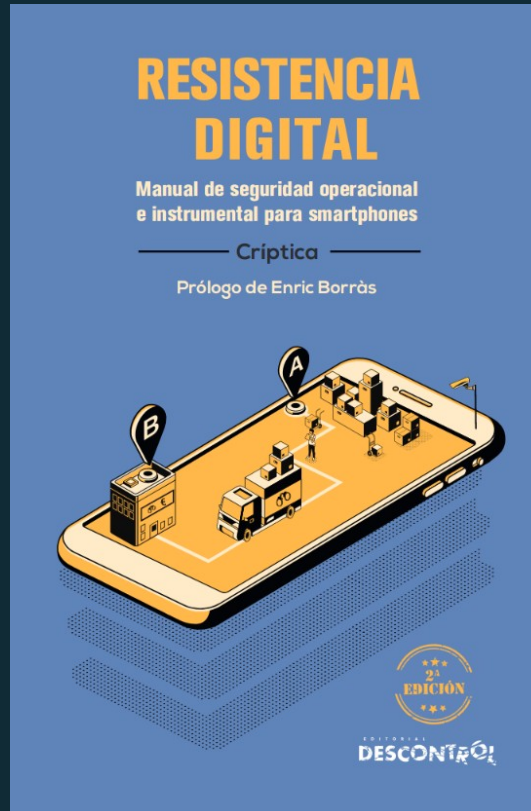


# Resistencia Digital

Manual de seguridad operacional e instrumental para smartphones



Carlos Fernández  
RootedCon 2020



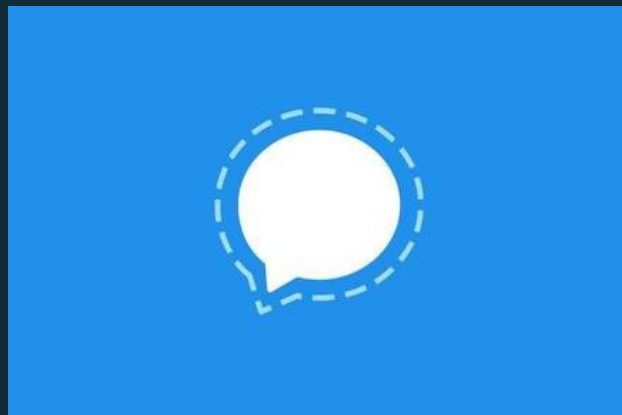
# Acerca de Críptica

- Asociación cultural fundada en 2015
- Sin ánimo de lucro
- Eventos, materiales y formaciones de privacidad
- El año pasado publicamos el libro *Resistencia Digital: Manual de seguridad operacional e instrumental para smartphones*



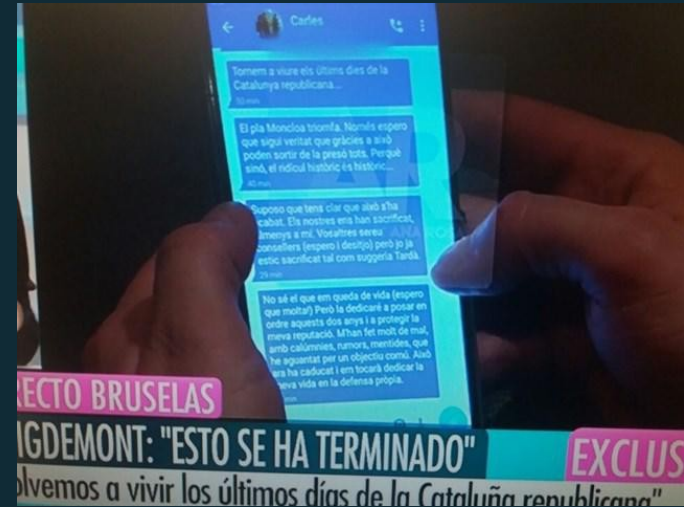
# Seguridad Instrumental

La que se consigue a través del uso de herramientas seguras



# Seguridad Operacional (OPSEC)

La que se consigue a través del uso de hábitos seguros



# Perspectivas en el libro

- Seguridad operacional e instrumental
- Cinco autores con experiencia, conocimiento y puntos de vista diversos

## **Carlos Fernández**

Analista de seguridad informática.

## **Enric Luján**

Profesor de Ciencia Política en la UB y estudiante de doctorado en temas de filosofía y tecnología.

## **Rocío Moreno**

Enfermera, apasionada de la informática y las nuevas tecnologías.

## **Víctor Rizo**

Desarrollador de software (acdb6c6bee7a0d27ce100d1a-b60ff1c7).

## **Eduard Sanou**

Desarrollador e impulsor del software libre.

# Altamente accesible

- Versión física por 12€. Publicado bajo licencia Creative Commons (CC BY-NC-ND)
- Disponible gratis en versión digital
  - PDF: [https://www.criptica.org/material/resistencia\\_digital.pdf](https://www.criptica.org/material/resistencia_digital.pdf)
  - EPUB: [https://www.criptica.org/material/resistencia\\_digital.epub](https://www.criptica.org/material/resistencia_digital.epub)
  - MOBI: [https://www.criptica.org/material/resistencia\\_digital.mobi](https://www.criptica.org/material/resistencia_digital.mobi)



¿Por qué?





# 2013-2015: Revelaciones de Edward Snowden

TOP SECRET//SI//NOFORN

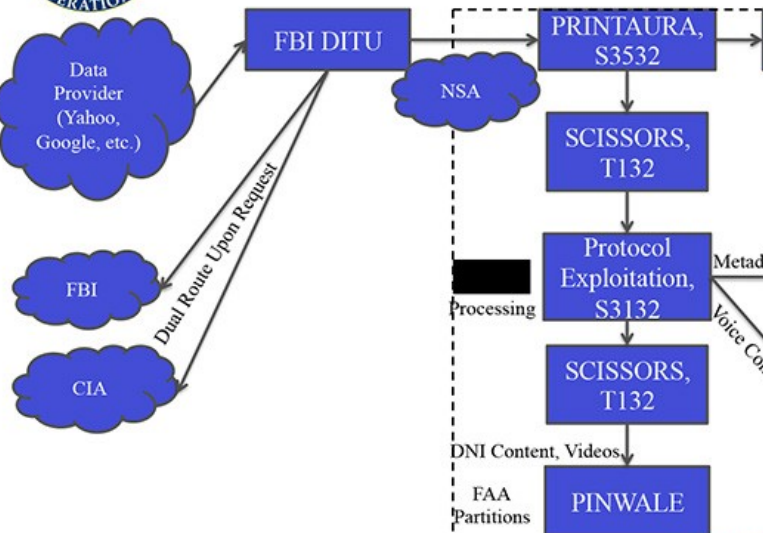


## Current Efforts - Google

TOP SECRET//SI//ORCON//NOFORN

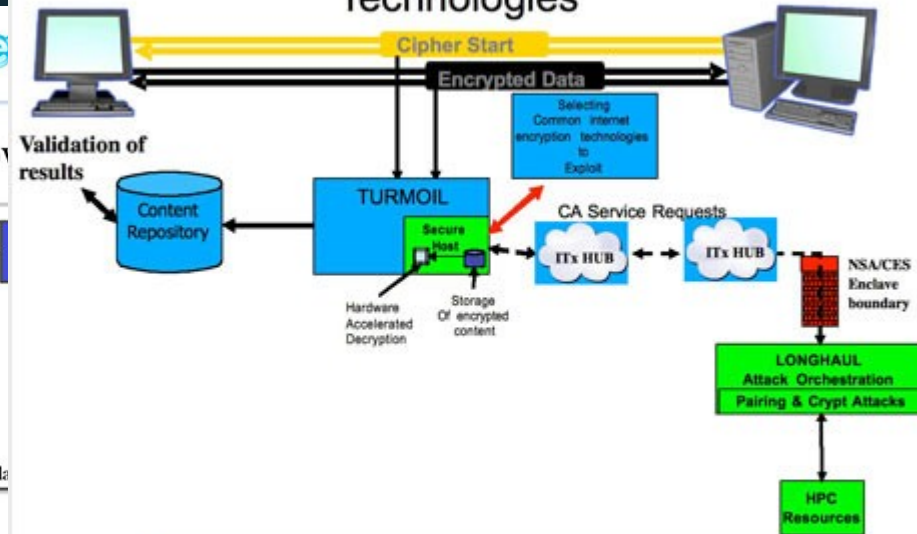


## (TS//SI//NF) PRISM Collection Dataflow



TOP SE

## Exploitation of Common Internet Encryption Technologies



TOP SECRET//SI//REL TO USA, FVEY//2013//NF

TOP SECRET//SI//ORCON//NOFORN



Yo no soy nadie. No tengo nada que esconder.

# Tras la frase...

- Idea errónea: Sólo los “malos” tienen cosas a esconder y yo no soy malo.
- ¿Malo para quién? Para quien ostenta poder, cualquier persona que le desafía gana la etiqueta de “malo”: Activista, disidente político, periodista de investigación...
- No sabes cómo te afectará mañana la información que generas hoy
- Derecho a la intimidad

# Intimidad

- Tenemos derecho a una vida privada
- ¿Por qué cierras el pestillo del baño?
- ¿Vivirías en una casa de cristal?
- ¿Me dejarías conocer todos tus problemas personales, familiares amorosos?
- ¿Por qué no me dejas leer tus mensajes, analizarlos y compartirlos con quien yo quiera?
- ¿Puedo seguirte por la calle todo el día?
- **¿Acaso tienes algo que esconder?**

# Privacidad como garante de otros derechos

- La vigilancia condiciona nuestras libertades:
  - Comportamiento
  - Reunión
  - Asociación
  - Expresión
  - Pensamiento
- En definitiva: La privacidad es fundamental para una sociedad democrática



# ¿Nada que ocultar?



***“Decir que no te preocupa la privacidad porque no tienes nada que ocultar es como decir que no te preocupa la libertad de expresión porque no tienes nada que decir”.***

**E. Snowden**

¿Está todo perdido?

# Hay esperanza

## Open Source Privacy Tools NSA Can't Crack: OTR, PGP, RedPhone, Tor And Tails

By [Lucian Armasu](#) December 30, 2014

US & WORLD

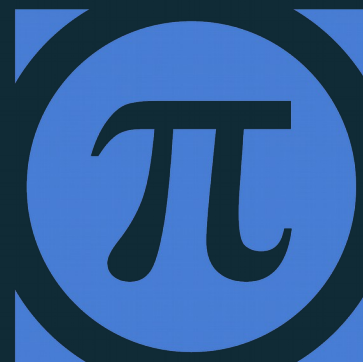
## New documents reveal which encryption tools the NSA couldn't crack

By [Russell Brandom](#) | Dec 28, 2014, 6:23pm EST

Source [Chaos Computer Club Conference 2014](#) and [Der Spiegel](#)



# Defensa: Manos a la obra



LA QUADRATURE DU NET



privacytools.io

# 2015-2018: Lo que aprendimos de dar talleres

- Las cosas muy técnicas no se entienden: PGP, OTR, criptografía asimétrica, firmar, validar firmas...
- Si las herramientas no son seguras por defecto y fáciles de usar, se acaban usando mal en algún momento
- Es importante saber de qué quieres protegerte, la estrategia varía radicalmente
- Las analogías y el lenguaje ameno funcionan bien para transmitir los conocimientos de seguridad y privacidad
- Los buenos hábitos son fáciles de explicar y sencillos de seguir
- Los usuarios han relegado los ordenadores personales a un segundo plano: El smartphone es el nuevo rey

# Filosofía

- Modelado adversarial
- Seguridad operacional
- Privacidad por diseño
- Código abierto
- Descentralización
- Usabilidad



# El dispositivo smartphone

- Centraliza mucha información en un solo lugar
- Altamente íntimo
- Gran cantidad de sensores
- Ecosistema de aplicaciones invasivas
- Favorece el uso de servicios centralizados, almacenamiento en la nube...
- Siempre encendido, siempre encima y siempre localizado
- No es precisamente el ecosistema ideal para proteger la privacidad

Ya que se va a usar, al menos que se  
haga de la mejor manera posible

# Resistencia Digital

- Cómo desarrollar una cultura de la seguridad en torno al smartphone al alcance de todo el mundo.
- Primera parte: OPSEC
- Segunda parte: Seguridad orientada a modelos de amenaza en el Smartphone y privacidad en redes sociales.
- Tercera parte: Seguridad Instrumental
  - Comparativa de apps de mensajería
  - Reseñas de aplicaciones respetuosas con la privacidad

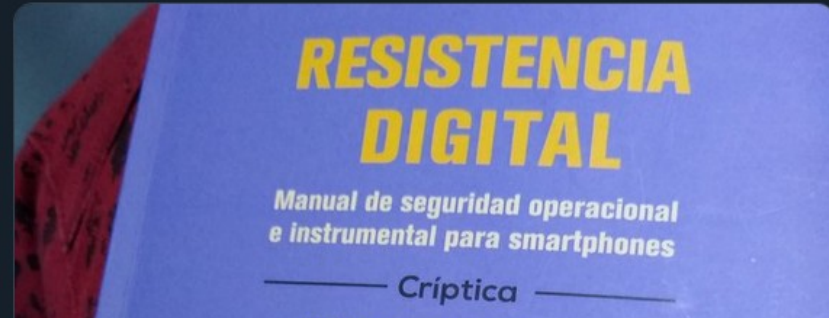
# Publicación y



Soy la Froken  
@Martixx

Tengo una bonita cola de libros por leer, pero no me arrepiento de haber hecho un LIFO a "Resistencia digital" de @CripticaOrg

Los 12€ mejor invertidos del navaja negra.



ayuda habría sido simplemente imposible. [criptica.org/blog/resistenc...](https://criptica.org/blog/resistenc...)

Y ahora, ¿cuál debería ser el siguiente paso? 😊

Show this thread



David Couso  
@crudo8

Hace días acabe el libro de #ResistenciaDigital de @CripticaOrg "manual de seguridad operacional e instrumental para smartphones".

Me quedo corto diciendo que es más que recomendado.

Gran trabajo. Búsquenlo en su página y léanlo.



Ha  
@i



Joaquín Niv  
@

Acabad



David Marugán  
@RadioHacking

Me acabo de leer de una sentada "Resistencia Digital" de @CripticaOrg, y editorial @DescontrolEd. Sinceramente un libro excepcional: mezcla hábilmente #OPSEC y seguridad instrumental "para todos los públicos". Profundo en sus planteamientos y útil en su esencia. Imprescindible.



#ResistenciaE  
lizcastro, sin c  
j/resistenc...



# Seguimos activos



**Críptica**  
@CrípticaOrg

Hay mucho trabajo detrás de esto, pero valdrá la pena: Junto con otras asociaciones ([@PDLI\\_](#), [@facua](#), [@internautas](#)), hoy llevamos al Defensor del Pueblo el [#DecretazoDigital](#), con intención de que se abra un recurso de inconstitucionalidad.



El recurso contra el decreto que permite al Gobierno interv...  
La norma permite al Gobierno controlar la infraestructura física que soporta Internet sin autorización judicial previaUn...  
[eldiario.es](#)

8:00 AM · Jan 15, 2020 · [Twitter Web App](#)

80 Retweets 81 Likes



# Gracias por vuestra atención

- Web: <https://criptica.org>
- RSS: <https://www.criptica.org/index.xml>
- Twitter: @CripticaOrg
- Canal de Telegram : [t.me/cripticaorg](https://t.me/cripticaorg)
- Matrix: [#criptica:matrix.org](https://matrix.to/#/#criptica:matrix.org)

