Breve Manual de Usuario

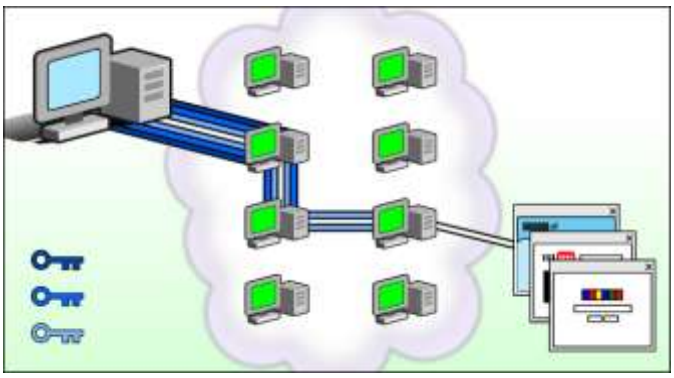
Este manual de usuario contiene información acerca de cómo descargar Tor, cómo usarlo, y qué hacer si **Tor** no es capaz de conectarse a la red. Si no puede encontrar la respuesta a su pregunta en este documento, envíe un correo electrónico a help@rt.**Tor**project.org.

Por favor note que se provee de soporte en una base voluntaria, y que se recibe una gran cantidad de correos cada día. No hay necesidad de preocuparse si no se recibe respuesta de manera inmediata.

Cómo funciona Tor

Tor es una red de túneles virtuales que le permite mejorar su privacidad y seguridad en Internet. **Tor** funciona enviando sus datos a través de tres servidores aleatorios (también conocidos como *relays*) dentro de la red **Tor**, antes que esos datos sean enviados hacia el Internet público.

La imagen muestra a un usuario navegando en diferentes sitios web a través de **Tor**. Los monitores de color verde representan los relés de la red **Tor**, mientras que las tres llaves representan las capas de cifrado entre el usuario y el relé de cada uno.



Tor hará anónimo el origen de su tráfico y codificará todo entre usted y la red **Tor**. **Tor** también codificará su tráfico dentro de la red **Tor**, pero no puede hacerlo entre la red **Tor** y el destino del tráfico.

Si usted está comunicando información delicada, por ejemplo, al acceder a un sitio con un nombre de usuario y contraseña, asegúrese de que está usando HTTPS (p.ej.: **https**://torproject.org/, no **http**://torproject.org/).

¿Cómo descargar Tor?

La descarga recomendada para la mayoría de los usuarios es el Paquete de navegador **Tor**. Este paquete contiene un navegador preconfigurado para navegar en Internet de forma segura a través de **Tor** y no requiere instalación alguna. Usted descarga el paquete, descomprime el archivo e inicia **Tor**.

Existen dos maneras diferentes para obtener el software **Tor**.:

- Usted puede navegar al **Tor** Project website y descargarlo desde ahí,
- o puede usar GetTor, el sistema de correo de respuesta automática.

Cómo obtener Tor via correo electrónico

Para recibir el Paquete de Navegador **Tor** para Windows, envíe un correo a gettor@torproject.org con **windows** en el cuerpo del mensaje. Puede dejar el asunto en blanco.

También puede solicitar el Paquete del navegador **Tor** para Mac OS X (escriba **macos-i386**) y para Linux (escriba **linux-i386** para sistemas de 32 bits o **linux-x86_64** para sistemas de 64 bits).

Por el contrario, si desea una versión traducida de **Tor**, escriba **help**. Recibirá un correo electrónico con instrucciones y una lista de idiomas disponibles.

Nota: Los Paquetes de Navegador **Tor** para Linux y Mac OS X son algo grandes, y podría no ser posible el recibir ninguno de estos paquetes con una cuenta de Gmail, Hotmail o Yahoo. Si no puede recibir el paquete que desea, envíe un correo a help@rt.torproject.org y le enviaremos una lista de servidores espejo para su uso.

Tor para smartphones

Usted puede tener **Tor** en su dispositivo Android al instalar el paquete llamado *Orbot*. Para información acerca de cómo descargar e instalar Orbot, por favor vea el**Tor** Project website.

También tenemos paquetes experimentales para Nokia Maemo/N900 y Apple iOS.

Cómo verificar que cuenta con la versión correcta

Antes de ejecutar el Paquete de Navegador **Tor**, debe asegurarse que cuenta con la versión correcta.

El software que usted recibe está acompañado de un archivo con el mismo nombre del paquete y la extensión **.asc**. Este archivo .asc es una firma GPG y le permitirá verificar que el archivo que ha descargado es exactamente el que usted pretendía obtener.

Antes de que pueda verificar la firma, tendrá que descargar e instalar GnuPG:

Windows: http://gpg4win.org/download.html
MacOSX: http://www.gpgtools.org/
Linux: La mayoría de distribuciones Linux vienen con GnuPG preinstalado.

Por favor observe que puede ser necesario que edite las rutas y los comandos usados abajo para lograr que funcione en su sistema.

Erinn Clark forma los Paquetes del navegador **Tor** con la llave 0x63FEE659. Para importar la llave de Erinn, ejecute:

```
gpg --keyserver hkp://keys.gnupg.net --recv-keys 0x63FEE659
```

Después de importar la clave, compruebe que la huella sea correcta:

```
gpg --fingerprint 0x63FEE659
```

Usted debería ver:

```
      pub   2048R/63FEE659 2003-10-16
      Huella de clave = 8738 A680 B84B 3031 A630  F2DB 416F 0610 63FE E659
uid                  Erinn Clark &lt;erinn@torproject.org&gt;
uid                  Erinn Clark &lt;erinn@debian.org&gt;
uid                  Erinn Clark &lt;erinn@double-helix.org&gt;
sub   2048R/EB399FD7 2003-10-16
```

Para verificar la firma del paquete que ha descargado, ejecute el siguiente comando:

```
gpg --verify tor-browser-2.2.33-2_en-US.exe.asc tor-browser-2.2.33-2_en-US.exe
```

La salida debe decir `&quot;Good signature&quot;`, firma válida. Una firma inválida significa que el archivo pudo haber sido alterado. Si usted ve una firma inválida, envíe los detalles acerca del origen de la descarga, cómo verificó la firma y la salida de GnuPG en un correo electrónico a help@rt.torproject.org.

Una vez que ha verificado la firma y ha visto la salida *"Good signature"*, proceda y descomprima el paquete de archivos. Entonces debería ver un directorio similar a **tor-browser_en-US**. En ese lugar encontrará otro directorio llamado **Docs**, el cual contiene un archivo llamado **changelog**. Debe de asegurarse que el número de versión en la primera línea del archivo changelog corresponde con el número de versión en el archivo.

Cómo usar el Paquete de Navegador Tor

Después de descargar el Paquete del Navegador **Tor**, extraigalo en su escritorio o en una memoria USB. Deberá obtener un directorio que contiene algunos archivos. Uno de éstos es un ejecutable llamado "Start **Tor** Browser" (o "start-tor-browser", dependiendo de su sistema operativo).

Cuando inicie el Paquete del navegador **Tor**, usted verá primeramente el programa Vidalia iniciarse y conectarse a la red **Tor**. Después, usted verá un navegador confirmando que usted se encuentre utilizando **Tor**. Esto se hace desplegando https://check.torproject.org/. Ahora ya puede navegar por Internet a través de **Tor**.

Por favor observe que es importante que utilice el navegador que viene con el paquete y no su propio navegador.

Qué hacer cuando Tor no se conecta

Algunos usuarios notarán que Vidalia se congela mientras intenta conectarse a la red **Tor**. Si esto sucede, asegúrese de estar conectado a Internet. Si necesita conectarse a través de un servidor proxy, vea *Cómo usar un proxy abierto* más abajo.

Si su conexión normal a Internet está funcionando, pero **Tor** sigue sin poder conectarse, intente lo siguiente: abra el panel de control de Vidalia, presione *Registro de Mensajes* y luego seleccione el tab *Advanced*. Puede ser que **Tor** no conecte porque:

Su reloj de sistema mal configurado: Asegúrese que la fecha y hora en su sistema es correcta, y reinicie **Tor**. Puede ser que necesite sincronizar su reloj de sistema con un servidor horario en Internet.

Usted está tras un cortafuegos restrictivo: Para decirle a **Tor** que solo use los puertos 80 y 443, abra el panel de control de vidalia, clickee en *Configuración de retransmisión* y luego en *Red*, ahí marque la casilla que dice *Mi cortafuegos sólo me permite conectarme a ciertos puntos*.

Su anti-virus está bloqueando Tor: Asegúrese que su programa de anti-virus no esté previniendo que **Tor** realice conexiones de red.

Si **Tor** sigue sin funcionar, es probable que su Proveedor de Internet (ISP) esté bloqueándolo. Frecuentemente esto puede ser evitado mediante el uso de **Puentes de Tor**, relays ocultos que no son tan fáciles de bloquear.

Si necesita ayuda para saber por qué **Tor** no se puede conectar, envíe un correo a help@rt.torproject.org e incluya las partes relevantes del registro de mensajes.

Cómo encontrar un puente

Para usar un puente, usted necesita primero encontrar uno; puede navegar a bridges.torproject.org, o puede enviar un correo electrónico a bridges@torproject.org. Si decide enviar el correo electrónico, asegúrese de escribir **get bridges** en el cuerpo del correo. Sin esta línea, no obtendrá respuesta alguna. Por favor note que necesita enviar este correo desde una dirección gmail.com o yahoo.com.

Configurar más de un puente hará su conexión **Tor** más estable en que caso que algunos de los puentes se vuelvan inaccesibles. No hay garantías que un puente que use hoy funcione mañana, es necesario hacerse el hábito de actualizar la lista de puentes frecuentemente.

Cómo usar un puente

Una vez que ha configurado los puentes a utilizar, abra el tablero de control de Vidalia y haga clic en *Configuración*, *Red* y marque la casilla que dice "Mi ISP bloquea la conexión a la red Tor". Introduzca los puentes en el campo de abajo, pulse *OK* y reinicie **Tor**.

Cómo usar un proxy abierto

Si el usar un puente no funciona, intente configurar **Tor** para usar cualquier proxy HTTPS o SOCKS y así obtener acceso a la red **Tor**. Esto significa que si **Tor** es bloqueado por su red local, proxies abiertos le pueden dar el acceso a la red **Tor** y a la red sin censura.

Los pasos siguientes asumen que usted tiene una configuración de **Tor**/Vidalia funcional y que ha encontrado una lista de proxies HTTPS, SOCKS4, o SOCKS5.

1. Abra Vidalia y presione en *Configuración de retransmisión*.
2. Haga click en *Red* y seleccione *Uso un proxy para acceder a Internet*.
3. En el campo *Address*, ingrese la dirección del proxy abierto. Esta puede ser un nombre de equipo o una dirección IP.
4. Ingrese el puerto del proxy.
5. Generalmente no se necesita un usuario y contraseña. Si lo hace, ingrese la información en los campos respectivos.
6. Seleccione el tipo de proxy a usar. En el campo *Type* elija entre HTTP/HTTPS, SOCKS4, o SOCKS5.
7. Presione el botón *Aceptar* y tanto Vidalia como **Tor** están ahora configurados para usar un proxy y así acceder a la red **Tor**.

Preguntas frecuentes

Esta sección responderá algunas de las preguntas más comunes. Si su pregunta no se está aquí, por favor envíe un correo electrónico a help@rt.torproject.org.

No se puede extraer el archivo

Si usted está usando Windows y no puede extraer el archivo, descargue e instale 7-Zip.

Si no es posible descargar 7-Zip, trate de renombrar el archivo de .z a .zip y use winzip para extraer el archivo. Antes de cambiar el nombre del archivo, *haga que Windows le muestre las extensiones del archivo:*

- **Windows XP**

1. Abra Mi PC
2. Haga clic en *Herramientas* y seleccione *Opciones* de carpeta en el menú ...
3. Haga clic en la pestaña *Ver*
4. Desmarque Ocultar extensiones para los tipos de archivo conocidos y haga clic en Aceptar.

- **Windows Vista**

1. Abrir PC
2. Haga clic en Organizar y elegir opciones de carpeta y búsqueda en el menú
3. Haga clic en la pestaña *Ver*
4. Desmarque Ocultar extensiones para los tipos de archivo conocidos y haga clic en Aceptar.

- **Windows 7**

1. Abrir PC
2. Haga clic en Organizar y elegir opciones de carpeta y búsqueda en el menú
3. Haga clic en la pestaña *Ver*
4. Desmarque Ocultar extensiones para los tipos de archivo conocidos y haga clic en Aceptar.

Vidalia pregunta por una contraseña

Usted no debería tener que introducir una contraseña al iniciar Vidalia. Si se lo pide, lo más probable es que sufra alguno de estos problemas:

- **Ya está ejecutando Vidalia y Tor**: Esto puede suceder, por ejemplo, si usted instaló el paquete de Vidalia y ahora intenta ejecutar el Paquete de Navegador **Tor**. En ese caso, usted debe cerrar los viejos Vidalia y **Tor** antes que pueda ejecutar el Paquete de Navegador **Tor**.
- **Vidalia se cerró, pero Tor sigue corriendo**: Si la ventana pidiéndole contraseña tiene un botón Reset, puede presionarlo y Vidala se reiniciará con una nueva contraseña de control al azar. Si no ve un botón Reset, o si Vidalia no puede reiniciar **Tor** por usted; vaya a su manejador de procesos o tareas y detenga a **Tor**. Luego use Vidalia para reiniciarlo.

Para más información, revise el FAQ en el sitio web del Proyecto **Tor**.

El flash no funciona

Por razones de seguridad, Flash, Java y otros plugins están inhabilitados para ***Tor****. Los plugins funcionan independientemente de Firefox y pueden realizar alguna actividad en su equipo que arruinaría su anonimato.*

La mayoría de los videos de YouTube funcionan con HTML5, y es posible ver esos videos mediante **Tor**. Necesita unirse a la prueba de HTML5 en el sitio web de YouTube antes de poder usar el reproductor HTML5.

Nota: el navegador no recordará que usted se unió a la prueba de HTML5 una vez que lo cierre, necesitará re-ingresar a ella la próxima vez que ejecute el Parquete de Navegador Tor.

Revise por favor el FAQ de Torbutton para mayores informaciones.

¿Desea utilizar otro navegador?

Por razones de seguridad, le recomendamos sólo navegar por la web a través de Tor con el Tor Browser Bundle. Técnicamente es posible usar **Tor** con otros navegadores, pero al hacerlo será vulnerable a posibles ataques.

¿Por qué Tor es lento?

Tor a veces puede ser un poco más lento que su conexión a Internet habitual. Después de todo, el tráfico se envía a través de muchos países diferentes, a veces a través de océanos de todo el mundo!