TARJETAS

SEGURIDAD DIGITAL

Entiende mejor cómo nos estamos comunicando, desde lo que hacemos con los dispositivos que utilizamos -teléfono, computador, tablet-, cómo viaja nuestra información, dónde se aloja y cómo se regula el tratamiento de nuestros datos. En este panorama, nuestra privacidad y seguridad se ven amenazadas.

Por eso, recogemos una serie de herramientas digitales desarrolladas por organizaciones y redes de programadores en todo el mundo de manera cooperativa y voluntaria y que, en términos generales, funcionan con donaciones y cooperación de parte de grupos y personas afines. Estas herramientas son alternativas al modelo comercial y vigilante de las comunicaciones y aunque no son gratuitas -pues la verdad es que cuestan mucho trabajo y esfuerzo-, a muchas de ellas podemos acceder libremente.

SUMARIO

<INTRO DUCCIÓN

¿TIENES ALGO QUE ESCONDER?

¿TEMES QUE EL GOBIERNO CONOZCA LO QUE HACES, CON QUIÉN TE COMUNICAS Y A TRAVÉS DE QUÉ MEDIOS?

¿CORRES ALGÚN RIESGO POR LO QUE DICES O HACES EN LA RED?

... Aunque tu respuesta a cualquiera de las anteriores preguntas sea no, esta información puede interesarte si usas internet o teléfono celular.

Hoy día no importa dónde vivas o lo que hagas, si te comunicas a través de cualquier dispositivo electrónico te están vigilando permanentemente. La vigilancia no proviene directamente de los gobiernos, sino de las corporaciones que proveen toda la infraestructura para las comunicaciones y que han desarrollado regulaciones propias para el manejo de datos. Esos que luego de mucho tiempo (hasta cinco años en este país) pueden ser utilizados en tu contra por la inteligencia gubernamental u otros actores que pueden atentar contra ti y quienes te rodean.

No importa si realizas acciones legales o ilegales, si perteneces a un movimiento social en Colombia debes proteger tus comunicaciones.

Estas tarjetas son para el **cuidado común** de quienes trabajamos por la transformación del sistema económico desigual en que vivimos. Más allá de la seguridad, la privacidad o la vigilancia, hablaremos de cómo es posible cuidarnos y cuidar a las personas con quienes trabajamos y nos comunicamos. No podemos permitir que nuestros **hábitos de consumo nos pongan en riesgo** individual y colectivamente.Todo lo que hacemos vitualmente tiene consecuencias en el mundo real.

En tecnología e internet **no existe** un sistema infalible, 100% seguro y privado, pero es posible emplear acciones para protegernos de la vigilancia y los ataques. Para eso es importante entender que la seguridad digital no depende -sólamente- de usar uno u otro programa, sino de identificar las amenazas que enfrentas y cómo puedes prevenirlas y contrarrestarlas.

A LA HORA DE USAR INTERNET ES MEJOR ASUMIR QUE TODO LO QUE ALLÍ SE HACE Y SE DICE PUEDE LLEGAR A SER PÚBLICO.

RECUERDA QUE

la solución más eficaz puede ser la solución menos técnica.

¿PARA DÓNDE VA TODO LO QUE HACES EN INTERNET?

Cada día internet ofrece más servicios gratuitos para sus usuarios, pero esto no es más que una ilusión. Cuando un producto en internet es gratis es porque el producto eres tú. Las empresas ganan en la medida que tienen más información sobre sus consumidores, pues así pueden ahorrar esfuerzos y dirigirse exactamente a quienes tienen las mayores probabilidades de concretar una compra.

¡Pero yo no soy el tipo de persona que hace compras en internet, sólo lo utilizo para informarme y comunicarme!

A través del rastreo permanente, las empresas dicen estar beneficiando a sus consumidores al ofrecerles una mejor experiencia en línea, pero esto no es más que acceder a variables que, directa o indirectamente, convierten a quienes usamos la red, en perfiles de consumo. Estos incluyen tu dirección IP, ubicación, preferencias de compra, métodos de pago disponibles, búsquedas en la red por palabras clave, entre otros.

Más sobre vigilancia corporativa aquí:
bit.ly/1WaHxMH

LAS CORPORACIONES VIGILAN. LOS ESTADOS VIGILAN

¿Has oído hablar de internet.org?

Este proyecto creado por Facebook para 'dar internet a los más pobres' es una alianza con seis empresas de telefonía móvil (Samsung, Ericsson, Media Tek, Nokia, Opera Software y Qualcomm) para que desde cualquier dispositivo móvil sea posible conectarse a ciertas páginas sin necesidad de pagar datos. El proyecto funciona en alianza con gobiernos y empresas prestadoras de servicios de internet. En Colombia funciona a través de Tigo.

Los estados también aprovechan estos modelos de negocio cuando se apropian de los datos recolectados por corporaciones privadas, con la diferencia de que analizan datos en nombre de la seguridad. Por eso es que indirectamente apoyan esta forma de acumular dinero mediante leyes, normativas fiscales o incluso incentivos para que utilicemos plataformas cuyo negocio se basa en la vigilancia.

Entonces, si las corporaciones construyen perfiles de consumo que les permiten saber qué hemos comprado y qué vamos a comprar en el futuro, los estados contruyen perfiles de amenaza, es decir quiénes son o podrían ser una amenaza a la seguridad nacional e internacional. Esto lo hacen, al igual que las corporaciones -y a través de sus plataformas-, a partir de las búsquedas que hacemos, a quiénes seguimos, las palabras que utilizamos, nuestra ubicación, nuestra dirección IP, nuestros correos, números de celular, entre otros datos que voluntariamente entregamos en la red.

Más sobre vigilancia estatal aquí: bit.ly/1Xe8Sh8

¿ASÍ QUE NAVEGAS LIBREMENTE?

PRIVACIDAD NO PRIVATIZAR

En internet la privacidad no consiste en restringir accesos. Es la posibilidad de decidir, como usuarias, qué queremos compartir, en qué contextos y con quiénes, en un horizonte muy amplio que va desde la privacidad completa hasta la transparencia total.

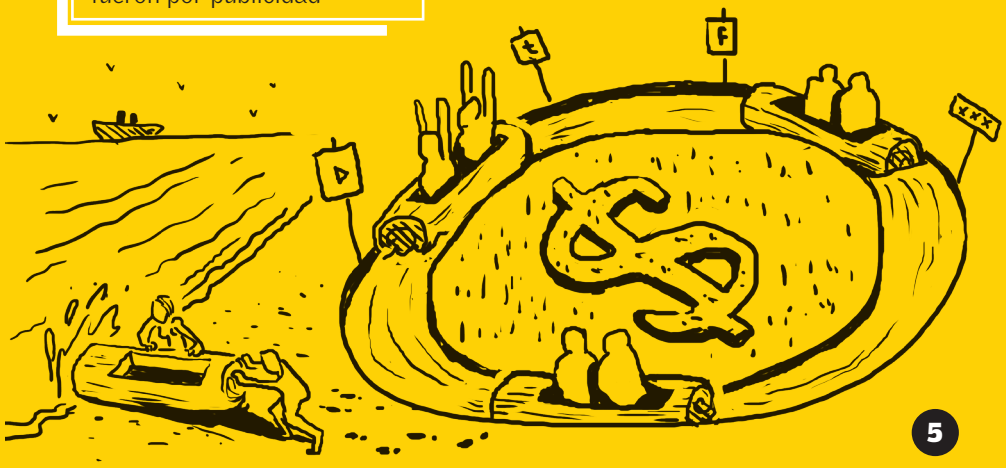
Como la conocemos hoy, la web pareciera darnos total libertad para buscar, compartir, comunicar o acceder a lo que deseamos, pero esto está bastante lejos de la realidad.

Cuando navegamos, páginas como el buscador de Google, Yahoo o MSN nos ofrecen, de acuerdo a nuestro perfil de usuario, lo que pareciera ser más relevante para nuestros intereses. Además, en sitios web como Facebook, Youtube o tantos otros, encontramos publicidad que podría interesarnos, justamente de empresas que pagan para que gente como nosotras vea sus anuncios.

Así, nuestra capacidad de navegación en la red es la punta de un iceberg con respecto a la cantidad de contenidos existentes allí. Una punta que no sólo es lo más visible sino lo que más tráfico concentra y al tiempo, lo que más dinero significa para las empresas.

¿SABÍAS QUE?

En 2011 Google tuvo ingresos por $37.900 millones de dólares, de los cuales el 96% fueron por publicidad



ESTADOS UNIDOS

3 Llega al servidor de la empresa de mensajería que usas en EEUU

4 Allí se busca automáticamente a quién va dirigido el mensaje

mario@outlook.com
andrea@outlook.com
luisa@outlook.com

Cables submarinos

COLOMBIA

Cables

2 Luego llega al servidor de tu ISP (Proveedor de internet)

Cables

1 Sale un mensaje desde tu equipo y llega al router

Wifi

"Nos vemos en la asamblea"

5 Vuelve al servidor del ISP de tu destinatario en Colombia

Cables

6 Que envía el mensaje a su red de antenas de celular

3G /4G

7 Llega el mensaje al celular de tu amigo. Todo en un segundo.

Como viaja la información en internet

A través de este recorrido tu información dejará rastros por donde pasa y será copiada varias veces. Aunque el destinatario del mensaje esté a una cuadra, lo que envías puede viajar a otro país y volver en segundos.

NIVEL 1

REDES SOCIALES

¿CUÁNTA INFORMACIÓN SOBRE TU VIDA PRIVADA, LABORAL O ACADÉMICA ESTÁ EN TU COMPUTADOR, CELULAR O CUENTAS DE INTERNET?

Imagina que te roban el computador o el celular.

Al encenderlos, ¿tienes una contraseña para ingresar al sistema?

Supongamos que no y quien lo tiene accede y abre el navegador, ¿entra directamente a tu correo? ¿a tu cuenta de Facebook, Twitter, Instagram u otra?

Digamos que tienes un correo de Gmail y sí se abre la sesión porque estás logueada permanentemente. ¿Tienes anclada tu cuenta a Google Drive, a tu directorio en el celular, a otras redes que puedas utilizar?

Seguramente has escuchado que al utilizar estas redes aportas a su enriquecimiento a costa de tu privacidad pero también, que a pesar de lo malo, es necesario aprovecharlas para llegar a mucha más gente. Con estas tarjetas esperamos que la decisión sea tuya, pero con información y herramientas alternativas a mano. Por eso empezamos con tu propio comportamiento en la red y el uso que das a plataformas masivas y comerciales.

FACEBOOK

La lógica con que entras es que cualquier persona, incluyendo la empresa, tiene derecho a mirar y utilizar cada contenido que subes, a menos que digas lo contrario. Y aún así, el contenido permanecerá en red para siempre.

Además te obliga a usar tu nombre real, hace seguimiento de tu actividad en la red aunque no tengas una cuenta propia, hace seguimiento a lo que escribes así decidas no publicarlo... Y sólo imagina que en 2013 tuvo ingresos por 7870 millones de dólares ;(

WHATS APP

Quizás una de las mejores alternativas para la comunicación. Sólo se requiere tener un teléfono inteligente y en casi cualquier plan de datos está incluido sin costo. Pero olvídate que tus mensajes son privados.

Descargando la aplicación para tu celular estás compartiendo automáticamente tu directorio de contactos con la compañía. En febrero de 2014 Facebook compró whatsapp por 19.000 millones de dólares. Así que todos tus contactos alimentan las bases de datos de Facebook.

TWITTER

Te permite hacer seguimiento en tiempo real a eventos y procesos sociales. Por eso ha sido protagonista en varias revoluciones recientes, como las de Europa y Oriente medio. Ha sido censurada por gobiernos totalitarios y aboga por la libre expresión.

Durante el segundo semestre de 2015, a petición de algunos gobiernos democráticos, cerró alrededor de 125.000 cuentas supuestamente relacionadas con el extremismo islámico, por incitar al terrorismo. En 2013 la empresa fue avaluada en 11.000 millones de dólares.

¿QUÉ OTRAS REDES USAS?

NIVEL 1

COMPARTI-MENTACIÓN

SEPARA TU INFORMACIÓN

LA COMPARTIMENTACIÓN SÓLO FUNCIONA SI:

- Logras que los dos (o más) perfiles no se relacionen entre sí. Es decir, **nunca** te comuniques con las mismas personas utilizando ambos perfiles.
- Usa Tor para anonimizar tu IP. Aprende cómo hacerlo en la *ficha 13*.

Al clasificar tus comunicaciones deberías tener al menos dos perfiles:

PERSONAL	ACTIVISTA
• Bancario • Salud y Pensión • Laboral • Compras • Familiar • Estudio Otros • Celular y SIM personal	• Mail activista permanente • Mail para cada proyecto • Mail de la organización • Facebook de la organización • Celular y SIM de la organización

CONSEJOS

- Consulta a tu familia, amigxs y compañerxs si están de acuerdo con que subas fotos de ellxs a las redes sociales.
- Puedes jugar con los nombres y palabras que usas para comunicarte. Las agencias estatales de inteligencia buscan palabras clave que puedan representar una amenaza. Utilicemos la creatividad :)
- Envía correos masivos siempre con copia oculta (Cco). ¿Confías en cada contacto?
- Antes de compartir información sensible, piensa a quién le va a llegar.
- Cierra sesión siempre que termines de revisar tus redes o correos.

SI QUIERES CAMBIAR TUS HÁBITOS EN LAS REDES INVITA A MÁS PERSONAS Y HÁGANLO JUNTAS.

NIVEL 1

CONTRASEÑA

ES LA ÚNICA HERRAMIENTA EN TUS MANOS PARA RESTRINGIR A OTRXS EL ACCESO A TUS REDES Y COMUNICACIONES, ASÍ QUE CUALQUIER CONTRASEÑA QUE ASIGNES DEBE TENER ALGUNAS CARACTERÍSTICAS:

DIFÍCIL

Lo bastante larga para ser segura, con mínimo 10 caracteres. Lo mejor es usar números, símbolos, letras minúsculas y mayúsculas, con frases o palabras impersonales. Nunca algo relacionado contigo, tu vida o la de tu familia

NO pepitaperez1982

SI 99lamazorcaestaRICA!

PRÁCTICA

¿La puedes recordar sin anotarla? Fácil de recordar y de teclear correctamente para ti.

ÚNICA

Una contraseña por uso y sin repetir.

PERSONAL

Conocida sólo por ti. No compartas tus contraseñas importantes con nadie y menos por correo electrónico, chat o teléfono. Si tienes una contraseña que debes que compartir (p.e., el internet inalámbrico de la casa u oficina), no uses la misma contraseña para cosas más importantes.

RECIENTE

Cambia la contraseña periódicamente, cada 3 a 6 meses.

Como es difícil memorizar múltiples contraseñas, existen herramientas como Keepass info.securityinabox.org/es/keepass_principal

NIVEL 2

<NAVEGACIÓN

Por eso cada vez se utiliza más el sistema de **AUTENTICACIÓN**, esto es la obligación de registrarse con usuario, contraseña y varios datos personales más. Aunque es posible no registrarse o poner datos falsos, estas plataformas dificultan la evasión de este requisito para el uso de servicios 'gratuitos'. Y en muchos casos te piden también anclar tus cuentas, como hace Google. Así, mientras consideramos que tenemos todos los servicios a la mano, las corporaciones obtienen perfiles más específicos de cada usuario.

¿CÓMO RASTREAN NUESTRA ACTIVIDAD EN LA RED?

Los sitios web utilizan:

COOKIES Pequeños archivos de texto que los servidores web almacenan en el disco duro del usuario y les permite rastrear los movimientos del usuario dentro del sitio, así como cualquier información voluntariamente provista allí. Así se va creando un perfil que puede usarse para interacciones de marketing, para mejorar la eficacia del sitio o detectar áreas de mejora comercial.

COOKIES DE TERCEROS Sirven para exhibir avisos publicitarios. Los utilizan empresas intermediarias entre anunciantes y páginas que quieran pautar. Muchos de los anuncios que uno ve al visitar un sitio no están albergados en éste, sino que vienen de una empresa desconocida. Estos terceros, además, rastrean nuestro comportamiento para medir el impacto de los anuncios que venden.

WEB-TRACKING es el seguimiento que se hace por parte de una web a la que accedes. Se registran datos como el momento del acceso, procedencia, navegador, sistema operativo desde el que se accede, etc. Esto sirve para hacer mejoras a las páginas (y por ejemplo para proteger de un ataque), pero también supone que se comparten datos sin tu consentimiento, pues no hay posibilidad de rechazar compartirlos.

NIVEL 2

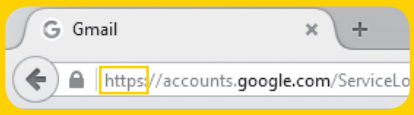
NAVEGADOR

FIREFOX es un navegador relativamente libre. Allí puedes activar la *navegación privada* que borra historial, búsquedas, cookies y archivos. Esto **no anonimiza** tu IP, para hacerlo revisa la *tarjeta 9*.

NAVEGA SÓLO CON FIREFOX, MANTENLO ACTUALIZADO Y CON LOS SIGUIENTES PLUG-INS:

NAVEGACIÓN SEGURA

Con la extensión https:// tu mensaje llega directamente al destinatario. Ninguno de los intermediarios puede acceder a él, sólo darle paso. Fíjate siempre en la parte de arriba si los sitios que visitas usan esta extensión.



http://

Compu --- wifi – proveedor -- Ice – Torre – GMAIL

https://

Compu -- xx -- xx – xx -- xx -- GMAIL

Instala *HTTPS Everywhere*, una extensión para que la navegación segura sea automática.
eff.org/https-everywhere

ELIMINAR COOKIES

Puedes negarte a entrar en una página cada vez que ésta te avisa que utiliza cookies de terceros, o puedes descargar una extensión para que cuando termines de visitar cualquier página se borren las cookies. Por ejemplo Privacy Badger.

Bájalo desde:
eff.org/privacybadger

NIVEL 2

NAVEGACIÓN ANÓNIMA

TOR (THE ONION ROUTER)

Es un navegador de código abierto para ocultar tu dirección IP en internet, manteniendo en secreto la información que viaja por la red. Aunque no es infalible, la Agencia Nacional de Seguridad (NSA) de EEUU lo ubica en el nivel más alto de seguridad.

Tor desactiva funciones web que pueden develar tu identidad, sin embargo esto limita y hace poco atractiva la navegación. Úsalo siempre para protejer tu perfil de activista (*ficha 9*). Para el resto puedes usar Firefox.

Para conocer más de Tor:
bit.ly/1P0Uz9V

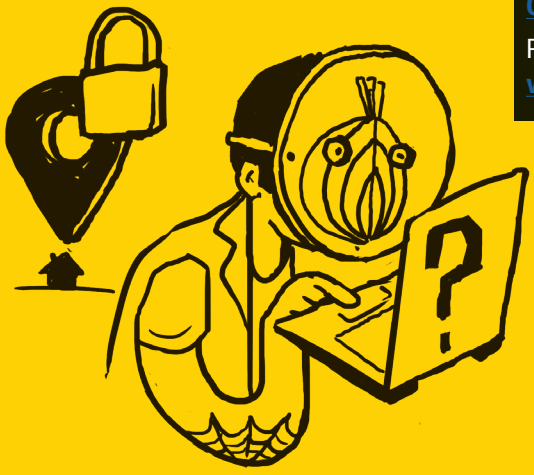
DIRECCIÓN IP (INTERNET PROTOCOL)

Cuando los computadores, tablet y teléfonos inteligentes se conectan a una red se identifican con un número IP, que les permite comunicarse entre sí. La dirección IP no cambia con el tiempo y cada dispositivo tiene su propia IP.

CON TU IP SE PUEDE SABER LA POSICIÓN GEOGRÁFICA E INCLUSO DIRECCIÓN CON CALLES Y CARRERAS DE DONDE TE ESTÁS CONECTANDO.

Para celular debes descargar dos apps:
Orbot
Orweb

Para computador descárgalo en:
www.torproject.org



ATENCIÓN

Tor no es suficiente, debes cambiar tus hábitos de navegación para garantizar la protección de tu identidad

NIVEL 2

NAVEGACIÓN ANÓNIMA

VPN

Si tu organización maneja información sensible y es necesario proteger a sus miembros virtual y físicamente, quizás puedes utilizar VPN (Virtual Private Network/Red Privada Virtual) o servidores Proxy, debido a lo siguente:

- Tus datos están protegidos de bloqueo o seguimiento, realizados por los operadores ISP.
- Tus datos parecen utilizar la dirección IP del servidor VPN (o Proxy), y no su dirección IP real.

Normalmente los servidores Proxy y VPN tienen costo, aunque hay algunas aplicaciones personales descargables gratuitamente, como OpenVPN **openvpn.net/index.php/open-source/downloads** para el caso de los VPN, o ultrasurf **ultrasurf.us** o Psiphon psiphon. **en.uptodown.com** para los proxys.

MÁS SEGURIDAD

Puedes combinar VNP y Tor para agregar una capa de seguridad a tu conexión.

NIVEL 3

COMUNI-CACIONES

EL CUIDADO DE LA INFORMACIÓN QUE MANEJAS ESTÁ A TU CARGO.

SI UTILIZAS UN COMPUTADOR

TUYO

¿Dónde lo dejas cuando no lo llevas contigo?

¿Ya le pusiste contraseña para ingresar al sistema?

¿Tienes una segunda copia (backup) de los archivos importantes?

COMPARTIDO

¿Esas personas son de tu entera confianza?

¿Pueden acceder a tus archivos sin problema?

¿Han hablado sobre prácticas de cuidado en el uso de internet?

PÚBLICO

¿Te aseguras de borrar cualquier documento que trabajes allí?

¿Sabes que, muchas veces, en estos computadores hay instalados programas espías y maliciosos?

La vigilancia es operada por máquinas que funcionan de acuerdo a algoritmos, con enormes capacidades de almacenamiento y que están encendidas las 24 horas. Estos sistemas pueden alertar y solo en ese caso será revisado por funcionarios.

SIEMPRE QUE UN COMPUTADOR ESTÉ CONECTADO A INTERNET CORRE EL RIESGO DE SER MONITOREADO

Cuenta siempre con un Antivirus y un cortafuegos. En su mayoría cobran el servicio pero siempre puedes conseguir versiones de prueba gratuitas, o versiones completas con menores capacidades, lo que es mejor que nada: el paquete de seguridad COMODO: bit.ly/1Jg88n7

NIVEL3

TELÉFONOS INTELIGENTES

O DE INTELIGENCIA

HABLAR DE SEGURIDAD EN CELULARES ES RELATIVO, PUES EL CELULAR ES EN SÍ MISMO UN DISPOSITIVO DE RASTREO.

ANTENAS

Su tecnología funciona con antenas instaladas en lugares estratégicos para que donde sea que te encuentres, alguna te de señal. **Siempre tienes una antena que reporta tu cercanía y así, es posible hacer seguimiento a tus trayectos** y rutinas, triangulando la señal que emiten las diferentes antenas.

Cuando te reúnes con muchas personas para una manifestación, las antenas registran cada celular encendido en el área.

Si no quieres que sepan tu ubicación, **quítale la pila**. Pero imagina una manifestación o asamblea a donde llegan muchos teléfonos que de pronto dejan de reportar señal. Lo mejor entonces es no llevarlo contigo.

Tu celular también puede ser utilizado **como un micrófono** y ser activado sin que te des cuenta.

INTERNET

Además, los teléfonos inteligentes se conectan a las redes de internet, bien sea a través de datos o de conexiones wifi. Muchas aplicaciones (como Google maps y Skype, entre otras) te piden activar tu GPS.

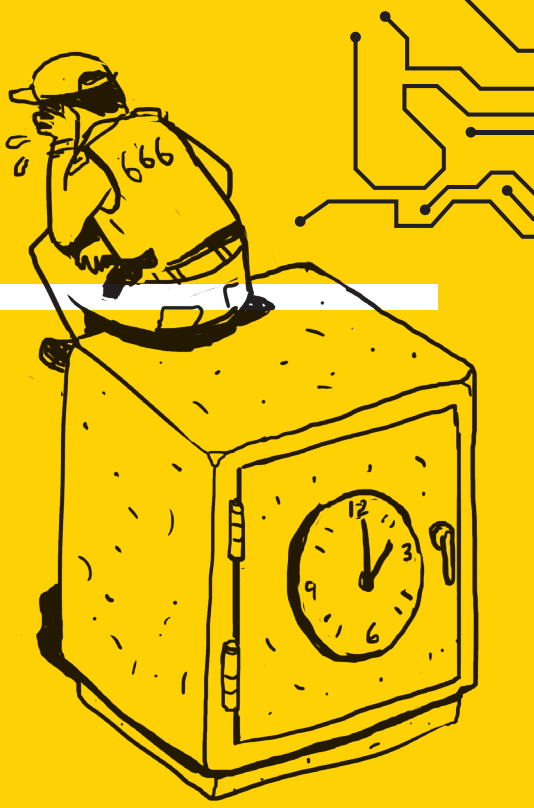
Tu celular es como una caja fuerte de información. Tu correo electrónico y tu directorio de contactos son, quizás, lo que más debes proteger.

El celular es igual una herramienta poderosa para el cuidado conjunto entre personas, así como para el registro y transmisión en vivo de acciones.

Tú decides si es mejor llevarlo o no a donde vayas.

NIVEL 3

ENCRIPTACIÓN



Con la anonimización es posible ocultar desde dónde y hacia dónde va tu actividad en las redes. Con la encriptación, el contenido de tus mensajes y tu información en general, está protegido por un código ilegible. La única manera de acceder al contenido es a través de una clave o contraseña. Para romperla se deben invertir grandes cantidades de tiempo y dinero.

El mensaje

sopa de caracol

cifrado podría ser

S3CRYPT:BEGIN:AESCTR:2F21:wqLCn8O5w5I3wrQ+:END

Puedes encriptar los mensajes que envías a través de correo electrónico, llamadas y mensajería instantánea, o la información que guardas en el disco duro. Aquí nos concentraremos en las comunicaciones.

EN EL COMPUTADOR

Si utilizas sistema operativo Windows o Mac, desde el navegador Firefox puedes instalar una extensión en este link:

mzl.la/1LSIBo6

Y te permitirá cifrar el contenido de tus correos (no importa si es gmail, hotmail, riseup u otro). Sólo necesitas que el destinatario conozca la clave (esa se la dices en persona).

O puedes instalar **PGP** (Pretty Good Privacy), que te permite enviar y recibir mensajes de quienes también lo tienen instalado. PGP consiste en que tienes una llave pública (un código), se la das a la persona con quien quieres comunicarte (y también ella te da la suya). Cuando recibes un mensaje, para acceder a él debes ingresar una firma privada (tu contraseña) y listo.

pgpi.org

NIVEL 3

APPS Y ENCRIPTACIÓN

EN EL CELULAR

Puedes encriptar tus mensajes SMS (que normalmente son bastante inseguros), las llamadas por internet (VoIP) y los chat.

En cualquier caso es necesario que tú y la personas con quien deseas comunicarte **tengan la misma aplicación** descargada.

HAY MÁS DE UNA FORMA DE INTERVENIR TODAS LAS COMUNICACIONES DE UN TELÉFONO INTELIGENTE. POR MÁS QUE UTILICES APPS QUE ENCRIPTAN EVITA HABLAR O COMPARTIR MATERIAL SENSIBLE.

LLAMADAS ONLINE

Ostel

RedPhone

Silent Phone

Signal

TEXTO SMS

SMS Secure

CHAT

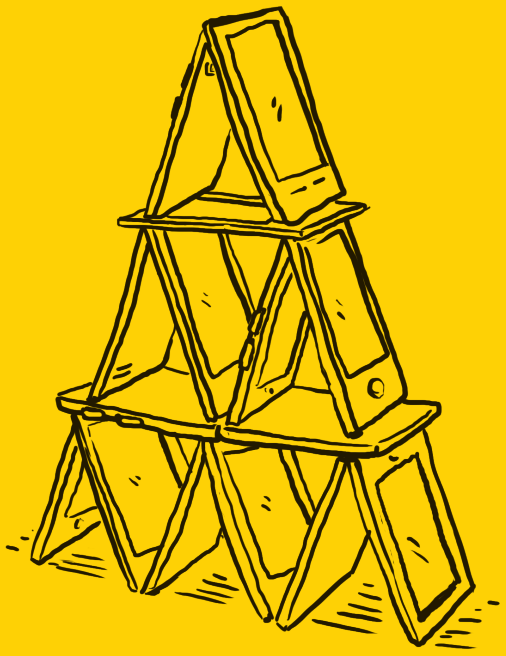
Chat Secure

Signal (iPhone)

FOTOS Y VIDEO

CameraV

guardianproject.info/apps



Estas herramientas las encuentras en:

Available on the App Store

ANDROID APP ON Google play

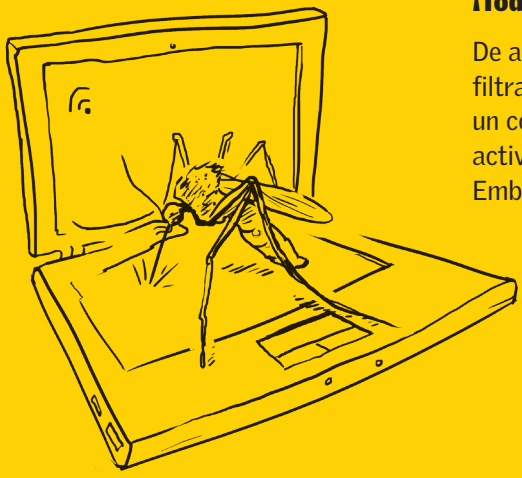
NIVEL 3

VIGILANCIA MULTINACIONAL

¿QUIÉN PODRÁ DEFENDERNOS?

En épocas de globalización no son los estados quienes vigilan sino empresas transnacionales contratadas por gobiernos de turno, con altísimos costos. ¿Y quién protege nuestros datos?

Hacking team es una empresa italiana que vende a los gobiernos herramientas tecnológicas de espionaje y de invasión a la intimidad. A mediados de 2015 sus comunicaciones fueron filtradas y así se conoció con qué países tiene contratos y los montos de éstos.



GALILEO * DA VINCI * PHANTOM SISTEMA DE CONTROL REMOTO (RCS)

El RCS es el software que vende Hacking Team. Se instala de manera silenciosa a través de un hipervínculo que llega en un correo electrónico malicioso (como cualquier virus).

Una vez haces click en el hipervínculo, RCS toma control de tu equipo y puede registrar su uso, por ejemplo:

Llamadas, acceso a correo y redes, historial de navegación, acceso a fotos y documentos eliminados del disco duro. Además puede activar tu micrófono, cámara y teclado para espiar lo que haces.

¡Todo esto sin tu consentimiento!

De acuerdo con algunos correos filtrados, Hacking Team tenía un contrato con la DEA y realizó actividades de vigilancia desde la Embajada de EEUU en Bogotá.

NIVEL 3

ESPIONAJE EN AMÉRICA LATINA

CONTRATOS DE HACKING TEAM

- **HONDURAS** $355.000 dólares pagados desde 2014.
- **MÉXICO**: la lista es extensa. Son o fueron clientes de Hacking Team los gobiernos de los estados de Durango, Querétaro, Puebla, Campeche, Baja California, Tamaulipas y Yucatán. A nivel nacional también contrataron los servicios la Policía Federal, la Procuraduría General del Estado de México, el Centro de Investigación y Seguridad Nacional y las secretarías de Seguridad Pública del Distrito Federal, la de Marina y la de Defensa Nacional. Muchos de estos contratos están clasificados como "expirados" en la actualidad.
- **CHILE**: el gobierno de Chile firmó contratos con Hacking Team por una suma de $2.85 millones de dólares.
- **COLOMBIA**: DIPOL contrató los servicios de Hacking Team desde el 2013, por más de $335.000 dólares.
- **ECUADOR**: la Secretaría Nacional de Intligencia SENAIN está usando su tecnología y ha pagado $535.000 dólares.
- **PANAMÁ**: contrato ya finalizado a través de la Seguridad Presidencial, pero los montos de varios contratos alcanzaron los $750.000 dólares.

NIVEL 3

VIGILANCIA ESTATAL EN COL

LEYES, CONTRATOS Y OTRAS VARIEDADES

¿RECUERDAS EL ESCÁNDALO DE LAS CHUZADAS?

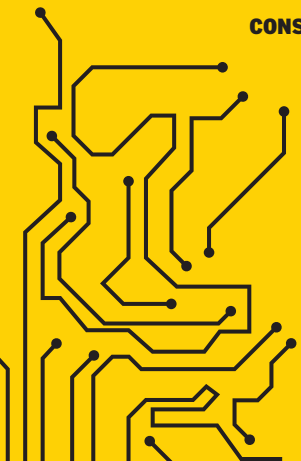
El desaparecido DAS interceptó llamadas telefónicas, tráfico de correo electrónico y listas de contactos nacionales e internacionales y utilizó esta información para construir perfiles psicológicos de quienes vigilaban y para seguirles a ellxs y a sus familias. Por eso fue disuelto en 2011 y parte de su personal pasó a ser parte de la Fiscalía.

Pero éste no es el único caso de interceptaciones ilegales por parte de las autoridades en Colombia. Menos ahora, cuando la vigilancia se hace a las comunicaciones en internet y no sólo a las telefónicas.

En los últimos años las autoridades colombianas han adquirido software para la vigilancia de internet, traspasando límites en el marco legal, confundiendo la interceptación legal de comunicaciones para la investigación criminal (en procesos abiertos) con el monitoreo con fines de inteligencia.

SÓLO LA FISCALÍA PUEDE AUTORIZAR UNA INTERCEPTACIÓN EN LAS COMUNICACIONES

CONSTITUCIÓN POLÍTICA Y CÓDIGO PENAL



Organismos de inteligencia están usando, desde hace algunos años, grandes plataformas para monitorear permanentemente nuestras comunicaciones, pero además se están valiendo de software malicioso para el hackeo de dispositivos, aunque hay leyes vigentes que lo penalizan.

El Código Penal (Art. 269A, 269C, 260E) reconoce como delito el acceso abusivo a un sistema informático, la interceptación de datos informáticos y el uso de software malicioso.

NIVEL 3

PLATAFORMAS PARA LA VIGILANCIA

PUMA / Plataforma Única de Monitoreo y Análisis

- Sistema de monitoreo que permite la interceptación masiva, pasiva e indiscriminada de las comunicaciones. Fue costeado por la Policía y gestionado por la DIJIN
- Se presentó en 2007. En 2013 se avanzó en la contratación para su ampliación (un contrato por 50 mil millones de pesos), pero este proceso fue detenido por los riesgos que representa para los derechos humanos y el derecho a la libertad de expresión.
- Contratado a la empresa Verint Systems (estadounidense-israelí) y La Curacao (su representante en Colombia), que en 2014 tuvo ingresos por 910 millones de dólares.

Con Verint Systems y La Curacao también se contrató el Sistema Integral de Grabación Digital (SIGD), un sistema de vigilancia masiva manejado por la DIPOL, es decir un sistema ilegal de interceptación del cual se tiene muy poca información.

ESPERANZA

- Sistema de interceptación gestionado por la Fiscalía (tienen acceso la Policía y antes el DAS) – Su objetivo es iniciar procesamientos judiciales caso por caso
- Funciona desde finales de la década de 1990
- Regido por la Constitución y Código de Procedimiento Penal
- Contratado a la empresa STAR Colombia Inteligencia & Tecnología, que en 2009 tenía reservas por 1200 millones de pesos, con tan solo 11 empleados.

Recursos en protección digital

- Surveillance Self Defense. Electronic Frontier Foundation. **ssd.eff.org/es**
- Manual Básico de Seguridad Informática Para Activistas. Mënalkiawn. 2013. **bit.ly/1R8HE6Z**
- Cuadernos de Autodefensa Digital, Smartphones. HacksturLab & Editorial Descontrol. 2015.
- Criptotarjetas. Rancho Electrónico. **bit.ly/1pyHwrw**
- Quema tu móvil. 2010. **bit.ly/1M8he45**
- Digital Security for Activists. **zine.riseup.net**
- Security in-a-Box, Tools and Tactics for Digital Security. Tactical technology Collective y Front Line Defenders. **bit.ly/1HI41vI**
- Mejor Navegación en Internet (Better Web Browsing). Riseup. **bit.ly/1YAdnnq**
- Manual Antiespías: Herramientas para la protección digital de periodistas **bit.ly/224PPJu**
- Serie: No temas a Internet. Derechos Digitales. **derechosdigitales.org/notemasainternet**

Algunos Documentos

- Cuando el Estado hackea. Fundación Karisma. **bit.ly/1M8hLmy**
- Vigilancia de las comunicaciones por la autoridad y protección de los derechos fundamentales en Colombia. Electronic Frontier Foundation, Fundación Karisma y CCJ. **bit.ly/1RSmWvn**
- Vigilancia en Colombia. Fundación Karisma. **bit.ly/1phHAfq**
- Un estado en la sombra: vigilancia y orden público en Colombia. Privacy International. **bit.ly/1IEKxIn**
- Demanda y oferta: la industria de la vigilancia al descubierto. Privacy International. **bit.ly/1YAe40f**

Sin Miedo

Pero mejor si nos vemos en la calle ;)

A LAS REDES SIN MIEDO

HERRAMIENTAS

Este manual hace parte de una caja de herramientas para enfrentar las distintas formas en que se manifiesta la represión estatal en Colombia.

A las Calles Sin Miedo es una apuesta colectiva que recoge conocimientos y prácticas de protección para quienes luchamos por la transformación social.

www.sinmiedo.com.co

OTRAS HERRAMIENTAS

- Medios Libres
- Auxilios Médicos
- Auxilios Legales
- Manejo del Miedo
- Defensa Popular
- Juego Compa

La impresión de estas herramientas fue financiada por Hivos people unlimited