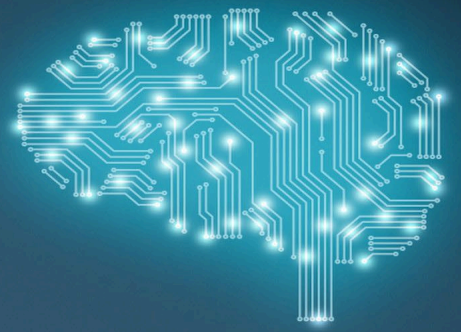
Inteligencia Artificial: Un estudio de su impacto en Ciberseguridad



María Lourdes Martín Martín

Ingeniería Informática

Dr. Friman Sánchez Castaño

Dr. David Isern Alarcón

Estructura

- Objetivos de investigación
- Introducción
- Desarrollo
- Conclusiones y futuras líneas de investigación

Objetivos de la Investigación

Identificar las principales características, usos y aplicaciones de la Inteligencia Artificial en el campo de la Ciberseguridad.

Objetivos específicos

- Analizar las amenazas y vulnerabilidades en el panorama actual de la Ciberseguridad.
- Reconocer los fundamentos de la IA.
- Descubrir y estudiar cuáles son las aplicaciones de la IA empleadas en Ciberseguridad.
- Analizar cómo los algoritmos de la IA que se utilizan para prevenir y detectar ataques cibernéticos también sirven para responder ante esas amenazas.
- Estudiar como la IA analiza las vulnerabilidades, las identifica y clasifica para proponer soluciones y verificar su reparación.

Introducción

Sanidad

Banca

Inteligencia Artificial

Movilidad

Comercio

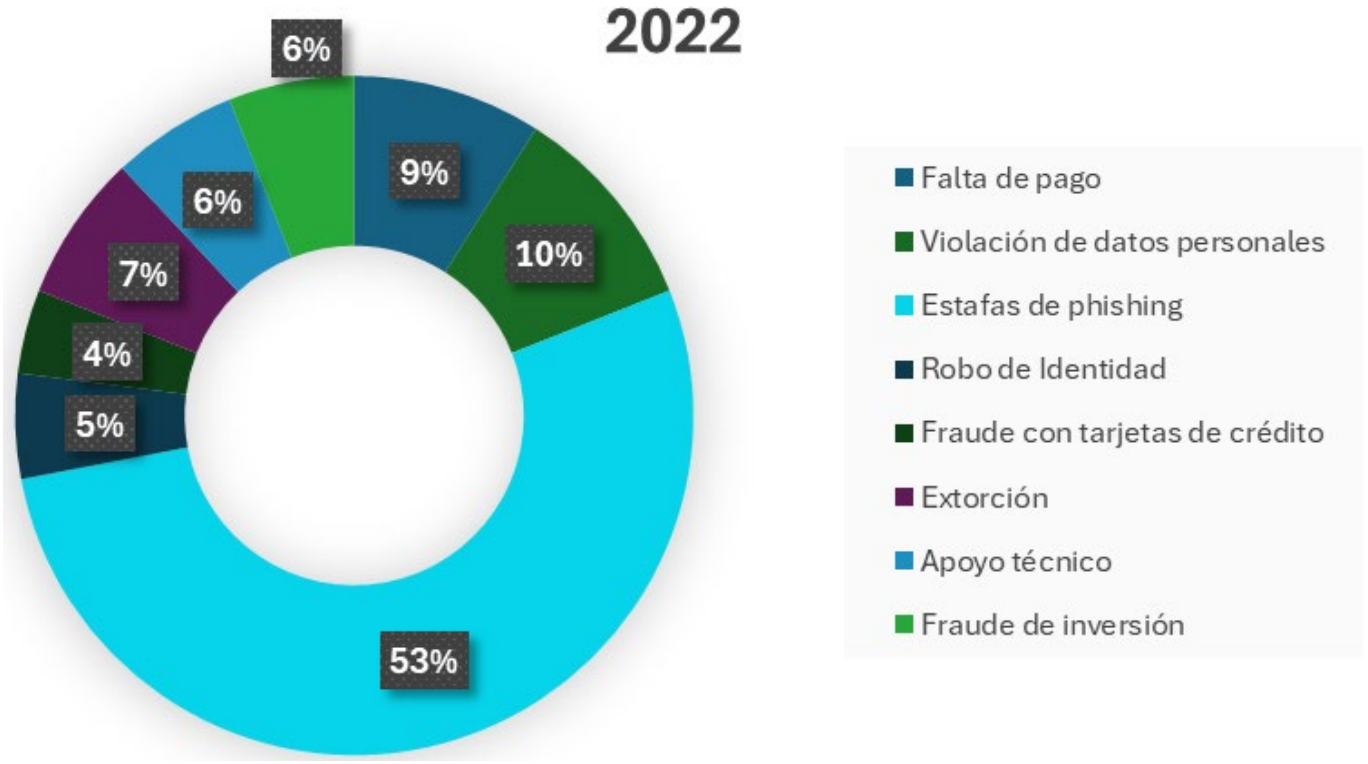
Energía

Desarrollo

Cibercriminalidad y Ciberseguridad

El auge de la ciberdelincuencia está estrechamente ligada al desarrollo tecnológico informático.

Los ataques cibernéticos son actividades maliciosas dirigidas a dispositivos informáticos, sistemas y redes utilizando Internet.

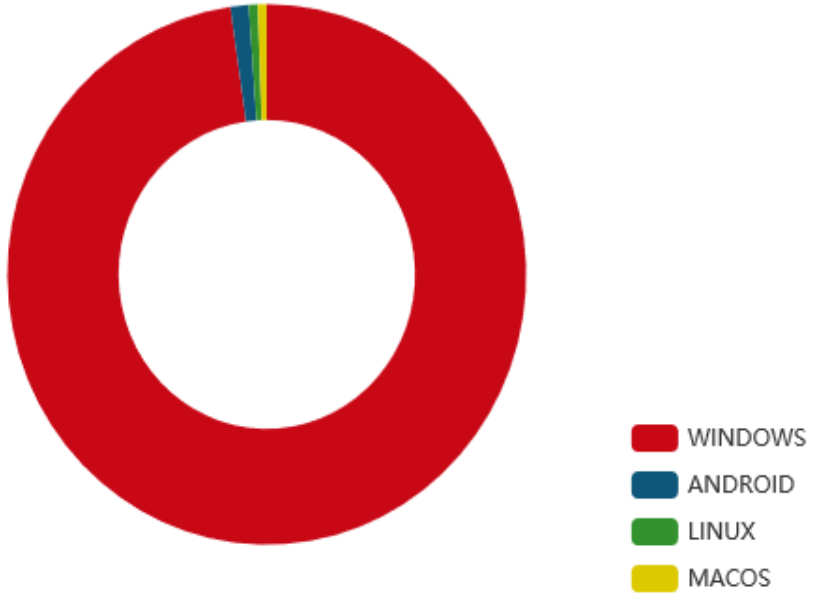


Ciberseguridad

Confidencialidad

Integridad

Disponibilidad



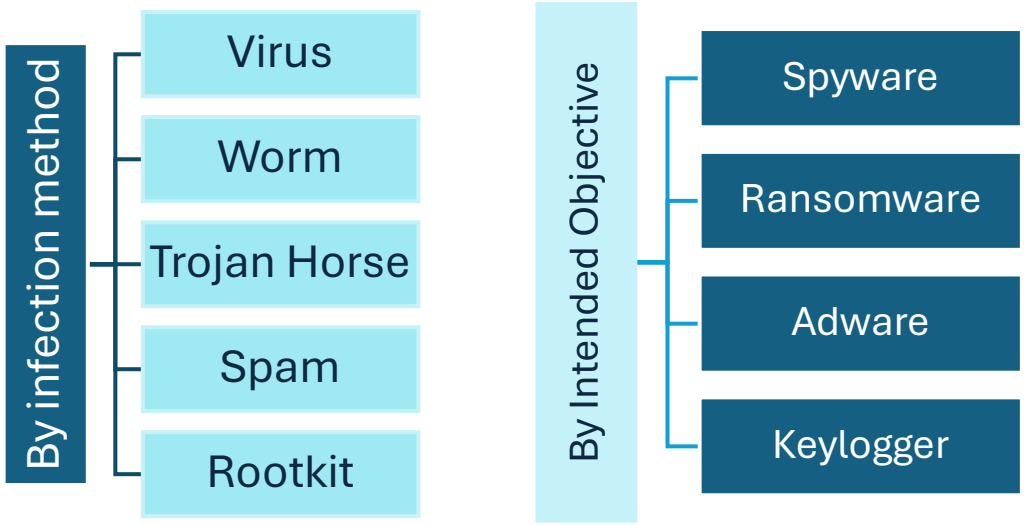
Nuevos Malware en el año	45.473.701
Nuevos Malware en los últimos 14 días	3.611.406
Total, Malware	1.386.823.807

Los ciberataques y los riesgos de seguridad

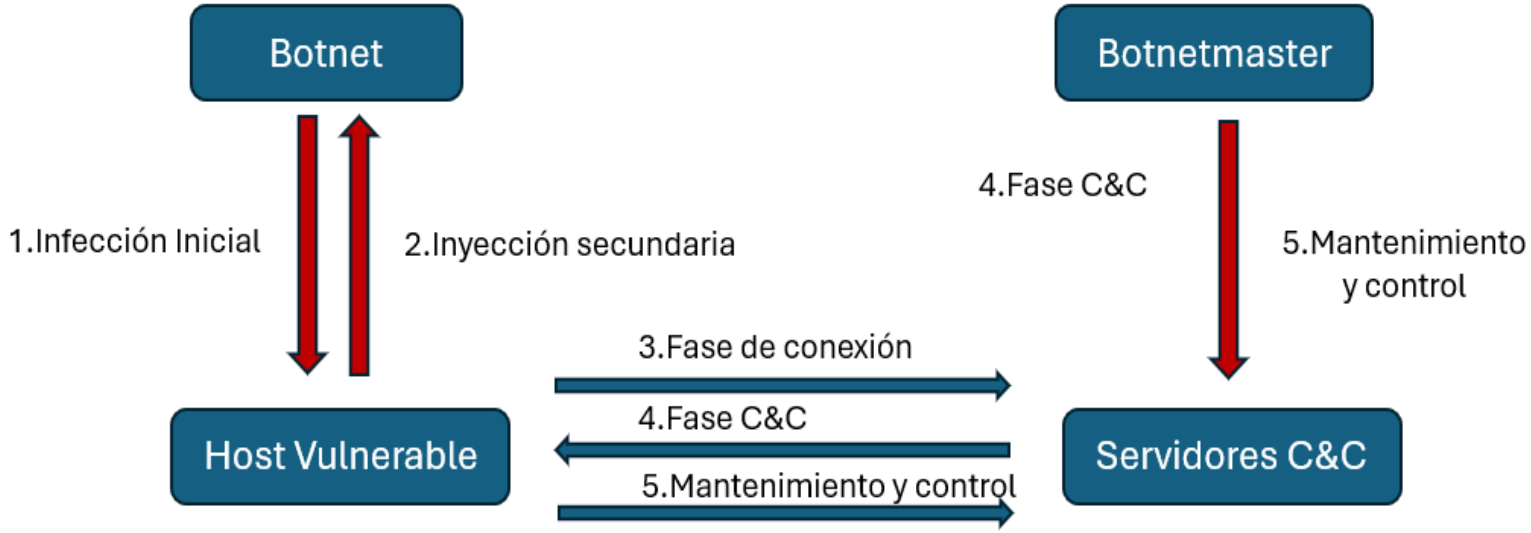
Cyber Attacks

- Ramsomware
- Man in the middle attack
- Zero day exploit
- DNS Tunneling
- XSS Attack
- Social engineering
- DoS ans DDoS attack
- SLQ injection
- Phishing
- Malware

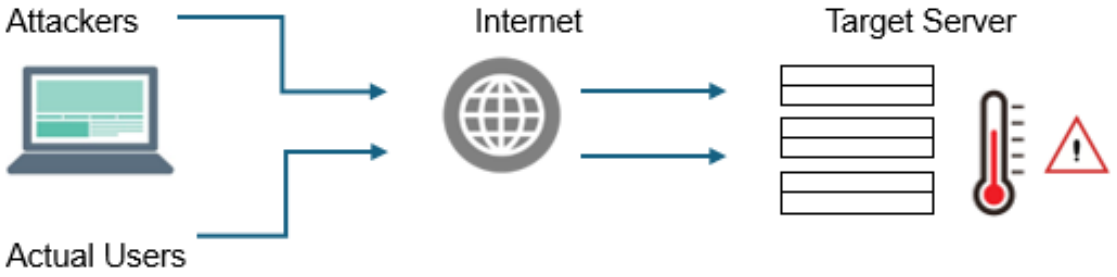
Clasificación de malware por método de infección y de intención del objeto

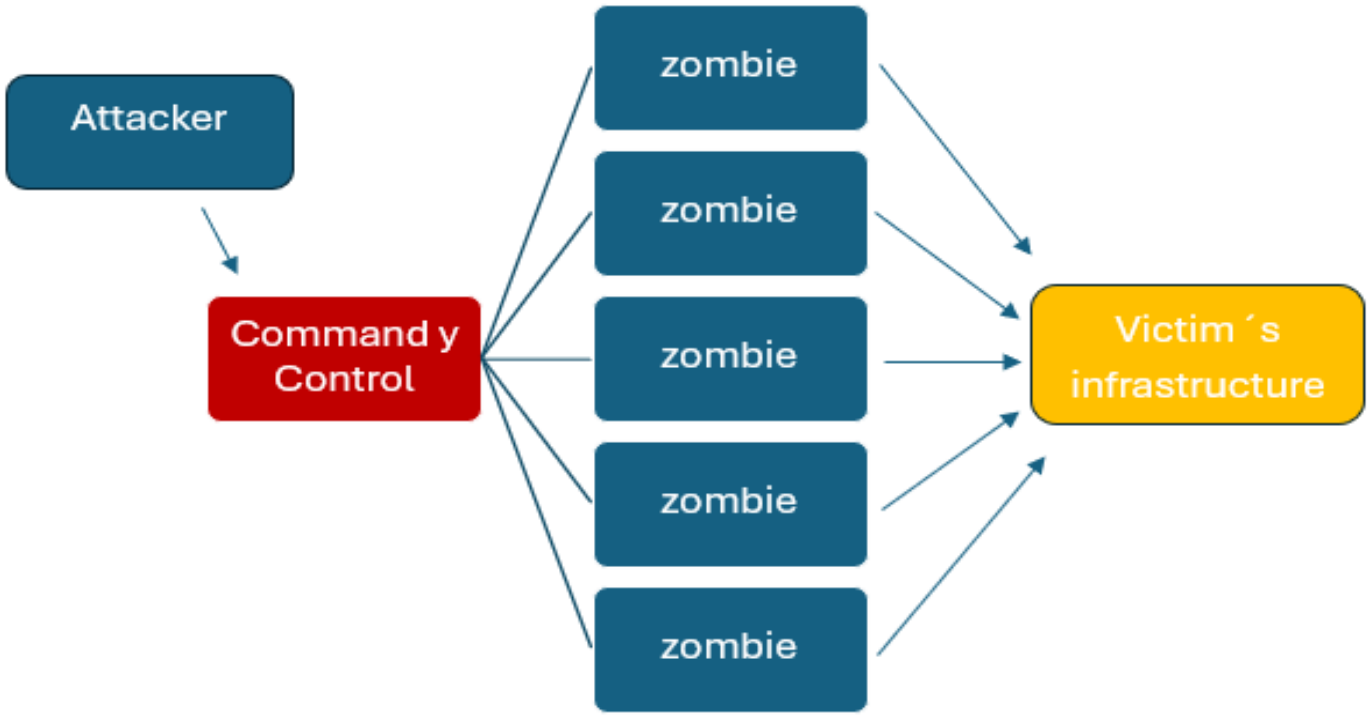


Ciclo de vida de una Botnet



Ataque distribuido de denegación de servicio (DDoS).





Retos en la Ciberseguridad

El panorama de las amenazas está creciendo y evolucionando continuamente:

- Nuevo desarrollo tecnológico: tecnologías como la computación cuántica, las redes 5G y la computación en el borde traen nuevos desafíos de ciberseguridad.
- Proteger de forma correcta la seguridad y la privacidad de la información es un constante reto.
- Malware sin archivos, ransomware, ataques DDoS.

IA en Ciberseguridad

Fundamentos de la Inteligencia Artificial

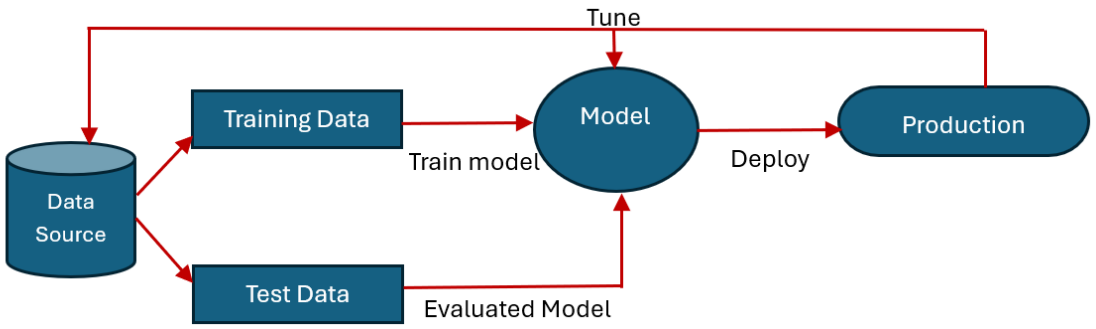
Inteligencia Artificial
La teoría y el desarrollo de sistemas de información capaces de realizar tareas que normalmente requieren de inteligencia humana.

Machine Learning
Proporciona a los sistemas la capacidad para aprender sin programación explícita previa.

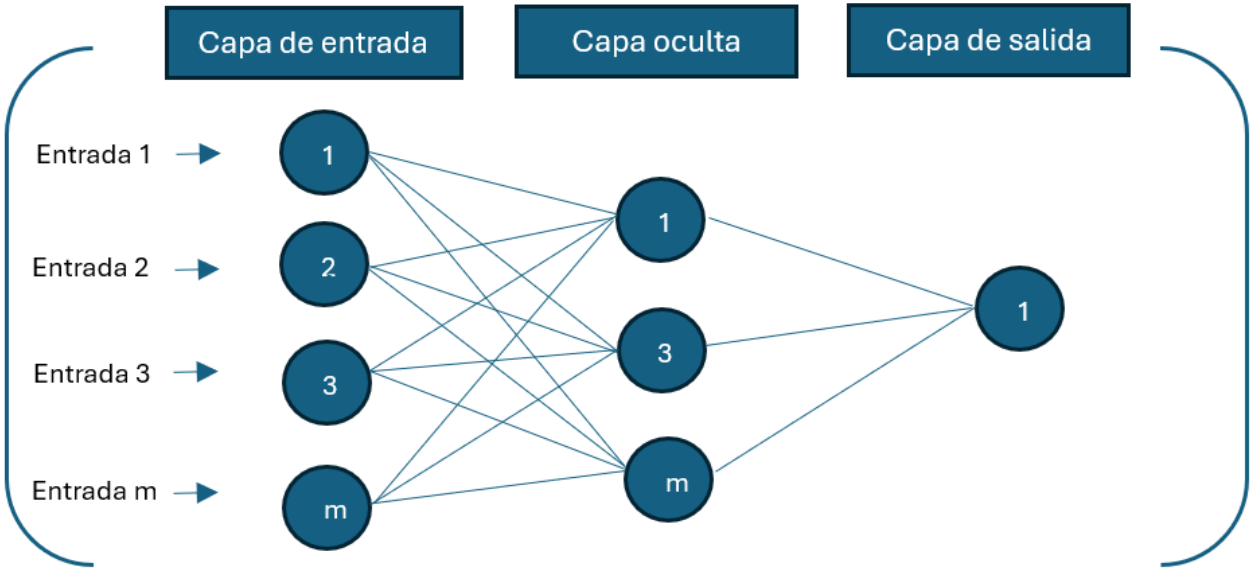
Deep Learning
Algoritmos desarrollados simulando el comportamiento del cerebro humano en lo que se denominan redes neuronales artificiales.

Aprendizaje automático (Machine Learning, ML)

- Aprendizaje supervisado
- Aprendizaje no supervisado
- Aprendizaje semi-supervisado
- Aprendizaje por refuerzo



Aprendizaje Profundo



Algoritmos de Clasificación

- Regresión logística
- Máquinas de vectores de soporte (SVM)
- Árboles de decisión y bosques aleatorios
- Redes neuronales
- K-Vecinos más cercanos (K-NN)

IA generativa

Redes Generativas Adversarias (GANs):

- Regenerador: crea datos sintéticos parecidos a los datos reales.
- Discriminador: intenta distinguir los datos reales de los sintéticos.

Técnicas de ciberseguridad impulsadas por IA

- Aprendizaje automático (ML) y el aprendizaje profundo (DL).
- Detección de anomalías
- Procesamiento natural del lenguaje (PNL)
- Análisis predictivo
- Automatización y Orquestación

Detección de amenazas y análisis de comportamiento

Sistemas de detección y prevención de intrusiones (IDPS): Darktrace con Enterprise Immune System.

El Sistema de detección y prevención de intrusiones (IDPS).

Sistemas de respuesta automatizada: Darktrace Antigena

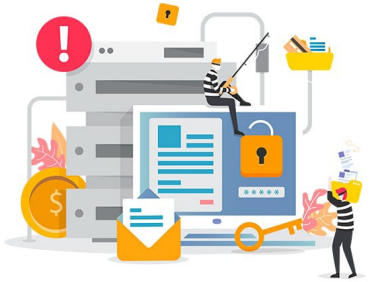
Ciencia forense digital y respuesta a incidentes (Digital forensics and incident response (DFIR)).

Respuesta automática y orquestación

La orquestación → La automatización → La respuesta

Predicción de amenazas

- La predicción de código dañino
- La predicción de ataques de phishing
- La predicción de ataques DDoS
- Darktrace Antigena
- Palo Alto Networks



- Vulnerabilidades y pentesting automatizado
  - Análisis de vulnerabilidades
  - Pruebas de penetración (pentesting)
- IA Generativa y Ciberseguridad
  - Redes generativas adversarias (GANs)
  - Psicología inversa

Caso de estudio

Girton Grammar School

Snorkel Flow

Limitaciones, desafíos y el futuro de la IA aplicada a Ciberseguridad

Calidad y disponibilidad de datos

Dependencia excesiva de la IA, e interpretabilidad

Ataques adversarios

Desafíos

Futuro

Priorización de amenazas de alta precisión.

Ciberresiliencia

Arquitectura de confianza cero

Conclusiones

- Relación que hay entre la IA y la Ciberseguridad.
- Sensibilidad mayor sobre la protección de la privacidad de los usuarios.
- Equilibrio entre la IA y la automatización con la experiencia humana.
- Preparación para el futuro.

Áreas para futura investigación

Argumentos que podrían abrir nuevas investigaciones o seguir ampliando las actuales.

Desarrollar una investigación de como introducir y fomentar la educación en IA y Ciberseguridad en todos los niveles.