



Tor para feministas

¿POR QUÉ CONFIAR EN TOR?

Tor está diseñado para la privacidad. No sabemos quiénes son nuestros usuarios y no mantenemos registros de la actividad de los usuarios. Los operadores de retransmisión de Tor no pueden revelar la verdadera identidad de los usuarios de Tor. La revisión continua del código fuente de Tor por parte de las comunidades académicas y de código abierto garantiza que no haya puertas traseras en Tor, y nuestro contrato social promete que nunca lo haremos.

INGRESA EN LA COMUNIDAD TOR

Tor es posible gracias a un conjunto diverso de usuarios, desarrolladores, operadores de retransmisión y defensores de todo el mundo. **Necesitamos tu ayuda para hacer que Tor sea más sencillo y seguro para las personas de todo el mundo.** Puedes ser voluntario de Tor escribiendo código, manteniendo un repetidor, creando documentación, ofreciendo soporte al usuario o difundiendo entre las personas de tu comunidad qué es Tor. La comunidad de Tor se rige por un código de conducta, y mostramos nuestro compromiso con la comunidad en nuestro contrato social. Consigue más información sobre Tor visitando nuestro sitio web, nuestro wiki, encontrándonos en IRC, uniéndote a una de nuestras listas de correo o inscribiéndote en Tor News en newsletter.torproject.org.

Descargar Tor

TOR PARA ESCRITORIO Y MÓVILES

torproject.org/es/download

EL FUTURO ES CIBERFEMINISTA

Fernanda dirige un colectivo de mujeres centrado en los derechos reproductivos en Brasil, donde el aborto es ilegal. Fernanda y sus compañeras crearon un sitio web con información sobre el acceso al aborto, el control de la natalidad y otros recursos para las personas que buscan información reproductiva. Si se vinculara este sitio web a ellas, las podrían arrestar, o peor. Para protegerse, Fernanda y sus colegas crearon el sitio web utilizando los **servicios cebolla de Tor**. Los servicios cebolla no sólo las protegen de ser descubiertas como operadoras del servidor, sino que también ayudan a proteger a los visitantes de su sitio web al requerir que usen el Tor Browser. De hecho, Fernanda utiliza el **Browser** para toda su navegación en la web solo para estar segura. Ella también usa una aplicación de Tor llamada **OnionShare** para enviar archivos a otras activistas de forma segura y privada.

¿CÓMO FUNCIONA TOR?

Amal quiere visitar la web de Bekele en privado, así que abre el **Navegador Tor**. El Navegador Tor selecciona un circuito aleatorio de tres relays, que son

ordenadores de todo el mundo configurados para enrutar el tráfico a través de la red Tor. El Navegador Tor a continuación encripta la solicitud del sitio web tres veces y la envía al primer relay Tor del circuito.

1. El primer relay elimina la primera capa de encriptación pero no se entera de que el destino es la web de Bekele. El primer repetidor solo sabe la siguiente ubicación en el circuito, que es el segundo repetidor.

2. El segundo repetidor elimina otra capa de cifrado y envía la solicitud de página web al tercer repetidor.

3. El tercer repetidor elimina la última capa de cifrado y envía la solicitud de la web a su destino, pero no sabe el sitio web Bekele, pero no sabe que la solicitud proviene de Amal.

Bekele no sabe que la solicitud proviene de Amal a menos que ella se lo diga.