SEON

Guía de herramientas para rastrear IPs en 2022

SEON Technologies Ltd.
seon.io

info@seon.io
+44 20 8089 2900

Tabla de Contenidos

¿Quieres obtener tanta información acerca de una dirección IP como sea posible? Estás en el lugar correcto.

Nuestra guía sobre herramientas para rastrear IPs y búsquedas de IP te mostrará qué es posible con esto y cómo podría beneficiar a tu compañía.

¿Qué es una herramienta de rastreo de IP?

Las herramientas para rastrear IPs te permiten aprender más acerca de un usuario de internet con base en su dirección IP. Es una forma del enriquecimiento de datos: comienzas con un único punto de datos (una dirección de IP) para recolectar información adicional.

Existen docenas de herramientas de rastreo de IP diferentes. Algunas verifican proxies, mientras que otras observan si una dirección aparece en una lista negra. El rastreo de IP también se conoce como rastreo de direcciones IP, búsqueda de IP, verificadores de IP o incluso analíticas de IP.

Con el rastreo de IP de SEON puedes identificar tráfico generado por bots, detectar conexiones entre usuarios o determinar qué tan riesgosa es una transacción. Es ideal en la fase de incorporación, durante el inicio de sesión del usuario o en la fase de compra.

¿Por qué realizar una verificación de IP?

Las herramientas para rastrear IP entregan una gran gama de información. Para algunos, esta información es útil durante una investigación OSINT. Para otros, sirve para reducir la posibilidad de lidiar con defraudadores u otros malhechores.

Sin embargo, la mayoría de los rastreos de IP tienden a realizarse por equipos técnicos en el contexto de la administración de sistemas o la investigación de seguridad.

¿Qué datos puedes recolectar de un rastreo de IP?

Sin entrar en detalles técnicos, aquí tienes el tipo de información que puedes obtener después de enriquecer los datos de un rastreo de IP:

Validez de la dirección IP

Una simple prueba del ping de una IP te revelará si la dirección está recibiendo o no datos. En términos simples, se trata de revisar si la dirección IP es válida.

El tiempo de respuesta de la prueba de ping debería ser rápido (menos de 10 ms). Todo lo que supere los 100 ms podría mostrar que hay problemas con esa conexión, lo que incluye el hecho de que esté atravesando proxies y nodos (ver más abajo).

Verificación de listas negras

Cientos de servidores de correo electrónico en el mundo colaboran para mantener listas de direcciones IP fraudulentas, peligrosas o que hacen spam. Estas IPs se recolectan en el DNSBL (Domain Name BlackList) y RBL (RealTime Blacklist), entre otras listas.

Es suficientemente fácil revisar si una dirección IP aparece en alguna de estas listas. Si aparecen, debería ser motivo de alerta ya que probablemente han sido usadas anteriormente para enviar spam por correo electrónico.

Detección de servidor proxy

La detección de proxy te permite saber si un usuario oculta su dirección IP utilizando un proxy, VPN (Virtual Private Network) o un nodo Tor. Este tipo de conexiones están diseñadas para sortear restricciones geográficas o mantener anónimo al usuario.

Aunque no necesariamente apunta a actividad fraudulenta, esto debería incrementar los niveles de riesgo de lidiar con este usuario. Algunos usuarios se conectan a través de proxies por razones de privacidad. Sin embargo, otros ocultan sus IPs para enmascarar su verdadera identidad en línea deliberadamente.

Hostname y dominio del IP

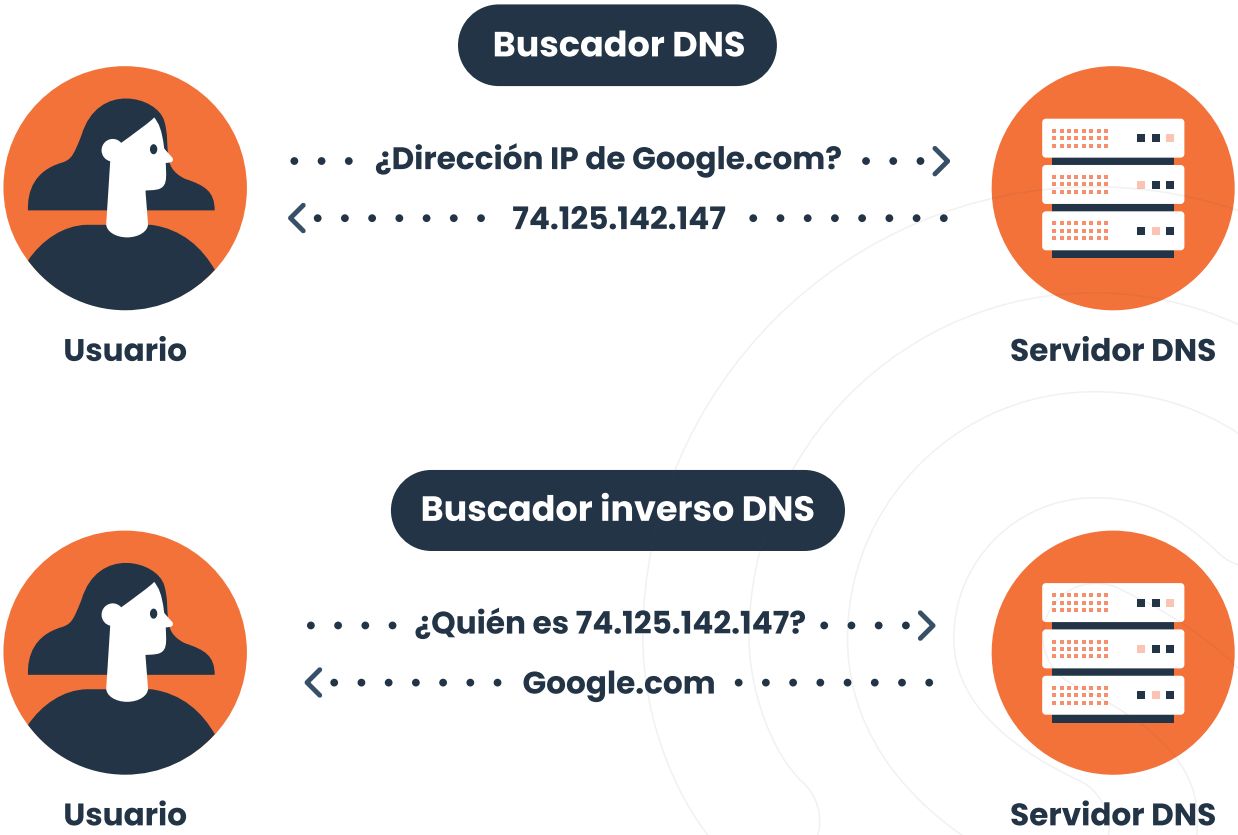
Toda dirección IP está conectada a un hostname y un dominio. Al utilizar un buscador inverso DNS, puedes consultar servidores DNS para obtener un registro PTR (pointer), el cual almacena direcciones IP.

Esto funciona por dos razones:

1. Como una capa adicional de información que puede servir para la resolución de problemas de red, identificar correos electrónicos spam o ingresar más detalles de usuario como parte de un proceso de análisis de huella digital.

2. En segundo lugar, también puedes averiguar si una conexión se oculta por razones de anonimato o si otros sitios web también se alojan en el mismo DNS.

Averiguar el hostname ayuda con otra característica importante del rastreo de IP: la geolocalización.



Geolocalización

Las direcciones IP son emitidas por los proveedores de servicios de internet o Internet Service Providers (ISPs), quienes las seleccionan aleatoriamente de su rango. Ese rango de direcciones IP potenciales está ligado a una localización geográfica aproximada. Al realizar una revisión rápida, puedes darte una idea sobre desde dónde se está conectando alguien.

Ten en cuenta que la precisión de la localización varía de un ISP al siguiente. Las cosas se complican todavía más con las IPs de dispositivos móviles, las cuales pueden cambiar de forma dinámica en la medida que el usuario se conecta a través de torres móviles diferentes que pueden conducir a una IP asignada a varios dispositivos y usuarios reales al mismo tiempo, cuando la carga de trabajo del servidor es pesada. Puedes leer acerca de esto en nuestra guía sobre los proxies móviles.

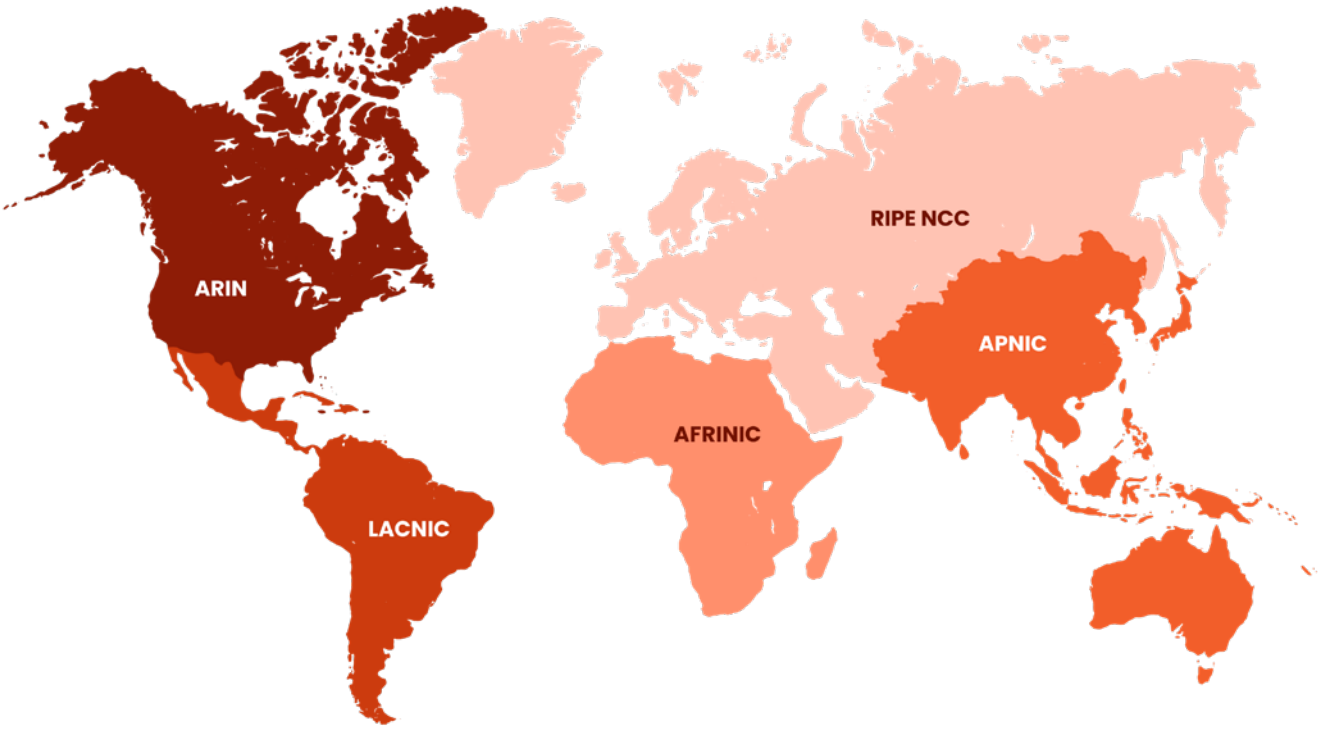
Aún así, obtener una idea de la geolocalización de un usuario tiene muchas ventajas, incluso aunque debas tener reservas respecto a los resultados.

Es posible señalar un lugar en el mundo con precisión increíble, pero también es posible equivocarse en un gran margen, especialmente al lidiar con personas que no quieren ser localizadas.

Información WHOIS

WHOIS es un protocolo de respuesta diseñado para identificar a los dueños de una dirección IP. Toda dirección IP en internet es gestionada por una de las cinco organizaciones de registro de internet:

- **African Network Information Center (AFRINIC):** para direcciones IP africanas
- **American Registry for Internet Numbers (ARIN):** direcciones IP para Estados Unidos, Canadá y varias islas del Caribe y el Noratlántico
- **Asia-Pacific Network Information Centre (APNIC):** direcciones IP para Asia, Australia y países vecinos
- **Latin American and Caribbean Network Information Centre (LACNIC):** direcciones IP para latinoamérica y partes de la región caribeña
- **Réseaux IP Européens Network Coordination Centre (RIPE NCC):** direcciones IP para Europa, el Medio Oriente y Asia Central



Esto es útil para confirmar la información de geolocalización que tú ya tienes o para identificar discrepancias en los datos. También puede apuntar al dueño de un sitio web, ya que puedes buscar los servicios WHOIS por nombre, lo que es un punto de datos adicional con el que trabajar.

Verificación de puerto abierto

Los servidores proxy y las computadoras que funcionan como servidores tienden a tener al menos un puerto abierto. Si sabes qué puerto es este, puedes identificar el servidor y su tasa de riesgo.

Por ejemplo, sabemos que algunos proveedores de proxy inescrupulosos revenden conexiones SSH hackeadas en las que el puerto 22 siempre se encuentra abierto.

Si puedes identificar que el puerto 22 está abierto, puedes empezar a levantar alertas. Puede que no signifique necesariamente que estás lidiando con un malhechor, pero es información con la que es útil contar como parte de tu proceso de perfilamiento digital.

¿Cómo rastrear una IP?

Hay dos métodos en los que se tiende a realizar una búsqueda de IP:

- **Revisión manual:** Identificas la dirección IP y ejecutas el código tú mismo. También puedes pegarlo en una herramienta dinámica en línea (la cual únicamente ejecuta el código por ti). Esto es muy bueno para revisiones únicas.
- **Servicios de terceros:** dado que puedes extraer mucha información a partir de las IPs, hay algunos servicios online que te permiten ejecutar todas las revisiones al mismo tiempo. Estos tienden a ser servicios de pago. Puedes importar estas listas de IPs o conectarte al servicio a través de APIs.

4 de las mejores herramientas para rastrear IPs disponibles en el 2022

Aviso:

todo lo escrito en este artículo se obtuvo de la investigación en internet, lo que incluye reseñas de usuarios. No tuvimos tiempo de probar todas las herramientas manualmente. Sin embargo, nos aseguramos de que la información fuera correcta a partir del primer trimestre del 2022.

SEON

SEON es una plataforma completa de prevención de fraude. Viene con una selección de herramientas de búsqueda, que incluye un poderoso módulo de rastreo de IP. En términos de las revisiones, obtienes una mezcla de métodos de recolección de datos propia con revisiones comunes como:

- **geolocalización**
- **información y tipo de ISP**
- **detección de puerto abierto**
- **Tor, VPN, proxy web o público**

- **listas de spam**
- **revisiones de velocidad, que incluyen la frecuencia con la que una IP aparece en tu sitio, además de la fecha en la que fue vista por primera y última vez**

Pero donde SEON realmente destaca es en su posibilidad de **realizar estas revisiones a escala** mediante llamadas API, entregando resultados en menos de 200 milisegundos. Para las compañías que necesitan rastrear miles de direcciones IP, esta es la mejor manera de obtener tanta información como sea posible, lo más rápido posible.

El buscador de IP de SEON también está completamente integrado con otras características de detección de fraude, tales como:

- **Análisis de puntuación de riesgo** para saber si una IP apunta o no a una riesgosa.
- **Análisis de huella digital:** puedes combinar los datos de IP con datos de dispositivo y revisiones de redes sociales, por ejemplo.
- **Sugerencias de machine learning:** SSEON puede sugerir reglas con base en los datos históricos de tu negocio. Esto es útil para identificar patrones que los analistas humanos puedan haber pasado por alto.
- y mucho más.

Se trata de uno solo de los módulos de todo un sistema de prevención de fraude de extremo a extremo, pero también puedes utilizar el módulo para rastrear IP por sí solo. Además, esto funciona particularmente bien a través del plugin ligero de Google Chrome para revisiones manuales rápidas.

Ventajas de SEON para rastrear IPs

- **Recolecta muchísima información:** ISP, proxy, uso de VPN y más.
- **Filtra usuarios fraudulentos:** SEON entrega una puntuación de riesgo para ayudarte a decidir si debes aceptar a un usuario en tu sitio, permitir un inicio de sesión o aceptar una transacción.
- **Se combina con otros módulos de enriquecimiento de datos:** puedes combinar los datos de IP con la huella digital del dispositivo o con los datos de correo electrónico o teléfono para conformar un perfil de cliente completo.
- **Precios flexibles:** tienes una prueba gratuita de 30 días y contratos que se pueden cancelar en cualquier momento.

análisis de IP + huella digital del dispositivo

Más efectivo para detectar intentos de robo de identidad o cuentas múltiples, especialmente cuando puedes alimentar todos los datos a los algoritmos correctos (como las reglas de velocidad antes mencionadas)

análisis de IP + búsqueda de correo electrónico o teléfono

Para obtener una perspectiva más clara acerca de quiénes son tus usuarios e incrementar la precisión de tus puntuaciones de riesgo.

Contras de SEON para rastrear IPs

- **Demasiado sofisticado para revisiones básicas:** SEON no es de ninguna manera difícil de usar, pero es una herramienta de especialista que únicamente será aprovechada al máximo por gerentes de riesgo.

Precios de SEON

- Obtienes una prueba gratuita de 30 días y un contrato que se puede cancelar en cualquier momento. El costo empieza desde $99 al mes.

IPLocation.io

El sitio web IPLocation.io es un verdadero tesoro de herramientas para rastrear IP. En él encontrarás, sin ningún orden en particular: verificador de bases de datos de listas negras, una herramienta de ping, calculadoras de rango de IP, conversor de IP a decimales y mucho más.

Lo mejor es que todas estas herramientas están disponibles de forma gratuita. Simplemente copia la dirección IP y pégala en la página de la herramienta apropiada. Puedes acceder a todas las diferentes herramientas de búsqueda en la barra lateral, además de la información útil acerca de cómo funcionan, incluyendo detalles técnicos.

¿El único inconveniente? Bueno, IPLocation.io no está preparada para correr grandes lotes de direcciones IP. No existe una API, por lo que tendrás que buscar en otro lado para integrar sus resultados en los reportes de inteligencia de tu negocio.

Ventajas de IPLocation.io

- **Docenas de herramientas disponibles:** y no únicamente para rastrear IPs. También tienen herramientas de SEO, de correo electrónico y de ciberseguridad.
- **Todo está accesible gratis:** usar el sitio web no tiene ningún costo.

Contras de IPLocation.io

- **Una revisión a la vez:** no puedes enviar una lista de direcciones IP o conectar el servicio a través de una API.

Precio de IPLocation.io

- ¡Es gratis!

MaxMind

MaxMind ofrece dos servicios relacionados con la IP, que incluyen una API de prevención de fraude para transacciones de riesgo y sus bases de datos de GeoIP. Nos enfocaremos en esta última, ya que proporciona excelente inteligencia a partir de una dirección IP para personalización, publicidad, gestión de derechos digitales y cumplimiento, entre otros.

Las bases de datos GeoIP se usan actualmente por más de 5.000 negocios en todo el mundo. Se estima que cubre un impresionante 99.9999% de todas las direcciones IP en uso. La base de datos se actualiza semanalmente y ha tenido un excelente tiempo de operación de 99.98% desde el 2002.

El servicio de base de datos es accesible a través de API, carga manual de archivos o servicio web.

Ten en cuenta que el precio puede ser un poco confuso ya que hay seis tipos diferentes de ofertas de MaxMind. Sin embargo, incluye una versión Lite gratuita de herramientas que puedes probar para ver si te ayudan con tus investigaciones de rastreo de IP.

Ventajas de MaxMind

- **Excelente geolocalización:** MaxMind puede detectar a dónde apunta una IP prácticamente en cualquier parte del mundo.
- **Mucha flexibilidad** tanto en términos de precio como de integración. Existen diversas licencias para elegir, por lo que puedes pagar por MaxMind de la manera que más tenga sentido para tu negocio.

Contras de MaxMind

- **Productos segmentados:** Primero tienes que seleccionar si quieres su servicio web GeoIP o MiniFraud y la integración entre ambos no es clara. Incluso seleccionar el producto GeoIP adecuado es un desafío ya que existen muchas licencias para elegir.
- **Precios opacos:** elegir un producto de MaxMind ya es difícil. Pero también tienes que tener una llamada de ventas para obtener una idea de cuánto cuesta.

Precios de MaxMind

- Debes ponerte en contacto con MaxMind para averiguarlo, aunque existe una versión gratuita limitada.

IPQualityScore

IPQualityScore, o IPQS como se le llama a veces, ofrece una amplia variedad de herramientas para rastrear IP, que incluyen detección de Tor, revisión de reputación de IP y revisiones de listas negras de IP.

Para los expertos en ciberseguridad, también puedes obtener lo que ellos llaman “threat intelligence feeds”, que se conecta con su propia red honeypot, diseñada para identificar amenazas de ciberseguridad.

Una vez en el ecosistema de productos de IPQualityScore, también puedes fijarte en otras herramientas de prevención de fraude como la detección de bots, verificación de correo electrónico, detección de fraude de contracargo y monitoreo de la dark web.

Ventajas de IPQualityScore

- **Paquete completo de herramientas de rastreo de IP y prevención de riesgo:** existen muchas opciones para elegir dentro de IPQualityScore, ya sea que quieras conocer más acerca de las IPs o fortalecer tu protección de ciberseguridad.
- **Oferta gratuita:** puedes obtener hasta 5.000 rastreos de IP gratuitos por mes.

Contras de IPQualityScore

- **Precios opacos:** Aunque cuentan con una generosa oferta gratuita, es difícil determinar cuánto le costará a tu negocio usar IPQualityScore.

Precios de IPQualityScore

- La compañía opera a través de un modelo freemium, pero los planes de pago están ocultos a la vista. Necesitas ponerte en contacto con ellos para obtener una cotización.

Prevención y detección de fraude con una herramienta para rastrear IP

En SEON, siempre buscamos las mejores formas de obtener información a partir de los datos mínimos. Esto es con el propósito de que conozcas con quién estás tratando, específicamente para bloquear a defraudadores antes de que puedan dañar tu negocio.

Nuestra herramienta de rastreo de IPs es una de las más sofisticadas del mercado. La última actualización viene con la posibilidad de rastrear IPs dañinas, reducir los falsos positivos y, por supuesto, aprender todo lo que se pueda acerca de una dirección IP.

Una vez que implementes la herramienta de rastreo de IP en tu pila de detección de fraude, tienes acceso a toda la información que necesitas para realizar conjeturas bien fundamentadas y automáticas a gran escala.

Preguntas frecuentes acerca del rastreo de IP

¿Puedo rastrear una dirección IP?

Sí. Una dirección IP puede revelar mucho acerca de la persona que se conecta con ella, tal como su geolocalización, proveedor de servicio de internet y más. Ten en cuenta que las VPN y los proxies están diseñados para suplantar las direcciones IP, así que los resultados podrían ser erróneos.

¿Rastrear una IP es legal?

Sí. Las direcciones IP se consideran de dominio público. Cualquier herramienta para rastrear IP que derive información a partir de estas direcciones es legal y cumple con el GDPR.

¿De dónde provienen los datos del rastreo de IP?

Los datos de rastreo de IP se encuentran en bases de datos de los ISP, listas negras públicas y bases de datos propias. Por ejemplo, algunas compañías crean sus propias listas de direcciones IP sospechosas, que identifican al crear trampas honeypot.

¿Qué es una puntuación de fraude de IP?

SEON utiliza puntuaciones de fraude de IP en la detección de fraude, para ayudar a sorprender a los malhechores. Preparamos una guía completa de las puntuaciones de fraude de IP para tu lectura.

SEON

SEON Technologies Ltd.
seon.io

info@seon.io
+44 20 8089 2900