GUÍA DE PRIVACIDAD

Tor

Los principios, sin tecnicismos

Qué es, cómo oculta quién eres en internet y hasta dónde llega.

01

Qué es Tor

Tor es una red que te permite usar internet sin que las webs sepan quién eres ni que quienes ven tu conexión sepan qué visitas. Funciona con miles de ordenadores de voluntarios repartidos por el mundo, y se usa gratis con un navegador llamado Tor Browser.

SIN UNA EMPRESA EN MEDIO

No hay un único intermediario que lo sepa todo: el trabajo se reparte entre varios.

HECHO POR VOLUNTARIOS

Cualquier persona puede aportar un ordenador para que la red crezca y sea más difícil de bloquear.

CÓDIGO ABIERTO

Cualquiera puede leer cómo funciona, revisarlo y proponer mejoras.

02

Cinco ideas previas

Si ya sabes cómo funciona la navegación en internet, salta directamente a la sección 4.

1. **La dirección IP.** Es como tu dirección postal en internet. Las webs la ven cuando entras y suele revelar tu ciudad y tu proveedor.
2. **Los metadatos.** Son los datos sobre tu actividad: con quién te conectas y cuándo. Aunque el contenido esté cifrado, los metadatos cuentan mucho de ti.
3. **El intermediario.** Quien hace de puente entre tú y una web. Si es uno solo, tiene que saberlo todo de ti.
4. **El cifrado.** Convierte un mensaje en algo ilegible para quien no tiene la llave.
5. **Las capas.** Cifrar varias veces seguidas, como envolver un regalo en tres papeles. Cada persona quita uno y solo uno.

03

El problema: tu dirección te sigue a todas partes

Cada vez que visitas una web, esa web recibe tu dirección IP. Tu proveedor de internet, además, ve a qué servidores te conectas. Con el cifrado HTTPS el contenido de lo que haces queda protegido, pero no con quién hablas. Y las empresas de publicidad pueden enlazar todas tus visitas para construir un perfil sobre ti.

> **Un solo intermediario no basta.** Una VPN o un proxy esconde tu dirección de la web, pero su dueño sí la conoce, y conoce también qué visitas. Solo has cambiado en quién confías. Tor reparte esa confianza entre varios.

04

Los tres principios de privacidad

Tor protege tu anonimato con tres ideas que funcionan a la vez.

TRES RELEVOS

Tres saltos

Un camino por tres ordenadores distintos.

TRES ENVOLTORIOS

Capas de cifrado

Cada ordenador quita solo su capa.

NADIE LO SABE TODO

Roles separados

Quien ve tu IP no ve tu destino.

Tres saltos

En lugar de ir directo a la web, tu tráfico pasa por tres ordenadores voluntarios, llamados relays: uno de entrada, uno intermedio y uno de salida. Cada uno solo conoce al anterior y al siguiente. Es como un mensaje que pasa por tres mensajeros que no se conocen entre sí.

Capas de cifrado

Antes de salir de tu ordenador, el mensaje se envuelve en tres capas de cifrado, una para cada relay. El primero quita la suya y pasa el resultado al segundo, que quita la suya, y así hasta el tercero. Por eso se llama enrutado de cebolla: la información va dentro de varias capas que se pelan una a una.

Nadie lo sabe todo

El relay de entrada ve tu dirección, pero no sabe qué web visitas. El de salida ve la web, pero no sabe quién eres. El intermedio no sabe ninguna de las dos cosas. Para saber quién visita qué, habría que controlar a la vez la entrada y la salida del camino.

> Los tres mecanismos funcionan juntos: el camino reparte el conocimiento, las capas impiden leer lo que pasa y los roles separados evitan que alguien lo una todo.

05

Una visita, paso a paso

1. Tu navegador descarga una lista pública y firmada de los relays disponibles.
2. Elige tres: uno de entrada, uno intermedio y uno de salida.
3. Acuerda con cada uno una llave secreta, sin que nadie más pueda descubrirla.
4. Envuelve tu petición en tres capas de cifrado, una por relay.
5. Cada relay quita su capa y reenvía el resultado. El de salida entrega la petición a la web.
6. La respuesta vuelve por el mismo camino, y cada relay le añade su capa. Tu navegador las quita todas.

06

Qué mantiene segura la red

DIRECTORIO POR CONSENSO

Un grupo de servidores independientes, de distintos países, publica cada hora la lista de relays. Hace falta que la mayoría esté de acuerdo.

PUENTES PARA QUIEN ESTÁ BLOQUEADO

Son relays que no figuran en la lista pública, y que se disfrazan de tráfico normal, para que un censor no los pueda bloquear todos.

Tor también permite crear sitios y servicios cuya ubicación está oculta, con direcciones que terminan en .onion. Ni el visitante sabe dónde está el servidor, ni el servidor sabe quién lo visita. Tor Browser, además, hace que todos sus usuarios parezcan iguales.

REFERENCIA

Glosario rápido

TÉRMINO	EN UNA FRASE
Relay	Ordenador voluntario que reenvía tráfico por la red
Guardia	El relay de entrada, que ve tu dirección y se mantiene fijo durante semanas
Relay de salida	El último, que ve la web de destino
Circuito	El camino de tres relays que sigue tu tráfico
Servicio onion	Sitio con ubicación oculta, cuya dirección termina en .onion
Puente	Relay no listado públicamente, para quien tiene Tor bloqueado

> **Siguiente paso.** La guía completa, "Tor a fondo", explica cada una de estas piezas con más detalle, con sus cifrados y sus fórmulas, capítulo a capítulo.

Fuentes: The Tor Project, Help Net Security y CyberInsider.