Universidad Distrital Francisco José de Caldas
Facultad de Ingeniería

Herramienta de Diagnóstico Unificado para el Análisis de Seguridad y Geolocalización de Direcciones IP

Proyecto de Investigación

Investigador Principal:
Juan Manuel Serrano Rodríguez
Código: 20211020091
jmserranor@correo.udistrital.edu.co

Área de Investigación:
Ciberseguridad y Análisis de Redes

Grupo de Investigación:
Modelamiento en Ingeniería de Sistemas

Línea de Investigación:
Inteligencia de Amenazas Cibernéticas

9 de septiembre de 2025

1. Introducción

Este proyecto consolida, en un único flujo de consulta y presentación, información pasiva sobre direcciones IP usando exclusivamente fuentes gratuitas y de acceso público: (i) conjuntos de datos de Censys disponibles en Google BigQuery y (ii) la base GeoLite2 de MaxMind. No se usarán APIs con planes limitados ni servicios propietarios de pago.

1.1. Propósito

Aprovechar estas dos fuentes abiertas para producir una vista integrada que incluya, como mínimo: presencia observada en escaneos de Censys (puertos/servicios y certificados asociados) y geolocalización aproximada (país/ciudad si aplica) desde GeoLite2, presentadas de forma clara y reproducible.

1.2. Alcance

El trabajo comprende: (a) consulta y filtrado de datos en BigQuery (tablas públicas de Censys), (b) resolución local con GeoLite2, y (c) una plantilla de reporte que estandariza la lectura de resultados. No se crean nuevas fuentes ni métricas propietarias; se organiza y documenta lo existente.

1.3. Restricciones

- Solo se emplean fuentes gratuitas (BigQuery con datasets públicos de Censys y GeoLite2) - Geolocalización es aproximada y sujeta a las limitaciones de la base - No se ejecutan escaneos activos; se usa reconocimiento pasivo

1.4. Entregables

- Consultas de ejemplo en BigQuery sobre datasets de Censys - Procedimiento para resolución/localización con GeoLite2 - Estructura de reporte para presentar hallazgos de manera consistente

2. Estado del Arte

Existen numerosas herramientas para reputación, reconocimiento y geolocalización de IP. Muchas requieren suscripción o imponen límites estrictos en APIs gra-

tuitas, lo que complica la replicación abierta. Este proyecto se centra en dos pilares gratuitos y ampliamente aceptados.

2.1. Censys en Google BigQuery

Censys publica datasets que capturan observaciones de servicios y certificados en Internet. Su disponibilidad en BigQuery permite consultas SQL reproducibles sobre grandes volúmenes, sin necesidad de claves de API ni dependencias de planes comerciales.

2.2. MaxMind GeoLite2

GeoLite2 ofrece bases gratuitas para geolocalización aproximada de direcciones IP. Es una referencia común en proyectos abiertos y académicos cuando no se requiere la precisión y soporte de las versiones comerciales.

2.3. Razonamiento de exclusión de otras fuentes

Se excluyen herramientas comerciales o con APIs fuertemente limitadas (p. ej., VirusTotal, SecurityTrails, servicios premium de geolocalización) para mantener gratuidad, acceso sostenible y reproducibilidad del flujo propuesto.

2.4. Implicación

Concentrarse en Censys (BigQuery) y GeoLite2 permite un pipeline abierto, verificable y suficiente para construir una vista integrada básica (servicios observados + geolocalización aproximada) sin costos ni dependencias propietarias.

3. Problemática

3.1. Necesidad y contexto

La información relevante para contextualizar una dirección IP existe, pero suele estar fragmentada entre múltiples servicios y modelos de acceso. Parte importante del ecosistema impone límites de uso por API o requiere suscripciones, lo que afecta reproducibilidad y acceso.

3.2. Criterio de selección de fuentes

Para garantizar gratuidad, acceso sostenible y replicabilidad, este proyecto se restringe a:

- **Censys en Google BigQuery**: conjuntos de datos públicos que permiten consultas reproducibles sobre observaciones de puertos/servicios y certificados sin depender de claves de API
- **MaxMind GeoLite2**: base gratuita ampliamente utilizada para geolocalización aproximada de IP

3.3. Limitaciones asumidas

- La geolocalización es aproximada (propia de GeoLite2)
- Las observaciones de Censys reflejan cortes/ventanas de tiempo de los datasets públicos
- Sin escaneo activo ni enriquecimientos propietarios

3.4. Objetivo práctico

Reducir la fricción operativa mediante una presentación integrada y documentada de estas dos fuentes, priorizando claridad, trazabilidad y facilidad de replicación sin costos.