ISDEFE-CETEDEX
Open Innovation Lab
RETOS

1. RETO 1. INTELIGENCIA ARTIFICIAL EN PLANIFICACIÓN LOGÍSTICA

1.1. DESCRIPCIÓN

Aplicar algoritmos de inteligencia artificial para optimizar la planificación de rutas y asignación de recursos en operaciones logísticas, tanto en entornos militares como civiles. Se espera que las soluciones sean capaces de considerar múltiples variables (distancia, prioridad, recursos disponibles, condiciones cambiantes) para generar planes de acción eficientes y adaptables. El desarrollo debe estar orientado a una implementación sencilla, con posibilidad de escalarse posteriormente a sistemas más complejos o integrarse en infraestructuras existentes.

1.2. OBJETIVO

Desarrollar un prototipo funcional que integre IA para la toma de decisiones en planificación logística con datos simulados o históricos, que pueda ser adaptado posteriormente a necesidades específicas de Defensa.

1.3. CRITERIOS DE SELECCIÓN DE PROPUESTAS

- Simplicidad y claridad de la solución propuesta (30%)
- Capacidad de adaptación a condiciones cambiantes (25%)
- Experiencia previa en IA aplicada a logística o movilidad (25%)
- Potencial de transferencia dual (civil-militar) (20%)

2. RETO 2. AUTOMATIZACIÓN DE CIBERATAQUES DEFENSIVOS

2.1. DESCRIPCIÓN

Crear herramientas que simulen ataques cibernéticos de forma automatizada para evaluar la capacidad de defensa de sistemas relacionados con drones, comunicaciones o dispositivos conectados. Estas simulaciones deben realizarse de manera controlada y ética, evitando impactos no deseados. El objetivo es disponer de un entorno seguro donde testar defensas digitales mediante IA y automatización, con especial atención al seguimiento y reversibilidad de los efectos provocados.

2.2. OBJETIVO

Diseñar un sistema que permita ejecutar pruebas controladas de penetración (pentest automatizado), sin comprometer la estabilidad del entorno y dentro de parámetros éticos y seguros.

2.3. CRITERIOS DE SELECCIÓN DE PROPUESTAS

- Experiencia en red teaming o pentesting (25%)
- Control preciso del alcance y efectos del ataque simulado (30%)
- Inclusión de mecanismos de reversión y trazabilidad (25%)
- Capacidad para incluir IA en la generación de escenarios de prueba (20%)