

MÁSTER PRESENCIAL EN CIBERSEGURIDAD – \_ªEd.

DESARROLLO DE UNA HERRAMIENTA ENFOCADA A DETECTAR REDES DE BOTS EN REDES SOCIALES

TFM elaborado por: David Fernández Peña

Tutor/a de TFM: Andrés Iglesias

- Madrid y fecha -

# ÍNDICE:

[ÍNDICE: 1](#_Toc1106106469)

[1. INTRODUCCIÓN. 2](#_Toc1176581712)

[2. OBJETIVOS. 3](#_Toc735751931)

[3. CONCLUSIONES. 3](#_Toc2029169389)

[4. BIBLIOGRAFÍA. 3](#_Toc1602013687)

[5. ANEXOS. 3](#_Toc1486052787)

# INTRODUCCIÓN.

El auge de las redes sociales ha transformado radicalmente la forma en que las personas se comunican e interactúan en línea. Plataformas como Twitter (ahora X), Instagram o Facebook han permitido el intercambio instantáneo de ideas, opiniones y noticias en tiempo real, creando un entorno dinámico de información.   
Sin embargo, este ecosistema también ha sido explotado por actores malintencionados que buscan manipular y distorsionar el flujo de información a través de la creación y uso de redes de bots. Los **bots sociales** son cuentas automatizadas que pueden imitar el comportamiento humano en las redes sociales, publicando contenido, interactuando con otros usuarios y, en muchos casos, promoviendo agendas específicas o difundiendo desinformación.

Investigaciones previas han demostrado que los bots pueden influir en el discurso político, aumentar artificialmente la popularidad de ciertos temas y distorsionar la percepción pública. Además, estudios han revelado que, durante eventos críticos como elecciones o crisis internacionales, los bots han jugado un papel significativo en la creación y propagación de narrativas falsas.

A pesar de los avances en la detección de bots, sigue siendo un desafío identificar con precisión estos actores maliciosos debido a su capacidad de evolucionar y adaptarse a nuevas estrategias para evadir los sistemas de detección. Por ejemplo, los bots han mejorado sus mecanismos para parecer más humanos, haciendo que su detección sea más compleja y, en muchos casos, indistinguible del comportamiento legítimo.

Twitter, debido a su estructura de red abierta y su influencia en la opinión pública, ha sido un terreno fértil para la proliferación de bots sociales. Estos bots no solo afectan la calidad de las interacciones en línea, sino que también pueden ser utilizados para manipular procesos democráticos, fomentar la visibilidad de ciertas cuentas o productos, difundir noticias falsas y amplificar la desinformación.  
  
Es por eso por lo que Twitter será la red social elegida para el desarrollo de la herramienta de detección que abarca este documento.

# OBJETIVO.

Este trabajo tiene como objetivo desarrollar una herramienta eficaz para la detección de redes de bots en Twitter. La importancia de esta herramienta radica en su capacidad para identificar patrones de comportamiento automatizados que se esconden tras la fachada de cuentas aparentemente legítimas. Utilizando una combinación de técnicas de Machine Learning, esta herramienta busca mejorar la precisión de la detección de bots.

Twitter es una plataforma ideal para el análisis de redes de bots debido a su gran volumen de datos, su accesibilidad a través de su API y una gran cantidad de datasets nacidos de trabajos similares en la plataforma.  
Sin embargo, también presenta retos significativos debido a la variabilidad de los datos disponibles y la evolución constante de los patrones de comportamiento de los bots.

La detección eficaz de bots en las redes sociales no solo tiene implicaciones para la integridad de las plataformas, sino que también es crucial para la seguridad de la información y la estabilidad de los sistemas democráticos. La capacidad de los bots para influir en el debate público, manipular los mercados y distorsionar las narrativas políticas subraya la urgencia de desarrollar soluciones robustas para su identificación. Con el auge de la desinformación y las noticias falsas en línea, una herramienta de detección de bots que sea precisa y eficiente podría ser un recurso valioso para gobiernos, empresas y usuarios de redes sociales que buscan protegerse de estas amenazas.

En resumen, este trabajo propone el desarrollo de una herramienta que, basada en algoritmos de Machine Learning permita la identificación de redes de bots en Twitter, contribuyendo así a la mejora de la seguridad y la transparencia en las interacciones en línea.

# CONCLUSIONES.

# BIBLIOGRAFÍA.

# ANEXOS.