# DAEMON

MANUAL DE ACCIÓN DIGITAL PARA COMUNIDADES

HERRAMIENTAS-ORGANIZACIÓN

## ACTÚA
## PROTEGE
## COMPARTE

PAULA DE LA HOZ

COMUNIDADES-GRUPOS SOCIALES-ACCIÓN LOCAL

**No pidas garantías. No esperes a que te salve algo, alguien o una biblioteca. Sálvate a tí mismo y si te hundes, al menos te hundirás sabiendo que ibas a la orilla correcta.**

RAY BRADBURY \\ FARENHEIT 451

# ÍNDICE


**00** **NECESIDADES DIGITALES EN COMUNIDADES**

El peso de la intervención digital en el activismo de comunidad.

**01** **KIT DE INICIACIÓN**

Lo fundamental para empezar a protegerse y proteger.

**02** **FEMINISMO**

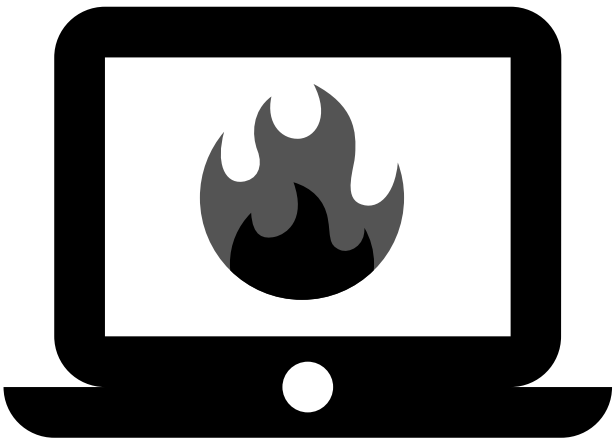
Activismo digital y feminismo.

**03** **ANEXO TÉCNICO**

Anexo de conecptos, instrucciones y extras.

**04** **BIBLIOGRAFÍA**

Recursos y otros ensayos.

# 00/NECESIDADES DIGITALES

En comunidades

Hay aproximadamente cuatro billones de usuarios[1] en Internet en todo el mundo en 2019. Esta cifra es consecuencia de una sociedad cuyos cimientos se basan en el tratamiento de la información y la velocidad a la que pueda transmitirse. Sin embargo no hablamos de una tecnología que se haya desarrollado a lo largo de los siglos, para comprender mejor nuestra situación nos basta con situarnos en la década de los setenta. En aquel entonces los ordenadores, herramientas pensadas principalmente para automatizar determinadas funciones de investigación, empezaron a plantearse como nodos de una red: Arpanet, Telenet, Cyclades o Junet[2], fueron proyectos que surgieron en esa época con la intención de mantener en contacto cientos de ordenadores. Aunque proyectos como Arpanet seguían teniendo un propósito enfocado a la investigación, se había abierto la puerta de un concepto mucho más amplio.

**EL ANONIMATO DIGITAL EMPEZÓ A COMPRENDERSE COMO UN PRODUCTO MÁS DEL QUE SACAR PARTIDO A FINALES DE LA DÉCADA DE LOS OCHENTA.**

En los noventa llegaría otro pico en la historia de Internet, que puso el broche final al siglo XX e impulsó el Internet que conocemos hoy día: La World Wide Web. Su creador, Tim Berners-Lee inventó la WWW en 1989 y la liberó al público en 1991, dando la posibilidad a todos los usuarios de la red de crear de forma gratuita una página web. En ese momento, las empresas de todo el mundo comenzaron a ver un importante medio de publicidad (entre otras cosas) en las páginas web, lo que provocó la llamada Burbuja de las Puntocom. Algunas de las empresas con más popularidad durante esta época fueron Yahoo o Ebay, entre otras muchas. Así pues, a la vez que el interés por el uso de Internet aumentaba, también lo hacía la preocupación de unos pocos por la neutralidad de la red. Así surgieron comunidades de técnicos y usuarios que veían en este creciente interés por parte de las empresas un posible riesgo a la integridad digital de los usuarios en el futuro; no se equivocaban. Entre estas comunidades que aparecieron en la década de los noventa se encuentra la Electronic Frontier Foundation[5], una asociación aún activa dedicada a la protección de derechos digitales.

En su ensayo de esa misma época “La ética hacker y el espíritu de la era de la información” Pekka Hinammen profundiza en el trasfondo de la comunidad “hacker” comprendida en un sentido mucho más constructivo de lo que Hollywood ha expuesto a lo largo de los años. Y es que en esta misma época, antes de entrar al nuevo milenio, dos grandes grupos de “hackers” se enfrentaban en una guerra underground: Por un lado uno de los grupos se dedicaban a aprovechar vulnerabilidades de las nuevas tecnologías para extorsionar, romper y robar información o dinero; el otro grupo dedicaba sus esfuerzos a la investigación y compartir información de cómo funcionaba la tecnología en los Bulletin Board System (pre-foros en los que había que entrar por turnos y donde podían dejarse mensajes entexto plano).

El peso cultural de la comunidad hacker a la entrada del nuevo siglo determinaría un punto de inflexión que aún cuesta superar: la necesidad de implantar un sistema adecuado de seguridad para proteger a los usuarios; la defensa de la neutralidad de Internet como algo más que una necesidad para cibercriminales; **la preservación de la soberanía distribuida de la red.**

## SOMOS ~~USUARIOS~~ PERSONAS EN LA COMUNIDAD DIGITAL.

En un mundo en donde la tecnología es la base de todo lo relevante que hacemos (trabajo, información personal, educación, comunicación…) es incómodo pensar que puede ser insegura. La verdad, la situación más realista, es que lo que usamos es inseguro. Siempre lo es, puesto que no existe un sistema blindado ante cualquier error. Lo único que podemos encontrar son sistemas más seguros que otros, y el usuario medio debe conocer esta realidad para que pueda actuar en consecuencia y ser más responsable con la información que comparte en la red. Gran parte de las herramientas que se utilizan de forma profesional en cibersegurdad se han desarrollado en un contexto desinteresado de comunidad; se han publicado con una licencia libre. El conocimiento sobre seguridad gitital sigue creciendo gracias a blogs y eventos enfocados a compartir información, .

En la actualidad existen comunidades de todo tipo, desde las dedicadas específicamente a la protección de derechos digitales y la seguridad[4], hasta comunidades de acción local, de vecinos, animalistas, etc. Aunque cada una tenga necesidades diferentes, varias sufrirán ataques similares. A lo largo de 2018, por ejemplo, hubo un ataque dirigido a miembros de Amnistía Internacional[5] a través de Whatsapp. Facebook comparte datos de sus usuarios con terceros, comprometiendo la integridad digital (y a veces física) de activistas. Conocer nuestro contexto digital nos permite protegernos y tomar medidas para proteger a otros, para reducir el riesgo de los integrantes. Y no sólo eso, las herramientas digitales bien utilizadas permiten flexibilidad y organización sin necesidad de comprometer la seguridad

# MANOS A LA OBRA

## 01/KIT DE INICIACIÓN

Para una comunidad cibersegura

Comenzaremos listando una serie de mitos y mentiras sobre ciberseguridad que impiden al usuario medio reconocer su responsabilidad y poder.

- **La seguridad sólo es posible comprometiendo la privacidad.** Esto es una absoluta falacia que se promueve con la intención de sacar adelante proyectos abusivos contra grupos minoritarios además de la recolección masiva de datos. Con la intervención de la nueva ley de protección de datos algunos de estos proyectos se han descartado, pero la premisa sigue siendo la favorita a la hora de tratar asuntos por "la seguridad de los usuarios". Proteger a las personas no necesariamente requiere comprometer su privacidad, hay otro camino.
- **No necesito privacidad puesto que no tengo nada que esconder.** Tal como dijo Edward Snowden[6], esa frase equivale a decir que la libertad de expresión es necesaria porque no tienes nada que decir. Proteger, defender y usar tus derechos digitales y tu privacidad en Internet es parte de un movimiento más grande, la defensa de algo que otras personas necesitan o están perdiendo poco a poco. Si no protegemos con uñas y dientes lo que tenemos, lo echaremos de menos cuando no lo tengamos.
- **TOR es una herramienta para criminales**. No, como todo pueden usarlo criminales. Es una herramienta para el anonimato. Por muchos motivos, en muchos contextos.

# HERRAMIENTAS

Lista de herramientas para la protección digital

Antes de listar las herramientas necesarias para proteger una comunidad, listaremos una serie de flancos a proteger. Toda comunidad se basa en la comunicación entre sus integrantes, por lo que nuestro primer punto a proteger va a ser éste. Hay diferentes medidas y niveles a la hora de proteger la comunicación entre usuarios, veremos las diferentes opciones. La presencia digital en las redes es fundamental para hacerse oír, este punto es especialmente comprometido y discutido incluso entre comunidades especializadas en cuestiones digitales, analizaremos con detalle nuestras opciones. Para continuar, la seguridad de los datos en cuestión que utilicemos: almacenamiento, datos privados de participantes, documentos compartidos y proyectos. Finalmente, un último apartado de seguridad física en situaciones normales (del día a día) y en manifestaciones u otros contextos más vulnerables.

## SEGURIDAD DE LAS COMUNICACIONES

Puede que con el objetivo de proteger a los integrantes de una comunidad haya que cambiar algunas dinámicas a las que nos hemos acomodado. Es fundamental comprender que no tiene porque ser una transición directa, no hace falta aplicar una terapia de choque a todos los integrantes. Pero cambiar paulatinamente sí que debe ser un recordatorio concienzudo, un eco en las reuniones y conversaciones del grupo. Antes de instalar nuevas aplicaciones y poner las manos sobre el teclado hablemos de los peligros a los que estamos expuestos.

Para empezar muchas de las aplicaciones[7] que se utilizan comúnmente para la mensajería instantánea o mensajería en general son propiedad de empresas que públicamente han admitido compartir datos con terceros, filtrar información y venderla. Dichas aplicaciones (como Whatsapp) parecen gigantes inevitables que usa todo el mundo pero hay alternativas para nuestra comunidad, y con un poco de insistencia de nuestro círculo social en general. Facebook (compañía detrás de Whatsapp e Instagram) se ha disculpado más veces de las que ha puesto algún medio para remediar todos esos errores en la gestión de la privacidad de sus usuarios.

Pero a veces no hace falta este tipo de filtración. Los ataques dirigidos que comprometieron a miembros de Amnistía Internacional forman parte de un tipo de ciber ataque llamado *phishing*. El *phishing* consiste en engañar a la víctima para que envíe datos confidenciales, pulse un enlace corrupto, o filtre información que el atacante necesite. En este caso las víctimas pulsaron un enlace que infectó sus teléfonos móviles con un programa espía que controlaba sus comunicaciones, y por ende pudieron llegar a más miembros de la asociación. Gran parte de los ataques más dañinos hasta la fecha comienzan con despistes del usuario final, una comunidad educada en protección digital solventa gran parte de los posibles ataques.

El ataque **MITM** (*Man in the middle*) consiste en aprovechar una vulnerabilidad en la seguridad del medio de comunidad para interponerse entre el emisor y el receptor, tanto para robar información del mensaje (pasivo) como para impersonar al emisor y modificar el mensaje final (activo). ¿En qué situaciones nos podemos encontrar esto? Cuando usamos HTTP en lugar de HTTPS, por ejemplo .Cada vez encontramos menos páginas con este problema, incluso suele saltar un aviso de seguridad cuando entramos en sitios precedidos por HTTP. Sin embargo algunas páginas antiguas siguen teniéndolo.

## ¿Y AHORA QUÉ?

¿Cómo podemos protegernos frente a todas estas amenazas? Tranquilidad, vayamos poco a poco. Al principio hablábamos sobre la mensajería instantánea. Una de las alternativas más fáciles a **Whatsapp** y **Telegram**. Sigue sin ser la opción más segura, quizás la aplicación usable más segura para este tipo de mensajería sea **Signal**. La ventaja más fuerte de Telegram frente a Signal es la flexibilidad a la hora de gestionar grupos y canales de información. Un grupo de Telegram puede ser o no público; pueden usarse bots para hacer pasar una prueba de "*Captcha*" a nuevos miembros; gestión de roles de administración flexible; Descripción de grupos. Signal es más limitada en ese sentido, sin embargo ofrece mayor seguridad de las comunicaciones.

En las protestas de Hong Kong, Telegram ha tenido gran relevancia. Para empezar, existe un canal en donde van informando de manifestaciones, noticias y movimientos de los activistas de forma ordenada para que los lectores (supuestamente de Hong Kong, aunque es público) puedan participar conociendo la situación general. Además, uno de los grupos principales de organización (también empezó siendo público, pues pude entrar a echar un vistazo, aunque posteriormente se cerró) sirvió de medio principal para que algunos protestantes actuasen de forma ordenada. Tuvo tanta importancia que la policía de HK apresó temporalmente a su administrador bajo la excusa de alterar el orden público con el grupo que había creado.

Pero no sólo de mensajería instantánea vive una asociación. El correo es otra herramienta fundamental. Es común que la herramienta preferida para esto sea Gmail. ¿Habéis notado que Gmail sugiere respuestas para los mensajes? ¡Vaya! ¿Cómo funcionará eso? Si queremos que nuestra comunicación por correo sea segura (frente a **Google**, también), debemos buscar una alternativa a esta conveniente pero intrusiva herramienta (y en general conjunto de herramientas) que nos ofrece Google. En este caso, diré que nuestra mejor alternativa es **Disroot**[8], puesto que no sólo nos ofrece un correo si no también otras herramientas útiles que podemos echar de menos de Google, tales como documentos compartidos, nube digital, videollamadas, hojas de cálculo y mucho más. ¿Cuál es el truco? Ninguno, se sostiene con el trabajo de una comunidad especializada. Como hemos mencionado anteriormente, la privacidad tiene mucho que ver con la cultura libre.

## EL SOFTWARE LIBRE DEFIENDE LA SEGURIDAD TRANSPARENTE

Un punto extra en la seguridad de nuestras comunicaciones es cifrarlo. Aunque existen muchas formas de cifrar mensajes desde mucho antes de que la cultura digital se estableciera en nuestra sociedad, a la hora de proteger nuestros mensajes elegiremos una concreta: Un par de claves. Esto consiste en que ambos receptor y emisor se generan un par de claves, una pública y otra privada; La pública, como su nombre indica se compartirá con los contactos (puede publicarse en una web, un servidor de claves, enviarla por correo, etc) y otra, la privada, se guardará celosamente y no se compartirá bajo ningún concepto. La pública le servirá a tus contactos para cifrar mensajes de forma que sólo puedan ser descifrados con la clave privada.

Para que la comunicación sea completamente segura, ambos emisor y receptor deberán tener un par de claves. Para poder generar estas claves, existen varias alternativas. Antes de discutirlas, una pequeña cuña de nuestro sistema. Si bien pueden generarse este tipo de claves desde cualquier sistema operativo, GNU **Linux** OS (con sus muchas distribuciones) nos ofrece una transparencia y un soporte de comunidad mucho más seguro que **Windows**. De modo que, tanto por su cultura libre como por su seguridad, se recomienda el uso de Linux. Algunas distribuciones comunes (familiares para el usuario medio) pueden ser **Ubuntu**, **Elementary**, o **Mint** por ejemplo, aunque existen muchísimas y puede elegirse uno acuerdo con las necesidades de la comunidad específica[9].

De vuelta a las claves, nuestras opciones son variadas: para el usuario habituado a la terminal de Linux pueden usarse líneas de comando[10] con una herramienta llamada **gpg.** Para los usuarios inexpertos que quieran ir sobre seguro, existen aplicaciones con interfaz gráfica (incluso *add-ons*) para crear claves como por ejemplo **Mailvelope** de **Mozilla Firefox**.

Contra el *phishing*, la única solución es que los miembros de la comunidad estén educados en que existe este tipo de ataque y deben tener cuidado a la hora de compartir información o de confiar en el origen del mensaje. Si el mensaje requiere información urgente y confidencial, aseguraos de tener un plan de acción ordenado, en el cual determinada información sólo deba pasarse cifrada, requiera una llamada telefónica a algún responsable de esos datos, y que la urgencia no se interponga en la seguridad. No perder la calma, y ante la duda nunca actuar por prisas. Si nos llega un enlace sin contexto, no lo pulsaremos hasta asegurarnos previamente de que su contenido es legítimo, preguntando "¿qué contiene éste enlace?" si sabemos que la fuente es un contacto fiable, o ignorándolo de primeras si es de un desconocido. Aunque el contacto sea fiable, su dispositivo puede estar comprometido, y puede que sin saberlo estén usando su buen nombre para mandar enlaces corruptos. ¡Mucho cuidado! Un correo electrónico, además, puede manipularse para que parezca que el emisor es de fiar cuando no lo es. Existen programas que automatizan estos ataques (como *Gophish*[11]) así que es relativamente común. Esto no significa que tengamos que convertirnos en paranoicos, pero sí **estar atentos**.

## CUIDADO CON LAS PRISAS, URGENCIAS Y DATOS SENSIBLES

Es importante remediar cualquier servicio que se utilice que tenga http y no https. Si es una herramienta interna, debe remediarse inmediatamente, si es una herramienta externa lo mejor es buscar una alternativa. Http significa que cualquier dato que cruce ese servicio irá sin cifrar; Terminantemente prohibido usarlo más aún si pide contraseñas y datos sensibles. Una solución temporal o preventiva es instalar **https everywhere**[12], un *add-on* que nos permite forzar el cifrado mientras navegamos, en caso de que falte. Pero es una medida preventiva, en ningún caso debe ignorarse por mucho tiempo un uso continuado de http.


## SEGURIDAD EN LAS REDES

La presencia en las redes permite a determinadas asociaciones y grupos a publicar actualizaciones, quedadas, noticias y más. Antes mencionábamos los peligros de utilizar redes como Facebook o Instagram, también podríamos mencionar Twitter que sin ser de Facebook también ha filtrado información y censura contenido. La decisión sobre el uso de las redes es muy personal y depende de cada caso, pero ha de mencionarse que existen alternativas, las cuales no son empresas y por lo tanto sus intereses y objetivos son diferentes.

Para el caso de Twitter, por ejemplo, **Mastodon** es una alternativa popular con bastante movimiento. En general me gustaría introducir el concepto de "**Fediverso**"[13]. El Fediverso es una colección de redes sociales que nos permite publicar contenido en un contexto comunitario, distribuído e independiente de Google, Facebook o Twitter. Es mundo interesante que vale la pena investigar, y que por lo general además aloja a usuarios abiertos a escuchar y ayudar a otras comunidades.


## SEGURIDAD DE DATOS

El post-it en la pantalla del ordenador ya no es una opción válida. Para guardar contraseñas, una de las mejores opciones es usar un gestor de claves, como por ejemplo **Keepass**. Keepass nos permite guardar de forma centralizada pero segura nuestras contraseñas. Es recomendable tener un backup en una unidad aparte del ordenador del archivo de claves, en caso de una emergencia. Si decidimos usar un servidor para guardar información de miembros, datos sensibles o información en general del grupo, debe protegerse dicho servidor: Controlar quién tiene permisos de administración, un sólo *root*, una política de contraseñas personalizada, contraseñas con expiración no muy tardía, ningún usuario sin contraseña, *ssh* con clave… Todo esto forma parte de un proceso llamado **Hardening** de servidores[14], y es un paso fundamental.

Aunque existen diversas guías en internes de como hacer *hardening* básico sobre un servidor, es recomendable conseguir la ayuda de un administrador de sistemas cualificado para ello. En caso de guardar datos en local (en el propio ordenador), es recomendable hacerlo en una partición cifrada.

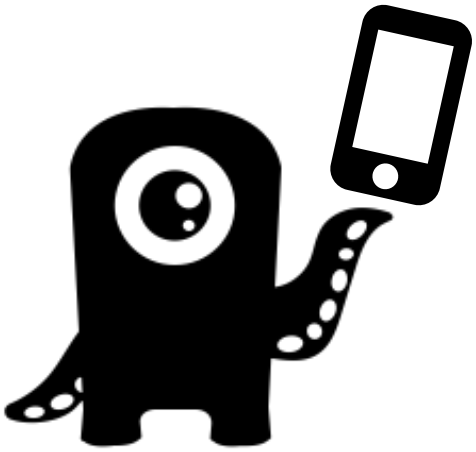
Una herramienta muy útil para hacerlo es **LUKS**. De este modo, puede guardarse información con cierta tranquilidad y de forma ordenada. Esto puede ser útil incluso si la seguridad física del ordenador se ve comprometida, aunque es útil conocer algunos de los ataques físicos (en el que se ve comprometido directamente el hardware) que puede sufrir un ordenador o un dispositivo.

## SEGURIDAD FÍSICA ORDINARIA

Al igual que en las comunicaciones, antes de listar las posibles medidas, hablemos de los posibles ataques de este tipo. Existen diversas formas de comprometer los dispositivos de un miembro de la organización, de modo que podría comprometer a otros miembros, como el ataque a miembros de Amnistía Internacional que mencionábamos antes. Su ordenador o su móvil son los objetivos fundamentales de esta clase de ataques.

Un *pendrive* puede no ser un *pendrive* ordinario[15], puede ser un dispositivo que emule la entrada por teclado al ordenador, que esté programado para en segundos implantar un programa espía, un virus o cualquier amenaza en el ordenador. Para ello debe tenerse mucho cuidado de qué dispositivos permitimos que se conecten en el ordenador o a quién dejamos acercar a nuestro ordenador. Una forma sencilla de prevenir estos ataques si somos despistados es tener protectores contra el polvo en nuestras entradas de USB. De este modo, es más complicado que no nos demos cuenta de que alguien introduce un *pendrive* en nuestro ordenador.

Es fundamental acostumbrarnos a bloquear la pantalla cuando nos alejamos aunque sea brevemente del ordenador (pulsando tecla de sistema+L o manualmente en opciones →bloqueo de pantalla), no debe verse como una acción agresiva o de falta de confianza. Aunque sepamos que la otra persona es de fiar, es una buena práctica para acostumbrarnos a hacerlo siempre. Lo mismo ocurre con el teléfono móvil, que además es recomendable que tenga un patrón de seguridad a ser posible que no sea de huella dactilar. La huella es segura, pero ceder esa información puede no serlo tanto. Respecto al móvil, además debemos mantener la pantalla limpia, de otro modo un atacante puede observar las marcas del patrón del movimiento del dedo para desbloquear la pantalla de un móvil desatendido, ¡ademas es sano tener una pantalla limpia! Otra buena práctica es cubrir la webcam y cámaras del móvil con pegatinas para este fin. Las venden en muchos sitios, veréis que la mayor parte de los profesionales de ciberseguridad lo hacen incluso en sus dispositivos privados.



## SEGURIDAD FÍSICA ESPECÍFICA

La participación en protestas y manifestaciones para reivindicar causas concretas pueden, en algunos casos, suponer un peligro añadido a la seguridad ordinaria. Es por ello que en estos casos es recomendable que tanto grupos como individuos conozcan a qué se exponen. El rango de situaciones en un contexto de protesta es amplio, por lo tanto en este apartado se analizará de una forma superficial y general. Hablaremos principalmente de la seguridad en dispositivos móviles y *wereables*, puesto que es menos probable llevar consigo un portátil encima en estos casos. Sobre los *wereables* simplemente es mejor dejarlos en casa; las pulseras y relojes inteligentes por lo general acumulan información de nuestra localización, ruta, pasos, etc. Esta información es mejor limitarla en estos casos por prevención. En el caso de los teléfonos móviles, hay una serie de recomendaciones dependiendo de la situación:

- Limpiar la información del móvil, hacer un *backup* en nuestro ordenador antes de salir.

- Cifrar el móvil o al menos parte, donde almacenaremos lo importante. Para esto necesitaremos *rootear* el móvil, y debemos tener en cuenta que afectará a la velocidad de nuestro teléfono. SI decidimos cifrarlo, el paso anterior es fundamental (crear un *backup*) puesto que es posible que en el proceso se pierda información. También es recomendable tener patrón de desbloqueo. Es un buen momento para comentar que como alternativa a *Google Play* (que registra y enlaza a tu cuenta tus descargas) existe **F-Droid** (entre otros) y a *Android* en general **LineageOS**, por ejemplo.

- Si hacemos fotos durante la protesta, enviarlas a una nube (no la de *Google*, a ser posible **NextCloud**), a tu correo y/o a un grupo de confianza de la comunidad en remoto que no esté en la protesta y gestione la publicación en directo en medios de confianza (como comentábamos de las redes del **Fediverso**).

- Desconectar **Wifi**, **Bluetooth**, **localización**, **NFC** si tiene y en general mantenerlo en modo avión salvo que sea necesario (para mandar las fotos, por ejemplo). En Estados Unidos está muy expandido el uso de WEA (*wireless emergency alerts*) de modo que se pueden mandar de forma localizada SMS de alerta, algo que se utiliza muy comúnmente para tiroteos, ataques terroristas o emergencias medioambientales. Este tipo de tecnología también se ha utilizado, sin embargo, para localizar y alertar a los participantes de manifestaciones. Existen ataques mediante los cuales, un dispositivo puede emular una red habitual Wifi a la que tu móvil se conecta de forma automática y capturar el tráfico del dispositivo, sin que lo notes porque sigues teniendo conexión a Internet. Para más información sobre este tipo de ataque, buscar *"Pinneaple Wifi"*. El participante, depende del contexto, podría plantearse también el uso de una **VPN** (*Virtual Private Network*) que permite a sus usuarios navegar e intercambiar información a través de internet como si de una red privada se tratase, En este caso el usuario debe asegurarse que ésta es de confianza, porque si no es igualmente problemático.

# 02/FEMINISMO

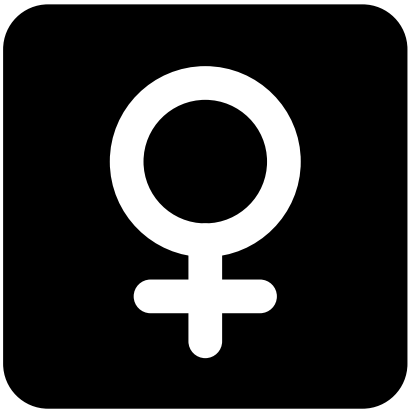
Protección y sororidad digital

Las vulnerabilidades digitales de las comunidades feministas son las mismas que podemos encontrar en cualquier otra comunidad, sin embargo creo importante mencionar que existen manuales, comunidades y herramientas dirigidas específicamente a la protección, desarrollo técnico y apoyo a las mujeres. Si es una comunidad que trata a mujeres víctimas de algún tipo de acoso, es posible que algunos de sus dispositivos estén comprometidos o vigilados. En tal caso, es recomendable

**CUANTO ANTES, MEJOR.**

sustituir dichos dispositivos comprometidos y hacer una limpieza general de las cuentas de la afectada. Para ello, cambiar todas las claves de sus cuentas por nuevas idealmente difíciles de recordar o averiguar (y guardar en *Keepass* o un programa similar), que contengan números, letras, símbolos y patrones aleatorios. Si es posible usar doble autenticación, seleccionar siempre esta opción. Esto puede hacerse a través de códigos mandados a un número a través de SMS o con unos dispositivos hardware específicos parecidos a un pendrive llamados **YubiKey** o **FIDO U2F** (una versión más asequible de la misma idea de dispositivo). En este caso, siempre que se quiera hacer *login* en la cuenta, se deberá introducir el USB en el dispositivo.

Para pedir formación en situaciones específicas o contra ataques de ingeniería social (como los que mencionábamos antes con técnicas como el *phishing*) o en general formación técnica, puede acudirse a grupos y asociaciones de ciberseguridad conformados por mujeres, si así lo prefiere la comunidad. En España, por ejemplo, está **Wics**, conformado por profesionales de varias áreas de ciberseguridad o **WoSEC** (Women of Security), en Madrid, que apoya demás charlas de varios niveles por parte de profesionales. También **Ética Hacker** tiene contacto con mujeres del sector y su fundadora promueve la divulgación en seguridad.



**Hasta que no sean conscientes, no se rebelarán, y hasta que no se rebelen no serán conscientes.**

GEORGE ORWELL \\ 1982

# 03/ANEXO TÉCNICO Y REFERENCIAS

¡Consultar siempre que sea necesario!

## LISTA DE REFERENCIAS

Durante todo el manual se han hecho referencias a diferentes fuentes. A continuación, la lista de referencias:


1) Datos sacados de www.internetlivestats.com.
2) El dorado, una historia crítica de internet - Enric Puig Punyet, Clave Intelectual.
3) Asociación estadounidense dedicada a la protección de los derechos digitales: www.eff.org.
4) En España encontramos Interferencias, Trackula o Críptica. Los QR a las páginas, respectivamente son:

Interferencias.tech

trackula.org

criptica.org

5) Más información de los ataques en www.20minutos.com.mx/noticia/346176/0/amnistia-internacional-denuncia-ciberataques-a-periodistas-en-argentina.
6) Edward Snowden, ex agente de la NSA compara la privacidad con la libertad de expresión en una entrevista en la Universidad de Arizona. uanews.arizona.edu/story/edward-snowden-compares-privacy-freedom-speech.
7) Más información sobre seguridad en dispositivos móviles en el libro de licencia libre "Resistencia Digital" publicado por Críptica.
8) Más información y registro en disroot.org.
9) Puede buscarse la distribución perfecta usando el buscador de distrowatch.com/search.php.
10) Para más información de cómo generar un par de claves desde la terminal, leer el anexo técnico en este mismo capítulo.
11) Más información en getgophish.com.
12) HTTPS Everywhere es una aplicación desarrollada por la Electronic Frontier Foundation www.eff.org/https-everywhere.
13) El Fediverso es una serie de redes sociales libres creadas por la comunidad. Para más información visitar fediverse.party.
14) Uno de los tutoriales más completos (en inglés) para servidores Linux es éste: www.tecmint.com/linux-server-hardening-security-tips.
15) El **rubber ducky** (shop.hak5.org/products/usb-rubber-ducky-deluxe) y sus versiones caseras (inc0x0.com/2018/10/budget-usb-rubber-ducky-digispark-attiny85) nos permiten imitar la entrada de teclado en un ordenador y lanzar ataques en terminales desatendidas.

# USO BÁSICO DE LA TERMINAL DE LINUX

Para empezar, cuando abrimos una terminal nos sitúa en home por defecto. si escribimos "ls" y le damos a "*Enter*" nos saldrá una lista de los directorios que hay en home, posiblemente "Documentos", "Descargas", "Imágenes", etc. "**ls**" quiere decir "listar", por eso nos lista todos los archivos y directorios que hay. Si por lo que sea queremos saber más sobre este comando escribiremos "**man ls**" y pulsamos "*Enter*"; "man" nos sirve para saber más sobre cómo funciona un comando, viene de "manual", instrucciones. Por ejemplo si escribimos "ls -l" nos saldrá más información sobre cada elemento que lista. Imagina ahora que queremos entrar en el directorio "Documentos" o "Documents", depende de en qué idioma lo tengas. Para eso se usa el comando "cd Documentos" y pulsamos Enter, de ahora en adelante se entiende que siempre que queremos ejecutar un comando pulsaremos Enter.  Ahora, donde nos salía "usuario@ordenador:~$ " nos debe salir "usuario@ordenador:~/Documents$ " esto es porque "**~**" simboliza *home* y "**~/Documents**" es la carpeta Documents dentro de *home*.

Ya sabemos listar y entrar en directorios. Ahora vamos a crear un directorio en Documentos. Para eso, usamos el comando "**mkdir**" (make direcory). "**mkdir ejemplo**" creará una carpeta llamada "ejemplo" en Documentos. También podríamos haberla creado desde home si indicamos que se haga en Documentos, escribiendo "**mkdir /Documentos/ejemplo**". Podemos crear archivos vacíos con el comando "**touch archivo**". podemos editar archivo con un editor de texto normal, pero si por lo que sea queremos usar la terminal, también puede hacerse, ahora explico cómo.

El comando "echo" (eco) nos permite imprimir por pantalla cosas. Por ejemplo si hacemos "**echo 'hola mundo'** " nos mostrará en la siguiente línea "hola mundo". Eso es porque por defecto saca el mensaje por terminal, pero podemos cambiar el destino final del mensaje y meterlo en un archivo, si escribimos "**echo 'hola mundo' > archivo_ejemplo**" creará un archivo_ejemplo (si no está creado ya) y escribirá dentro "hola mundo". Si una vez hecho esto escribimos "echo 'hola de nuevo' > archivo_ejemplo" sobreescribirá el mensaje original y pondrá el nuevo, "hola de nuevo". Si lo que queremos es añadir líneas sin sobreescribir el contenido usaremos ">>" en lugar de ">", por ejemplo "echo 'amigo mio' >> archivo_ejemplo", hará que el contenido de nuestro archivo_ejemplo sea:

hola de nuevo
amigo mio

si quieres comprobar el contenido del archivo desde la terminal, basta con hacer "**cat archivo_ejemplo**" y te mostrará el contenido. Los archivos y directorios pueden tener diferentes tipos de privilegios, o el propio usuario puede ejecutar cosas con diferentes privilegios. Los privilegios nos permiten limitar las acciones en terminal y el PC en general, son muy importantes. para ejecutar algo con permisos de administrador (si se tiene la contraseña) hay que usar "sudo". Por ejemplo "**sudo apt install git**", este comando nos permite instalar con un gestor de paquetes (llamado apt) un programa llamado "**git**", con permisos de administrador (sudo). Si queremos usar el usuario *root*, que es administrador (ojo, es peligroso, solo hacer cuando se esté seguro de todo) podemos hacer "**sudo su**" (ejecuta *superusuario*) y entrar en modo administrador.

# CÓMO CREAR UN PAR DE CLAVES DESDE LA TERMINAL DE LINUX

Para crear un par de claves en una terminal de Linux usaremos gpg. Si no está instalado lo instalamos usando:

**# apt install gpg**

Nota: Cuando usamos # significa que estamos en root y $ un usuario normal. Para hacer cosas con permisos desde un usuario normal añadiremos el prefijo "sudo". En este caso por ejemplo sería:

**$ sudo apt install gpg**

Una vez tenemos instalado gpg, procedemos a crear el par de claves. Primero escribimos:

**$ gpg –full-gen-key**

Una vez le demos a la tecla *Enter*, seguiremos los pasos que nos indica la propia herramienta. Para empezar nos pedirá que elijamos el algoritmo de cifrado, podemos usar el que viene por defecto: RSA, al igual que el tamaño, salvo que queramos algún tamaño en especial. Más tarde nos pedirá una fecha límite para nuestra clave, por ejemplo un año (1y). Aceptamos la configuración si está correcto todo escribiendo "o".

A continuación escribiremos los datos que nos indica, nombre, email al que queramos enlazar la clave y si queremos dejar alguna firma o comentario. Todo esto estará enlazado a la clave. Una vez que acabemos de configurar la información y creemos la clave podemos exportar el archivo a compartir (la clave pública) usando:

**$gpg --armor --export {ID} > pubkey.asc**

siendo {ID} (sin los corchetes) el ID de nuestro usuario. La clave pública obtenida ahora debemos compartirla con nuestros contactos. Para descifrar un archivo que nos envíen cifrado con nuestra clave pública, tan sólo tenemos que escribir en la terminal, situados en la misma carpeta donde el archivo cifrado:

**$ gpg --decrypt mensaje_cifrado.asc > mensaje.txt**

Si nos mandan una clave pública, para cifrar mensajes usaremos:

**$ gpg --encrypt --sign --armor -r email_de_mi_contacto@ejemplo.com mensaje.txt**

De este modo nos aseguraremos de tener una comunicación segura. Recuerda:

La clave a compartir es la **pública**, nunca compartir la privada.

Podemos revisar los permisos en home que tienen los usuarios del sistema ejecutando:

**$ls -ahl /home/ 2>/dev/null**

En general podríamos ver los permisos de todos los directorios salvo de uno, como por ejemplo "Ejemplo" usando:

**#find / -perm -222 -type d -not -path "/Ejemplo/*"**

o

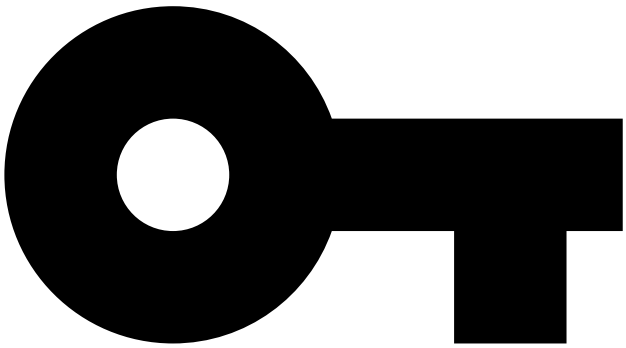
**$sudo find / -perm -222 -type d -not -path "/ejemplo/*"**

Podríamos comprobar las reglas sobre las contraseñas del sistema usando:

**$grep "^PASS_MAX_DAYS\|^PASS_MIN_DAYS\|^PASS_WARN_AGE\|^ENCRYPT_METHOD" /etc/login.defs 2>/dev/null**

Debemos comprobar que tan solo el usuario *root* tiene permisos de absoluto administrador. Para ello al ejecutar el siguiente comando sólo debería salir un usuario:

**awk -F: '($3 == "0") {print}' /etc/passwd**



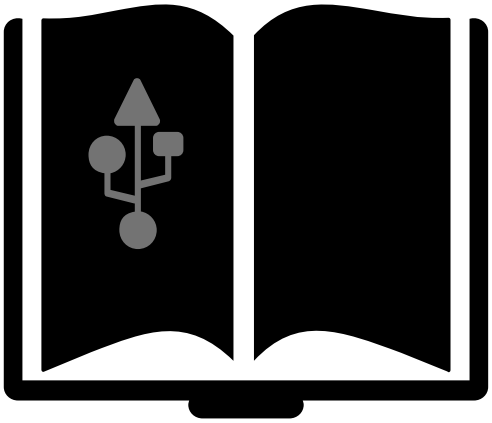
# 04/BIBLIOGRAFÍA

Lista de recursos

## LISTA DE LIBROS PARA AMPLIAR

Lista de libros relacionados con la temática:


- The architechture of privacy - Courtney Bowman, Ari Gesher Editorial O'Reilly
- La sociedad en la red: una visión global – Manuel Castells Editorial Alianza
- El Dorado. Una historia crítica de internet – Enric Puig Punyet Editorial Clave Intelectual
- La democracia Internet. Promesas y límites – Dominique Cardon Editorial Prometeo
- Netocracy: the new power elite and life after capitalism – Alexander Bard y Jan Söderqvist
- El nuevo Leviatán: Una historia política de la red – Enrique Alonso Editorial díaz/pons
- Cypherpunks Freedom and the future os the Internet – Julian Assange
- El Fin de la privacidad – Reg Whitaker
- Ética Hacker y el espíritu de la era de la información – Pekka Himanen
- Mundo Orwell Manual de supervivencia para un mundo hiperconectado – Ángel Gómez de Ágreda Editorial Ariel
- Albafetización crítica – Inés Bebea Editorial ondula
- Resistencia Digital – Críptica Editorial Descontrol

Contacto con la autora:

Paula
Telegram: @terceranexus6
Correo: terceranexus6@disroot.org
Mastodon: https://cybre.space/@terceranexus6
A través del grupo Interferencias en Telegram: https://t.me/inter_ferencias