

SISTEMA OPERATIVO
SEGURO CON

Tails

the **amnesic** incognito **live** system



colectivo
disonancia

| ¿QUÉ ES TAILS?

Es un sistema operativo portátil, basado en Debian GNU/Linux, diseñado para mantener un **anonimato** considerable y la **seguridad** en la información. Funciona como un *live system*, es decir, que el sistema operativo se instala y ejecuta desde una memoria USB, por lo que **no requiere instalarse en un computador**.



AMNÉSICO

Cuando Tails se ejecuta, no utiliza el disco duro del computador, sino sólo la memoria RAM, que se borra una vez apagado el dispositivo. De esta manera, **el uso de Tails no deja huella o registro de lo que se hizo** en el computador ni en la memoria USB.

Solamente de manera opcional se puede crear un compartimento cifrado en la memoria USB para almacenar permanentemente alguna información.



HERRAMIENTAS

Tails es un sistema operativo que ya cuenta con varios programas instalados y listos para usar, como el navegador Tor; OnionShare, para compartir archivos; Thunderbird, para gestionar correos, entre otros.

Esto hace de Tails **un sistema operativo para uso inmediato**, sin requerir demasiadas configuraciones.



PORTÁTIL Y CONFIABLE

Una vez instalado en una memoria USB, **puede usarse con seguridad en un cualquier computador**, sea personal o no. Esta portabilidad es confiable ya que, como Tails está hecho con Software Libre, entrega las garantías suficientes para saber que su código fuente no oculta programas maliciosos ni rastreo del usuario.



PODEMOS USAR TAILS PARA:

> _DENUNCIAS, PERIODISMO DE INVESTIGACIÓN Y FILTRACIONES

Manejar documentación sensible o realizar filtraciones y denuncias de elevado riesgo requiere de un entorno digital confiable como Tails para tener la seguridad necesaria.



PODEMOS USAR TAILS PARA:

> **_CASOS DE PERSECUCIÓN POLÍTICA**

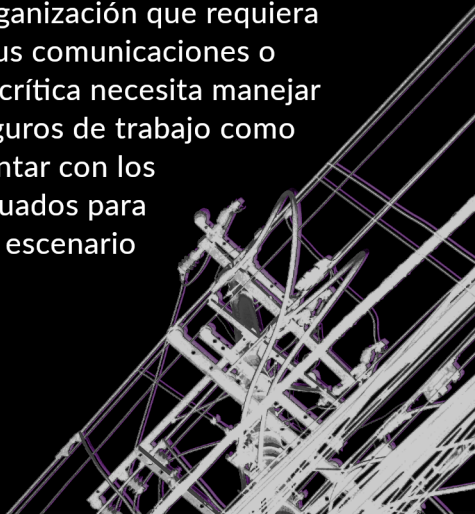
El hostigamiento y la amenaza política obliga a quienes enfrentan esa situación a proteger la actividad que realizan en la red, evitando dejar huellas en ella.



PODEMOS USAR TAILS PARA:

> **_RESGUARDO CRÍTICO ANTE AMENAZAS**

Cualquier organización que requiera resguardar sus comunicaciones o información crítica necesita manejar entornos seguros de trabajo como Tails para contar con los medios adecuados para enfrentar un escenario amenazante.



Asumir la vigilancia masiva y la persecución política implica que debemos **manejar distintas estrategias** de autodefensa digital.

Por esto, es relevante considerar Tails como una herramienta indispensable para **protegernos colectivamente cuando necesitamos** trabajar con información sensible o al evitar al máximo los riesgos en nuestras comunicaciones.

Más información sobre Tails y cómo instalarlo se encuentra en su sitio web:



<https://tails.boum.org/>