¿Quién necesita anonimato en línea?

Muchas veces se asocia anonimato a comportamientos indeseables o incluso ilegales. Sin embargo, el anonimato garantiza el derecho a expresarnos y a reunirnos, a la protesta social y la disidencia política; nos permite comunicarnos y acceder a información en contextos represivos. ¿Quién podría beneficiarse de utilizar una herramienta como Tor?

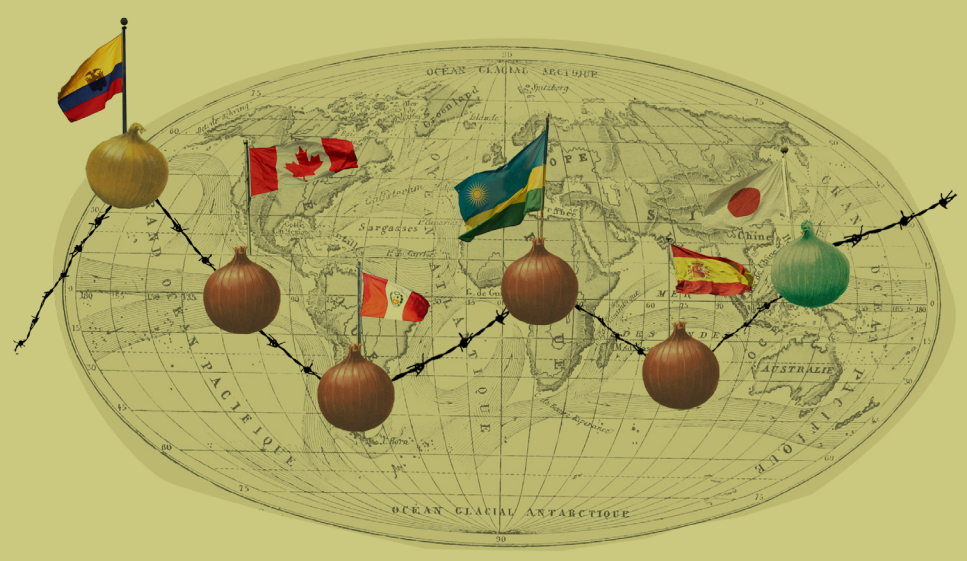
- Usuarios de internet intentando esquivar la censura en su país o región.
- Periodistas comunicándose con fuentes en riesgo.
- Activistas que pueden estar siendo vigiladas o vigilados.
- Personas que quieran denunciar un ilícito, pero temen a las represalias.
- Personas que sufran una enfermedad estigmatizada y requieren información y apoyo.
- Personas que se oponen al registro de sus actividades en línea.
- Y muchas otras más.

¡Únete a Tor!

Instala un nodo de salida en tu organización

El anonimato en internet permite proteger la privacidad, la libertad de expresión y combatir la censura. Tor es un software y una comunidad internacional dedicada a proteger nuestra identidad en línea.

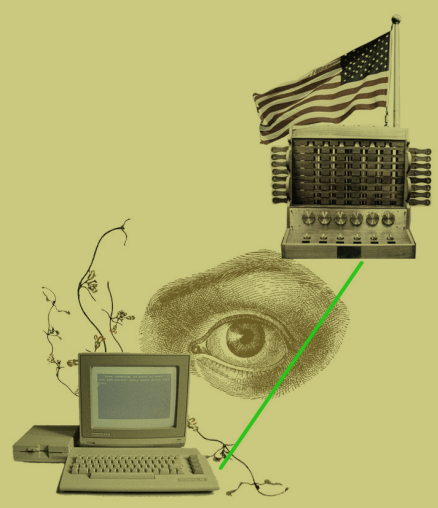
DERECHOS DIGITALES América Latina



¿Por qué es importante que existan más nodos de salida de Tor en Latinoamérica?

La red Tor se sostiene gracias a los nodos, intermedios y de salida, que canalizan la información para garantizar el anonimato en la navegación. La red se hace más robusta en la medida que hay más nodos disponibles y más personas navegando a través de Tor.

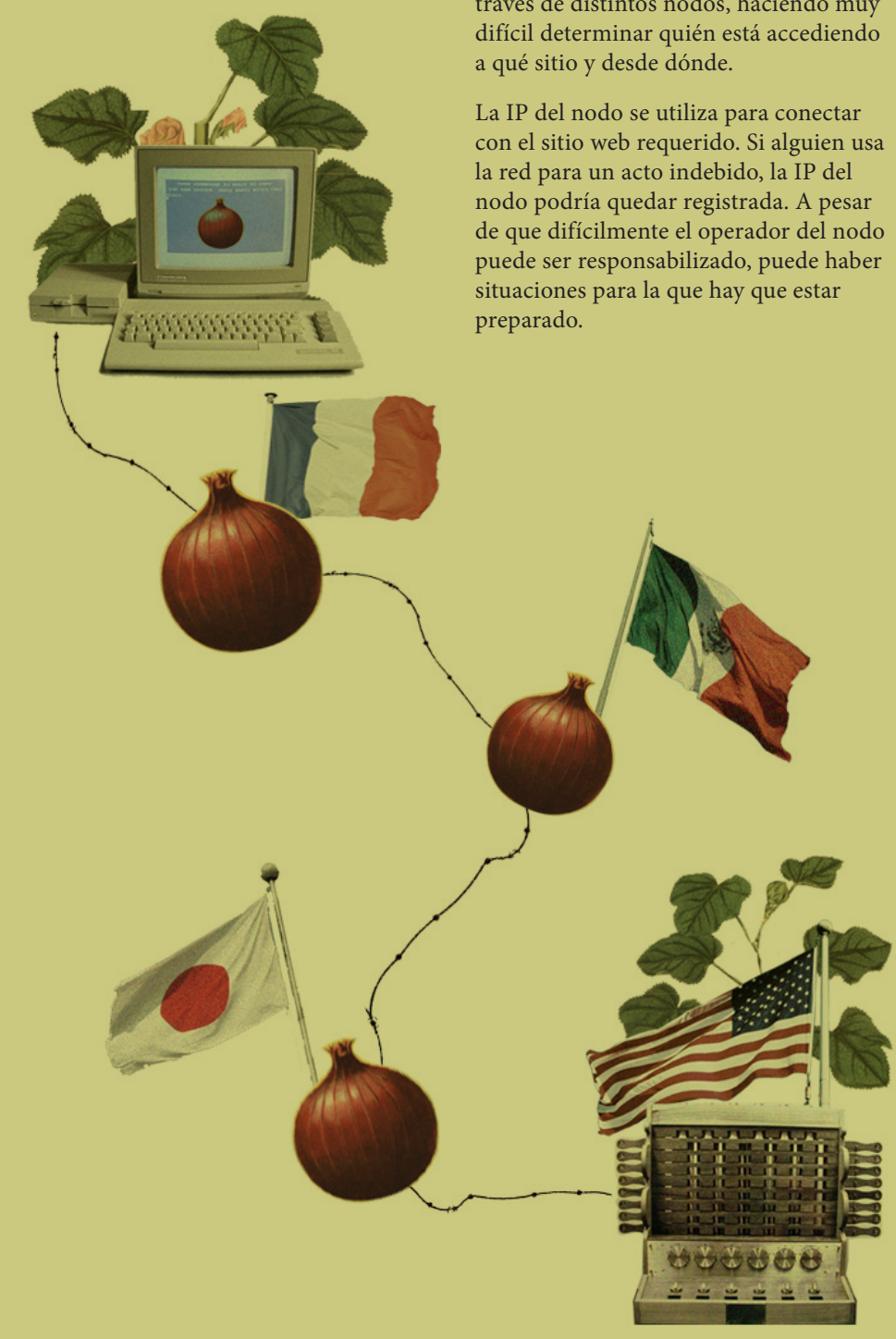
En América Latina, donde constantemente se están dictando leyes en favor del monitoreo y la ciber vigilancia masiva, defendemos nuestro derecho a la privacidad promoviendo la navegación anónima entre usuarios y usuarias, y la instalación de nodos entre personas, organizaciones e instituciones, pues hasta ahora nuestra participación en la red mundial no alcanza el 2%. Necesitamos mejorar esa cifra.



¿Cómo funciona Tor?

Cuando visitas un sitio web, se establece una conexión directa entre tu dispositivo y el servidor que aloja el contenido al que quieres acceder. A través de la dirección IP asignada a nuestro dispositivo, es posible determinar desde dónde se ha realizado la conexión. Cuando lo haces a través de la red Tor, la conexión es cifrada y redirigida de forma aleatoria a través de distintos nodos, haciendo muy difícil determinar quién está accediendo a qué sitio y desde dónde.

La IP del nodo se utiliza para conectar con el sitio web requerido. Si alguien usa la red para un acto indebido, la IP del nodo podría quedar registrada. A pesar de que difícilmente el operador del nodo puede ser responsabilizado, puede haber situaciones para la que hay que estar preparado.



¿Qué es Tor?

Tor es una red de computadoras-nodo, distribuidas alrededor del mundo y mantenidas por voluntarios, que permiten anonimizar la conexión a internet, ocultando la dirección IP y cifrando el tráfico de datos.

El acceso a la red se realiza por medio de Tor, un software que sirve tanto para conectarse a la red, como para habilitar nodos, que pasan a formar parte de ella. La manera más sencilla de utilizar la red Tor es mediante el Tor Browser, un navegador web que incorpora el software Tor y permite revisar sitios web de forma anónima.

El software es desarrollado y mantenido por The Tor Project, Inc, organización sin fines de lucro, con sede en Estados Unidos.

Un proyecto impulsado por:

DERECHOS DIGITALES América Latina

Tor

Más información

Visita *tor.derechosdigitales.org*, sitio preparado por Derechos Digitales con valiosa información sobre Tor, su funcionamiento y la comunidad latinoamericana parte de la red.

Instalar un nodo de salida de Tor

La red Tor funciona gracias a miles de voluntarios que mantienen los nodos que la componen, ayudando así a la defensa del derecho a la privacidad en línea, a la libertad de expresión y al combate de la censura.

A mayor número de nodos de salida, la red se vuelve más fuerte, rápida y estable. Sin embargo hay muy pocos nodos de salida en América Latina. Por ello, la ayuda de organizaciones e instituciones que crean en la defensa de los derechos humanos es fundamental. ¿Quieres sumarte?

Consideraciones

TÉCNICAS

¿Qué capacidad técnica requiero?

Para garantizar la estabilidad del nodo, necesitas:

- Ancho de banda mayor a 10 Mbps simétricos, exclusivos para el nodo.
- Una dirección IP pública fija exclusiva para el nodo
- Un router que permita conexiones abiertas, tanto de entrada como de salida en puertos particulares.
- Computadora encendida 24/7; al menos 520 MB de memoria RAM y 200 MB de espacio en disco duro, exclusivos para Tor.
- Además, asegúrate de que tu proveedor de internet no prohíba operar nodos de salida de Tor.

LEGALES

¿Es legal el anonimato en México?

Sí. Tanto la Constitución nacional como los acuerdos internacionales suscritos por México reconocen el derecho al anonimato, a la privacidad de las comunicaciones y a la libertad de expresión.

¿Es legal instalar un nodo de salida en México?

Sí. Mientras no exista una prohibición expresa, la ley permite utilizar herramientas para la protección de la privacidad y la libertad de expresión, derechos humanos reconocidos internacionalmente.

¿Existen impedimentos al uso de herramientas para el anonimato?

No. El uso de Tor no está sometido a ningún tipo de limitación: las herramientas de cifrado están reconocidas como una alternativa para garantizar la seguridad y confidencialidad de la información. Así mismo, los proveedores de internet están impedidos de bloquear el acceso a cualquier red, incluidas las que permiten la actividad anónima de sus usuarios.

Sin embargo, hay que considerar que la Ley Federal de Telecomunicaciones y Radiodifusión establece que los proveedores de internet deben almacenar, por un periodo de 2 años, todos los datos relacionados a la conexión de sus clientes. Esto significa que toda la actividad asociada a la IP del nodo de salida será registrada.

¿Qué puede pasar si se comete un ilícito utilizando la IP de mi nodo de salida?

En México no existe una legislación que determine que el operador de un nodo de salida pueda ser corresponsable de los delitos que puedan realizarse a través del uso de la red Tor.

Sin embargo, en caso de ser declarado por un juez, los equipos pueden ser confiscados para ser periciados como parte de la investigación. El operador del nodo debe cooperar en todo momento con las autoridades y de ninguna manera negarse a facilitar la ayuda necesaria para la realización de su trabajo, pues esto podría constituir un delito.

Aunque requiere de ciertos conocimientos y capacidades técnicas, la instalación de un nodo de salida es relativamente sencilla.

Instalación en tres pasos

Instala Tor
En tor.derechosdigitales.org encontrarás indicaciones para hacerlo en Debian, pero también se puede instalar en otras distribuciones Linux y algunas versiones de BSD.

Configura el nodo
Asígnale un nombre, un puerto y un ancho de banda. Indica que se trata de un *ExitRelay*.

Revísalo
Reinicia y pruébalo. Luego de un par de horas, busca tu IP en la lista pública de torproject.com.

RECOMENDACIONES PARA LA INSTALACIÓN

- Asigna un subdominio al nodo: tor-exit.miorganizacion.org
- Luego, agrega una nota en el registro WHOIS, explicando que se trata de un nodo de salida de Tor.
- Crea una página HTML de aviso, indicando que se trata de un nodo de salida Tor y explicando el tipo de tráfico que se permite a través del nodo.

¿Tienes un compromiso fuerte con el derecho a la privacidad y la libertad de expresión? ¿Quieres ser parte del proyecto Tor? Habilitar un nodo puede ser de gran ayuda.

Si necesitas más información o apoyo, visita htt ps://tor.derechosdigitales.org o escríbenos a tor@derechosdigitales.org