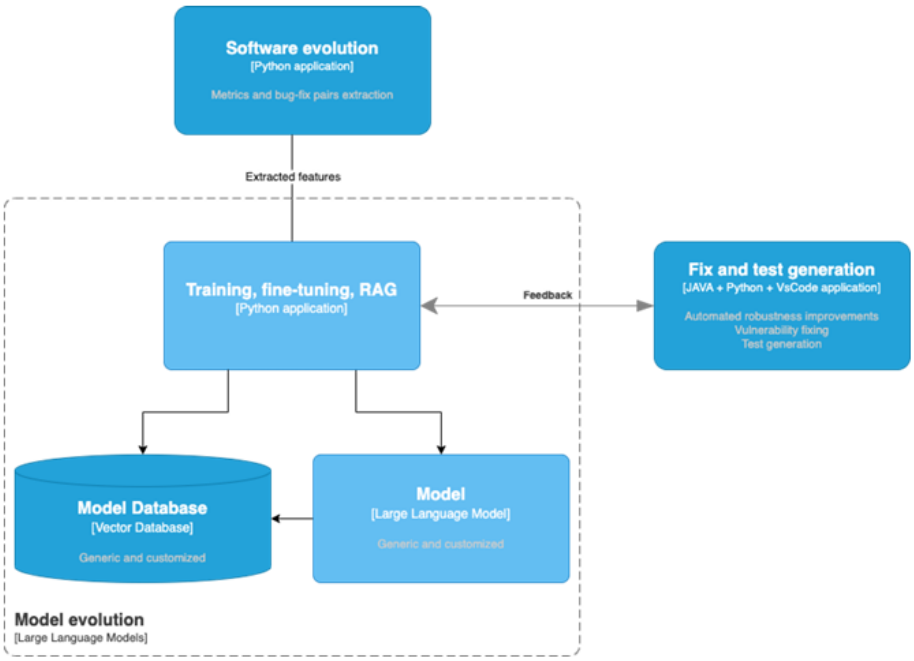

Figura 4.5 Componentes de Model Evolution [38].

- Training, Fine-tuning, RAG: Aplicación Python responsable del desarrollo del modelo de aprendizaje automático, utilizando técnicas como la Generación Aumentada por Recuperación (RAG).

- Model Database: Base de datos vectorial que almacena datos genéricos y personalizados necesarios para el entrenamiento y ajuste del modelo.

- Model: Modelo de Lenguaje Grande que sirve tanto para aplicaciones generales como específicas de proyectos.

Componentes de Model Evolution

Contenedor que comprende componentes críticos que interactúan con procesos internos y entidades externas para mejorar el software:

- Fix Generation: Aplicación Python que genera correcciones de código basadas en las salidas del modelo y las integra en el repositorio del proyecto.

- Test Generation: Crear pruebas automatizadas para verificar la funcionalidad del software.

- Test Execution: Utiliza tecnologías Python y JAVA para ejecutar las pruebas y proporcionar un bucle de retroalimentación humana.

- Fix Visualizer: Plugin de VSCode que ofrece una representación visual de las correcciones generadas y permite a los desarrolladores comprender y evaluar las correcciones en su entorno de código.

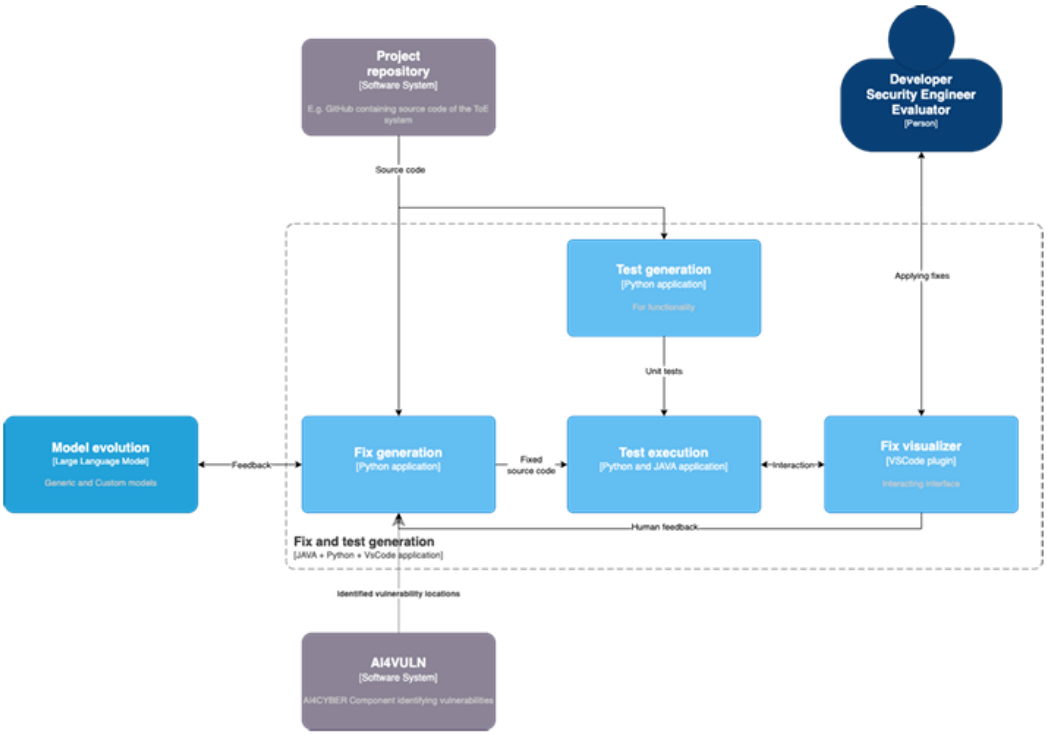

Figura 4.6 Componentes de Fix and Test Generation [38].

Tras realizar una explicación detallada de los componentes que conforman el sistema AI4FIX, se define que la mejora de la robustez está en proceso de desarrollo en el momento, ya que los modelos aún no están entrenados. Según pruebas iniciales, los LLM pueden mejorar fragmentos de código, pero requieren un control estricto sobre la degradación funcional, por lo tanto, primero se debe desarrollar la generación de pruebas.

4.1.4. Generación de Pruebas

Tras haber investigado las herramientas disponibles para generación de pruebas, se presentan siete populares métodos de automatización de pruebas impulsadas por IA, con capacidades únicas, adaptadas a diferentes necesidades de prueba en entornos web, móviles, de escritorio y de API.

- Testsigma: Una herramienta de prueba de IA para aplicaciones web, móviles, de escritorio y APIs, con funcionalidades de auto-reparación y procesamiento de lenguaje natural para la creación de pruebas.

- TestCraft: Construido sobre Selenium, esta herramienta está diseñada para pruebas manuales y automatizadas, especialmente para software basado en web.

- ACCELQ: Herramienta sin código que permite la automatización de pruebas en múltiples canales, centrada en la automatización enfocada en procesos empresariales.

- Applitools: Ofrece pruebas visuales de IU impulsadas por IA y monitoreo, integrándose con pruebas existentes y proporcionando características de prueba en varios navegadores y dispositivos.

- Testim: Plataforma impulsada por IA para aplicaciones web personalizadas, que permite la creación rápida de pruebas de IU y de extremo a extremo con estabilización de IA.

- Sauce Labs: Proporciona pruebas exhaustivas en dispositivos, navegadores y sistemas operativos, con funcionalidades para pruebas funcionales y pruebas en paralelo.

- Functionize: Herramienta basada en la nube que utiliza aprendizaje automático e IA para facilitar la creación de casos de prueba utilizando procesamiento de lenguaje natural, adecuada para navegadores de escritorio y móviles.

4.1.5. Interfaces de Comunicación

Esta subsección describe la interfaz de interoperabilidad JSON entre AI4FIX y AI4VULN, así como el intercambio de información con AI4COLLAB utilizando Kafka, plataforma de transmisión de código abierto que se usa para el procesamiento de datos en tiempo real. Mediante esta estructura JSON, AI4VULN puede compartir su salida (vulnerabilidades potenciales encontradas) con AI4FIX para generar correcciones y pruebas relevantes.

4.2. Sistema de Identificación de Vulnerabilidades (AI4VULN)

4.2.1. Enfoque de Investigación

Por otro lado, AI4VULN está dedicado a la identificación eficiente usando técnicas de ejecución simbólica potenciadas por IA. El componente desarrolla modelos de aprendizaje automático capaces de determinar qué caminos de ejecución en el código pueden ser truncados u omitidos, enfocándose en aquellos con mayor probabilidad de contener debilidades. El aspecto propuesto permite un análisis más profundo y efectivo.

La técnica busca reducir el espacio total de estados, facilitando que la ejecución simbólica se concentre en caminos con mayor riesgo de problemas de seguridad. Ello mejora la eficiencia del análisis de seguridad al evitar caminos que probablemente no contengan señales de fragilidad.

4.2.2. Contexto del Sistema

En el nivel del sistema, el input para AI4VULN es el repositorio del sistema Java que se va a analizar. El desarrollador, que inicia el proceso de búsqueda de vulnerabilidades, proporciona a AI4VULN las rutas de los archivos. El sistema de software AI4VULN luego, procesa el código con análisis estático. Como resultado, el desarrollador recibe una lista de posibles debilidades, que también se envían al sistema AI4FIX para su corrección automática.

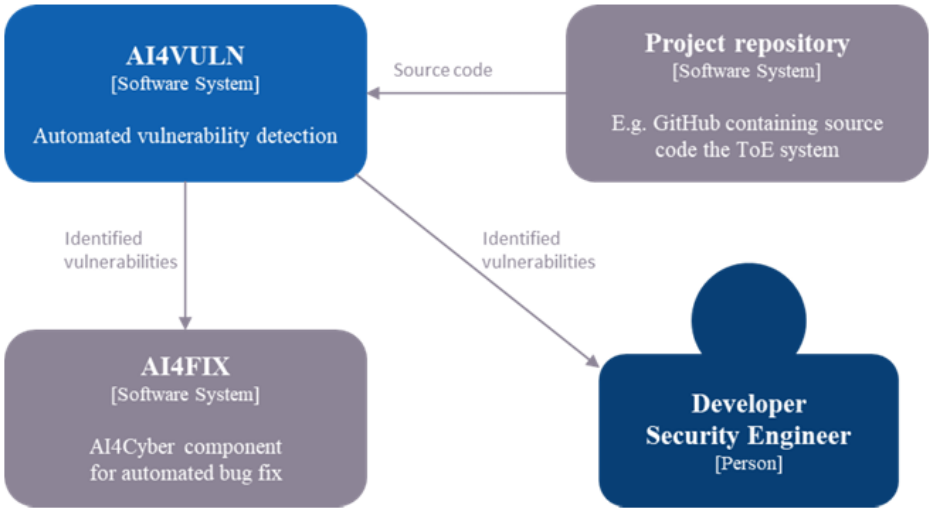

Figura 4.7 Contexto del Sistema de AI4VULN [38].

4.2.3. Modelo de Contenedor

En la Figura 4.8 se muestran los componentes del sistema de software AI4VULN. Aunque se cuenta con cuatro estructuras principales, solo el Motor de Ejecución Simbólica puede descomponerse más, puesto que los demás son contenedores más simples.

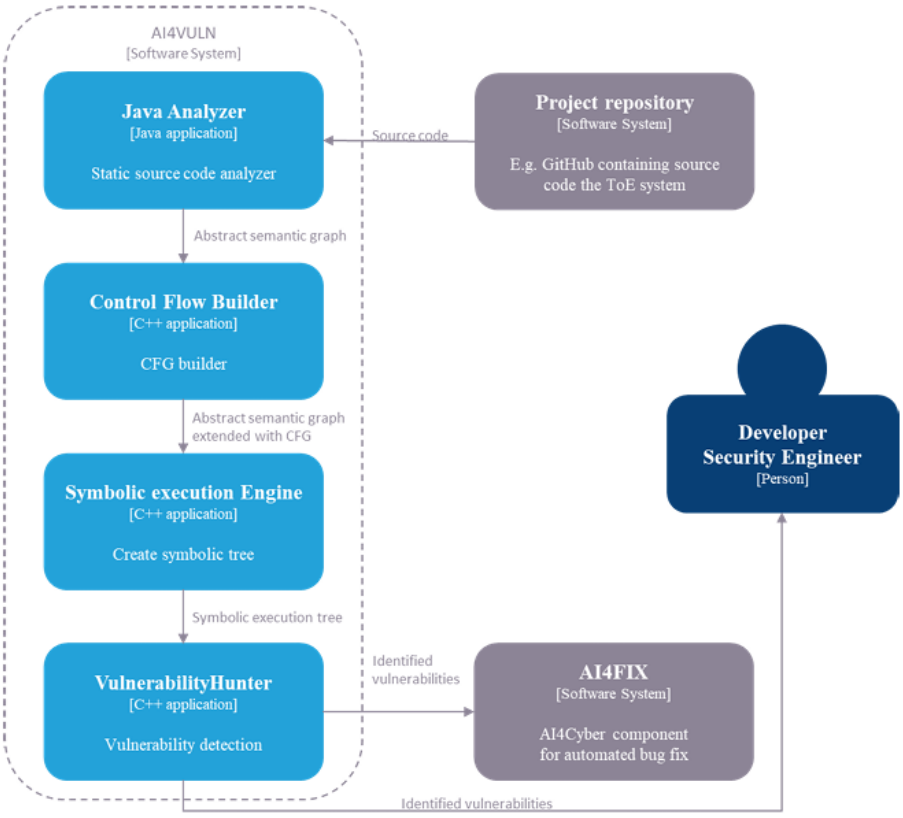

Figura 4.8 Modelo Contenedor de AI4VULN [38].

Componentes de Symbolic Execution Engine

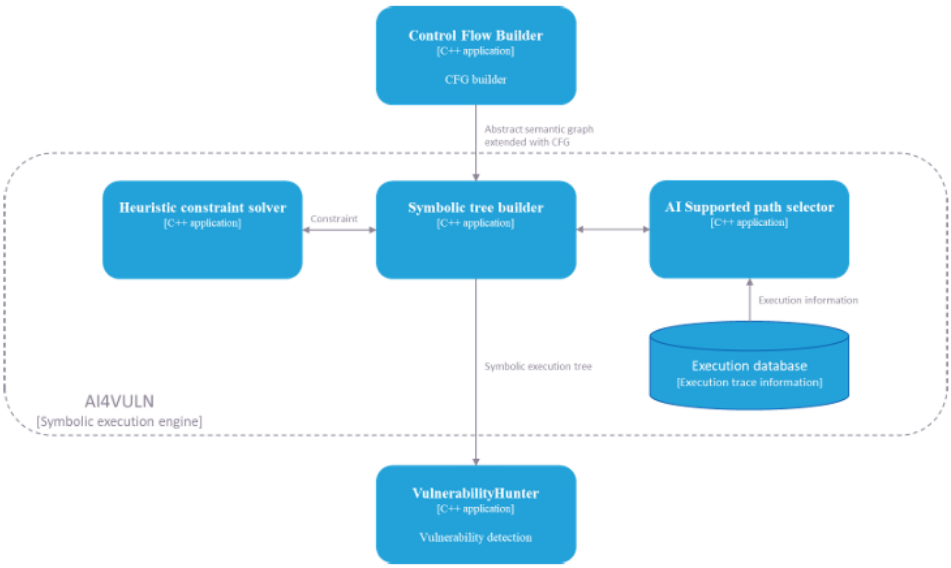

Figura 4.9 Componentes de Symbolic Execution Engine [38].

El motor simbólico utiliza el Grafo de Flujo de Control (CFG) y el Grafo Semántico Abstracto (ASG) para generar un árbol de posibles caminos de ejecución.

El proceso de generación es apoyado por dos componentes: el solucionador de restricciones y el selector de caminos. El solucionador puede eliminar ramas de ejecución no satisfacibles. Dado que ejecutar el solucionador de restricciones puede ser muy demandante de recursos, se introducen heurísticas para acelerar la operación.

El selector de caminos con soporte de IA es responsable de priorizar el examen de las ramas de ejecución en las que es más probable encontrar fragilidades. Si limitamos el tiempo de ejecución y la memoria utilizable, errores importantes pueden quedar sin descubrir. Se entrena a la IA en una base de datos que contiene ramas de ejecución con vulnerabilidades.

4.2.4. Conjunto de Datos de JiraMiner

Para poder determinar si un commit es relevante para la seguridad, eran necesarios datos etiquetados de una fuente confiable, para ello se construye una herramienta que recopila ejemplos de proyectos de código abierto. El conjunto de datos JiraMiner se recopila de los proyectos de Apache disponibles en la plataforma de seguimiento de problemas JIRA y sus correspondientes repositorios de GitHub para el código.

Jira a GitHub

Cada issue en JIRA tiene un campo de descripción que describe el problema y lo que se debe hacer para resolverlo. En la interfaz web de JIRA, existe una sección llamada "Issue Links" que contiene enlaces a otros issues, pull requests de GitHub o commits. Sin embargo, esta sección no está disponible en la API REST de JIRA, lo que complica el acceso automatizado a estos enlaces.

Cada problema tiene también un gran número de campos personalizados, la mayoría de los cuales no están llenos. Uno de los problemas que se pueden encontrar es que los enlaces no estén disponibles para cada issue resuelto puesto que no todos tienen enlaces a GitHub. Por otro lado, se ven proyectos que directamente no usan GitHub para el seguimiento de cambios, siendo un inconveniente que destacar. Además, con relación a proyectos en Jira, se diferencian algunos que tienen múltiples repositorios en GitHub, siendo esta una forma poco ortodoxa de unirlos.

Para solucionar lo comentado, debido a que se pueden formar duplicados y datos engañosos, se recopilan los pull requests y enlaces de commits desde las descripciones, comentarios y registros de trabajo. Posteriormente, se filtran los duplicados y se eliminan los commits irrelevantes para asegurar que la información obtenida sea precisa y útil.

GitHub a Jira

Se recopilaron todos los repositorios de GitHub referenciados en los proyectos de JIRA, lo que resultó en más de 6000 repositorios recopilados. Se mantuvieron solo aquellos donde el propietario del repositorio es "Apache", lo que redujo la cantidad a 1354 repositorios. Para estos repositorios, se recopilaron todos los pull requests y se extrajeron las claves de los issues a partir de los títulos de los pull requests. Si un pull request tiene un issue correspondiente en JIRA, entonces es probable que el título del pull request comience con la clave del issue.

Durante el proceso de correspondencia de pull requests de GitHub con issues de JIRA, surgieron varios problemas significativos: algunos issues eran tan nuevos que no estaban presentes en los datos descargados de JIRA; las claves de los issues a menudo contenían errores tipográficos, lo que complicaba la correspondencia precisa; y algunos proyectos, como Apache AIRFLOW, habían eliminado sus proyectos de JIRA o restringido su acceso, dificultando el seguimiento y la vinculación de los cambios realizados.

Para solucionar estos problemas, se realizó un proceso de corrección de errores tipográficos encontrando la coincidencia más cercana en el proyecto existente, superando un umbral de similitud determinado. Sin embargo, en muchos casos, esta solución no fue suficiente, y las claves de los issues tuvieron que ser examinadas manualmente para asegurar una correspondencia precisa.

5 CASO PRÁCTICO: TRUSTWORTHY AI FOR CYBERSECURITY REINFORCEMENT AND SYSTEM RESILIENCE

En este caso práctico se implementará y evaluará un sistema basado en inteligencia artificial, diseñado para mejorar la ciberseguridad en un entorno simulado de un centro de comando y control militar. Usando herramientas y simuladores al alcance, se creará un entorno virtual que replicará las operaciones críticas de un centro de comando y control. La simulación permitirá analizar y gestionar las vulnerabilidades de seguridad, priorizando las amenazas basadas en su impacto potencial.

5.1. Entorno y Contexto del Caso Práctico

El entorno de simulación consistirá en una red virtual creada con VirtualBox, que conectará varias Máquinas Virtuales (VMs) configuradas con Ubuntu Server. Estas VMs representarán los diferentes componentes de un centro de comando y control militar, incluyendo servidores de comunicaciones y bases de datos.

5.1.1. Herramientas para la Implementación

Para llevar a cabo la simulación propuesta, se requerirá un conjunto de herramientas gratuitas que permitan la creación y gestión del entorno virtual, la implementación de técnicas de inteligencia artificial y la monitorización de los resultados. A continuación, se detallan las herramientas necesarias:

1. VirtualBox [40]: Software de virtualización y de código abierto que permite crear y gestionar VMs. Con ello, se obtiene la posibilidad de simular los diferentes componentes del centro de mando y control, además de poder realizar la configuración de redes virtuales para la interconexión.

2. Ubuntu Server [41]: Distribución gratuita de Linux que funciona como soporte para una amplia gama de aplicaciones de servidor, proporcionando estabilidad.

3. Open Vulnerability Assessment Scanner (OpenVas) [42]: Herramienta de escaneo de vulnerabilidades que identifica problemas de seguridad en redes. OpenVAS permite la realización de estos escaneos de forma automatizada, generando informes detallados sobre las debilidades encontradas.

4. Python: Lenguaje de programación con una gran variedad de bibliotecas para el desarrollo de la inteligencia artificial, y análisis de datos.

    4.1. Scikit-Learn [43]: Biblioteca de Python que facilita la implementación de algoritmos de machine learning. Tiene como funcionalidad clave, sus modelos de clasificación y regresión.

5. Grafana [44]: Plataforma de código abierto para monitorear y visualizar datos en tiempo real con creación de dashboards interactivos.

6. Wireshark [45]: Analizador de protocolos de red gratuitos con captura y análisis de tráfico de red. Este es capaz de identificar patrones de ataques.

5.1.2. Configuración del Entorno Simulado

Para comenzar con la configuración de dicho entorno se ha de instalar el software de VirtualBox, para crear diferentes máquinas virtuales.

Figura 5.1 Administrador VirtualBox.

En este caso se crearán cuatro VMs:

- VM1: Servidor de Comunicaciones.
- VM2: Base de Datos.
- VM3: Gateway de Red.
- VM4: Sistema de Monitoreo de Red.

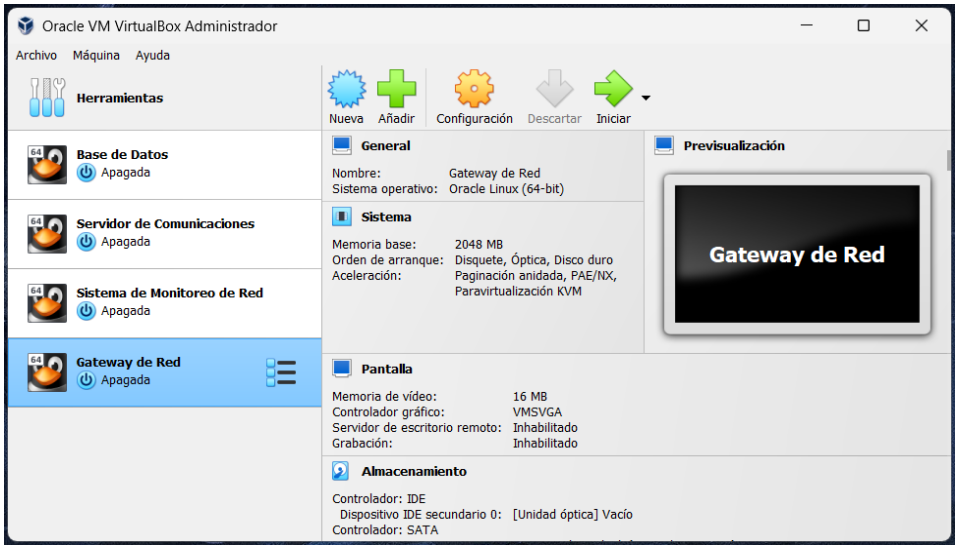

Figura 5.2 Componentes del Centro de Mando y Control creados como Máquinas Virtuales.

A destacar es la creación de las máquinas virtuales como servidores de Ubuntu, es decir, al crear cada una, se debe instaurar una imagen con extensión .iso que hace que la VM que se está creando sea de una u otra forma, en nuestro caso necesitamos el de servidor.

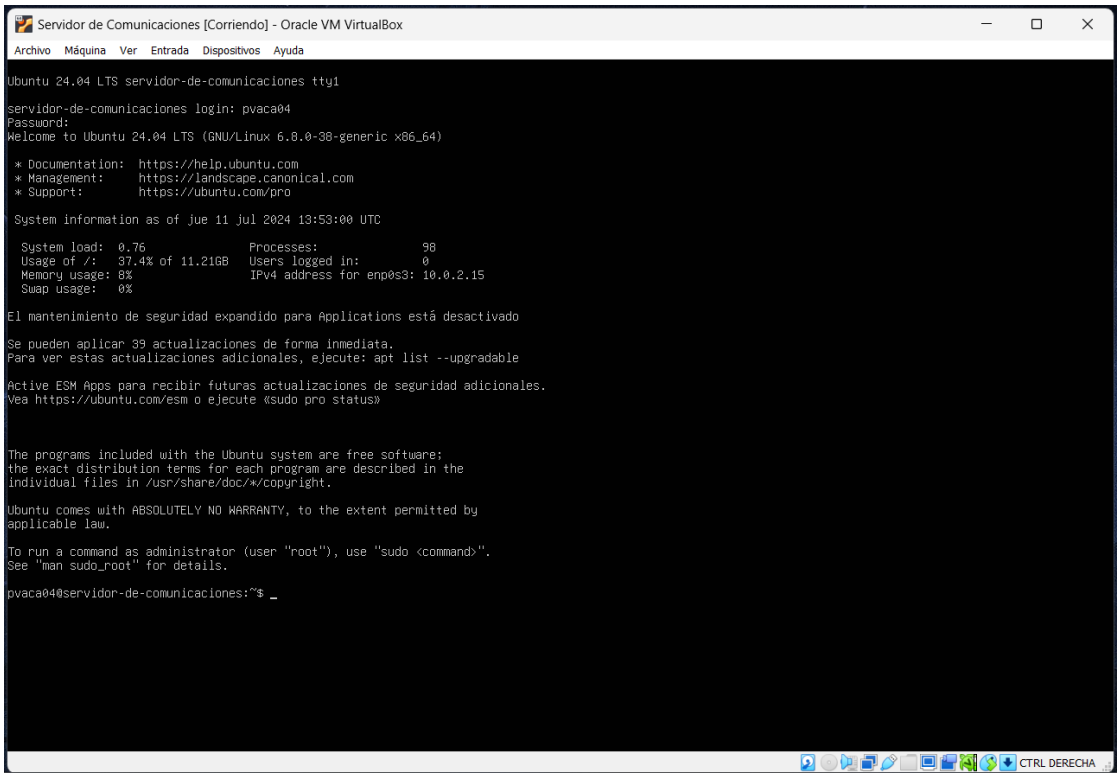

Figura 5.3 Inicio de sesión en el Servidor de Comunicaciones con Ubuntu Server.

Tras ello, se instaura una red interna que interconecta cada una de las VMs, asignando IP estáticas a cada una de forma que sea más sencillo la comunicación entre las máquinas virtuales. Para ello se realiza lo siguiente [46]:

- Configuración de cada VM en Red Interna, para lo que se activa el adaptador 2.

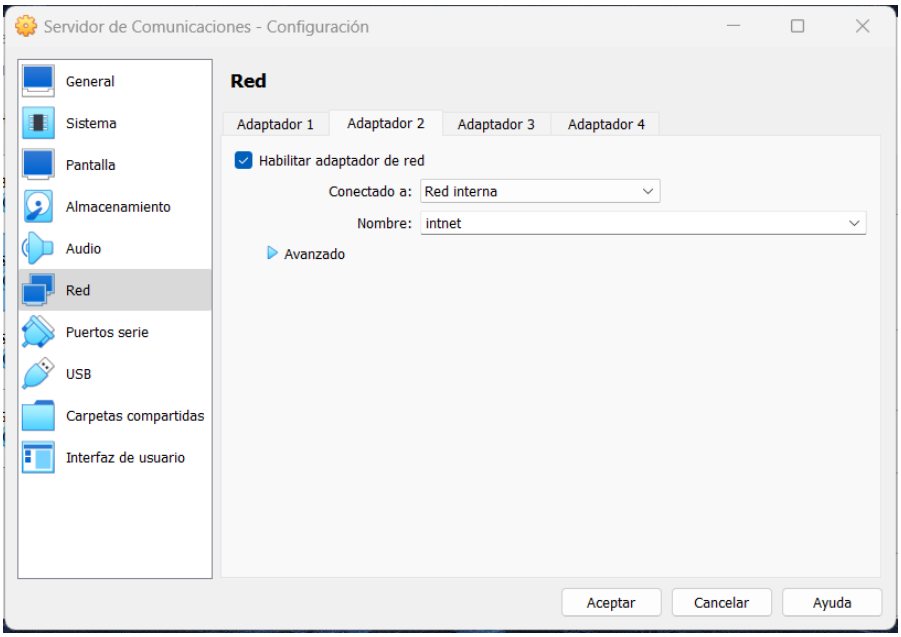

Figura 5.4 Configuración de un segundo adaptador como Red Interna.

Existen diversos modos acerca de cómo configurar la conexión entre los diferentes componentes de control simulados por la gran capacidad de VirtualBox, pero se escoge la opción más cómoda (Red Interna).

- Para configurar la red en una máquina virtual, es necesario acceder a la sección de configuración de esta. Dentro de esta configuración, encontraremos el apartado de Red, donde se mostrarán dos adaptadores de red. Estos adaptadores han sido creados previamente y es aquí donde estableceremos los parámetros necesarios para la Red Interna.

La Figura 5.5 ilustra cómo se configura la IP del Servidor de Comunicaciones, y, además, muestra cómo configurar la IP de Gateway. Cada máquina virtual establecerá como punto central la IP de esta misma, pidiendo la dirección en las VMs a conectar.

La dirección IP que asignemos a esta máquina virtual servirá como punto de acceso principal, facilitando la comunicación con las otras máquinas dentro de la red interna. Es fundamental asegurarse de que esta IP sea única dentro de la red interna para evitar conflictos y garantizar una comunicación fluida y efectiva [47 y 48].

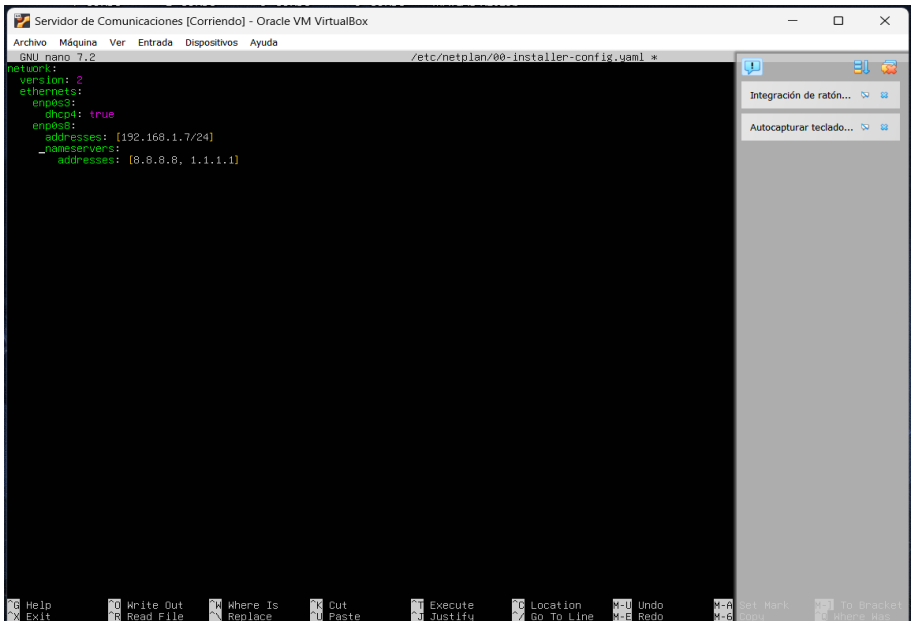

Figura 5.5 IP estática del Servidor de Comunicaciones.

Volviendo a la Figura 5.5, en ella se ven los comandos usados dentro de la lista de red del servidor de Ubuntu llamado “Servidor de Comunicaciones”. Tras ello, se deben aplicar los cambios y se comprueba que las IPs estáticas se han definido de forma correcta.

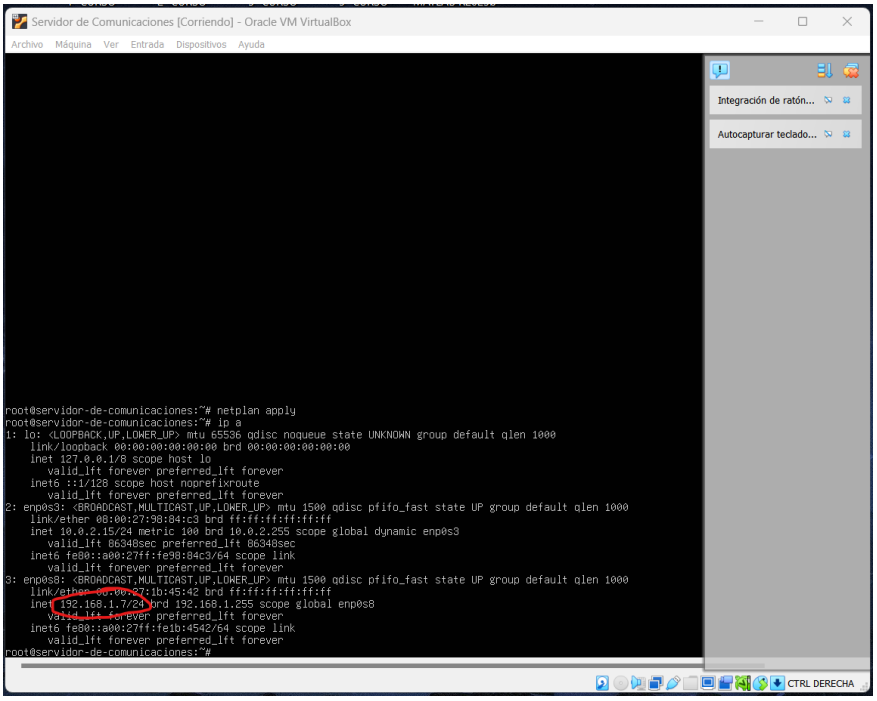

Figura 5.6 Aplicar cambios en dirección IP y comprobación de ello.

Para puntualizar acerca de la Figura 5.6, se ha rodeado en color rojo la dirección IP correspondiente a la VM con la que se está realizando la instalación primaria, de forma que se corrobora la creación de dicha dirección estática. Este proceso se repetirá para las distintas máquinas virtuales, configurándose cada una. A continuación, se comparte una tabla en la que se diferencian y recogen las diferentes direcciones establecidas para el desarrollo de la simulación.

Máquinas Virtuales	IPs
Servidor de Comunicaciones	192.168.1.7
Base de Datos	192.168.1.8
Gateway de Red	192.168.1.1
Sistema de Monitoreo de Red	192.168.1.9

Tabla 5.1 IPs de las respectivas VMs.

Una vez se ha conseguido llegar a este punto, se actualiza el sistema de forma que sea lo óptimo posible con los cambios añadidos.

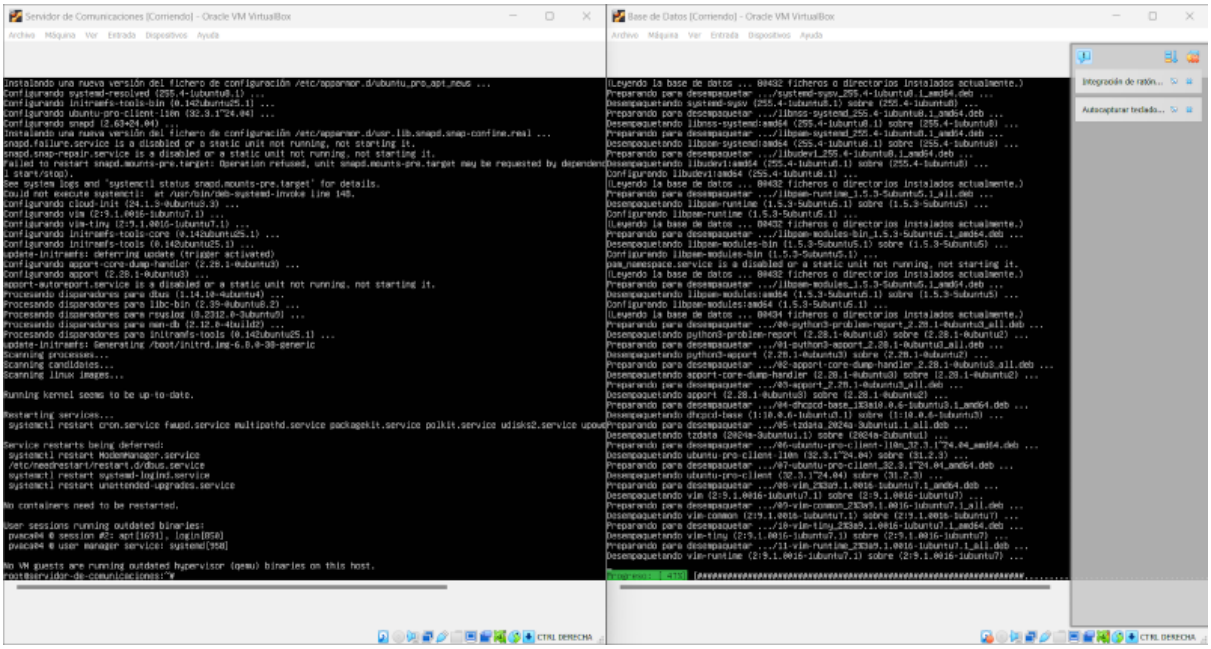

Figura 5.7 Actualización de sistema finalizada de la máquina virtual de “Servidor de Comunicaciones” y actualización en curso de la VM “Base de Datos”.

Para terminar con la configuración del entorno en el que realizar el caso práctico propuesto, se han de instalar y configurar las diferentes herramientas que se han mencionado anteriormente en este documento. Como se ha podido ir vislumbrando cada herramienta irá dirigida a una de las máquinas virtuales para preservar una mayor organización, y para asignar a cada una una función en específico que se verá en los resultados.

Comenzando con la aplicación que permitirá el escaneado de las vulnerabilidades, OpenVas, la cual se deberá encontrar en la VM1: Servidor de Comunicaciones. Para llevar a cabo este punto se impone la instrucción en el terminal: *sudo apt install openvas* [49], para después llevar a cabo su configuración.

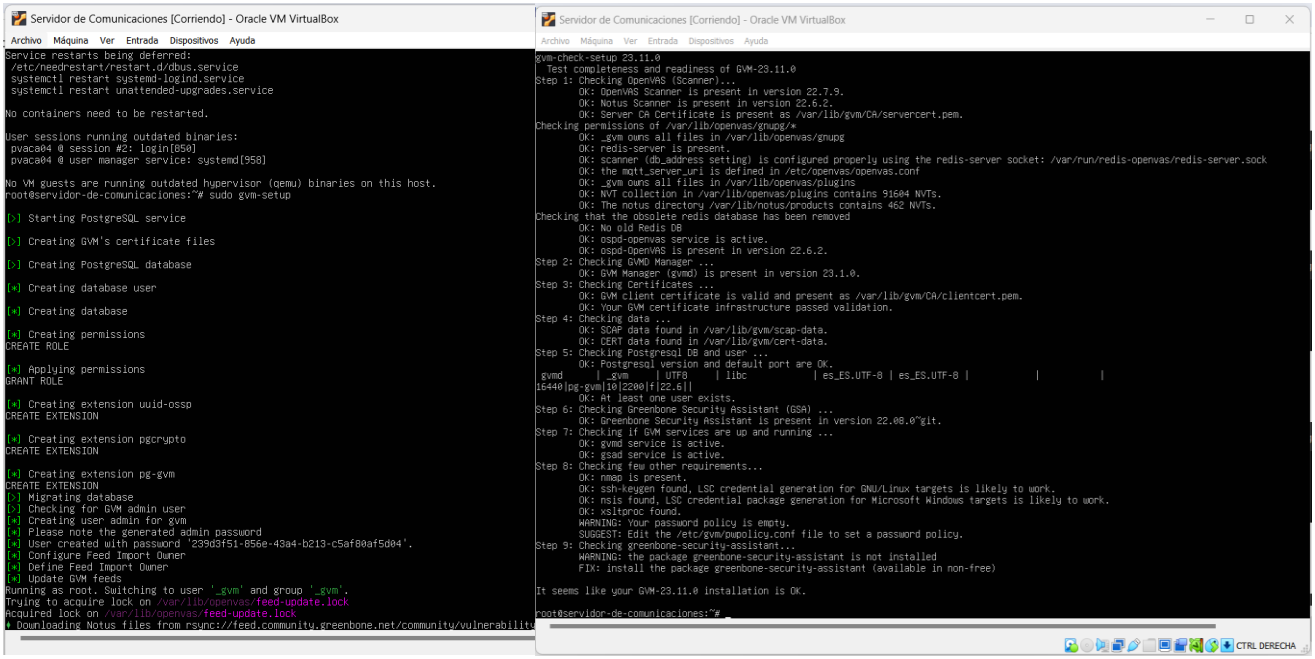

Figura 5.8 Construcción del Set Up de OpenVas y comprobación de una correcta configuración en VM1.

Para comprobar que todo había sido confeccionado como se esperaba, se realiza una ejecución: sudo gvm-check-setup. En la Figura 5.8, en la parte derecha se encuentran las comprobaciones paso por paso, chequeando cada apartado dentro de OpenVas.

Volviendo a las otras herramientas que se necesitan en este entorno, ahora se pasa a la instalación de Python, y su librería Scikit-Learn en la VM2: Base de Datos, de forma que se puedan analizar y procesar. Primero, se descarga y procesa la herramienta que servirá de apoyo a la programación en cuanto al análisis, Python (python3 en este caso) [50].

Cumpliendo con la ocupación mencionada anteriormente, el próximo task será la instalación de la librería que conviene usar en la simulación y la comprobación de una correcta configuración [51], lo cual se muestra en la siguiente figura.

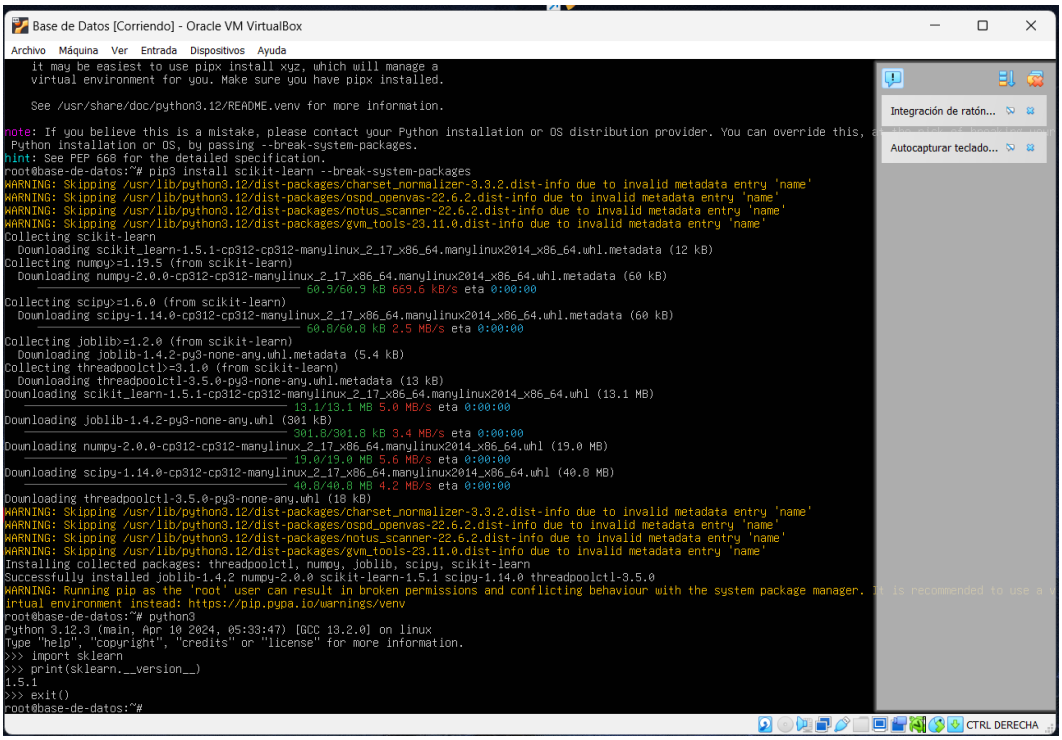

Figura 5.9 Instalación de Scikit-Learn y Python y comprobación de correcta configuración en VM2.

Observando la Figura 5.9 se confirma que se ha trabajado en la máquina virtual 2: Base de Datos. Por otro lado, se realiza la verificación a partir del "WARNING" situado en la parte más inferior de la figura. Tras él, se importa scikit-learn, pudiendo obtener la versión en la que se ha configurado sin ningún tipo de error.

Para completar la configuración de la VM3: Gateway de Red, se instala Wireshark, una herramienta fundamental para la captura y análisis del tráfico de red, y se configuran los permisos necesarios para su correcto funcionamiento. Primero, se actualiza la lista de paquetes disponibles en el sistema ejecutando *sudo apt update*, y luego se instala Wireshark con *sudo apt install wireshark*. Durante la instalación, se pedirá que permitas a los usuarios no privilegiados capturar paquetes; asegurándonos de seleccionar "Sí". Después de la instalación, es necesario agregar el usuario al grupo Wireshark usando *sudo usermod -aG wireshark $USER* y aplicar los cambios del grupo cerrando y volviendo a abrir la sesión con *newgrp wireshark*.

Para finalizar, se verifica que el usuario esté en el grupo wireshark con *groups* y se asegura de que los permisos del ejecutable de dumpcap están configurados correctamente con los comandos *sudo chown root:wireshark /usr/bin/dumpcap*, *sudo chmod 750 /usr/bin/dumpcap* y *sudo setcap 'CAP_NET_RAW+eip CAP_NET_ADMIN+eip' /usr/bin/dumpcap*. Con estos pasos, Wireshark estará listo para capturar y analizar el tráfico de red sin necesidad de permisos de root [52].

Finalmente, termina el desarrollo del entorno de simulación con la introducción de la herramienta de Grafana en la VM4: Sistema de Monitoreo de Red [53]. Mediante los comandos buscados, se debe agregar el repositorio de la aplicación. Cuando se completa esta acción ya es posible instalar Grafana de forma segura y correcta, puesto que sin haber incorporado el repositorio no es posible. Para ver el estado de Grafana, se inicia el servicio y se instaura en "disponible":

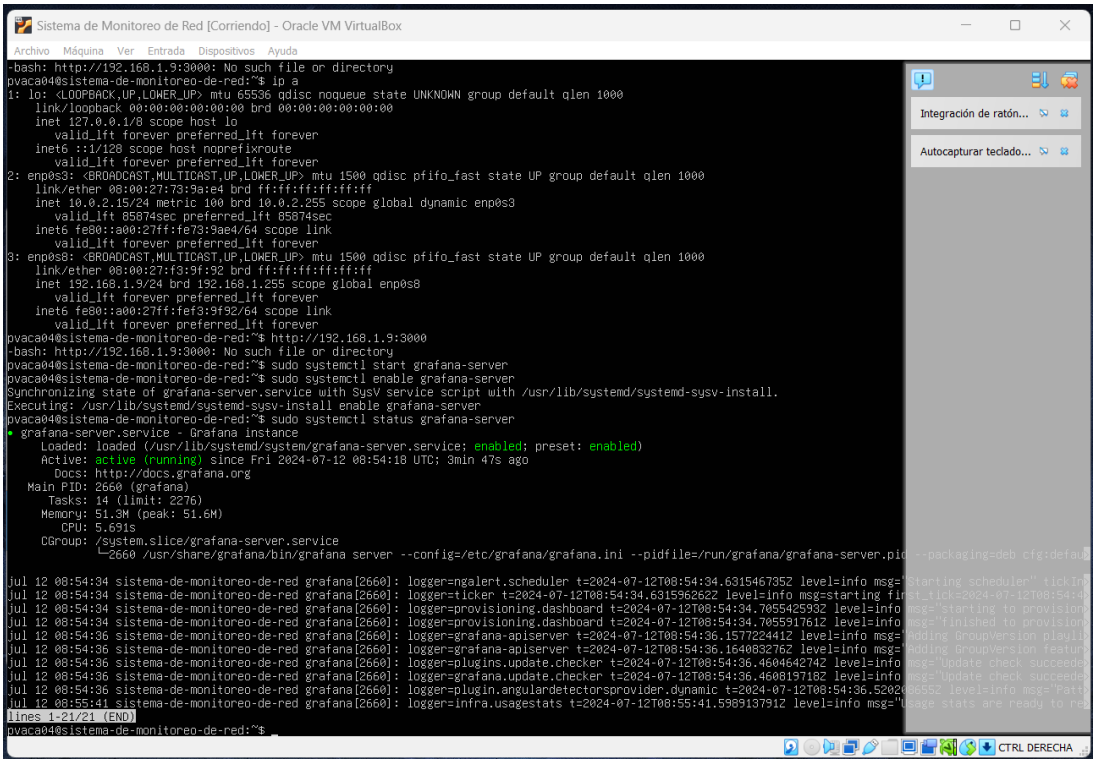

Figura 5.10 Validación de estado de herramienta Grafana en VM4.

Se puede destacar que se ha logrado establecer un ambiente virtual robusto y funcional, utilizando herramientas y tecnologías clave que permiten una simulación efectiva de un centro de comando y control militar.

Este proceso incluye la creación y configuración de múltiples máquinas virtuales, cada una con roles específicos y direcciones IP estáticas, lo que garantiza una comunicación fluida y un análisis detallado de las vulnerabilidades. La correcta instalación y configuración de software como VirtualBox, Ubuntu Server, OpenVAS, Python, Scikit-Learn, Grafana y Wireshark, aseguran que el entorno esté preparado para llevar a cabo simulaciones y análisis de seguridad, proporcionando una base sólida para el desarrollo y evaluación de técnicas aplicadas a la ciberseguridad.

5.2. Implementación y Resultados

Para la implementación de AI4VULN se debe iniciar OpenVas en el Servidor de Comunicaciones de forma que se corrobore la configuración establecida y se ejecuten escaneo de vulnerabilidades en las VMs.

En paralelo en la máquina virtual 2, se crean dos scripts, que sirven para procesar resultados de OpenVas, y para Feeds de Amenazas. Estos son:

```python
import pandas as pd
from sklearn.ensemble import RandomForestClassifier

# Cargar datos de vulnerabilidades
data = pd.read_csv('vulnerabilities.csv')
X = data.drop('severity', axis=1)
y = data['severity']

# Entrenar modelo
model = RandomForestClassifier()
model.fit(X, y)

# Predecir prioridades
priorities = model.predict(X)
data['priority'] = priorities
data.to_csv('prioritized_vulnerabilities.csv', index=False)
```

Figura 5.11 Fichero de Programa para Procesar Resultados de OpenVAS.

```python
import requests

feeds = [
    "https://example.com/threatfeed1",
    "https://example.com/threatfeed2"
]

for feed in feeds:
    response = requests.get(feed)
    with open(f"{feed.split('/')[-1]}.json", 'w') as f:
        f.write(response.text)
```

Figura 5.12 Fichero de Programa para Feeds de Amenazas.

En cuanto a la VM3: Gateway de Salida, se dispone de un display que muestra los niveles de vulnerabilidades, que luego serán guardados e introducidos en una gráfica de forma que sea más visual.

Por último, se ha configurado Wireshark de forma que estime si el tráfico SSH, el tráfico HTTP/HTTPS, el tráfico DNS y el escaneo de puertos, es mayor o menor en dos situaciones distintas.

5.2.1 Resultados de Simulaciones

Se realizaron dos simulaciones con el entorno descrito y su implementación, en las que se muestra el comportamiento simulado antes de AI4VULN y con este mismo en funcionamiento. Para ello, se han separado las vulnerabilidades en 4 clases, según sean más o menos críticas.

Se ha de observar antes de mostrar los resultados que las cifras mostradas son aproximadas puesto que no deja de ser una simulación, pero que entraría dentro del orden de las situaciones reales.

Vulnerabilidad	Antes de AI4VULN	Implementación AI4VULN
Críticas	9	20
Altas	16	20
Medias	20	30
Bajas	25	50
TOTAL	**70**	**120**

Tabla 5.2 Comparación Detección de Vulnerabilidades antes y después de la Implementación de AI4VULN.

Para ver los resultados de una manera gráfica, se muestra la Figura 5.13.

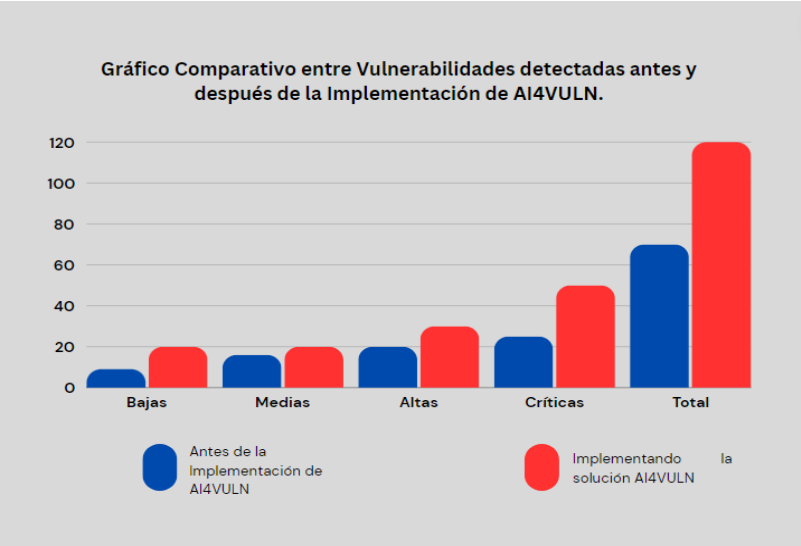

Figura 5.13 Vulnerabilidades detectadas antes y después de AI4VULN.

Análisis de Resultados

1. Incremento en la Detección de Vulnerabilidades:

    - La implementación de AI4VULN mostró un aumento significativo en la detección de vulnerabilidades, pasando de 70 a 120.

- Las vulnerabilidades críticas aumentaron de 9 a 20, lo que indica una mejora en la capacidad de identificar amenazas graves.

- Similarmente, las vulnerabilidades altas y medias también aumentaron, lo que sugiere que AI4VULN puede identificar un espectro más amplio de riesgos.

2. Mayor Precisión en la Clasificación de Vulnerabilidades: El incremento en las vulnerabilidades bajas de 25 a 50 muestra que AI4VULN no solo mejora en la detección de amenazas críticas, sino también en la identificación de problemas menores que podrían ser explotados si se combinan con otras vulnerabilidades.

3. Eficacia del Sistema de Monitoreo: Se han detectado con Wireshark diferentes tipos de tráfico malicioso, lo que ayuda a comprender mejor los patrones de ataque y las áreas vulnerables del sistema.

Tipo de Tráfico	**Detecciones Wireshark/día**
Conexiones SSH	2000
Solicitudes HTTP, HTTPS Maliciosas	1500
Consultas DNS Inusuales	300
Solicitudes SYN	1000

Tabla 5.3 Detecciones de Tráfico por Wireshark.

Estos resultados, aunque aproximados, proporcionan una visión clara del impacto de AI4VULN en un entorno controlado y cómo puede mejorar significativamente la seguridad del sistema.

6 CONCLUSIONES Y RECOMENDACIONES

6.1. Resumen de Hallazgos

El proyecto ha demostrado que la implementación de técnicas basadas en inteligencia artificial, específicamente AI4VULN, puede aumentar significativamente la detección de vulnerabilidades en sistemas de defensa. La integración de herramientas avanzadas y la configuración de un entorno virtual robusto han sido factores clave para el éxito de la simulación. Los resultados obtenidos muestran una mejora considerable en la identificación de vulnerabilidades críticas, altas, medias y bajas, subrayando la eficacia de los métodos basados en IA para fortalecer la ciberseguridad.

6.2. Contribuciones al Campo del Trabajo

El proyecto "Trustworthy AI for Cybersecurity Reinforcement and System Resilience" ha realizado contribuciones importantes en varios aspectos clave de la ciberseguridad aplicada en la industria de defensa:

1. Detección y Corrección Automática de Vulnerabilidades: AI4FIX y AI4VULN demuestran la capacidad de utilizar algoritmos avanzados para la detección y corrección automática de vulnerabilidades, reduciendo la dependencia de la intervención humana y aumentando la velocidad de respuesta a amenazas.

2. Mejora Robustez y Resiliencia del Sistema: La integración de estas herramientas permite una evaluación continua y la mejora de la robustez del sistema, asegurando que las correcciones no introduzcan nuevos riesgos y manteniendo la estabilidad a largo plazo.

3. Interfaz de Usuario Intuitiva: Las interfaces de usuario diseñadas centralizan la visualización de vulnerabilidades y las acciones tomadas, facilitando la colaboración entre equipos de desarrollo y administradores de sistemas, y mejorando la eficiencia en la gestión de la seguridad cibernética.

4. Actualización Continua y Adaptabilidad: La integración de inteligencia de amenazas y la capacidad de mantener actualizados los modelos de detección frente a las tácticas cambiantes de los ciberatacantes aseguran que el sistema puede adaptarse y responder a nuevas amenazas de manera efectiva.

Estas contribuciones muestran cómo la aplicación de inteligencia artificial en la ciberseguridad puede transformar las prácticas actuales, ofreciendo una respuesta más rápida y precisa a las amenazas y mejorando la resiliencia general de los sistemas en el sector de la defensa.

6.3. Recomendaciones para Futuras Investigaciones y Desarrollos en el Área de Trustworthy AI for Cybersecurity

El proyecto Trustworthy AI for Cybersecurity Reinforcement and System Resilience está dando pasos significativos hacia la aplicación de técnicas avanzadas de inteligencia artificial para fortalecer la seguridad cibernética. A través de componentes clave como AL4FIX y AI4VULN, se ha demostrado la capacidad de detectar y corregir vulnerabilidades de manera automatizada y eficiente. AL4FIX utiliza algoritmos avanzados para escanear sistemas y códigos en busca de fallos de seguridad, generando parches automáticos o recomendaciones de corrección basadas en modelos de datos históricos.

La inclusión de un módulo de monitoreo y evaluación asegura que las correcciones implementadas no introduzcan nuevos riesgos o afecten el rendimiento del sistema, garantizando así la estabilidad a largo plazo. Por otro lado, AI4VULN se especializa en la identificación y priorización de vulnerabilidades mediante análisis de riesgos que consideran el impacto potencial, la facilidad de explotación y la criticidad del sistema afectado. La integración de inteligencia de amenazas permite mantener actualizados los modelos de detección de vulnerabilidades frente a las tácticas cambiantes de los ciberatacantes.

Ambos sistemas están respaldados por interfaces de usuario intuitivas que centralizan la visualización de vulnerabilidades, acciones tomadas y el estado general de seguridad. Esta accesibilidad facilita la colaboración entre equipos de desarrollo y administradores de sistemas, mejorando la eficiencia en la gestión de la seguridad cibernética. En la simulación realizada esto no se ha puesto a prueba de forma exacta, pero se pone de manifiesto al ver los resultados obtenidos.

Para futuras investigaciones y mejoras, es crucial avanzar en la precisión de la detección de vulnerabilidades mediante el desarrollo de técnicas más sofisticadas como el aprendizaje profundo y el análisis estático y dinámico mejorado. Además, se debe evaluar la adaptabilidad y escalabilidad de los sistemas para manejar entornos tecnológicos diversos y grandes volúmenes de datos. Integrar contextos operativos específicos y conocimiento del dominio también mejorará la relevancia y efectividad de las recomendaciones de corrección.

Automatizar completamente las respuestas y mitigaciones frente a amenazas emergentes ayudará a reducir el tiempo de respuesta ante incidentes y a fortalecer la resiliencia del sistema. Finalmente, considerar los aspectos éticos y de seguridad en el uso de algoritmos de inteligencia artificial asegurará la transparencia, equidad y protección de datos sensibles en la gestión de la ciberseguridad.

En resumen, mientras que Trustworthy AI for Cybersecurity Reinforcement and System Resilience representa un avance significativo, hay múltiples oportunidades para mejorar la robustez, eficiencia y adaptabilidad de estos sistemas en un entorno digital cada vez más complejo y dinámico.

REFERENCIAS

[1] << European Commission >>. Página Web: https://cordis.europa.eu/project/id/101070450

[2] Antonio Fonfría << La industria de defensa en el mundo: hechos estilizados y tendencias >>. Página Web: https://seguridadinternacional.es/resi/html/la-industria-de-defensa-en-el-mundo-hechos-estilizados-y-tendencias/

[3] << La Industria de defensa global en el siglo XXI (1) >>. Página Web: https://www.infodefensa.com/texto-diario/mostrar/4725963/industria-defensa-global-siglo-xxi

[4] Eduardo Olier y Juan Manuel Corchado << Inteligencia artificial: aplicaciones a la Defensa >> Página Web: https://www.ieee.es/Galerias/fichero/docs_investig/2022/DIEEEINV01_2022_EDUOLI_Inteligencia.pdf

[5] << Indra >>. Página Web: https://www.indracompany.com/es/indra/faradai-inteligencia-artificial-frugal-robusta-inteligencia-avanzada-defensa

[6] << Indra presenta al Ejército de Tierra el sistema de mando y control para dominar el combate electrónico del futuro >>. Página Web: https://www.indracompany.com/es/noticia/indra-presenta-ejercito-tierra-mando-control-dominar-combate-electronico-futuro

[7] << Reconocimiento y localización de enemigos >>. Página Web: https://www.elconfidencial.com/tecnologia/novaceno/2022-02-11/soldados-eeuu-usaran-drones-bolsillo-combate_3373834/

[8] << Israel emplea la IA en la masacre en Gaza y el combate con Hamás >>. Página Web: https://www.eldiario.es/internacional/theguardian/israel-emplea-ia-masacre-gaza-combate-hamas-hemos-matado-gente-dano-colateral-tres-digitos_1_11262638.html

[9] Javier Candau << Ciberseguridad. Evolución y tendencias >> *artículo*. Página Web: https://dialnet.unirioja.es/descarga/articulo/8175398.pdf

[10] Arturo Ribagorda Garnacho << Panorama Actual de la ciberseguridad >> artículo. Página Web: https://www.mintur.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEconomiaIndustrial/410/ARTURO%20RIBAGORDA%20GARNACHO.pdf

[11] << Ciberseguridad en el IoT: escenario actual, buenas prácticas y riesgos >>. Página Web: https://www.ikusi.com/mx/blog/ciberseguridad-en-el-iot-2/

[12] << Qué es la Inteligencia Artificial >>. Página Web: https://planderecuperacion.gob.es/noticias/que-es-inteligencia-artificial-ia-prtr

[13] Joaquín Fournier Guimbao << Inteligencia Artificial: una carrera hacia un futuro tecnológico >> artículo. Página Web: https://www.ieee.es/Galerias/fichero/docs_opinion/2021/DIEEEO89_2021_JOAFOU_Inteligencia.pdf

[14] << Descubriendo las ramas de la Inteligencia Artificial >>. Página Web: https://www.smartmind.net/blog/ramas-ia/

[15] Denniye Hinestroza Ramírez y Juan Manuel Cárdenas << EL MACHINE LEARNING >> artículo. Página Web: https://repository.unilibre.edu.co/bitstream/handle/10901/17289/EL%20MACHINE%20LEARNING.pdf?sequence=1&isAllowed=y

[16] << Deep Learning y Redes Neuronales Artificiales >>. Página Web: https://nodd3r.com/blog/deep-learning-y-redes-neuronales-artificiales

[17] Jorge Franganillo << La inteligencia artificial generativa y su impacto en la creación de contenidos mediáticos >> artículo. Página Web: https://dialnet.unirioja.es/descarga/articulo/9132067.pdf

[18] << Las increíbles aplicaciones de inteligencia artificial en el ámbito militar >>. Página Web: https://www.toolify.ai/es/ai-news-es/las-increbles-aplicaciones-de-inteligencia-artificial-en-el-mbito-militar-2641668

[19] Ángel Gómez de Ágreda, Inmaculado Mohino Herranz, Rocio Barragán Montes, Francisco Antonio Marín Gutiérrez y Enrique Cubeiro Cabello << Usos militares de la inteligencia artificial, la automatización y la robótica (IAA&R) >> artículo. Página Web: https://publicaciones.defensa.gob.es/media/downloadable/files/links/u/s/usos_militares_inteligencia_artificial.pdf

[20] Jose María Navarro << La inteligencia artificial vence a los pilotos de combate de la USAF >>. Página Web: https://www.defensa.com/industria/inteligencia-artificial-vence-pilotos-combate-usaf

[21] René Leiva Villagra << Evolución Tecnológica y Ciberseguridad >> artículo. Página Web: https://www.revistaensayosmilitares.cl/index.php/tica/article/download/157/173

[22] << La perspectiva de una ciberguerra híbrida toma fuerza entre los riesgos cibernéticos >>. Página Web: https://future.inese.es/la-perspectiva-de-una-ciberguerra-hibrida-toma-fuerza-entre-los-riesgos-ciberneticos/

[23] << Ciberespionaje industrial: qué es y qué medidas para evitarlo >>. Página Web: https://www.redseguridad.com/actualidad/cibercrimen/ciberespionaje-industrial-que-es-y-medidas-para-evitarlo_20220127.html

[24] Ulises León Kandiko << INTELIGENCIA ARTIFICIAL, ÉTICA Y DEFENSA, REQUIEREN COMO EJE A LA CIBERSEGURIDAD >> artículo. Página Web: https://www.linkedin.com/pulse/inteligencia-artificial-%C3%A9tica-y-defensa-requieren-como-kandiko/

[25] << European Commission >>. Página Web: https://cordis.europa.eu/project/id/101070450

[26] << AL4CYBER >>. Página Web: https://ai4cyber.eu/

[27] Juan Ranchal << El Proyecto Maven (cuando la IA mata) ya está activo en combate real >>. Página Web: https://www.muycomputer.com/2024/02/29/el-proyecto-maven-cuando-la-ia-mata-ya-esta-activo-en-combate-real/

[28] << European Commission >>. Página Web: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/44181033/101121250/EDF

[29] << El Ejército de EE.UU. trabaja en una Inteligencia Artificial para decidir quién recibe ayuda médica en combate >>. Página Web: https://www.abc.es/tecnologia/redes/abci-ejercito-eeuu-trabaja-para-decidir-quien-recibe-ayuda-medica-combate-202204010139_noticia.html

[30] << In the Moment >>. Página Web: https://www.darpa.mil/program/in-the-moment

[31] << IA y Defensa: Explorando las Fronteras de la Tecnología Militar >>. Página Web: https://www.defensa.com/industria/inteligencia-artificial-defensa-explorando-fronteras-tecnologia

[32] Benjamín Carrasco << El Ejército incorpora un robot autónomo que facilita el trabajo en almacenes >>. Página Web: https://www.infodefensa.com/texto-diario/mostrar/3124595/ejercito-incorpora-robot-autonomo-facilita-trabajo-almacenes

[33] Diego Caceres Solis << Uso de la IA y Machine Learning en ciberseguridad >>. Página Web: https://openwebinars.net/blog/uso-de-inteligencia-artificial-y-machine-learning-en-ciberseguridad/

[34] Alisson B. Torres, Fredy G. Rendón y Juan F. Gutiérrez << Revisión de las técnicas de inteligencia artificial aplicadas en seguridad informática >> artículo. Página Web: https://www.ismsforum.es/ficheros/descargas/isms-gt-ia-021707141605.pdf

[35] Bernard Marr << What is an Artificial Neural Network? >> artículo. Página Web: https://bernardmarr.com/what-is-an-artificial-neural-networks/

[36] << European Commission >>. Página Web: https://cordis.europa.eu/project/id/815564/reporting

[37] Joaquín Sánchez << Ciberseguridad militar: Desafíos de la inteligencia artificial frente a los ciberataques >> artículo. Página Web: https://www.lisanews.org/ciberseguridad/ciberseguridad-militar-desafios-ia-frente-a-ciberataques/

[38] Ana Rosa Cavalli y Marck Pawlicki << AI-driven self-testing and automatic error correction for robustness - Initial version >> artículo. Página Web: https://ai4cyber.eu/wp-content/uploads/2024/02/AI4CYBER-D3.1-AI-driven-self-testing-and-automatic-error-correction-for-robustness-%E2%80%93-Initial-version_v1.0_202401311.pdf

[39] Jason Mansell y Panagiotis Radoglou << Data Management Plan - Initial version >> artículo. Página Web: https://ai4cyber.eu/wp-content/uploads/2024/02/D1.2_Data-Management-Plan-Initial-version_v1.0_20230301.pdf

[40] Jordi Bercial << VirtualBox: ¿Qué es y para qué sirve? >>. Página Web: https://www.geeknetic.es/VirtualBox/que-es-y-para-que-sirve

[41] << Ubuntu Server >>. Página Web: http://www.ubuntufacil.com/2013/04/ubuntu-server/

[42] << Greenbone OpenVAS >>. Página Web: https://www.openvas.org/

[43] << Scikit-Learn: Machine Learning in Python >>. Página Web: https://scikit-learn.org/stable/

[44] << Grafana >>. Página Web: https://grafana.com/

[45] << Wireshark >>. Página Web: https://www.ucm.es/pimcd2014-free-software/wireshark#:~:text=Wireshark%20es%20un%20analizador%20de,aprender%20m%C3%A1s%20sobre%20redes%20inform%C3%A1ticas.

[46] << Modo: Red Interna >>. Página Web: https://www.fpgenred.es/VirtualBox/modo_red_interna.html

[47] << Etiqueta: Configurar netplan >>. Página Web: https://jugandoaseringeniero.wordpress.com/tag/configurar-netplan/

[48] << Unix y Linux >>. Blog: https://unix.stackexchange.com/questions/681220/netplan-generate-gateway4-has-been-deprecated-use-default-routes-instead

[49] Shivam Mishra << Install OpenVAS GVM 22.4.0 on Ubuntu 22.04 >>. Página Web: https://medium.com/@shivammishraa/install-openvas-gvm-22-4-0-on-ubuntu-22-04-f377060c2793

[50] << Instalación de Scikit-Learn >>. Página Web: https://qu4nt.github.io/sklearn-doc-es/install.html

[51] << ¿Cómo saber si un módulo está instalado? >>. Página Web: https://es.stackoverflow.com/questions/69860/c%C3%B3mo-saber-si-un-m%C3%B3dulo-esta-instalado

[52] Daniel Benites << Cómo Instalar Wireshark en Ubuntu Server via CLI >>. Página Web: https://danielbenites.com/como-instalar-wireshark-en-ubuntu-server-via-cli/

[53] << Install Grafana on Debian or Ubuntu >>. Página Web: https://grafana.com/docs/grafana/latest/setup-grafana/installation/debian/