

Comunicaciones Seguras

Tails

Rafael Bonifaz: rafael@bonifaz.ec

Tails

- Distribución GNU/Linux basada en Debian
- Orientada a la privacidad y anonimato
- Todo el tráfico de Internet viaja por Tor
- Live DVD/USB
- No guarda nada en el disco duro (Amnesia)
- Software libre

Principales herramientas de Tails

- Navegador de Tor
- Chat cifrado con Pidgin y OTR
- Correo electrónico a través de Icedove con enigmail
- Gestión de contraseñas con KeepassX

Persistencia

- Cada vez que se reinicia el equipo se pierde información y configuración
- Se puede crear una partición para persistencia dentro de la memoria flash
- La partición es cifrada con una contraseña
- Permite guardar datos, pero además la configuración de:
 - Conexión de redes wifi
 - Cuentas de pidgin
 - Cuentas de correo electrónico
- La memoria flash se puede utilizar en otro sistema operativo a través de la contraseña

Requerimientos

- Computador compatible con i386
- La posibilidad de arrancar el equipo desde DVD o preferentemente desde pendrive o SD
- Preferentemente 2 GB de memoria RAM

Proceso de instalación

- Seguir el tutorial desde la página web: descargar, verificar e instalar
- Verificar la imagen con el plugin de firefox o a través de PGP
- Instalar según el sistema operativo
 - En Debian existe el instalador
 - Se puede quemar un DVD
 - Desde un DVD se puede instalar en la memoria flash

Verificar Tails

- Sin tener la clave de Tails firmada

```
$ gpg --recv-key 98FEC6BC752A3DB6
```

```
$ gpg --keyid-format 0xlong --verify tails-i386-2.6.iso.sig tails-i386-2.6.iso
```

```
gpg: Firmado el mar 20 sep 2016 12:24:50 ART
```

```
gpg: usando RSA clave 0x98FEC6BC752A3DB6
```

```
gpg: Firma correcta de "Tails developers (offline long-term identity key) <tails@boum.org>"
```

```
gpg: alias "Tails developers <tails@boum.org>"
```

```
gpg: ATENCIÓN: ¡Esta clave no está certificada por una firma de confianza!
```

```
gpg: No hay indicios de que la firma pertenezca al propietario.
```

```
Huellas digitales de la clave primaria: A490 D0F4 D311 A415 3E2B B7CA DBB8 02B2 58AC D84F
```

```
Huella de subclave: BA2C 222F 44AC 00ED 9899 3893 98FE C6BC 752A 3DB6
```

Verificar Tails

- Con clave de Tails firmada

```
$ gpg --keyid-format 0xlong --verify tails-i386-2.6.iso.sig tails-i386-2.6.iso
```

```
gpg: Firmado el mar 20 sep 2016 12:24:50 ART
```

```
gpg: usando RSA clave 0x98FEC6BC752A3DB6
```

```
gpg: Firma correcta de "Tails developers (offline long-term identity key) <tails@boum.org>"
```

```
gpg: alias "Tails developers <tails@boum.org>"
```

```
Huellas digitales de la clave primaria: A490 D0F4 D311 A415 3E2B B7CA DBB8 02B2 58AC D84F
```

```
Huella de subclave: BA2C 222F 44AC 00ED 9899 3893 98FE C6BC 752A 3DB6
```


Tails Installer



To run Tails Installer you need an ISO image which can be downloaded from the Tails website: <https://tails.boum.org/download/>

Install

- Install Tails on a new USB stick.
- The USB stick that you install on is formatted and all data is lost.

Upgrade

- Upgrade a Tails USB stick to the version of an ISO image.
- The encrypted persistent storage of the Tails USB stick that you upgrade is preserved.

Need help? Read the [documentation](#)

Alternativas a Tails

- **Whonix:** conjunto de 2 máquinas virtuales que consiste en un gateway y un work station
 - <https://www.whonix.org>
- **SubgraphOS:** todavía no existe una versión estable, pero se puede probar.
 - <https://subgraph.com/sgos/>
- **Qubes OS:** Una distribución que separa aplicaciones a través de máquinas virtuales XEN
 - <https://www.qubes-os.org/>

Migrar cuentas a Tails

Aplicación	Desktop	Tails
Tor Browser	Exportar en formato .json en la carpeta Persistent de la memoria flash	Importar el archivo .json desde la carpeta <code>~/TorBrowser</code>
KeepassX	Copiar archivo de contraseñas a la carpeta Persistent de la memoria flash	Abrir archivo de contraseñas
Icedove / Enigmail	<ul style="list-style-type: none">• Exportar llaves públicas y privadas desde Thunderbird/Icedove o gpg• Anotar información de configuración. Usuario servidores, etc.. (KeepassX)	<ul style="list-style-type: none">• Configurar Icedove con los datos de la cuenta• Importar llaves públicas y privadas desde Enigmail• Configuración se guarda en
Pidgin	- Copiar los archivos otr* desde la carpeta <code>~/purple</code>	Pegar los archivos en la carpeta