# Herramienta de Diagnóstico Unificado para el Análisis de Seguridad y Geolocalización Aproximada de Direcciones IP en el Contexto Colombiano

Juan Manuel Serrano Rodríguez
Código: 20211020091
Facultad de Ingeniería
Universidad Distrital Francisco José de Caldas
Bogotá, Colombia
jmserranor@correo.udistrital.edu.co

## I. FORMULACIÓN DEL PROBLEMA

Tanto usuarios técnicos como ciudadanos comunes se enfrentan a una creciente necesidad de evaluar la legitimidad y seguridad de las direcciones IP con las que interactúan. Ya sea al analizar los registros de un firewall, verificar la procedencia de un correo electrónico o investigar un servicio en línea, la información requerida para un diagnóstico completo se encuentra dispersa en múltiples plataformas: una para consultar puertos abiertos, otra para la geolocalización, una tercera para la reputación y una cuarta para identificar al propietario de la red.

Esta fragmentación de datos representa una barrera significativa para la toma de decisiones informadas en materia de ciberseguridad. La falta de una herramienta unificada, accesible y de código abierto obliga a realizar un proceso manual, lento e ineficiente, que a menudo queda fuera del alcance de usuarios no especializados.

Este proyecto propone solucionar este problema mediante el desarrollo de una herramienta web de diagnóstico centralizada. Dicha herramienta permitirá a un usuario ingresar una dirección IP o dominio y recibir un informe consolidado que integre datos de seguridad pasiva, geolocalización aproximada, reputación y contexto de red. El objetivo es crear una base sólida para una plataforma de reconocimiento pasivo que democratice el acceso a la inteligencia de amenazas, utilizando exclusivamente herramientas y fuentes de datos gratuitas.

## II. OBJETIVOS ESPECÍFICOS

### *A. Objetivo 1: Integración de Fuentes de Datos de Reconocimiento Pasivo Gratuitas*

Desarrollar un sistema backend capaz de consultar y unificar información de diversas fuentes de datos 100% gratuitas, garantizando la viabilidad del proyecto sin incurrir en costos. Las fuentes a integrar son:

- **Análisis de Puertos y Servicios:** Ejecutar consultas SQL sobre los conjuntos de datos públicos de Censys en Google BigQuery para obtener un perfil histórico de los servicios y puertos expuestos por la IP objetivo, operando dentro del nivel gratuito de la plataforma.
- **Geolocalización Aproximada Local:** Descargar e implementar la base de datos GeoLite2 City de MaxMind. Las consultas de geolocalización se realizarán localmente contra este archivo, lo que garantiza un rendimiento extremadamente rápido y elimina por completo los límites de uso.
- **Contexto de Red y Propiedad:** Realizar consultas WHOIS a los servidores públicos de los Registros Regionales de Internet (como LACNIC para la región) para identificar el Número de Sistema Autónomo (ASN), el ISP propietario del bloque de IP y los datos de contacto de abuso.
- **Reputación y Amenazas:** Integrar la API gratuita de AbuseIPDB para verificar si la dirección IP ha sido reportada por actividades maliciosas y obtener un puntaje de confianza, gestionando el uso dentro de los límites establecidos por su plan gratuito.

### *B. Objetivo 2: Desarrollo de un Modelo de Puntuación de Riesgo y Contexto*

Diseñar un modelo algorítmico que procese los datos recolectados para generar una evaluación clara y concisa de la IP analizada. El modelo deberá:

- Asignar un factor de riesgo a los servicios expuestos, priorizando aquellos de mayor criticidad (ej. RDP, SMB, bases de datos abiertas).
- Incorporar el puntaje de reputación de AbuseIPDB como un factor clave en la evaluación de riesgo general.
- Presentar la información de geolocalización y propiedad de forma clara, enfatizando siempre la naturaleza aproximada de la ubicación.
- Calcular una puntuación de riesgo final (ej. Bajo, Medio, Alto, Malicioso Conocido) para la IP analizada.

### C. Objetivo 3: Implementación de un Dashboard de Diagnóstico Interactivo

Desarrollar una aplicación web de cara al usuario que sirva como la interfaz para la herramienta. El dashboard deberá:

- Proveer una interfaz simple donde el usuario pueda introducir una dirección IP o un dominio para su análisis.
- Presentar el informe consolidado en una vista organizada y fácil de entender, con secciones para seguridad, ubicación, reputación y propiedad.
- Visualizar la ubicación aproximada (ciudad/país) obtenida de la base de datos GeoLite2 en un mapa interactivo.
- Ofrecer recomendaciones de seguridad contextuales y automatizadas basadas en los hallazgos (ej. "Puerto 3389 (RDP) abierto. Este es un riesgo alto de ataque de ransomware").

## III. RESULTADOS ESPERADOS

### A. Resultado Principal: Plataforma Web "IP Intelligence Dashboard"

Una herramienta web funcional y de acceso público que, a partir de una IP, presente un informe completo con los siguientes componentes:

- **Panel de Seguridad:** Un resumen de los puertos y servicios detectados por Censys, con advertencias claras sobre configuraciones de alto riesgo.
- **Mapa de Ubicación Aproximada:** Un mapa visual que muestre el país y la ciudad asociados a la IP, junto con un descargo de responsabilidad claro y visible sobre la naturaleza aproximada y no exacta de la geolocalización por IP, explicando que representa la ubicación del proveedor de servicios.
- **Informe de Red y Reputación:** Información detallada sobre el ISP, el ASN (obtenida del WHOIS) y un resumen de los reportes de actividad maliciosa, incluyendo el puntaje de confianza de AbuseIPDB.
- **Puntuación de Riesgo General:** Una calificación final que resuma el nivel de amenaza o exposición de la IP analizada, facilitando su interpretación rápida.

### B. Resultado Secundario: Manual Técnico de Integración y Metodología

Un documento técnico detallado que servirá como guía para la replicación y expansión del proyecto. Incluirá:

- La arquitectura del sistema, mostrando el flujo de datos desde las fuentes hasta la presentación final en el dashboard.
- Los procedimientos y el código para descargar, configurar y consultar localmente la base de datos GeoLite2.
- Las consultas SQL exactas utilizadas en Google BigQuery.
- La lógica y fundamentación del modelo de puntuación de riesgo, asegurando la transparencia del análisis.
- Una guía para el despliegue de la aplicación web.

## IV. REFERENCIAS

### REFERENCES


[1] Censys. "Public Data in Google BigQuery". [En línea].
[2] LACNIC. "Consulta de WHOIS". [En línea].
[3] MaxMind. "GeoLite2 Free Geolocation Data". [En línea].
[4] AbuseIPDB. "API Documentation". [En línea].