CONEXIÓN SEGURA A LA RED

INFORMACIÓN LIBRE

Reddit.com/r/InformacionLibre
conexionsegura@safe-mail.net

PRECAUCIONES

Antes de comenzar con los aspectos mas técnicos de esta guía, pedimos al lector primero revisar las reglas mas básicas de seguridad de nuestra información, como lo son: restringir el acceso a otras personas al equipo que utilizaremos para este fin, guardar discreción, evitar las descargas y paquetes que no sean necesarios, actualizar el sistema con frecuencia y no conectarnos a Internet desde redes que estén relacionadas con nosotros.

Es importante siempre tener en cuenta que al utilizar una conexión en la que queremos permanecer anónimos, no podemos ingresar a nuestras cuentas personales o sitios que puedan estar relacionados de alguna manera con nosotros o nuestros hábitos de navegación. El mejor sistema y las configuraciones mas complejas no lo protegerán contra errores de sentido común.

Es necesario utilizar un Sistema Operativo libre y de código abierto (como GNU/Linux) por numerosas razones y se deben evitar los populares sistemas comerciales Windows y Mac OS.

Si distribuyes esta información y mas personas utilizan las redes de Tor y VPN, mas privacidad podremos lograr.

EQUIPO

1. Computadora portátil, 2 GB de RAM como mínimo (se recomiendan 3 GB o más). Deben estar en buen estado el disco duro, la tarjeta del inalámbrico, los puertos USB y el lector de CDs.

2. Memorias USB y CDs.

Recomendaciones: Busque su equipo en el mercado informal o en los negocios de empeño. Proporcione nombre y datos falsos si le son requeridos y simplemente actúe con naturalidad: no está haciendo nada indebido.

Debe estar consciente de que en esta laptop no debe ingresar archivos que contengan su información personal, fotografías o cualquier dato relacionado con su identidad.

UBUNTU LINUX

De todas las distribuciones posibles de Linux debemos utilizar Ubuntu, por las siguientes razones:

- Es un sistema estable y sus desarrolladores han demostrado ser capaces.
- Está diseñado para ser fácil de utilizar.
- Tiene una comunidad numerosa que revisa el código y apoya a nuevos usuarios.
- Cuenta con las librerías y los paquetes necesarios para correr nuestro software.

ARCHIVOS-IMAGEN

Aunque puede probar con la versión 14, esta guía está enfocada en Ubuntu 12.04. Para instalar Ubuntu en la máquina, es necesario primero cargar su archivo-imagen a un CD o memoria USB.

¿Qué es un archivo-imagen? Tal cual, es una imagen de la información (el código y demás) que necesitamos para correr o instalar un sistema. No necesita saber mucho mas de estos archivos y es típico que vengan en la extensión ISO, aunque existen otros formatos.

Para descargar Ubuntu 12.04, le sugerimos hacerlo desde el *torrent* oficial: asi su descarga será mas rápida. Lo que tiene que hacer es primero descargar el archivo-torrent y abrirlo con la aplicación que haya elegido para trabajar en esta red (como BitTorrent o utorrent). El software se encargará de descargar el archivo.

El archivo-torrent que debe descargar es *ubuntu-12.04.5-desktop-i386.iso.torrent* y se encuentra en la dirección siguiente:

http://www.ubuntu.com/download/alternative-downloads

La razón por la que elegimos esta versión y no la mas reciente 14.04, es que ha sido ya ampliamente probada, tiene todo lo necesario y no incluye tantos paquetes que no utilizaremos.

CARGAR UN ARCHIVO-IMAGEN A UN CD/DVD

Si dispone de quemador, el proceso resulta mucho mas sencillo: simplemente abra su software para quemar, inserte un disco nuevo, elija el archivo y la opción "Quemar como archivo imagen" o en inglés "Burn as image-file".

CARGAR UN ARCHIVO-IMAGEN A UN USB

Si no tiene acceso a un quemador, podemos cargar Ubuntu en una memoria USB sin necesidad de equipo adicional. Esto lo podemos hacer con la aplicación UNetbootin.

Nos dirigimos al sitio de UNetbootin: *http://unetbootin.sourceforge.net/* y descargamos el archivo correspondiente a nuestro Sistema Operativo. Insertamos nuestro USB, corremos la aplicación y elegimos el archivo ISO de Ubuntu que descargamos. Seleccionamos el USB y damos en continuar para que UNetbootin cargue el archivo a nuestra memoria.

CORRER UBUNTU: MENÚ DE INICIO O "BOOT MENU"

Para instalar el sistema, debemos introducir el disco o memoria que cargamos y reiniciar desde nuestro Windows/Mac. Debemos estar muy atentos a acceder al "Menú de inicio" o "Boot Menu" justo al principio: típicamente es la tecla F9, F10 o Esc la que hay que presionar rápidamente (tenemos un par de segundos) para acceder a esta configuración antes de que cargue lo demás. En el monitor le aparecerá (al iniciar) la tecla que es necesario presionar para acceder a la configuración.

Una vez nos aparezca la pantalla con distintas opciones, debemos tener mucho cuidado de no alterar nada y solo dirigirnos al Menú de inicio para indicarle a nuestra computadora desde donde queremos que cargue al iniciar: CD/disco óptico o USB en el caso de la memoria.

En la mayoría de las máquinas esto simplemente implica elegir con las teclas 'arriba' y 'abajo' la opción deseada y dar Enter. En algunas es necesario acomodar cierto orden de los dispositivos (generalmente de arriba a abajo) con las mismas teclas o con F4,F5, etc.

Cualquiera que sea el caso, indicamos a nuestra computadora el medio que queremos correr y esperamos a que cargue.

INSTALACIÓN

Lo primero que nos pedirá el asistente de instalación es que escojamos nuestro idioma y ya sea probar o instalar Ubuntu. Si sabe un poco de inglés, le sugerimos seleccionar este idioma ya que de lo contrario tendrá que hacer descargas e instalaciones adicionales para complementar otro idioma y podrían presentarse otros inconvenientes.

Damos click en la opción de instalación y en la ventana siguiente checamos "Descargar actualizaciones mientras se instala" (o su equivalente en inglés), omitimos el software de terceros. Click en continuar y elegimos "Borrar disco e instalar Ubuntu". En la última ventana simplemente elegimos nuestro disco y damos click en instalar.

Mientras transcurre la instalación, el asistente le pedirá que introduzca información de usted y de su ubicación. Desde luego si desea reservar su identidad, no ingrese su información y utilice fórmulas genéricas como "usuario", "equipo1", etc. No cheque la opción "Encrypt home folder", pues protegeremos nuestra información usando software especializado.

CONFIGURACIÓN

Una vez se haya completado la instalación y accedemos al sistema por primera vez, podemos ver que tiene un ambiente gráfico muy particular. Del lado izquierdo, verticalmente están alineados íconos de cierto tamaño y en la parte superior se aprecia el botón Ubuntu, que nos da una herramienta de búsqueda.

Este es el ambiente gráfico "Unity", que es pesado y algo molesto para muchos usuarios por lo cual haremos algunas adecuaciones para que nuestro sistema corra de forma mas veloz.

Damos click en el botón Ubuntu e introducimos en el espacio de búsquedas la frase: terminal.

Estamos buscando el ícono de la terminal BASH, que es el intérprete de comandos y una de nuestras herramientas mas importantes. Cuando aparezca esa pequeña pantalla negra, damos click en ella y ahi tenemos nuestra terminal.

Puede apreciar que la terminal le da una línea de comando, en la que usted lee su nombre de usuario, el de su PC y enseguida el símbolo "$", que identifica la línea de la terminal. De ahora en adelante, cada vez que usted vea en este documento el símbolo "$" significa que nos referimos a introducir comandos en esta consola.

Antes que nada hay que actualizar Ubuntu. Para ello empezamos con el comando "sudo", con el cual le indicamos al sistema que debe correr nuestra instrucción con permisos de super-usuario y para ello introduciremos nuestra clave. Seguido del comando "apt-get" y lo que requerimos, es decir la actualización.

```
$ sudo apt-get update
```

Nos pedirá nuestra clave, y enseguida nos da un resumen de los cambios que se llevarán a cabo. Debemos de contestar 'y' para que continúe. Ubuntu se conectará a sus servidores para descargar e instalar las actualizaciones sin mayor esfuerzo por parte de nosotros. Una vez que finalice, hacemos lo mismo con:

```
$ sudo apt-get upgrade
```

Antes de cambiar nuestro ambiente gráfico, debemos hacer algunas modificaciones. Lo que queremos es remover ciertos paquetes que se conectan con los servidores de Ubuntu ("llaman a casa") para informarnos de música, videos y cosas asi. Aunque son inofensivos, queremos el mayor control que se pueda tener sobre nuestro tráfico:

```
$ sudo apt-get -y remove unity-scope-video-remote

$ sudo apt-get -y remove unity-scope-musicstores
```

Ya actualizado, debemos instalar el manejador de paquetes "Synaptic", con el que facilmente podemos añadir software:

```
$ sudo apt-get install synaptic
```

Le decimos que si, esperamos a que se hagan los cambios y estamos listos para correr la aplicación:

```
$ sudo synaptic
```

Corremos la aplicación con "sudo" porque requerimos permisos de super-usuario para realizar cambios en los paquetes de nuestro sistema.

Podemos apreciar que nos aparece una ventana, y en su parte superior un espacio para introducir búsquedas ("Quick filter"). Introduzca la frase: lxde

LXDE es un ambiente gráfico diseñado para consumir la menor cantidad de recursos posible y optimizará el uso de Ubuntu de manera importante.

Una vez aparezcan los resultados del filtro, busque el paquete en la lista (dice simplemente "lxde"), dé click derecho en el y cuando aparezca el menú emergente elija "Mark for Installation". Hecho esto Synaptic sabe que usted quiere instalar LXDE, pero espera la instrucción final: dé click en el botón "Apply" para aplicar los cambios y enseguida acepte los paquetes adicionales requeridos. Tome un descanso y espere a que se descarguen e instalen los nuevos paquetes.

Cuando haya finalizado todo este proceso, reinicie el sistema. Ubuntu correrá normalmente y le presentará el login que vio anteriormente. ¿Puede ver al lado de su nombre de usuario un pequeño círculo con el logo de Ubuntu? Dé click en el, y cuando aparezca el menú, elija LXDE. Introduzca su contraseña.

Ubuntu viene incluido con Firefox, que es el navegador mas seguro. Corra este programa y en el menú vaya a "Edit" y luego click en "Preferences". En la ventana que aparece, nos ubicamos en la pestaña "General" y cambiamos la página de inicio de Firefox ("Home page") a www.google.com.

ESCRITORIO

Linux viene con cierta funcionalidad en su escritorio. De hecho, en LXDE podemos trabajar con dos escritorios que elegimos en la barra inferior, del lado izquierdo. Son los recuadros al lado de los íconos y si mueve su cursor por encima le aparecerá "desktop1" y "desktop2"

Si por algo se le llegan a "perder" sus ventanas y no sabe que ha sucedido, lo mas seguro es que el sistema cambió de un escritorio a otro al entender mal el movimiento de su ratón. De click en uno de estos recuadros.

PRIMEROS PASOS CON LA TERMINAL

Con el ambiente LXDE, debe localizar la terminal en el botón del sistema (parte inferior izquierda), luego Accesories, click en LXterminal.

Aparece nuestra terminal y nos encontramos una vez mas en nuestra carpeta principal ("home") para introducir comandos. Antes de esto es pertinente aclararle que Linux diferencía el uso de mayúsculas y minúsculas, por lo tanto "Ls" no va a ser comprendido por la terminal, pero si "ls".

Para enlistar los contenidos de la carpeta, utilizamos el comando "ls":

```
$ ls
```

CAMBIAR DE UBICACIÓN

Podemos ver las carpetas en azul y algún otro archivo. Con el comando "cd" cambiamos nuestra ubicación al directorio que deseamos. Probemos con "Music":

```
$ cd Music
```

Ahora nos encontramos en /Music, una carpeta que se encuentra vacía. Para regresar al directorio superior, en este caso nuestra carpeta "home", utilizamos un espacio y dos puntos después de "cd":

```
$ cd ..
```

Note el espacio entre el comando y los dos puntos. Quien utilizó comandos en MS-DOS, recordará que esta instrucción no llevaba un espacio intermedio ("cd.."). En Linux se debe utilizar.

Un beneficio que nos da la terminal BASH, es el poder pedirle autocompletar los nombres de carpetas y archivos. Veamos un ejemplo: desde su carpeta "home", ingrese en la terminal la frase "cd Do" y presione TAB dos o tres veces. La terminal nos muestra ahora dos carpetas, es decir "Documents" y "Downloads" debido a que no sabe aun a cual nos queremos dirigir. Probamos con una letra mas e introducimos "cd Dow" seguido de la tecla TAB. Ahora la terminal autocompletó nuestro comando.

Cuando el nombre de una carpeta o archivo contiene espacios, se deben indicar los espacios de manera especial. Suponga que creó una carpeta de nombre *Mis archivos.* Para llamar esta carpeta se debe señalar como sigue:

```
$  cd Mis\ archivos/
```

Para evitar esta dificultad podemos pedir autocompletar (TAB) cuando tecleemos sus primeras letras, o bien podemos usar comillas:

```
$ cd "Mis archivos"
```

COPIAR

Para copiar archivos, usamos el comando "cp". Ingresamos primero el nombre del archivo seguido de la carpeta a la cual lo queremos copiar. Probemos copiando el archivo *examples.desktop* desde nuestra carpeta "home" a la carpeta "Music":

```
$ cp examples.desktop Music
```

BORRAR

Para eliminar, la terminal cuenta con el comando "rm". Vayamos a la carpeta del ejemplo anterior ("cd Music") e ingresamos el comando para borrar el archivo que recién copiamos:

```
$ rm examples.desktop
```

Regresamos a nuestro "home" y limpiamos nuestra terminal para poder trabajar con mayor facilidad:

```
$ cd ..

$ clear
```

EXPLORAR LOS CONTENIDOS DE UN ARCHIVO

Muchos usuarios tienen que trabajar con archivos grandes que hacen que los editores de texto no puedan cargar en nuestro ambiente gráfico. En la terminal, podemos utilizar el comando "cat" que nos muestra el contenido de un archivo

sin consumir muchos recursos.

Pruebe con el archivo "leer.txt", que le fue enviado junto con esta guía. Después de copiarlo a su carpeta home, o cualquiera que desee, introduzca el comando:

```
$ cat leer.txt
```

LAS TUBERÍAS O "PIPELINES"

La terminal nos da flexibilidad al utilizar los comandos ya que los podemos "encadenar" para que trabajen juntos de la forma que queremos. Esto lo podemos lograr con el símbolo de barra vertical ("|") entre cada uno de ellos. Pongamos un ejemplo con el comando de filtrado ("grep"). Desde su carpeta home ingrese:

```
$ ls | grep Do
```

El comando "ls" nos regresaría los contenidos de la carpeta, pero usando una tubería ("|") le pedimos que envíe ese contenido a la función "grep", que aplica el filtro y nos regresa solo aquello que contenga "Do", es decir "Documents" y "Downloads".

Podemos hacer lo mismo con "cat". Ingrese la siguiente instrucción para filtrar el correo electrónico en el archivo leer.txt:

```
$ cat leer.txt | grep @
```

Por la arroba, la función grep filtró la línea que contiene nuestro e-mail.

SOFTWARE INCLUIDO EN UBUNTU

En el menú del sistema podrá ver que puede usar los paquetes de Libre Office, equivalentes a Microsoft Office. Lo que debe tener en cuenta es que Libre Office en Linux trabaja con sus propios formatos y si desea que un archivo que creó sea leido por usuarios de Windows/Word, debe guardar el archivo en el formato que se desea. Esto se hace en "Save As..." o "Guardar como..." desde Write, Calc o cualquier herramienta de Libre Office que estemos utilizando: solo especifique el formato antes de guardarlo.

Por otro lado, los archivos de Windows como documentos de Word, Excel y demás, son leídos sin ningún problema por Libre Office y otras herramientas de Linux.

Si no localiza alguno de los símbolos en su teclado, pruebe la aplicación "Character Map" (Menú, Accesories) y en los scripts "Common" y "Latin" encontrará todos los caracteres requeridos. El editor de texto en Ubuntu es "gedit".

EL SISTEMA DE ARCHIVOS

En Linux, todo es una carpeta o un archivo. Si inserta una memoria USB, o un CD, estos son accesibles como carpetas. Desde su 'home' en la terminal, introduzca dos veces:

```
$ cd ..
```

Ahora se encuentra en la carpeta raíz. Enliste sus contenidos:

```
$ ls
```

Los directorios que muestra son los que contienen su sistema y debe tener mucho cuidado con ellos. Vayamos a uno:

```
$ cd media
```

Enliste el contenido de esta carpeta. Si tiene un CD, memoria o algún otro dispositivo montado, aparecerá en esta ubicación y podrá trabajar desde la terminal en el. Para volver a su carpeta principal:

```
$ cd
```

TECNOLOGÍAS Y SOFTWARE DE PRIVACIDAD

Es necesario dar algunas explicaciones en relación a ciertos conceptos que estaremos manejando con frecuencia.

IP.- Son las direcciones de nuestro equipo en Internet. Nuestra IP local o interna es la que nos identifica en nuestra red local (que utilizamos para acceder a Internet) y empieza: 192.168.#.#.

Nuestra IP externa tiene el mismo formato pero es variable en todas sus partes y es compartida por todos los equipos conectados a su red. Esta es la dirección que conocería Google si nos conectamos a sus servidores directamente.

VPN.- Para nuestro objetivo, VPN es simplemente el servicio que nos presta una empresa (que creemos favorece la comunicación libre y privada) en el cual nos ofrece sus servidores como intermediarios en nuestras conexiones. Como el tráfico lo enviamos y lo recibimos encriptado, exclusivamente con sus servidores, nuestro proveedor de Internet no puede ver o registrar nada mas que tráfico encriptado hacia el servicio de VPN, y nuestros destinos (ejemplo Google) solo verían una conexión desde una IP de la empresa. Como creemos que muchos de sus clientes estarán conectados de igual forma al servicio, es complicado relacionar el tráfico.

Para contar con verdadera privacidad, es importante investigar sobre el servicio que planeamos utilizar y sería mejor que contara con los siguientes beneficios:

- Forma de pago anónima (Bitcoin). No nos es de utilidad un VPN al que le debemos pagar con nuestra tarjeta de crédito o algún otro medio que revele nuestra información.

- El servicio de VPN debe incluir todos los protocolos y no solo el HTTP, es decir el protocolo del navegador. En la gran mayoría de los casos esto no es un problema.

- Política sobre registros ("No logs"). Claramente favorecemos a un servicio que no guarde en sus servidores nuestra IP, actividad y demás información. Como es difícil saber si estas empresas cumplen con su compromiso, debemos informarnos en foros y otros sitios sobre la experiencia de otros usuarios.

- Configuración de su servicio para "OpenVPN", software libre y de código abierto que utilizaremos para conectarnos con el servicio.

Mas adelante en esta guía veremos como recabar sin mayor esfuerzo esta información.

TOR.- Mención aparte merece Tor. Si el VPN es anonimato por una política empresarial, Tor es anonimato por diseño.

Tor es una red abierta, compuesta por voluntarios en la que su tráfico es encriptado y redirigido através de los equipos conectados a ella. Cuando nuestras computadoras trabajan en red de esta manera, funcionan como *nodos*. Veamos que camino seguiría con Tor nuestro tráfico a Google:

Usuario **> >** 1er nodo **> >** 2do nodo **> >** nodo final **> >** Google

1. El primer nodo solo ve tráfico encriptado y sabe la IP del usuario (si no estamos usando VPN antes) y la IP del segundo equipo. No conoce la IP del nodo final ni el destino de nuestro tráfico.

2. El segundo nodo conoce la IP del primer y del último nodo, no conoce la IP del usuario ni el destino del tráfico. Tampoco ve nuestro tráfico.

3. El último nodo conoce la IP del segundo, el destino de nuestro tráfico y lo podría ver si no estuviéramos utilizando un protocolo seguro a Google, como HTTPS.

El software de Tor elige cada vez diferentes caminos al azar, utilizando nodos diferentes y el diseño de esta tecnología, como se puede ver, solo le da acceso a cada nodo a la información estrictamente necesaria para que funcione la red.

Aunque Tor nos permite mejorar nuestra posición de manera importante, debemos hacer dos señalamientos:

- Con frecuencia Tor está bloqueado en redes públicas y de banda ancha, por lo cual debemos utilizar un primer "puente" (como un VPN) para acceder.

- Acceder a Tor protege nuestra identidad, pero nuestro tráfico no será

bienvenido en muchos lugares ya que la IP del nodo final casi siempre estará boletinada ("Blacklist").

SOFTWARE DE VIRTUALIZACIÓN.- Es el software que nos permite correr máquinas virtuales dentro de nuestro Sistema Operativo principal (llamado "Host"). Imagine Windows 7 corriendo dentro de una ventana de su sistema Linux.

Utilizar máquinas virtuales nos da grandes ventajas:

1.- Se generan nuevos números de serie para los componentes de nuestro equipo: de esta manera no tememos a que alguna entidad los lea.

2.- Las máquinas virtuales no son mas que archivos en un ambiente aislado, de manera que contamos con protección en el caso de que descarguemos algún troyano o virus en ellas.

Si ya tuvimos suficiente actividad en alguna máquina y no sabemos si sigue limpio su sistema, podemos borrarla sin problema pues es posible hacer varias copias con rapidez.

3.- Es posible encadenar nuestro tráfico de formas convenientes sin configuraciones complejas. Por ejemplo: podríamos encadenar nuestro servicio de VPN con Tor para desbloquear este último y hacer mas fuerte nuestra privacidad.

Existen dos buenas opciones en el software: Virtualbox y VMWARE. Esta guía se enfocará en **Virtualbox** pues funciona adecuadamente y es código abierto. El código de VMWARE es cerrado por lo tanto no nos da las garantías que sí ofrece Virtualbox.

INSTALANDO OPENVPN

Aunque muchas de las compañías de VPN ofrecen su propio software que nos facilita la configuración, preferimos utilizar desde luego software confiable. Hay varias maneras de instalar OpenVPN pero le pedimos limitarse a la siguiente, desde la terminal:

```
$ sudo apt-get install network-manager-openvpn
```

Instalando este paquete en particular, nos habilita para manejar la configuración de OpenVPN desde nuestro manejador de redes.

UTILIZANDO EL VPN

Este es el procedimiento mas común con un servicio de VPN:

1.- Pagar el tiempo que queremos de servicio con Bitcoin.

2.- Generalmente se descarga un archivo ZIP que incluye la configuración, la llave de encripción y certificados. Extraemos sus contenidos y al archivo de configuración lo debemos editar y agregarle al final, con cuidado la línea:

```
redirect-gateway def1 bypass-dhcp
```

Es importante esta línea pues asi todo tipo de tráfico será enviado al VPN y no solamente el del explorador. No olvide los guiones.

Guardamos los cambios y damos click en el manejador de redes (el ícono de las dos pequeñas PCs en la barra) y luego "VPN connections", después "Configure VPN". Click en el botón "Import" y elegimos el archivo de configuración que acabamos de alterar. Dé click en "Save".

Debe aparecer la nueva conexión: nuevamente en el escritorio nos vamos al ícono del manejador, una vez mas a "VPN connections" pero ahora damos click en el nombre de nuestro VPN. Esperamos a ver el mensaje que nos avisa que nos hemos conectado con éxito.

INSTALANDO VIRTUALBOX

La mejor manera de descargar e instalar nuestro software de virtualización también es desde la terminal:

```
$ sudo apt-get install virtualbox
```

ACCEDER A LA RED DE TOR CON "WHONIX"

¿Cuál es la mejor manera de conectarnos a la red de Tor? Le sugiero que utilice **Whonix,** un sistema enfocado a usuarios que quieren proteger su identidad. Como siempre, es un proyecto libre y de código abierto.

En realidad Whonix, mas que un sistema, es una plataforma que debe correr en máquinas virtuales y consta de dos sistemas:

- El "Gateway", que "Torifica" todo el tráfico que le enviamos, es decir se encarga de prepararlo y encriptarlo para dirigirlo por Tor. Esto significa que podemos trabajar cómodamente sin necesidad de configurar cada paso que damos con Tor, como sería el caso sin el Gateway.

- El "Workstation", que sería el sistema regular en el que trabajamos con el explorador, cliente de email, Bitcoin, etcétera. Envía todo al Gateway y está diseñado para ofrecer seguridad.

Ambos se utilizan en una máquina virtual desde Virtualbox y primero debemos correr el Gateway esperando que se conecte a Tor. Una vez conectado, podemos iniciar el Workstation para que conecte (localmente claro, en nuestra máquina) con el Gateway.

Solo para ilustrar un poco mas las bondades del "Gateway": podemos Torificar Windows, Mac o cualquier sistema entero que configuremos correctamente para enviarle el tráfico y nos podemos olvidar de complicaciones.

Para descargar la plataforma Whonix, visite el sitio *whonix.org* y haga click en "Downloads". Descargue los archivos: Whonix-Gateway-8.2.ova y Whonix-Workstation-8.2.ova

Estos archivos OVA son similares al archivo ISO de Ubuntu que descargamos para instalar nuestro sistema. Le pedimos limitarse a la versión 8.2 pues las mas recientes aun se encuentran en fase de prueba.

INSTALANDO WHONIX EN VIRTUALBOX

Whonix-Gateway

Además de cargar los archivos-imagen a un CD o USB, podemos también utilizarlos en una máquina virtual. Abra el software de Virtualbox (Accesories) y en el menú dé click en "File", después "Import Appliance" y luego click en "Choose". Elija en su disco el archivo Whonix-Gateway-8.2.ova y en la siguiente ventana checamos el recuadro "Reinitialize the MAC address of all network cards". Haga click en "Import" y por último en "Agree".

Asegúrese de no estar conectado a Internet para proceder

En este punto la máquina ha sido creada y vemos que aparece el Whonix-Gateway en el manejador de Virtualbox. Haga click en su nombre y enseguida click en "Settings". En la nueva ventana nos vamos a la pestaña "System" y aqui centramos nuestra atención en la barra deslizadora de la memoria, o "Base Memory". Cualquiera que sea la cantidad de memoria que tenga asignada (768?) la cambiamos a 256 MB. Con esto automáticamente el Gateway sabe que no debe iniciar el ambiente gráfico y el uso de Whonix será mucho mas rápido.

Click en "Ok", elegimos una vez mas la máquina en el manejador y luego al ícono "Start", el de la flecha verde. La máquina debe iniciarse y antes debe saber que para trabajar con ella es importante su tecla CTRL derecha: luego de trabajar dentro de su ventana, puede recuperar el cursor de su sistema principal presionando esta tecla.

Esperamos a que cargue. Como es la primera vez que corre esta máquina, Whonix debe ser preparado y el proceso demora un poco. Notará que el sistema realiza un primer reinicio y luego de cargar por segunda vez nos presenta ciertos avisos que nos quieren dar los desarrolladores. Damos enter en "Understood" (tenemos que usar las flechas en el teclado) hasta que nos pida que señalemos desde donde actualizaremos Whonix. Elegimos la opción 1 "Yes, automatically install updates from the Whonix team" y luego "1. Whonix stable repository".

En el diálogo siguiente también la opción 1 ("I'm ready to enable Tor") y cuando nos pregunte si debe conectarse a Tor, elegimos "Yes", aunque no tengamos conexión a Internet. Damos luego "Ok" un par de veces y nos mostrará un último aviso, "Tor was succesfuly reloaded".

Notará que Whonix-Gateway trata de conectarse con la red de Tor, que no logrará pues no tenemos conexión a Internet. Después de algunos intentos, terminaremos con la línea de terminal "user@host $" y debemos introducir el siguiente comando:

```
$ sudo shutdown -h now
```

Con este comando ordenamos al sistema apagarse, y es el único comando que

usaremos en el Gateway. Cuando ya trabaje para conectarse a Tor y simplemente quiera ordenar al Gateway apagarse luego de una sesión, sostenga su tecla CTRL y enseguida presione su tecla "C" para interrumpir y que nos dé una linea de terminal, en la cual usamos el comando anterior.

Whonix-Workstation

Vayamos ahora al Workstation. Impórtelo de la misma manera que el Gateway pero claro ahora elegimos el archivo Whonix-Workstation-8.2.ova

Nuevamente nos aseguramos de no tener conexión a Internet y no tener el Gateway corriendo. Damos click en "Start" y comienza nuestra máquina. Esta primera vez que corremos el Workstation es la única que lo hará solo: una vez configurado, debemos siempre iniciar el Gateway previamente y esperar a que se conecte a Tor antes de comenzar la máquina del Workstation.

Notará que el Workstation sigue un camino similar al Gateway: hace la preparación inicial y luego reinicia. Cuando el sistema vuelve a cargar, se dará cuenta de que en algún punto nos presenta la linea de terminal "user@host $" como si estuviera esperando algún comando de nosotros: ESTO NO ES ASI. Simplemente espere a que cargue la interfaz gráfica.

Una vez cargue, se dará cuenta que no es muy fácil trabajar en el Workstation si no maximiza su ventana. Vaya al menú y dé click en "View" y enseguida a "Switch to Fullscreen", en el mensaje solo click en "Switch". Ya podrá apreciar mejor el sistema y podrá notar la barra en la parte inferior, el escritorio, los íconos y demás. Para recuperar el mouse de su Host presione la tecla CTRL derecha. Deslice la barra hacia abajo hasta que le aparezca un menú.

En la interfaz gráfica correrá una terminal que nos presentará algunos de los avisos y preguntas del Gateway. Contéstelas de la misma manera. En este punto se intentará conectar localmente con el Gateway (que "Torificará" su tráfico) y desde luego no lo logrará pues no lo tenemos corriendo. Vaya a la parte inferior de la pantalla y ubique el botón del sistema, que contiene una "K". Click en el, luego "Leave", después "Shutdown" y enseguida "Turn off". Por último solo damos click en "Ok" en la pantalla que nos avisa que apagaremos nuestra máquina virtual.

USO DE WHONIX

Conecte con su VPN. En Virtualbox, inicie el Gateway y espere a que se conecte a Tor, es decir que le muestre el siguiente mensaje: "Tor Bootstrap Result: Connected to Tor". El Gateway no requiere de comandos (solo para apagarlo) de manera que en la línea "user@host $" usted solo debe seguir esperando.

Una vez se realice la conexión, inicie el Workstation. Nuevamente espere a que cargue la interfaz gráfica, no introduzca comandos en "user@host $". Cuando tengamos el escritorio, esperamos a que nos muestre el mismo mensaje: "Tor Bootstrap Result: Connected to Tor", solo que ahora lo mostrará en una ventana.

Vayamos al botón del sistema (el de la "K"), luego "Applications", enseguida "Internet" y por último click en "Web browser". En este navegador introduzca en la barra de direcciones el siguiente sitio: *check2ip.com*

El sitio *check2ip.com* nos dirá nuestra IP y otra información importante acerca de nuestra conexión. Si despliega el sitio, con toda seguridad Whonix está conectado a Tor pues el sistema exclusivamente envía el tráfico a esa red.

Aunque contamos con este explorador, es importante descargar el navegador oficial de Tor ("Tor Browser") ya que está configurado para proveernos de privacidad. Nos dirigimos desde el navegador que abrimos a la dirección *torproject.org/download/download-easy.html.en*

Nos presentará la página de descarga del navegador para GNU/Linux y damos click en el botón "Download". Nos aparece una ventana, seleccionamos "Save File" y aceptamos.

Abrimos una terminal. Desde la carpeta en donde guardamos el archivo, extraemos sus contenidos con el siguiente comando:

```
$ tar -xvf tor-browser-linux32-3.6.4_en-US.tar.xz
```

Si el nombre del archivo le parece largo para teclear, recuerde que puede pedir autocompletar con la tecla TAB una vez comience con las primeras letras.

Nos vamos a la carpeta en donde se extrajeron los archivos:

```
$ cd tor-browser_en-US
```

El nombre del archivo que iniciará el navegador de Tor es "start-tor-browser" y lo corremos con el comando "./" (un punto y una diagonal), seguido del nombre del archivo:

```
$ ./start-tor-browser
```

Para volver de una máquina virtual a su Host, presione la tecla CTRL derecha. Para apagar el Whonix-Gateway, de click en su ventana, presione CTRL+C, e introduzca el comando: $ sudo shutdown -h now

CONFIGURACIONES DE NUESTRO TRÁFICO

#1 – USUARIO **> >** VPN **> >** DESTINO

Esta es la mas sencilla de nuestras configuraciones y solo implica usar un VPN en nuestro Sistema Operativo principal (como ya vimos), aunque siempre debemos trabajar en máquina virtual.

#2 – USUARIO **> >** VPN **> >** VPN **> >** DESTINO

Podemos utilizar un segundo servicio de VPN y asi añadir protección extra. Esta configuración se logra simplemente utilizando el primer VPN en el Host (Sistema principal) de manera regular, y el segundo VPN lo agregamos de la misma forma pero en la máquina virtual. Es recomendable utilizar de nuevo Ubuntu en Virtualbox pues es mas sencillo configurar el VPN que en Whonix *(Ver en información adicional: Ubuntu en Virtualbox)*

Todo el tráfico que enviemos desde la máquina virtual seguirá esta configuración.

#3 – USUARIO **> >** VPN **> >** TOR **> >** DESTINO

Una configuración que nos da fuertes niveles de privacidad pues combinamos anonimato por política y anonimato por diseño. Seguimos con el VPN en el Host y después en dos máquinas virtuales, como ya se ha mostrado, corremos el Whonix-Gateway seguido del Workstation.

Todo el tráfico que enviemos desde el Workstation seguirá esta configuración.

#4 – USUARIO **> >** VPN **> >** VPN **> >** TOR **> >** DESTINO

Partiendo de la configuración #2, en la máquina virtual (también Ubuntu, no es Whonix en este caso) descargamos y corremos Tor Browser como se ha descrito. Asegúrese de estar conectado a ambos servicios VPN antes de correr Tor Browser. *(Ver en información adicional: Ubuntu en Virtualbox)*

PRÁCTICAS MAS IMPORTANTES DE UNA CONEXIÓN SEGURA

1.- Siempre trabaje dentro de una máquina virtual.

Cree una "copia maestra", es decir una máquina en la que exclusivamente instalará los paquetes que desea (como OpenVPN, Truecrypt, Bleachbit) y ya no será utilizada: solo la clonaremos para crear copias en las que si vamos a trabajar. Después de algunas sesiones y descargas podemos empezar a dudar de nuestra copia y facilmente la podemos eliminar. Es importante proteger el sistema principal y en el nos limitamos a administrar nuestros recursos.

En cuanto a Whonix, el Workstation está diseñado para aislarse de su sistema principal y lo protege contra fugas DNS.

Recuerde respaldar su información antes de borrar una máquina virtual.

2.- Cualquier configuración inicia primero con la conexión de su Sistema Operativo principal a un servicio de VPN.

Con esto logramos esconder nuestro tráfico a Tor (configuraciones 3 y 4) y desbloquearlo en las redes que lo censuran.

NOTA: Si su servicio VPN es conocido, podrá obtener información de sus políticas y la experiencia de otros usuarios. La desventaja es que será claro que usa VPN y ciertos negocios de cadena que ofrecen WiFi (como *Starbucks*) también tienen bloqueados los VPN (además de Tor). Para evitar esto habría que hacer arreglos adicionales.

3.- No acceda a Internet utilizando una red que pueda ser relacionada con usted.

4.- Tenga cuidado con su actividad y hábitos de navegación.

5.- Si pierde la conexión con su primer VPN (Host), detenga todo tráfico y sobre todo el de Tor antes de intentar una reconexión. De lo contrario sus aplicaciones (típicamente el navegador) podrían seguir intentando conectar pero sin pasar por el VPN y estaríamos fugando información a su proveedor de Internet. Vea el capítulo *Checar nuestras conexiones.*

ENCRIPCIÓN DE DATOS Y COMUNICACIONES

Existen dos tipos de encripción: simétrica y asimétrica. En la encripción simétrica nuestra información es encriptada y descifrada *con la misma llave*, de manera que tendríamos que encontrar un canal seguro para hacérsela llegar a un destinatario.

Mas moderna es la encripción asimétrica, en la que son generadas dos llaves. Una de estas llaves es la *pública,* que compartimos sin problema con los demás para que con ella encripten cualquier mensaje que nos quieran hacer llegar.

La otra llave es la *privada,* con la que nosotros desciframos los mensajes y desde luego es muy importante protegerla y no compartirla.

Estos algoritmos están diseñados para que no se pueda obtener la llave privada desde la llave pública, aunque es importante cerciorarnos que utlizamos una encripción sólida.

Los expertos en criptología recomiendan como encripción suficiente:

- En la encripción simétrica, se pueden utilizar los cifrados AES – Twofish – Serpent en cascada, de 256 bits. En el algoritmo de hasheo se puede utilizar el Whirlpool.
- En la asimétrica, RSA de 4096 KB.

ENCRIPCIÓN SIMÉTRICA: TRUECRYPT

Truecrypt tiene una historia muy particular. Es una herramienta libre y de código abierto que fue desarrollada hace algunos años por partidarios de la privacidad. Con el tiempo llegó a la versión 7.1a, que fue ampliamente utilizada por activistas, periodistas, informantes y toda persona que quería proteger su información. El mismo Edward Snowden recomendó su uso y existen casos interesantes en torno a Truecrypt:

- Daniel Dantas, banquero brasileño acusado de delitos financieros fue detenido en poder de volúmenes encriptados de Truecrypt que el gobierno de Brasil y posteriormente el FBI fallaron en crackear.

- David Miranda, asociado del periodista Glenn Greenwald fue detenido también con información protegida por Truecrypt en el aeropuerto de Londres. Se cree que esos volúmenes contenían documentos filtrados por Edward Snowden y al parecer han intentado crackearlos sin éxito.

Todo lo anterior nos sugiere que Truecrypt es una herramienta eficaz y segura de utilizar, sin embargo algo extraño sucedió a finales de Mayo de 2014: el sitio de Truecrypt amaneció con un aviso de sus desarrolladores en el que decían que la aplicación no era segura, que utilizaran BitLocker de Microsoft y que ponían a disposición una nueva versión, la 7.2, en la que solo se puede descifrar, mas no encriptar.

Esto generó muchas dudas, pues el código siempre fue abierto, recomendado por Snowden y además el mismo FBI ha fallado para crackear volúmenes encriptados de Truecrypt 7.1a. Ciertas teorías fueron discutidas respecto al caso:

- Sus desarrolladores fueron identificados y presionados por algún gobierno lo que causó que no quisieran seguir con el proyecto.
- Fueron sobornados para sabotear su propia creación.
- Existieron diferencias entre ellos, lo que propició la suspensión del proyecto.

Cualquiera que haya sido el caso, una legión de programadores se agrupó en un sitio en el que se auditó el código de Truecrypt y hasta el momento se ha concluido que Truecrypt 7.1a sí es seguro de utilizar.

El archivo que los auditores han hecho disponible para Linux está en la dirección: *github.com/AuditProject/truecrypt-verified-mirror*

En esta página verá que hay varias carpetas, dependiendo el Sistema Operativo. Dé click en "Linux" y el sitio nos mostrará los instaladores. El archivo que debemos descargar es *truecrypt-7.1a-linux-x86.tar.gz*

Damos click en el y enseguida en "View the full file" para descargarlo.

INSTALANDO TRUECRYPT

Una vez descargado, abrimos una terminal y nos dirigimos a la carpeta donde se guardó el archivo. Desde ahi extraemos sus contenidos:

```
$ tar -xvf truecrypt-7.1a-linux-x86.tar.gz
```

Extraerá un solo archivo, de nombre *truecrypt-7.1a-setup-x86* y este mismo corremos para iniciar la instalación:

```
$ ./truecrypt-7.1a-setup-x86
```

Accedemos en los avisos del asistente y continuamos hasta que finalice la instalación. El programa ahora se puede encontrar en el menú del sistema o alternativamente lo podemos llamar desde la terminal: $ truecrypt

ENCRIPTANDO CON TRUECRYPT

Truecrypt funciona creando volúmenes encriptados que se pueden montar y desmontar en nuestro sistema Linux, como si fuera otro disco o un USB. Estos volúmenes pueden ser archivos, particiones, discos y memorias enteras, etc.

Para crear un archivo-volumen, haga click en "Create volume", luego elegimos "Create an encrypted file container", "Standard Truecrypt Volume" y enseguida en la ventana siguiente debemos de introducir el nombre del archivo: click en "Select File", seleccione la carpeta que quiera e ingrese el nombre del volumen en "Name".

En las opciones de encripción, escogemos la opción "AES – Twofish – Serpent" y para el hash elegimos "Whirlpool". Seguimos y en el siguiente paso hay que especificar el tamaño que queremos para nuestro volumen. Si gusta, probamos primero con 1 MB.

Nos pedirá nuestra clave que utilizaremos para acceder a nuestra información y note que tenemos la opción de utilizar un archivo (de cualquier tipo) como llave adicional, es decir el botón "Keyfiles". Si bien esto haría mas segura nuestra encripción, le pedimos tener cuidado dado que la pérdida de un archivo-llave implica la pérdida de su información. Supongamos que eligió como *Keyfile* una fotografía de su mascota: si un solo pixel de ese archivo es modificado, Truecrypt no podrá abrir el volumen. ¿Cómo repondrá el archivo? ¿O un archivo de sonido?

Por el momento solo usamos una contraseña y se le sugiere que sea una mezcla de letras, números y símbolos. Una buena práctica es utilizar frases como:

misitio#1!google.com!
cuantos_perros_tengo?2

Repetimos la clave y en el tipo de volumen seleccionamos "Linux Ext 4". En el paso que sigue nos vamos con la opción "I will mount the volume only on Linux".

Llegamos al final y Truecrypt nos pide que movamos nuestro cursor, dentro de su ventana, de manera azarosa para poder hacer mas fuerte la encripción. Hacemos esto por unos 20 segundos y luego damos click en "Format". Si todo fue bien, nuestro volumen fue creado.

ACCEDIENDO A UN VOLUMEN DE TRUECRYPT

En la ventana principal de Truecrypt, damos click en el botón "Select file". Escoja el archivo de Truecrypt que acaba de crear, click en "Open". Note los espacios o "Slots" que abarcan gran parte de la ventana. Haga click en uno de ellos y enseguida en "Mount". Le pedirá su contraseña.

El archivo-volumen es montado. Damos doble click en el y podemos ver sus contenidos: esta vacío. Simplemente podemos crear archivos y guardarlos ahi o

copiar/descargar archivos a el. Cuando terminemos de trabajar, seleccionamos el volumen en la sección de "Slots" y damos click en "Dismount".

Atención: los volúmenes de Truecrypt solo se pueden desmontar desde la aplicación misma y no en el navegador de archivos.

Un beneficio interesante que se obtiene al trabajar con esta herramienta, es el poder descargar o copiar *directamente* archivos a los volúmenes de Truecrypt: asi el archivo en su disco solo ha existido encriptado. Es decir, todo lo que necesitamos para proteger archivos sin mayor esfuerzo es copiar archivos a nuestro volumen.

UTILIZANDO ARCHIVOS-LLAVE EN TRUECRYPT

Si considera la opción de utilizar *Keyfiles* a la hora de crear el volumen, le recomendamos que sea texto pleno. Escoja alguna frase, párrafo o texto que sea significativo para usted e intróduzcalo en un archivo. Recuerde bien la puntuación que utilizó, los espacios, acentos, mayúsculas y demás. Un solo caracter que varíe hará imposible descifrar, en el caso de que pierda el archivo y lo intente reponer.

Cuando elabore el archivo-llave, repita el proceso manualmente dos veces y si estos dos archivos devuelven el mismo hash MD5, probablemente ya tiene usted un archivo que podrá reponer si lo llega a perder. Asegúrese de poder replicar un archivo-llave antes de utilizarlo.

```
$ md5sum llave1.txt
```

Lo mismo con el segundo archivo y si nos regresa lo mismo, hemos replicado con éxito nuestro archivo-llave.

¿Cuál sería la mejor forma de guardar este archivo? Una buena opción es hacer varias copias en distintos USB, mezclado con otros archivos. Cuando quiera acceder a su información, introduzca la memoria y no copie el archivo a su disco duro: simplemente elegimos desde Truecrypt el archivo en el USB y desde ahi el programa lo lee. Una vez tengamos acceso al volumen, removemos nuestra memoria.

ENCRIPCIÓN ASIMÉTRICA: PGP

El software para utilizar PGP viene incluido en el *Whonix-Workstation* y es el paquete "KGpg". En el escritorio puede encontrar su ícono, y para abrirlo damos doble click en el.

En el menú nos vamos a "Settings" y luego "Configure KGpg". En la ventana de configuración nos vamos a la pestaña "GnuPG Settings" y deshabilitamos la opción "Use GnuPG agent".

Vamos a generar un par de llaves y para eso en el menú damos click a "Keys" y en seguida "Generate Key Pair". En el siguiente paso debemos introducir nuestro seudónimo o nombre, e-mail y opcionalmente un comentario. Elegimos el algoritmo RSA y en "Key Size" indicamos que nuestra llave será de 4096. Click en OK.

Ahora que tenemos nuestro par de llaves, podemos ver en la ventana principal una entrada con nuestros datos. La seleccionamos y luego damos click en el ícono que dice "Export Public Key". En la ventana siguiente las opciones "File" y "Export Everything" deben estar habilitadas y como puede ver, tiene la opción de elegir a que carpeta exportar y el nombre del archivo. Click en OK.

Su llave pública fue guardada en este archivo y ahora la puede compartir con sus amigos para que con ella encripten mensajes para usted. Sus datos también van incluidos, por lo tanto no es necesario proveerlos junto con su llave pues el software de sus contactos los va a leer de esta.

Para **encriptar** con KGpg, debe importar primero la llave pública de la persona a quien desea enviar un mensaje. Dé click en "Import key" y elija el archivo en donde tiene guardada la llave.

En la ventana principal, nos vamos a "File" y luego "Open editor". Una vez tengamos la ventana del editor, introducimos nuestro mensaje y hacemos click en "Encrypt", en la parte inferior. Aqui seleccionamos la llave de la persona a quien queremos contactar, enseguida hacemos click en "Options" y checamos "Allow encryption with untrusted keys". Aceptamos, y la versión encriptada de nuestro mensaje debe aparecer. Este mensaje lo podemos enviar por e-mail o bien guardarlo en un archivo utilizando un editor de texto. El editor de texto en Whonix es "KWrite" y se le puede localizar en el menú del sistema, Applications y luego en Utilities.

Para **descifrar** un mensaje encriptado que nos han enviado, simplemente volvemos a abrir el editor como se explica arriba, pegamos el mensaje y ahora damos click en "Decrypt". KGpg nos pedirá nuestra contraseña para que la aplicación pueda accesar nuestra llave privada y el mensaje ya debe aparecer descifrado.

COMBINANDO TRUECRYPT Y PGP

Decíamos que si utilizamos encripción simétrica (Truecrypt), tendríamos que encontrar un canal seguro para enviar la llave a un destinatario que quiera acceder a los volúmenes. Si esta persona utiliza PGP, podemos utilizar su llave pública para encriptar la contraseña y envíarle el mensaje encriptado junto con el volumen.

INFORMACIÓN ADICIONAL

COMO ACCEDER A INTERNET

Lo ideal sería conectarnos através de las redes de banda ancha 3G. Si en su pais es permitido adquirir (sin trámite) un dispositivo 3G para USB y su chip respectivo, puede accesar de esta manera pero es la opción mas costosa.

Mucho mas económico resulta:

- Utilizar redes inalámbricas abiertas o de negocios de cadena.
- Conectarse desde cyber-cafés o negocios de Internet.

Si decide utilizar WIFI o cable directo, es recomendable cambiar la dirección MAC de su tarjeta antes de intentar la conexión. Para esto deberá utilizar el paquete *macchanger.* Consulte Google para mas información.

CHECAR NUESTRAS CONEXIONES

PING

Hay un método muy rápido y eficaz para saber si tenemos conexión a Internet, a nuestro VPN, a Tor, etc. Solo necesitamos usar la terminal para enviar un simple "ping" a Google, que tiene una gran cantidad de servidores por todo el mundo:

```
$ ping google.com
```

Si podemos recibir la respuesta de Google a nuestro ping, existe conexión. Si la consola se queda en suspenso y no vemos llegar los paquetes, es que no seguimos conectados. Existen diferentes escenarios a considerar:

- Si en su Sistema Operativo principal, sin conexión a VPN, no recibe paquetes del ping, es que ha perdido la conexión a Internet.

- Si la conexión a Internet le devuelve paquetes pero luego de la conexión a su VPN, el ping falla, es que perdimos la conexión a nuestro VPN.

- Si los anteriores pings fueron exitosos pero después dentro del Workstation usted corre un ping en su terminal y no devuelve paquetes, está fallando algo con Tor.

Una vez la función le devuela un par de paquetes de Google, presione CTRL+C para terminar el ping.

Ping también es útil para 'mantener viva' una conexión: si su servicio de VPN es impaciente con su inactividad, puede dejar el ping correr un momento para hacerle saber que seguimos del otro lado de la línea. Esto se da sobre todo mientras esperamos que inicien las máquinas virtuales de Whonix.

El sitio *check2ip.com* nos da información de nuestra IP y otros datos de nuestra conexión. Corra el navegador y visite este sitio para verificar su conexión (desde el sistema principal, Virtualbox, etc, según necesite).

BLEACHBIT

Este software nos es de utilidad, pues limpia nuestro sistema de datos que ya no deseamos y además utiliza métodos de sobre-escritura para hacer muy dificil la recuperación de esos archivos. La instalación es la mas simple:

```
$ sudo apt-get install bleachbit
```

Abrimos el programa, y antes de realizar alguna limpieza nos vamos en el menú a "Edit", luego click en "Preferences". En la ventana que nos aparece nos vamos a la pestaña General y ahi checamos la opción "Overwrite files to hide contents".

Podemos realizar una limpieza en las ubicaciones que nos muestra en la ventana, del lado izquierdo. Vemos que la puede realizar en Firefox (para limpiar las cookies), en el APT, el bash y otras que podemos checar. Después de elegir lo que queremos limpiar, hacemos click en el botón "Clean", luego "Delete".

Si queremos deshacernos de un archivo o una carpeta en específico, nos vamos a "File", luego "Shred files" (o folders) y elegimos el archivo que queremos borrar de forma permanente.

MAT

El "Metadata Anonymisation Toolkit" es un paquete que nos ayuda a *remover* de ciertos archivos la información que nuestro software guarda en ellos acerca del autor, fecha de creación, modificación, etcétera. Esto es útil para cuando queremos enviar estos archivos y no queremos que revelen mas que su contenido.

También tenemos incluida una copia de MAT en el Workstation, que buscamos en el menú del sistema, luego "Applications", y "Utilities". Cuando tengamos su ventana, damos click en el símbolo de suma de color verde para agregar el archivo y luego click en el ícono de la barredora para limpiarlo. La aplicación creará una nueva versión del archivo sin la información extra.

Debemos tener en cuenta que MAT solo trabaja con archivos que contengan esta *metadata*, de lo contrario nos dirá que no puede trabajar en el.

COMO USAR GOOGLE PARA CONOCER UN SERVICIO VPN

Decíamos que un VPN nos será útil si acepta pagos en Bitcoin, no registra nuestra actividad y nos ayuda a configurar su servicio en OpenVPN.

Usemos primero el filtro "site:". Con este filtro, le indicamos a Google que nos regrese resultados exclusivamente del sitio que queremos. Veamos si el servicio en cuestión acepta Bitcoin:

```
site:sitiovpn.com bitcoin
```

Veamos que nos dice de OpenVPN y luego de su políticas de privacidad:

```
site:sitiovpn.com openvpn
```

```
site:sitiovpn.com "no logs"
```

En la última búsqueda utilizamos comillas pues queremos que filtre esta frase exacta y no las palabras por separado.

Por último simplemente introduzca el nombre del servicio en el buscador y ponga antención a los resultados de las primeras páginas. Si obtiene información de que esta compañía no es tan seria como parecía serlo, busque otra opción.

Desde la terminal, podemos solicitar información del registro si corremos:

```
$ whois sitio.com
```

En 2014, al parecer las compañías siguientes son de considerarse:

azirevpn.com – blackvpn.com – bolehvpn.com – cryptovpn.com – cyberghostvpn.com – earthvpn.com – express-vpn.com – in-disguise.com – nordvpn.com – perfect-privacy.com – privateinternetaccess.com – purevpn.com – torguard.net – versavpn.com – zorrovpn.com

UBUNTU EN VIRTUALBOX

Como el formato del archivo-imagen de Ubuntu es ISO, no lo podemos importar directamente (a diferencia de Whonix) y debemos primero crear una máquina virtual.

En la ventana de Virtualbox damos click en "New", luego "Next". En la siguiente ventana le damos el nombre "Ubuntu". Para sistema operativo y versión introducimos "Linux" y "Ubuntu", respectivamente.

Recomendamos asignar 1536 MB de memoria (si cuenta con 3 GB o mas). En las siguientes ventanas solo damos "Next" hasta llegar a "Storage details", en donde seleccionamos "Fixed size". "Next" una vez mas y en el paso final damos click en "Create". Esperamos y cuando nos aparezca la ventana "Summary", una vez mas click en "Create".

En la ventana principal de Virtualbox, click en nuestra máquina recién creada y nos vamos a "Settings". Cuando apareza la ventana, damos click en la pestaña "Storage" y donde dice "IDE controller" damos click en "Empty". A la derecha aparecerá una sección que dice "Attributes" y "CD/DVD Drive" al lado de un ícono de un CD. Click en este ícono y luego "Choose a virtual CD/DVD disk file". Localizamos en nuestro disco el archivo ISO de Ubuntu y damos click en "OK". Ahora podemos iniciar esta máquina ("Start") y el asistente de instalación de Ubuntu comenzará.

Aqui acaba esta guía y solo reiterarles que estamos abiertos a sus preguntas o sugerencias:

Reddit.com/r/InformacionLibre
conexionsegura@safe-mail.net