

# Primera Aproximación al Trabajo de Fin de Máster

Tu Nombre

14 de abril de 2025

## Título tentativo

**Análisis estático y dinámico de código fuente descargado de internet: detección de software malicioso en repositorios abiertos**

## Descripción general

Este trabajo de fin de máster tiene como objetivo estudiar técnicas de análisis de malware aplicadas a código fuente obtenido de internet. Se plantea evaluar la presencia de comportamientos maliciosos en repositorios abiertos mediante herramientas y metodologías tanto estáticas como dinámicas, buscando identificar patrones comunes en posibles amenazas encubiertas en proyectos aparentemente legítimos.

## Estructura preliminar y puntos clave

### 1. Introducción

- Contexto del malware en repositorios públicos.
- Motivación del estudio.
- Objetivos generales y específicos.

### 2. Estado del arte

- Análisis de malware: enfoques estáticos y dinámicos.

- Casos documentados de malware en GitHub y otros repositorios.
- Herramientas existentes para escaneo de código malicioso.

### **3. Metodología**

- Criterios para selección de proyectos/repositories.
- Entorno controlado para análisis dinámico (sandboxing).
- Técnicas de análisis estático (linting, detección de obfuscación, etc.).
- Pipeline de análisis automatizado.

### **4. Resultados esperados**

- Identificación de patrones o firmas maliciosas comunes.
- Clasificación de riesgos según tipo de proyecto o lenguaje.
- Limitaciones del enfoque propuesto.

### **5. Conclusiones provisionales**

- Potencial impacto del estudio en la comunidad open-source.
- Viabilidad de integrar este análisis en flujos DevSecOps.
- Proyecciones para trabajos futuros o ampliaciones del estudio.