Comunicarnos de forma segura cifrando nuestros correos, navegar anónimamente, encriptar nuestro ordenador, generar contraseñas indescifrables, mantenernos seguras y ajenas al ojo espía de la Megamáquina.

Gran parte de activistas utilizan la tecnología en su día a día para comunicarse y relacionarse con las demás, pero…

¿Hemos profundizado en introducir esta tecnología como herramienta de lucha contra el sistema?

En la guerra contra la máquina existen varios frentes abiertos y las medidas de seguridad a tomar están presentes en todos y cada uno de ellos.
Con esta guía queremos proyectar la idea de que por mucha tecnología que emplea el poder para controlarnos y mantener el panóptico, tenemos a nuestro alcance las herramientas necesarias para luchar contra él y a la vez protegernos de sus ataques.

MANUAL BÁSICO DE SEGURIDAD INFORMÁTICA PARA ACTIVISTAS

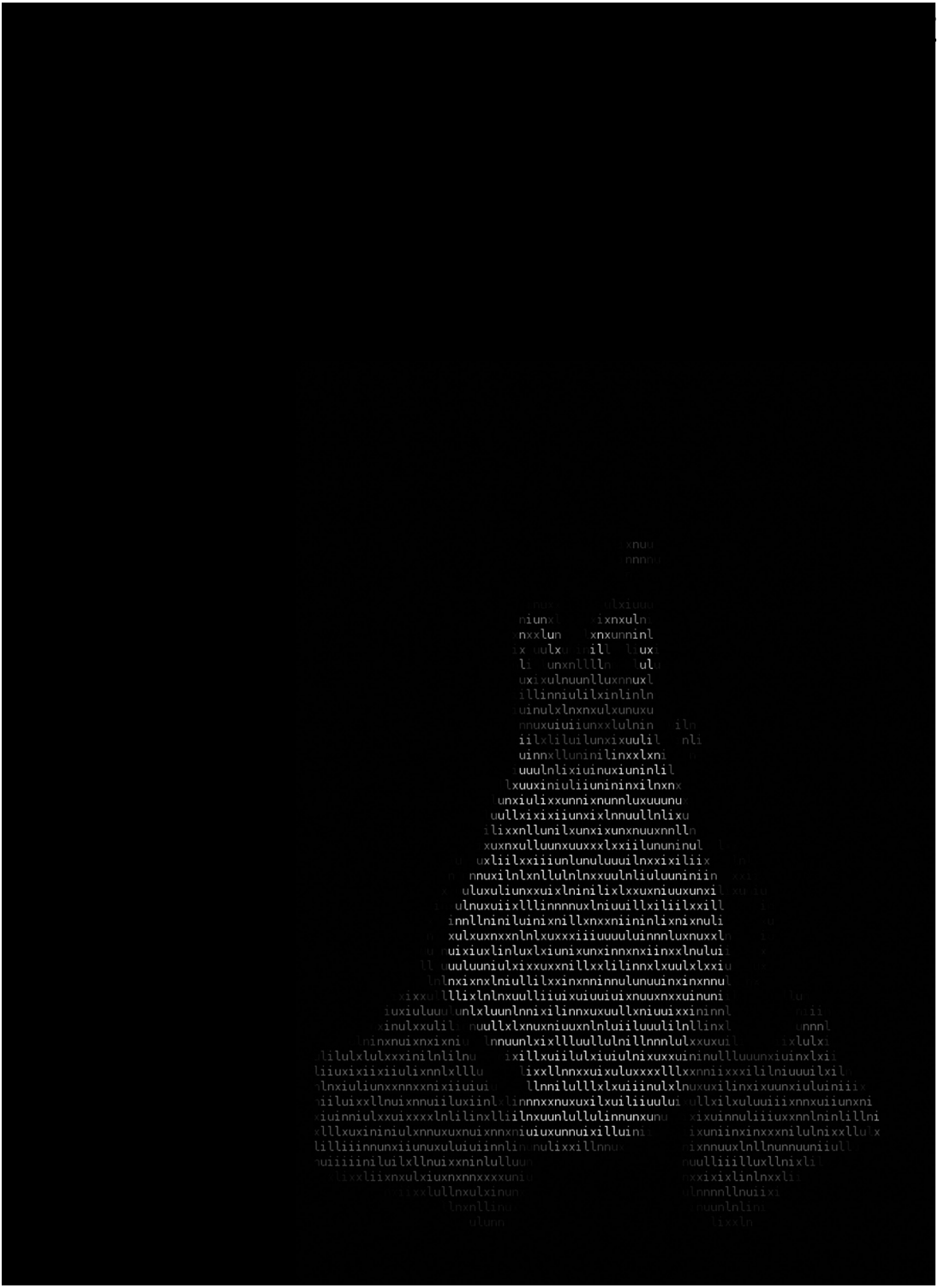
MANUAL BÁSICO DE SEGURIDAD INFORMÁTICA PARA ACTIVISTAS

Una Guía
Para Proteger Nuestros Ordenadores,
Y A Nosotras Mismas
Hacer Frente A La Represión
Y extender Una Cultura De Seguridad

Deep W[illegible]ret

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGP Desktop 9.9.0 (Build 397)

mQENBEldAygBCADXNQd7h3XryKcV8L+kaWvKcOyEPV3PpcaN2z2dOZFYzKTSpUQA
X1HTzWvNoaMzQnKHW3KEkx8wmKl3B7Oq4Hb4sCO17C39CAgtI+sLrIyKQTsgUYl4
fUDWcJAKQvb9m/w0tkGu/hOelqv/M0YY4Xa44LWL3OF0PEmdHBXz8eAaiQaVZYaX
AhpjHXdpEGyfImjenT0J0hEAWUezuyw88bSb/+EtNpEnwGXw15xjK/LHqWKZ4Ja2
bnmyVVoslvndWCqJGD+d/0LkIN4t5XXuarDbH1BV2SQmcJI/Rt+fPm2E+tK1i+3y
3NwTRacTI8kPfTG+a/1ERu00DqIiIjIFGFnNABEBAAG0IkJpdGUgQmFjayA8aW5m
b0BkaXJlY3RhY3Rpb24uaW5mbz6JAYcEEAECAHEFAkldA0swFIAAAAAAIAAHcHJI
ZmVycmVkLWVtYWlsLWVuY29kaW5nOHBncC5jb21wZ3BtaW1lBwsJCAcDAgoCGQEZ
GGxkYXA6Ly9rZXIzZXJ2ZXIucGdwLmNvbQUbAwAAAAMWAgEFHgEAAAAEFQgJCgAK
CRANL8KCwjXXSpezB/wOgVGHoFBIScV/12JrSduMmoXAfPnsNsRum/Os5xV9TaIB
IPVvx6bWzumOSyhoVAsg1ev3CFKo24cFefdgJyt8CHzkF+TJURdr09ymXSvYNNS8
RDys2HQCYhJ2Sc/gvEbmLMF834azXLUWahIHLLSV6Ed35AqZ1ujRNiGC9vLEfOLA
GxLNopiHTB3GP9OoSQlUbNpnsUdDZshBh8AyNya5UDCDZfe9Y7PqTkPNGleVF3gv
wDcSxUM/aTr1SDbLrpCQiOxR3P8YrvdemyOc3HYC/YVLsRTivAQUVwf5UB6PzWaR
UbRb/7015R24H7GVVw1OXLVZwIjDFGinreRJdfVyuQENBEldAygBCAC8AIBxlg3d
pf4kLeN0WtibUR9nAekwZUocRQGzLQMDyL74vT2QWc7t+3VFuEyyKtMxh/gXXbtb
nug6ikvzwRttGXKi3UqggoO25ym/OKQMJw0Q6I1B8e/hwYPzVdBr1FdtwqxNVeCX
g0TdaQVtZSI5PcC5C3dyuzwHG+sdXe/pXxmaQQ/s6wxFwmEm3e5/wNxywcEcRR5v
34BKX2sXVj3uupkeCE4nlEtSXD5vWIp4/i0ZUjDlHt1QmRP2/MrjkYDDR98fFI9b
ZI9SPRqhCTRMB+ssLAcWjct6OTENz+UoBSZg99hFIV33lRn1yMnVsnQYJqJ33ZIE
WfPE+gKEJerPABEBAAGJAkEEGAECASsFAkldAyoFGwwAAADAXSAEGQEIAAYFAkld
AykACgkQiadyneA9EL6cvwf+OiDRXOpoP/rDpInrxBxAC2Q33GBHpVDheLcD6Gra
V5oTrhInTJJHT2h7igskIkAWJGEQAKTr2AP7E+9f4WQTtx3Imkay0hX/zTA9i29g
dQj5J7/W90dX+io8QW7CT7e67YrXIMcPgxaCGV/NZX8JgzHpkiddkXtSEZkMzuHv
pdgLUG1J6hFe6u8yvAP8dtso93gxORs4T/XapvCSvh5wgtqaVJO6jrYReuP+HfJk
JA59EJH1vISc1eWHUKc2wBC4dil5UFngaiJcdz4l1PUqbHmcGiUIMjk411OsmT3a
PQCf+Us6SbqWM7WY4doutMdGAjG9N/y6nzHtYGTy6S3B0wAKCRANL8KCwjXXSnAp
B/9yWxJ23PZ2Zvx2HnX3zZJabsYlZsK8P5XqTIjsSN8tBjoy359Im757v2038sfT
cK0imRDho7vs6dtfl4lBcUNKav4Xg2RdgWQhL0+AM8/2cOViPZSP6ZpXy7/vxHQg
YZYxeagf6Rf5lmkdck4xR6YASqjAk5lEAqh+MwudBimCT1ZX4MQpG7u0iks1SDBF
G/x/cCqWh3KsOeTemrtJCa9l96P2WxVORRn7BQ72KoxGusBkvCq55UE4Sf10prec
21IXr7S6ACSWzv1hw7S91CDX32BagGluaE3E1/eF0krzZlr+tnOH5Sc9mAA3N7kJ
QGiBD1ijYoRBAD87MR2OVHJw9COmcsG4Q+QAaT5ffgBHo1PcrONLBq+FbYc6s/w
CDW+xaIEkS0DtbINOvSvLC8nWLXqpL+rwPNdSplFQ0/DSppy4ouwG1wwFY2s9zM2
vxpaKXrMu1OfNxHUORWBL/kaHdmFsJSJPXL5KJdycTG831q6Vl0TzYrzEwCg/4wh
fqjsPWbusE7ynvOy7XpX5lED/j3pVniejERRZ/+TZYHX/2lYYKHuhyrK9KHfnggH
b8K7k7DrVpOkYraLZdAsl47ikcc0eBYdXvyHgS7VFVXP+9FjU88sp5cEok4ZRYJQ
umoYh/+33E5TGcZ6oClz1zHDdsJjnfKfDqzehK6uPeYLierHVkmZmLGfkrB0DBGy
rcqyBADPGse8SBvJmj+xw3kAzPOn2t0JcdEfkCmyYzx0PuyDlVhe/yGfMppiLUno
QziezxqJRJHeEV5L7cEfkTVAHwcq++61ILzMZv8yPOnizeeT3Cb8+YE9d4nAkbvz
xuGFCnVJfVAg4Em88PzeCvhtf4+pCnbpfOlUCpfvEFiv8o5t+rQoO29sZWN0aXZy
lExhlEhhaW5lIDxsYWhhaW5lQGxhaG
AwIBAhkBAAoJEAZApTrwmHRnQ1kA
7ARHIytxcV8k6CBShFSKFbkCDQQ9Y
T7bxbrILOCDaAadWoxTpj0BV89AHxs
dlJPPT2N286Z4VeSWc39uK50T8X8dn
cjrUGvC/RgBYK+X0iP1YTknbzSC0ne
8KVbGl2Ou1WMuF040zT9fBdXQ6MdC
yAcpesqVDNmWn6vQCICbAkbTCD1n
8ss7lqLGzOianfpEjKuvtCuqe94GmipC
5n1IqBarhekZEQcz3xO0oREVbDm6C/
QHqjl97AzWHUOdGGS7L8okGVkTOW
KZcPghzOebyLbVclUXWwT2gb1j8g/iF
O3Yuq3B0IOX8e9PNINXKVREt3XLaj4/
rfp7xVJvBoJT3fdhrXPkEYkARgQYEQ
mgrK+6i2v0OgKJKG2VAXIhv6WQCfa
=w4aAbnmyVVoslvndWCqJGD+d/0Lk
3NwTRacTI8kPfTG+a/1ERu00DqIiIjFG
b0BkaXJlY3RhY3Rpb24uaW5mbz6JA
ZmVycmVkLWVtYWlsLWVuY29kaW5r
GGxkYXA6Ly9rZXIzZXJ2ZXIucGdwLm
CRANL8KCwjXXSpezB/wOgVGHoFBI
IPVvx6bWzumOSyhoVAsg1ev3CFKo2
RDys2HQCYhJ2Sc/gvEbmLMF834azX
GxLNopiHTB3GP9OoSQlUbNpnsUdDZ
wDcSxUM/aTr1SDbLrpCQiOxR3P8Yrv
UbRb/7015R24H7GVVw1OXLVZwIjDF
pf4kLeN0WtibUR9nAekwZUocRQGzL
nug6ikvzwRttGXKi3UqggoO25ym/OK
g0TdaQVtZSI5PcC5C3dyuzwHG+sdXe
34BKX2sXVj3uupkeCE4nlEtSXD5vWIp
ZI9SPRqhCTRMB+ssLAcWjct6OTENz
WfPE+gKEJerPABEBAAGJAkEEGAEC
AykACgkQiadyneA9EL6cvwf+OiDRXC
V5oTrhInTJJHT2h7igskIkAWJGEQAK
dQj5J7/W90dX+io8QW7CT7e67YrXIMc
pdgLUG1J6hFe6u8yvAP8dtso93gxOR
JA59EJH1vISc1eWHUKc2wBC4dil5UF
PQCf+Us6SbqWM7WY4doutMdGAjG9
B/9yWxJ23PZ2Zvx2HnX3zZJabsYlZsK
cK0imRDho7vs6dtfl4lBcUNKav4Xg2R
YZYxeagf6Rf5lmkdck4xR6YASqjAk5lE
-----END PGP PUBLIC KEY BLOCK-----



MANUAL BÁSICO DE SEGURIDAD INFORMÁTICA PARA ACTIVISTAS

UNA GUÍA
PARA PROTEGER NUESTROS ORDENADORES
Y A NOSOTRAS MISMAS
HACER FRENTE A LA REPRESIÓN
Y EXTENDER UNA CULTURA DE SEGURIDAD

MËNALKIAWN

Manual Básico De Seguridad Informática Para Activistas
Barcelona – Agosto de 2013

Escrito y Diseñado por Mënalkiawn (Andar en libertad)

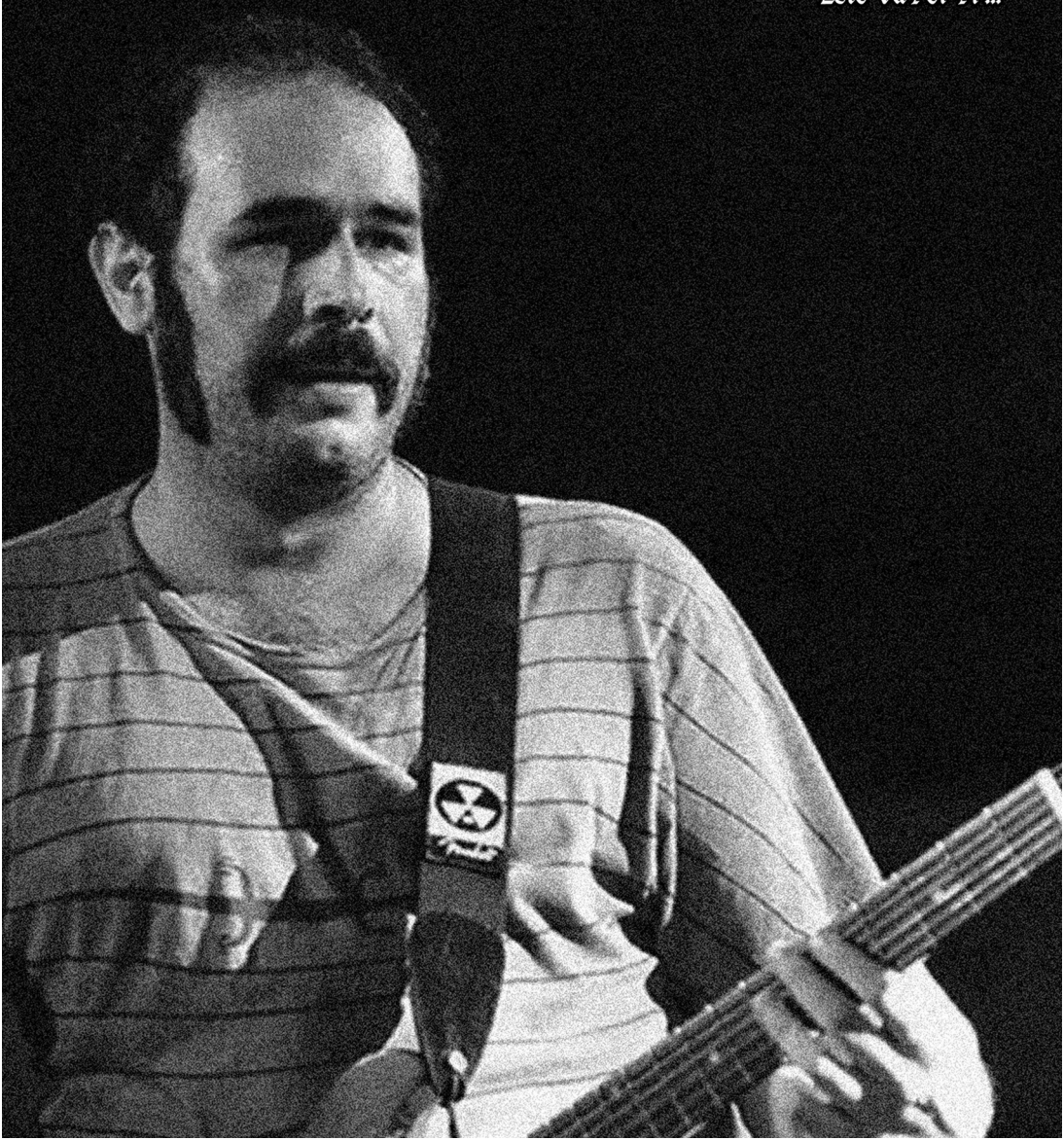
Todos los textos en cursiva que preceden a los capítulos, excepto la "declaración de principios" y el "prólogo" han sido extraídos del libro "Bienvenidos a la Máquina" (Editorial Klinamen)

URI CABALLERO

MÚSICO, ACTIVISTA, PERO SOBRETODO UN AMIGO

SIEMPRE ESTARÁS EN NUESTROS CORAZONES

Esto Va Por Ti ...




NO NOS
VAMOS PERROS

ÍNDICE

Una Declaración De Principios

"Cuando pienso en la mecánica del poder,
pienso en su forma capilar de existencia,
en el punto en el que el poder encuentra el
núcleo mismo de los individuos,
alcanza su cuerpo, se inserta en sus gestos,
actitudes, sus discursos, su aprendizaje,
su vida cotidiana"

Michel Foucault

Una Declaración de Principios

"…Actúo de forma que el ejército enemigo tome mis puntos fuertes por débiles,
Mis puntos débiles por fuertes, mientras que yo convierto en débiles sus puntos
Fuertes y desvelo sus fallos…
Disimulo mis huellas hasta hacerlas imperceptibles:
Guardo silencio para que nadie pueda oírme"

"Ho Yen Hsi" El Arte de la Guerra – Sun Tzu

Cuando se me ofrece colaborar redactando algún texto, de todas las ideas e inspiraciones que revolotean por mi cabeza, la que siempre está presente es la infancia.
Bajo mi punto de vista, la infancia puede ser una etapa de ideales y de principios inquebrantables, una etapa en que se plantean muchas dudas hasta el punto de cuestionar lo impuesto y no aceptar por ejemplo, el género que nos ha sido asignado y los roles y comportamientos equivalentes a tal género (cisgénero).

Otro pensamiento que me vino a la cabeza es:
¿Por qué tenemos que justificarnos cuando no actuamos en concordancia a lo establecido, en este caso, por el heteropatriarcado?

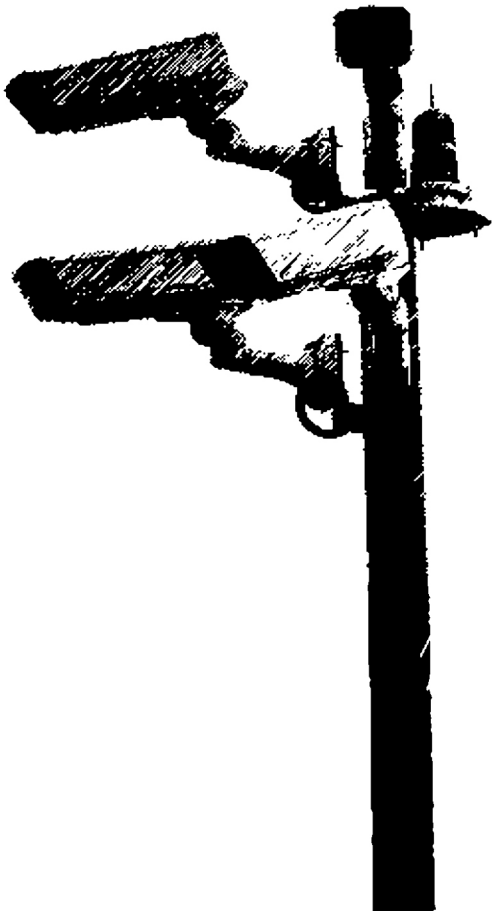
El heteropatriarcado sigue influenciándonos…

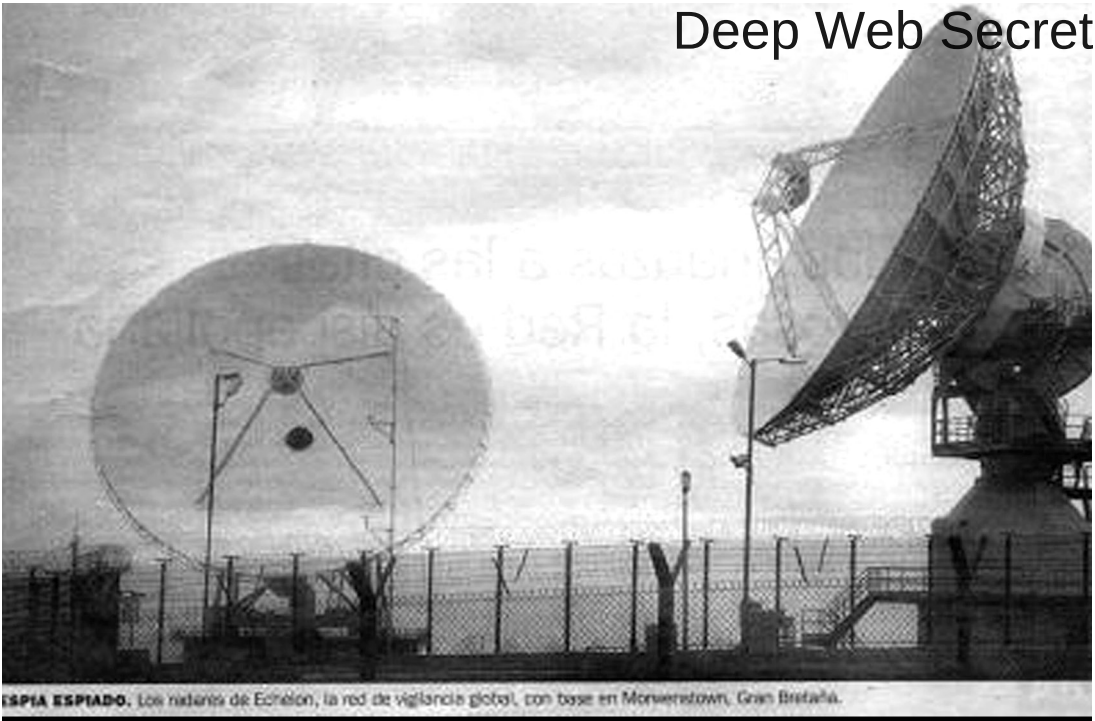
De pequeña se esperaba que fuera fina y educada, que vistiera con faldas y de rosa, que jugara con muñecas.
De mayor, se espera de mí que me depile, que sea madre, que tenga pareja, que rinda en el trabajo como cualquiera, en la vida dar todo lo que pueda sin respetar mi ciclo menstrual...
Explicaciones continuamente
Haber nacido con ovarios, no es sinónimo de madre
Tener pelos no obliga a depilarlos
Tendré pareja sólo si lo deseo, amando libremente
Daré todo lo que pueda en todos los ámbitos respetando mis necesidades físicas y psíquicas.

Y aquí me veo, casi dando explicaciones de por qué escribir un libro en femenino...
¡Somos personas! Tan sencillo como eso, persona, una persona, muchas personas
Suena bonito ¿alguna se siente excluida? revisa tus masculinidades y **destrúyelas**…

Larga Vida!

PRÓLOGO





ESPÍA ESPIADO. Los radares de Echelon, la red de vigilancia global, con base en Gran Bretaña.

"Si en una estación se encuentran
dos o más antenas de recepción
de satélite de más de 18 m,
es seguro que allí se escuchan
comunicaciones civiles."

"Echelon. La red de espionaje planetario" Pag. 61
(Editorial **Melusina**)

Prólogo

"Esta acción policial está perfectamente pensada para desacreditar el trabajo que se ha hecho por los animales. Su intención es la de dañar la reputación de las personas envueltas en campañas y de las campañas en sí mismas. Mediante los registros han conseguido que nuestra oficina, y cuatro oficinas más se queden durante una temporada en punto muerto. Nuestros ordenadores, así como nuestra base de datos, nuestros teléfonos móviles y datos sobre años de investigaciones han sido confiscados. No tenemos posibilidad de contactar con quienes nos apoyan. Nuestro teléfono y nuestro fax fueron inhabilitados durante algún tiempo, lo que nos hizo imposible contactar con los medios de comunicación."

Caso contra las 10 activistas por la Liberación Animal en Austria

Registros, controles, videovigilancia, registros de huellas dactilares, pruebas biométricas, detenciones, cárcel, REPRESIÓN.

El estado nos controla hasta límites totalmente impensables. Con los avances tecnológicos, la represión física y brutal de antes, se ha visto transformada en una sutil y a veces invisible, o casi invisible pero no menos letal, represión a escala internacional y global. La represión actualmente no está centrada únicamente en la lucha contra la disidencia, sino que esta se ha expandido hacia un control total.

La vigilancia se ha vuelto global, controlando cualquier aspecto de nuestras vidas. Puede encontrarse desde los sistemas de localización GPS, el control de redes sociales, chips RFID. Llegando incluso hasta el proyecto del DARPA llamado TIA (siglas en inglés de Sistema de Vigilancia Total - "Total Investigation Awareness") que tras las críticas pasó a llamarse, aunque de todos modos, TIA (siglas de Terrorism Information Awareness. Donde los datos almacenados y monitorizados se cuentan en Petabytes.
O incluso el nuevo anteproyecto del código penal en España para modificar la ley y que podría permitir que el estado envíe Troyanos (software espía) a los ordenadores de personas que estén bajo vigilancia y que todas podamos ser hackeadas y monitorizadas cuando a una jueza le plazca, bajo cualquier situación o actitud que le pudiera parecer sospechosa a dicha jueza.

Es obvio que nunca podremos luchar contra el estado en su propio terreno, pero dadas las circunstancias deberemos protegernos lo mejor que podamos.

Esta sociedad ha basado su comunicación y estilo de vida a través de la tecnología y nosotras no estamos exentas de ella. Podemos intentar utilizarla lo menos posible, pero lo que sí es cierto es que puede considerarse como un arma de doble filo y ahí es donde deberemos trabajar.

En los últimos años la represión ha invertido una gran cantidad de esfuerzos y dinero en la vigilancia a través de internet. Uno de los casos más próximos, en los que se demuestra que el estado intenta aplacar a la disidencia mediante el control a través de la red, es el que ha sucedido contra "Las 5 Anarquistas de Barcelona", quienes han sido detenidas y acusadas de Asociación Terrorista y enaltecimiento del terrorismo, por verter sus opiniones y sus ideas libertarias en el medio virtual y en las redes sociales.

Encarando el tema de las redes sociales existe un debate sobre el que ahora no opinaremos, pero al final de la guía se podrá encontrar un artículo, realizado por las compañeras de nadir.org, sobre el uso

o no de estas redes sociales por activistas y no activistas, y del que recomendamos su lectura.
Realmente esta guía no opinará sobre si debemos o no utilizar la tecnología como una herramienta de lucha política, ya que damos por hecho su uso. Como se adelantaba unas líneas más arriba, el uso de la tecnología, más explícitamente internet y ordenadores, puede ser un arma eficaz contra el sistema ya que ofrece muchas posibilidades de sabotaje, además de encarar una cultura adecuada de seguridad.

Existe bastante literatura sobre seguridad para activistas, alguna guía de contravigilancia y varios textos destinados a informar y difundir esta cultura de seguridad dentro del entorno de las que luchan contra este sistema asesino. En varios de estos textos se comenta el uso de herramientas para asegurar nuestras comunicaciones a través de internet o utilidades para navegar de forma anónima. Pero para nuestra desgracia, no hay demasiada información que profundice en la materia de la seguridad informática. Por este motivo, y a pesar de que quien ha realizado esta guía no es informática, sino alguien con el suficiente tiempo y ganas de enrolarse en la búsqueda de herramientas que pudieran asegurar un poco su ordenador, se tomó la decisión de hacer un manual sobre algunas aplicaciones que intentarán crear una cultura de seguridad en nuestras casas.

El texto que precede a este prólogo es parte de un artículo sobre la detención de 10 compañeras animalistas detenidas en Austria. En el caso de su detención, como siempre, la policía austriaca confiscó sus ordenadores entre otras cosas, e intentó leer y espiar las conversaciones que habían tenido lugar desde los correos del colectivo animalista. Como las personas pertenecientes al colectivo, tenían todas las conversaciones cifradas, los cuerpos de seguridad se dieron de bruces y no pudieron acusarlos de nada que estuviera en sus comunicaciones (que dadas las circunstancias ya es mucho).

Esta guía está estructurada en tres partes. La primera está destinada a la seguridad en internet: navegación anónima, conversaciones seguras... La segunda parte muestra algunos consejos sobre cómo

asegurar los ordenadores: cifrado de archivos, contraseñas...
También se ha destinado una tercera parte a la seguridad móvil, que aunque no se ha ahondado tanto en su uso y conocimientos, saber mandar un correo encriptado desde el móvil, por ejemplo, nunca viene mal.

Se insiste en que la falta de profesionalidad en la materia por parte de quien escribe esta guía, puede hacer que las explicaciones no sean del todo completas y didácticas (aunque se ha hecho lo que se ha podido), o quizá se haya olvidado algún detalle. Pido disculpas de antemano si se encuentra algún error dentro de la misma. Aun así hay que reconocer que se ha puesto mucho empeño en hacer del mundo de la informática, siempre demasiado técnico y preciso, algo básico y que no genere muchas complicaciones a la hora de entender las explicaciones.

Esta guía está destinada a usuarias de Windows, Linux y Android. Cuando decimos Linux, y esto es durante toda la guía, nos referimos a Ubuntu y derivados. Damos por entendido que si alguien usa Arch Linux, por ejemplo, sabrá adaptarse a la perfección.
Lo que sí hacemos es pedir disculpas a las posibles usuarias de Mac ya que en la guía no se encuentran referencias a este sistema operativo. Pero esto se debe a que hasta el momento no sé ni encender el ordenador Mac, por decir algo. Para estas personas, podemos confirmar que la mayoría de programas que hay en el manual, están disponibles para vosotras desde sus enlaces de descarga en sus páginas oficiales, con lo que podréis encontrar cómo usarlos con unas pocas búsquedas en
la red.

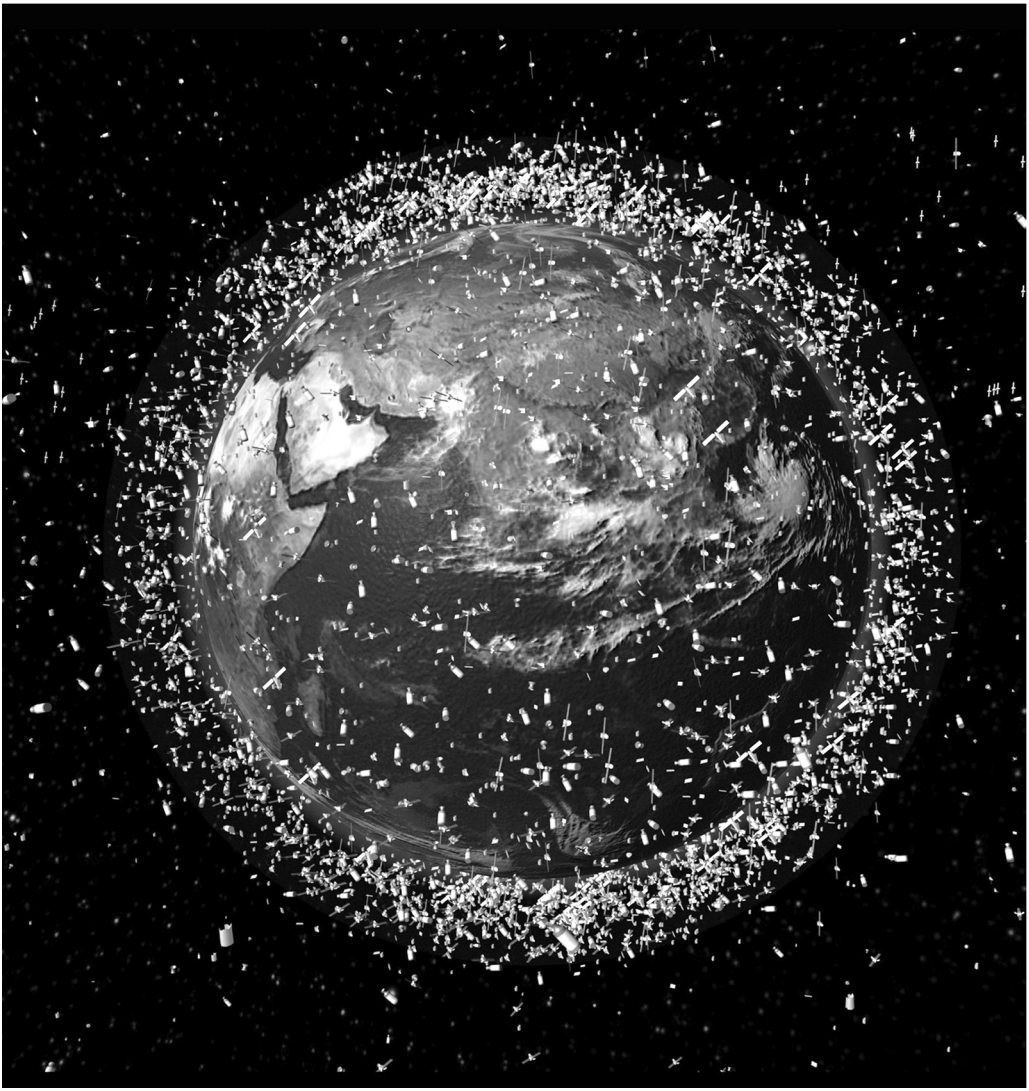
El impacto social de la tecnología ha llegado a un extremo del que no podemos escapar fácilmente por mucho que lo deseemos. Se ha convertido en una parte, por desgracia, muy importante de nuestras vidas y de nuestra lucha. Con todo esto, a mi entender quien toma la decisión de utilizarla como arma contra el sistema, deberán usarla siendo conscientes de sus beneficios y sus límites.

Teniendo en cuenta y pensando siempre que si se está planeando un montaje contra ti o hay en marcha un proceso de detención, lo primero que harán será confiscar tu ordenador, de ti depende que puedan usarlo en tu contra, o por el contrario que estés segura de que no podrán hacer nada y esto te generará a una fugaz pero sincera sonrisa, cuando pienses en el funcionario o funcionaria de turno a quien hayan encomendado la tarea de sacar información de tus datos.

Esperamos que esta guía sea de gran utilidad, a la vez que una contribución a mantener una cultura de seguridad en la lucha por la LIBERACIÓN TOTAL.

Salud y tened cuidado.

SEGURIDAD EN LA RED



"Insecto drone-espía para áreas urbanas, actualmente en producción, financiada por el gobierno de EEUU. Puede ser controlado a distancia y está equipado con cámara y micrófono. Puede posarse sobre Ud. y tomarle muestras de ADN o dejarle nanopartículas sobre su piel para su identificación por radio frecuencia (tecnología RFID) . Puede volar a través de una ventana abierta, y/o adherirse a su ropa hasta que usted se la ponga en su hogar."

Planeador de Control Doméstico (DCHD)

Firewall (Cortafuegos)

El Panóptico es un orden social, una forma de vida, una forma de estar en el mundo y relacionarse con él y con nuestros similares. Y el Ordenador es también un orden social, una forma de vida, una forma de estar en el mundo y relacionarse con él y con nuestros similares. Estamos dentro del Panóptico, dentro de la Máquina, dentro del Ordenador.

Un cortafuegos (*firewall* en inglés) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

Los cortafuegos pueden ser implementados en hardware o software, o una combinación de ambos. Los cortafuegos se

utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets. Todos los mensajes que entren o salgan de la intranet pasan a través del cortafuegos, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados.

Con esta presentación sobre un cortafuegos que nos propone la Wikipedia, podemos hacernos una pequeña idea de qué es o para qué sirve un Firewall, aunque la realidad a nivel profesional no es tan sencilla. No entraremos a detallar cómo es el funcionamiento de las conexiones en internet, teniendo en cuenta cómo funcionan los puertos o de qué manera podemos abrirlos y cerrarlos. Para empezar, porque quien escribe esta guía no sabe mucho más que esto que estamos contando, además de que sería irnos bastante por las ramas y la idea de esta guía es plantear unas cuantas aplicaciones para manteneros a salvo de espías y seguir un poco alejadas del control social que pretende el Gran Hermano.

Su importancia en nuestro caso reside en el hecho de que manteniendo bien configurado nuestro cortafuegos personal, nos mantenemos más seguras, ya que de esta forma podemos controlar nuestras conexiones entrantes y salientes. Esto significa que podemos estar conectadas a la red mediante unas aplicaciones en concreto, usando unos puertos específicos, y a la vez no permitir que exista ninguna conexión respecto a otras aplicaciones que pueda entrar en nuestra red.

Mediante los programas que a continuación se citarán podréis empezar a configurar de una forma bastante básica vuestro cortafuegos para permitir o denegar las conexiones en un momento determinado, decidiendo vosotras mismas qué programas queréis que estén conectados en cada momento.

Desde mi punto de vista, una buena manera de empezar a comprender y usar un Firewall es con un ejemplo tan básico

como el programa de descargas Emule o Amule, ya que teniendo activado el cortafuegos, lo más probable es que al principio no podáis descargar nada y deberéis permitir algún puerto concreto para poder empezar a usar ese gestor de descargas.

Como experiencia personal debo decir que una servidora tiene el cortafuegos activado por defecto y en el momento que aparece algún aviso en el transcurso de una búsqueda en la red o en el intento de una descarga, diciendo que debe abrir algún puerto en concreto, o que la conexión entrante está cerrada, se valora la posibilidad de dejar pasar el tránsito hacia el ordenador, dependiendo de si el sitio donde estoy accediendo es seguro o por el contrario es sospechoso de poder enviar algún troyano o algún virus, o de si es susceptible de poder rastrear la conexión.

UFW

Cómo todas las distros Linux, Ubuntu ya viene con un firewall (cortafuegos) instalado. Este firewall, de hecho, viene embebido en el kernel. En Ubuntu, la interfaz de línea de comandos del firewall fue reemplazada por un script un tanto más fácil de usar. Sin embargo, ufw (Uncomplicated FireWall) también dispone de una interfaz gráfica que es súper sencilla de usar.

Antes de instalar gufw, no es mala idea verificar el estado de ufw. Para ello, abrid un terminal y escribid:

```
sudo ufw status
```

El resultado debería decir algo similar a: *"Status: inactive"*. Ese es el estado por defecto del firewall en Ubuntu: viene instalado pero se encuentra desactivado.

Para instalar el modo gráfico, abrid el terminal y escribid:

```
sudo apt-get install gufw
```

Configurando gufw

Una vez instalado, podéis acceder a él desde *Sistema - Administración - Configuración del cortafuegos* (o algo así, depende de la versión).

Ufw opera por defecto aceptando todas las conexiones salientes y rechazando todas las conexiones entrantes (salvo aquellas relacionadas con las salientes). Esto significa que cualquier aplicación que utilices se va a poder conectar al exterior (sea Internet o parte de tu Intranet) sin problemas, pero si alguien desde otra máquina quiere acceder a la tuya, no va a poder.

Todas las políticas de conexión se encuentran almacenadas en el archivo */etc/default/ufw*. Extrañamente, ufw bloquea por defecto el tráfico IPv6. Para habilitarlo, editad el archivo */etc/default/ufw* y cambiá *IPV6=no* por *IPV6=yes*.

Creando reglas personalizadas

Haced clic en el botón *Agregar* en la ventana principal de gufw. Existen tres pestañas para crear reglas personalizadas: *Preconfigurado, Simple y Avanzado*.

Desde *Preconfigurado* podréis crear una serie de reglas para una determinada cantidad de servicios y aplicaciones. Los servicios disponibles son: FTP, HTTP, IMAP, NFS, POP3, Samba, SMTP, ssh, VNC y Zeroconf. Las aplicaciones disponibles son: Amule,

Deluge, KTorrent, Nicotine, Bittorrent, y Transmission.
Desde *Simple*, podéis crear reglas para un puerto predeterminado. Esto permite crear reglas para servicios y aplicaciones que no aparecen disponibles en *Preconfigurados*. Para configurar un rango de puertos, podéis ponerlos usando la siguiente sintaxis: *NROPUERTO1:NROPUERTO2*.

Desde *Avanzado,* podéis crear reglas más específicas utilizando las direcciones IP y los puertos de origen y de destino. Existen cuatro opciones disponibles para definir una regla: *permitir, denegar, rechazar y limitar*. El efecto de *permitir y denegar* es autoexplicativo. *Rechazar* devolverá un mensaje "ICMP: destino inalcanzable" al solicitante. *Limitar* permite ponerle un coto a la cantidad de intentos de conexión sin éxito. Esto te protege contra los ataques de fuerza bruta.

Una vez agregada la regla, ésta aparecerá en la ventana principal de gufw. También podéis ver el estado del cortafuegos abriendo el terminal y tecleando:

```
sudo ufw status
```

AVAST

Avast, cómo la mayoría de vosotras lo conocéis, no voy a decir muchas cosas sobre este antivirus. Sólo se puede decir que por desgracia y como ocurre con demasiada frecuencia, en Win no existen muchos antivirus que formen parte de la comunidad de código libre. Para las que no estén muy familiarizadas con el tema, quizás no les importe demasiado este hecho ya que la mayoría de software, con buscar un poco lo podemos encontrar crackeado en la red, y con eso nos quedamos tranquilas.
A parte de la dicotomía moral de intentar contribuir en Software Libre o por el contrario utilizar programas de empresas

transnacionales que están destrozando nuestros bosques, ríos y montañas, por no decir también, desiertos, el mar, el cielo... Lo malo de esta situación es que a menudo estos programas que encontramos gratis, llevan incorporada una puerta trasera, la cual permite, sin que nosotras podamos darnos cuenta, penetrar en nuestro ordenador y ver información nuestra, tal como correos, contactos, CONTRASEÑAS...

En otra sección hablaremos un poco más de estos rootkits o keyloggers, pero de momento sirve cómo introducción al hecho de que deberemos ir con cuidado y analizar qué descargamos.

Esta introducción la he formulado ya que personalmente pasé varias horas intentando encontrar Avast gratis con password en la red y al final me lo pasó un amigo.

¿Por qué buscaba este y no otro? Porque es fiable el muy jodido. Es fácil de usar, de instalar (con el crack incluso), no da muchos dolores de cabeza, puedes hacer exclusiones para zonas de tu ordenador que no quieres que escanee... Y lo mejor de todo. Justo acabamos de hablar del firewall o cortafuegos, y en esto Avast no hace falta ni que lo pensemos. En cuanto lo instalamos, nos preguntará qué tipo de seguridad queremos tener. La decisión de hacer más o menos seguro nuestro PC depende de cada una y en cualquier momento puedes modificar la configuración con un par de clics.

Realmente me gustaría dejar un enlace desde donde pudierais descargarlo, pero por desgracia no dispongo de éste.

Antimalware – Antirootkits

La "privacidad "no es más que una libertad ilusoria donde las elecciones económicas y políticas de una, e incluso la forma de ver el mundo y la propia identidad, están coartadas por los medios de producción de las corporaciones, el secuestro de la representación política y la propaganda de los medios de comunicación...

... El derecho a la privacidad es el perfecto anzuelo que ofrecer a las siervas cuya libertad está cuidadosamente restringida. A las prisioneras se les debe garantizar algunas horas al día para que ellas solas puedan escoger entre una serie de comidas congeladas y de programas de televisión. Si la prisionera se queja de las comidas congeladas o si no desea ver la televisión, ya no se le deberá dejar más sola. Pero si aprecian convenientemente éstas libertades garantizadas, se les deberá dejar una semana o dos de vacaciones para que escojan entre diferentes parques temáticos o tours turísticos.

Este capítulo, exceptuando dos herramientas que existen para Linux, está destinado para las usuarias de Windows ya que hasta el momento, aunque Linux también cuenta con Antivirus, la seguridad de sus distribuciones y su software los hace prácticamente innecesarios. Y lo mismo ocurre con la seguridad antimalware, antilogger o antirootkits.

Como se reconoce en varias ocasiones a lo largo de esta guía, no soy informática y mis conocimientos sobre este tema son bastante limitados. Lo único que sé es lo que he leído en artículos y tutoriales sobre cómo proteger la computadora y recomiendo que este tema cada una lo mire un poco por

su cuenta si quiere profundizarlo. Aun así vamos a poner algunos ejemplos sobre cómo proteger el ordenador de espías y de herramientas que puedan sacar información de nosotras a distancia.

¿Qué es un malware, rootkit, keylogger?

Sacado de la wiki: Un malware, también llamado badware, código maligno, software malicioso o software malintencionado, es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o Sistema de información sin el consentimiento de su propietario.

Hay muchos tipos de malware, entre los que se encuentran rootkits y keyloggers y sobre los que vamos a detallar un par de utilidades para encontrarlos y o evitar que se adentren en nuestro sistema.

Keylogger: Es un registrador de teclas. Es un tipo de software o un dispositivo hardware específico que se encarga de registrar las pulsaciones que se realizan en el teclado, para posteriormente memorizarlas en un fichero o enviarlas a través de internet. Es bien conocido que tanto empresas como sistemas de seguridad privada o cuerpos de policía los han utilizado para conseguir contraseñas de la gente, así que es bastante importante estar atentas ante cualquier intrusión y tener especial cuidado si alguna tiene alguna sospecha de poder estar bajo seguimiento del Estado. En realidad se pueden encontrar en formato de usb para esconder en ordenadores por poco dinero, en cualquier tienda del espía a un precio bastante bajo, con lo que imaginad lo que puede hacer la policía.

Rootkit: Es un software que se esconde a sí mismo y a otros programas, procesos, archivos, directorios, claves de registro, y puertos que permiten al intruso mantener el acceso a una amplia variedad de sistemas operativos como pueden ser

GNU/Linux, Solaris o Microsoft Windows para remotamente comandar acciones o extraer información sensible. O sea que es capaz de adentrarse en el sistema y el atacante puede a distancia , extraer información detallada. Estos rootkits se han puesto de "moda" ya que hay ocasiones en las que programas que son de pago pero se encuentran gratis en algunas páginas como "taringa", pueden esconderlos y utilizar nuestros recursos o extraer contraseñas de cuentas, datos bancarios (quien los tenga...), etc

Dada su importancia, aunque aquí hayamos mostrado muy escuetamente algo de información sobre el tema, recomiendo a aquellas que tengan información sensible en sus ordenadores. O sacarla ya mismo, o realmente buscar información que os haga sentir realmente seguras. De todos modos, con la información citada en este manual podréis estar bastante tranquilas.
Los programas que se muestran a continuación, hay que reconocer que hasta día de hoy, han ido dando algunos avisos sobre programas ya de por sí sospechosos. Así que podemos confirmar que cumplen su función.

SPYBOT SEARCH AND DESTROY

Spybot es un programa al estilo antivirus que trabaja mientras una está conectada y se encargará de intentar eliminar las posibles entradas de software malicioso. Además de que podréis escanear vuestro ordenador y eliminar aquellas entradas que haya localizado como sospechosas, troyanos o lo que veáis.

Ocurre a veces que aun encontrando algún Troyano (sobretodo con troyanos), no hay manera de conseguir eliminarlo. El consejo que doy es buscar en la red acerca de ese troyano

específico y ver cómo ha solucionado otras personas vuestro mismo problema.

Por poner un ejemplo. Hace unos años la página de frentedeliberacionanimal.com contenía un Troyano del que no había manera de desprenderse. ¿Quién lo puso ahí? Pues no lo sé. Pero una vez localizado el troyano con Spybot se acabó visitar de nuevo esa página. Ni idea de si esa página sigue abierta, pero por si acaso no hace falta comprobarlo.
Realmente en España no se conocen muchos casos sobre software malicioso mandado por la policía, pero por lo menos en EUA se conocen bastantes historias en las que activistas han sido infiltrados en sus ordenadores por espías virtuales.

Para descargarlo accederemos al enlace de descargas de su página web http://www.safer-networking.org/dl/ o si queréis el paquete completo habrá que buscarlo crackeado o con el serial en algún sitio de la red.
Una vez descargado se instala como cualquier instalación de Windows, después accederemos a él y haremos clic encima de la opción que dice *Inmunizar*. Con esto haremos que trabaje en modo silencioso e irá protegiendo el ordenador en tiempo real.

Aun así, siempre es aconsejable de vez en cuando escanear el equipo en busca de algo que se nos hubiera escapado para eliminarlo y evitar problemas mayores.

Para realizar el escaneo deberemos acceder a la ventana principal y pulsar en *Analizar problemas*. Éste se tomará bastante tiempo en realizar el escaneo. Una vez terminado seguiremos los pasos marcados para eliminar aquellos problemas que haya localizado. Como hemos dicho es probable que alguno se resista. Buscaremos información y lograremos solucionarlo.

ZEMANA ANTILOGGER

Como se ha comentado antes, un keylogger es un software malicioso destinado a registrar las teclas, para así poder "robar" contraseñas o aquello que escribamos.

Zemana Antilogger lo que hace es intentar localizar cualquier entrada de este tipo de software. Además de muchas otras posibilidades que se escapan un poco de esta básica guía para activistas y que se meten de lleno en el mundo de la seguridad informática.

Para descargar Zemana se puede descargar desde su página web http://www.zemana.com/download.aspx pero como ocurre con algunos de estos programas lo mejor será intentar descargarlo con el pass o el serial o lo que sea, para tener el paquete completo.

Para ejecutar Zemana lo que deberéis hacer es acceder a la ventana principal y una vez allí veréis algunas opciones destinadas a la protección de la computadora. Como si fuera un antivirus, estará trabajando protegiendo el ordenador en tiempo real y de vez en cuando aparecerán algunos avisos acerca de que algún programa que tengáis instalado y os dirá que es sospechoso. A partir de ahí será responsabilidad de cada una pensar qué software instala y qué puede llevar en su interior.

A modo de reflexión. En el tema que estamos hablando, sobre la lucha contra toda dominación. No hay porque preocuparse en pensar que el FBI ha puesto un keylogger en un programa de juegos de deportes o similares. Con lo que sí hay que tener cuidado es precisamente con nuestros correos o conversaciones no seguras. Y en estas ocasiones ya tendréis algunas herramientas dirigidas a vuestra protección, además

de que su explicación y funcionamiento será mucho más detallada.

De todos modos, aunque por desgracia no tengo mucha más información sobre estas herramientas, tanto la instalación como el uso de Zemana o Spybot, al ser aplicaciones de Windows, son realmente fáciles de comprender y os darán una sensación de seguridad que antes (seguramente) no tendríais.

CHROOTKIT – RKHUNTER

Aunque hayamos hablado un poco acerca de lo que es un Rootkit, realmente lo que hemos expuesto aquí no es nada comparado con lo que encontraréis en el caso que os dé por buscar más información sobre ello.

Siempre se ha comentado que en Linux no hay virus o rootkits, pero la realidad es otra. La verdad es que sí existen, pero claro está, no del mismo modo e intensidad de los que hay en Windows.

A continuación haremos una breve explicación sobre como escanear nuestro sistema Linux en busca de algún rootkit de estos. Para hacer este mini tutorial vamos a emplear dos utilidades que después de buscar bastante, son los únicos que he encontrado (no digo que no hayan más, sólo que mi reducida inteligencia ha sabido encontrar estos dos) y que por lo visto son los más usados para tal fin.

Estas herramientas son Chrootkit y Rkhunter y según parece hacen la misma faena. Buscar información que haya sido modificada y que sea sospechosa de contener un bicho de estos.

Para instalarlos bastará con teclear:

```
sudo apt-get install chrootkit
sudo apt-get install rkhunter
```

Una vez instalados los programas, lo primero que deberemos hacer será actualizar Rkhunter y para ello en el terminal nos pondremos en modo superusuario.

```
sudo su
```
o como alternativa
```
sudo bash
```

Y actualizaremos el programa. Primero lo llamaremos y después lo actualizaremos. En terminal

```
rkhunter
rkhunter --update
```

Ahora empezaremos el análisis del sistema. Cuando pongamos el código que continua aparecerá un informe del análisis y podréis comprobar si el programa ha encontrado algún fichero sospechoso. Puede que el programa una vez realizado el escaneo os aconseje alguna opción.

```
Rkhunter --checkall
```

Una vez terminado este proceso haremos un nuevo análisis con Chrootkit. Para empezar el escaneo llamamos al programa y él solo empezará a buscar.

```
Chrootkit
```

NOTA: Realmente no es que yo tenga mucha idea sobre estos programas. Los he usado algunas veces y de vez en cuando sale alguna pequeña alarma sobre algún fichero, pero nunca el nombre de ningún rootkit. Por lo que he podido leer, estos

programas no eliminan el problema, lo que hacen es señalar donde está el rootkit y en su caso, como se llama. Según parece, si el programa encontrara alguno de ellos, lo que hay que hacer es buscar información en la red acerca de cómo eliminarlo. Comento esto ya que cuando ejecutaréis estos programas tendréis delante vuestro una serie de datos que no sabréis muy bien qué hacer con ellos. Aun así dejaré un par de enlaces en el capítulo "Fuentes", que entre todos os ayudarán (o no) a comprender un poco más este proceso.

Esperemos que tengáis vuestros ordenadores a salvo de intrusos, sobretodo si sois las administradoras de algún blog o página web, ya que tened muy en cuenta que sois más vulnerables de ser atacadas por el Estado y sus armas cyberpoliciales.

Mail

Lo que una generación percibe como represión, la siguiente lo acepta como parte necesaria de la compleja vida diaria. La clasificación panóptica y disciplinamiento de la población es el método burocrático básico de gobierno. Y esto es así hoy más que nunca.

Pocas cosas se pueden decir acerca de qué es un mail, que no sepa casi todo el mundo. Rara es la persona que no tenga uno. Es más, durante la redacción de este capítulo se intentó recordar alguna persona conocida que no tuviera, sin contar alguien mayor un poco despistada con estas cosas de los ordenadores, y no se ha encontrado a nadie. Pensándolo bien, las ancianas que acuden a centros de personas mayores hacen cursillos de informática y es posible que algunas de ellas pudieran hacer esta guía mejor que quien la está escribiendo.

Todas las personas necesitan uno para conseguir trabajo, comprar por internet, o incluso en cualquier formulario que

rellene alguien, habrá una casilla destinada para nuestra cuenta. La mayoría de las veces completaremos nuestros datos con información falsa y ahí entra la cuenta del correo. Pero hay otras situaciones, como la de buscar trabajo, en la que se deberá escribir alguna que sea personal y estarás obligada, en el caso de que no la tengas ya, a crearte una para ese fin específico.

El hecho de reseñar en esta guía el asunto de los correos, viene motivado por la idea de mostrar un poco de información sobre qué administradores de correo ofrecerán mayor seguridad a la hora de comunicarnos con otras personas, o con qué correos se pueden encriptar los mensajes y con cuales no, ya que este hecho será uno de los factores más importantes a la hora de adentrarnos en el trabajo de llegar a tener conversaciones seguras.

Que se puedan cifrar o no los correos se planteará con mayor detalle en el capítulo dirigido a las "conversaciones seguras", mientras que en esta sección vamos a centrarnos al hecho de escoger un servidor de correos y por qué.

Como muchas de vosotras sabréis ya, empresas de servicios de redes sociales tales como Facebook, Twenti u otras, venden información de sus usuarias al mejor postor, sacando un beneficio de lo que las personas cuelgan en sus muros o donde les da la gana sin pensar en que esa misma información será utilizada para crear perfiles de usuarias, o mejor dicho perfiles de consumidoras en potencia. Además de que estas empresas, y ya no sólo pertenecientes a las redes sociales sino servidores de correo, no tienen ningún problema ni ponen algún impedimento a "regalar" o ceder información a estados o incluso empresas de seguridad privada, en el caso de que hayan requerimientos judiciales o indicios de delito contra una persona determinada.

Así que tengamos en cuenta que si utilizamos por ejemplo

hotmail para mandar correos sobre una manifestación o cualquier otra actividad delictiva (ya sabemos que pensar en hacer volar por los aires el parlamento de un país es delito, y que no hace falta que la praxis determine la resolución de nuestros pensamientos para terminar en la cárcel) y posteriormente la policía te detiene, Hotmail no tendrá reparos en colaborar con la justicia y subministrar una detallada lista de mensajes mandados y recibidos sin tener en cuenta eso que en algunos países se puso de moda para ensalzar la propiedad privada disfrazándola de derechos civiles, a la que llaman Privacidad.

Para comprender mejor esto recomiendo la lectura de un artículo que aparece en el último capítulo de este libro donde se hace mención a la información proporcionada por el "Washington Post", que reveló que seis grandes compañías de internet - Facebook, Google, Yahoo, Apple, Microsoft, AOL, Skype, Youtube y PalTalk - han colaborado con el FBI dando acceso directo a sus servidores a través de un programa dotado con 20 millones de dólares llamado PRISMA.

Hace tiempo leyendo el libro de Derrick Jensen y George Draffan "Bienvenidos a la Máquina", el cual es uno de los varios motivos que hicieron llegar a la conclusión que debemos tener herramientas para hacer frente a la represión, en este caso tejiendo redes de seguridad tanto a nivel personal como informática y que dio como resultado la edición de esta guía. Recuerdo la sensación de que no tenemos nada que hacer luchando contra el control social, ya que los tentáculos del poder son inmensos y llegan a los lugares más íntimos de nuestras vidas.

Pero el mismo libro también menciona alguna cita que dice algo así como, que "Bienvenidos a la Máquina" no es para que nos desanimemos y que las personas ansiosas por cambiar el actual estado de las cosas tire la toalla, sino que la intención de los autores era hacer llegar a la gente la máxima información posible sobre lo que quiere el poder, y de esa manera cuando

llega el momento de luchar, hacerlo siendo conscientes del monstruo al que nos enfrentamos, conociéndolo lo mejor posible en sus puntos fuertes, pero tanto más en sus debilidades.

Con esta guía se pretende lo mismo, salvando las distancias con el impresionante trabajo de Derrick y George. El hecho de saber que los gobiernos intentan monitorizar, algunos incluso lo consiguen, todas las conversaciones de las personas y no sólo de activistas, puede hacer sentir esa sensación de derrota en quienes se informen sobre estos temas. Pero por eso nos interesa saber de qué manera podemos protegernos frente a la ofensiva de los estados, utilizando los medios de que dispongamos para ello y confiando en quienes sabemos que hacen una labor dura, muy dura, enfrentándose a los propios gobiernos y encarando incluso juicios, para mantener seguridad en la red y en el caso que nos atañe ahora mismo, los correos.

Antes de seguir con el capítulo hay que comentar que por mucho que los correos sean cifrados, como ya aprenderemos un poco más adelante, nada en internet es seguro 100 por 100, NADA!! Siempre puede llegar alguien y descifrar aquello que creíamos totalmente invulnerable, y por este motivo se da tanta importancia a la hora de escoger quien guardará todos nuestros datos.

Para esta guía vamos a hacer una breve presentación sobre el colectivo riseup.

¿Qué es, quienes son y qué hacen por nosotras?

RISEUP

Riseup es una colectividad dedicada a proporcionar servicios de alojamiento privado y seguro, servicios de listas y de correo para individuas y organizaciones comprometidas con la justicia social y política. Dado que sus servicios son gratuitos, tu cuenta de correo es mucho más pequeña que las de otros proveedores orientados por publicidad e inseguros. Además, una nueva cuenta sólo puede ser registrada por aquellas quienes han recibido un código de invitación de miembros existentes, o explicando los motivos por los cuales quieren ser administradoras de una cuenta.
Riseup opera exclusivamente utilizando el protocolo de Capa de Conexión Segura (Secure Sockets Layer (SSL)) que te proporciona una conexión segura entre tu computadora y su servidor. Esta seguridad se mantiene mientras lees tu correo electrónico en un programa cliente, sobre un POP seguro y sobre conexiones IMAP y SMTP (estos se refieren a protocolos especiales utilizados por un programa de correo para descargar tu correo electrónico).

Riseup, como administrador de un servicio de correo privado y seguro, el trabajo de esta labor está a cargo de activistas comprometidas que harán todo lo que puedan por garantizar todas estas cualidades que estamos contando.

Riseup permite utilizar canales cifrados (como *https*, y otras versiones cifradas SSL de protocolos como IMAPs, POP3s, SMTPs) para transferir todo tipo de información (incluyendo la información de ingreso, y tus correos electrónicos), y no existen problemas vinculados a cifrado (por ejemplo, problemas relacionados a certificado de cifrado). Además de que es totalmente compatible con gestores de correo como Mozilla Thunderbird, del que hablaremos más adelante ya que con este programa podremos enviar mensajes cifrados y descifrarlos.

También tiene otros servicios como el uso de VPN (Red Privada Virtual) o la utilización de un Chat privado donde se puede comunicar de manera segura y cifrada.

Cuando una es administradora de una cuenta riseup, periódicamente recibirá información o noticias del colectivo donde cuentan en qué proyectos participa, o algún caso en el que habrá tenido que lidiar con el gobierno de EEUU para garantizar la seguridad de sus usuarias.

¿Cómo crear una cuenta riseup?

Para crear una cuenta, existen dos maneras distintas de hacerlo. La primera y la más utilizada es que personas o colectivos, reciban de otras cuentas riseup dos códigos de invitación. Para recibir estos códigos, se deberá hablar con otras administradoras de cuentas y estas tendrán que entrar en su página de configuración de usuaria – https://user.riseup.net, accediendo después donde dice *Invites* y haciendo clic donde pone *Crear un nuevo código de invitación*.

Una vez hayas recibido los dos códigos se deberá acceder a la página principal del correo de riseup: https://mail.riseup.net y allí, una vez puesto el idioma de la página que prefiráis, en este caso usaremos en español, deberéis hacer clic en *Pedir una cuenta*. Una vez hayáis entrado en esa sección habrá que seguir los pasos y rellenar la información que nos vaya pidiendo hasta llegar a la última página donde nos pedirá que escojamos entre las dos opciones para crearnos la cuenta.

En el caso que tengamos las invitaciones, las escribiremos ahí donde nos lo pide. En caso contrario, para crear la cuenta habrá que escribir donde dice *Cuéntenos acerca de usted*, el motivo por el cual queremos la cuenta. Esto se debe a que el uso de riseup está destinado exclusivamente para colectivos o personas activistas y que vayan a utilizarlo únicamente

para fines políticos y sociales. Esta es la manera que riseup ha encontrado para asegurarse de que si vas a utilizarlo, es porque realmente piensas y trabajas por un cambio real.

Una vez leído esta presentación de lo que es riseup, más o menos, hay que tener en cuenta que este colectivo trabaja muy duro para que las personas y grupos que luchan contra el sistema en todo el mundo tengan una cobertura de seguridad a nivel de comunicación, así que si estás pensando en usar este servicio, piensa en utilizarlo con cabeza y razonando que no se debe usar como cualquier otro servidor de correo comercial. En la página del colectivo *Security in a box* aconsejan a las usuarias de riseup tener también otras cuentas de algún servidor comercial para su uso particular y personal y utilizar la cuenta riseup exclusivamente para fines políticos.

Ya que las personas que trabajan en riseup lo hacen gratuitamente y ponen todo su empeño en tirar para adelante este proyecto y este no depende de subvenciones, piensa en hacer una donación, incluso aunque no tengas una cuenta suya. Para donar hay que entrar en la página https://help.riseup.net/es/donate y en esta aparecerán varias opciones para colaborar de la manera que cada una crea oportuno o buenamente pueda.

Viendo que uno de los puntales de la represión y control social actual está basado en la vigilancia a través de internet, las personas debemos darnos cuenta de que ahora mismo, quizá las principales herramientas de lucha contra la dominación están orientadas hacia colectivos como este.

Navegadores

Procter&Gamble (P&G) planeaba implantar etiquetas RFID en sus productos en 2005. La portavoz de P&G, Jeannie Tharrington, afirma que la etiquetas "nos permiten ver lo que las consumidoras compran, y eso nos permite ajustarnos a las demandas de las consumidoras de forma más precisa" y promete que P&G no va a abusar de los datos de los RFID porque "la privacidad es muy importante para nosotras".

Un navegador, o navegador web (del inglés, *web browser*) es una aplicación que opera a través de internet, interpretando la información de archivos y sitios web para que éstos puedan ser leídos.

La funcionalidad básica de un navegador web es permitir la visualización de documentos de texto, posiblemente con recursos multimedia incrustados. Los documentos pueden estar ubicados en la computadora en donde está el usuario, pero también pueden estar en cualquier otro dispositivo que esté conectado a la computadora del usuario o a través

de internet, y que tenga los recursos necesarios para la transmisión de los documentos (un software servidor web).

Con esta presentación de lo que es y para qué sirve un navegador, entraremos de lleno al tema que nos ocupa, que no es otro que saber por qué debemos escoger un navegador u otro. ¿Por qué deberíamos usar Firefox en vez de utilizar Internet Explorer?

La respuesta a grandes rasgos es bien sencilla. Internet Explorer deja un rastro increíble en la red, aunque no lo estemos usando. Para las que hayáis hecho una limpieza de archivos, datos antiguos, etc... de vuestros ordenadores, os habréis dado cuenta que aunque no utilicéis Internet Explorer para nada, el simple hecho de que esté instalado hace que siempre esté activo y mandando información (a Microsoft supongo aunque no estoy muy seguro). Al parecer, IE está siempre habilitado y guardando datos en nuestro ordenador de todo lo que vamos haciendo en este. Si no fuera así, ¿por qué es tan difícil desinstalarlo de nuestro PC?

Como recomendación de uso a nivel de seguridad informática vamos a aconsejar dos navegadores y que forman parte de la misma familia, la familia Mozilla. Uno es Firefox y el otro es Seamonkey.

Seamonkey no es tan conocido como Firefox, pero tiene unas cualidades y desventajas que vamos a detallar cuando llegue el momento.

Existe otros navegadores que en principio son bastante seguros como por ejemplo Opera o Google Chrome, pero aunque estos sean de una velocidad y fiabilidad impresionantes, no estoy muy seguro de si guardan registros que no podamos eliminar fácilmente. En el caso de Google Chrome, formando parte de la corporación Google, no es que sea muy de fiar.

En la sección siguiente se explicará un poco mejor la manera en la que haciendo búsquedas por la red dejamos rastro para a continuación, con las aplicaciones que mostraremos, podremos trabajar un poco más seguras. Pero de momento vamos a centrarnos en hacer una configuración de Firefox y Seamonkey para evitar ser rastreadas.

FIREFOX

Desde hace tiempo Firefox se ha caracterizado por su estabilidad y firmeza, pero sobretodo por la capacidad de configurar la privacidad en nuestras búsquedas y por el hecho de que seamos nosotras quienes determinemos de qué manera queremos utilizar la red.

Si quieres poner un viernes por la noche en Google "¿qué hago hoy?" y que salgan opciones de discotecas o conciertos a los que vas normalmente, o lo que sea que te guste hacer, quizás esta guía no es para ti. Puede parecer que esto sea una comodidad para algunas, pero desde luego en términos de seguridad no lo es, para nada. Si esto te ocurre es porque estás dando a Google demasiada información sobre ti y situaciones como esta nos recuerdan una vez más que Orwell estaba equivocado en cómo sería el futuro, ya que este es mucho peor de lo que sus pesadillas podían imaginar.

La intención principal de este capítulo es precisamente lo contrario a lo expuesto más arriba.

El texto que sigue a continuación es un artículo sacado de la página de Mozilla y nos muestra como configurar el navegador de manera que nuestra presencia pase inadvertida a los tentáculos de la máquina.

Configuración de la privacidad, el historial de navegación y la función no quiero ser rastreado

Este artículo describe las opciones que están disponibles en el panel *Privacidad* de la ventana *Preferencias* de Firefox.

El panel de *Privacidad* te permite:

-Controlar cómo administra Firefox tu historial de navegación, lo cual incluye las páginas que has visitado, los archivos que has descargado, la información que has introducido en los formularios y las cookies que los sitios web te han enviado.
-Controlar qué sitios pueden enviar "cookies" y eliminarlas de los sitios que te las han enviado.
-Controlar la forma en la que la barra de direcciones utiliza el historial para sugerirte coincidencias para lo que escribas en ella.

Rastrear

Decir a los sitios web que no deseo ser rastreado: Al marcar esta casilla les indicarás a los sitios web que no deseas ser rastreado por empresas de publicidad y terceros. **Respetar esta configuración es voluntario: a los sitios web no se les pide que lo hagan. - ¡Vaya tela...!**

Historial

La opción *Firefox podrá* controla cómo Firefox guarda la información sobre tu navegación por la web

Recordar historial

Cuando la opción *Firefox podrá* está establecida a *Recordar historial*: Firefox mantendrá una lista de las páginas que has visitado.

-Se mantendrá una lista con los archivos que has descargado en la *Ventana Descargas*.
-El texto que introduces en los campos de los formularios o de la barra de búsquedas será recordado, lo que te permite utilizar las entradas de nuevo.
-Firefox acepta cookies de los sitios hasta que caducan.

Haz clic en:

-*Limpiar tu historial reciente* para abrir la ventana Limpiar su historial reciente, que te permite borrar parte o la totalidad de tu historial de navegación rápidamente.
-*Eliminar cookies de manera individual* para mostrar la ventana de cookies. .

No recordar el historial

Cuando la opción *Firefox podrá* está establecida a *No recordar el historial:*
-Firefox no guardará ningún registro de tu historial de navegación.
-Los archivos que has descargado no se mostrarán en la ventana *Descargas*.
-Firefox no guardará el texto que introduzcas en los formularios o la barra de búsqueda.
-Firefox aceptará las cookies de los diferentes sitios web y las eliminará cuando cierres.

Usar *No recordar el historial* es equivalente a utilizar Firefox siempre en modo de navegación privada.
Haz clic en *Limpiar su historial reciente* para abrir la ventana *Limpiar su historial reciente*, que te permite borrar parte o la totalidad de tu historial de navegación rápidamente.

Usar una configuración personalizada para el historial

Cuando la opción *Firefox podrá* se establece a *Usar una*

configuración personalizada para el historial, las siguientes opciones estarán disponibles:
-Abrir automáticamente Firefox en una sesión privada de navegación: Si has seleccionado esta opción, Firefox no creará ningún historial la próxima vez que se ejecute.

-Recordar el historial de navegación y descargas: Si has seleccionado esta opción, Firefox guardará una lista con las páginas que has visitado y los archivos que has descargado.
-Recordar el historial de formularios y búsquedas: Si has seleccionado esta opción, el texto que hayas introducido en los campos de los formularios o en la barra de búsqueda será recordado por lo que podrás volver a usar esas entradas otra vez.

Aceptar cookies:

Si has seleccionado esta opción, Firefox aceptará cookies desde los sitios web. Haz clic en el botón *Excepciones*... para controlar qué sitios no están autorizados a establecer cookies.
-Aceptar las cookies de terceros: Si has seleccionado esta opción, Firefox aceptará cookies desde http://site2.com cuando estés visitando http://site1.com.

Mantener hasta:
-que caduquen: Si has seleccionado esta opción, Firefox permitirá a los sitios web que visites especificar durante cuánto tiempo deben mantener sus cookies.
-que cierre Firefox: Si has seleccionado esta opción, las cookies se eliminarán al cerrar Firefox.
-preguntar siempre: Si has seleccionado esta opción, Firefox te preguntará cuanto tiempo quieres guardar una cookie cada vez que visites un sitio.
-Limpiar el historial cuando Firefox se cierre: Tu historial será borrado cuando cierres Firefox. Haz clic *Configuración* para controlar qué elementos son borrados.

Haz clic sobre el botón *Mostrar cookies*... para ver la ventana de Cookies.

Barra de direcciones

-*Cuando uses la barra de direcciones, sugerir:*
La barra de direcciones es la barra horizontal que muestra las direcciones de los distintos sitios web (URL). Cuando escribes en la barra de direcciones, Firefox puede mostrar resultados que se correspondan con lo que tecleas en ella:
-*Historial y marcadores*: Si has seleccionado esta opción, la barra de direcciones mostrará los resultados de los distintos sitios web que has visitado y de los distintos marcadores que has guardado.
-*Historial:* Si has seleccionado esta opción, la barra de direcciones mostrará los resultados de los distintos sitios web que has visitado. Los sitios que has guardado en marcadores pero no has visitado no se mostrarán.
-*Marcadores*: Si has seleccionado esta opción, la barra de direcciones mostrará los resultados de los distintos marcadores que has guardado.
-*Nada*: Si has seleccionado esta opción, la barra de direcciones no mostrará nada mientras tecleas en ella.

COMPLEMENTOS FIREFOX

ixquick – En realidad ixquick no es un complemento. Es un buscador que es mucho más seguro que Google ya que utiliza https en vez de http, además de que según ellas mismas es el buscador más confidencial del mundo. Buscadlo en https://ixquick.com.

*AnonymoX 1.0.*1 - Desde la sección de complementos
Https everywhere - https://www.eff.org/https-everywhere
Google-sharing https://addons.mozilla.org/es/firefox/addon/googlesharing/
**Adblock Plus 2.2.3* – Desde la sección de complementos.

Después de instalar, clicar en *preferencias de filtros* y en la pantalla que sale, teclear en *añadir suscripción de filtros* y añadir:
EasyList, EasyPrivacy + Easy List, Fanboy's Spanish, Fanboy's Adblock List, Filtros Nauscópicos
*Este complemento más que para seguridad está destinado a eliminar los anuncios que salen en las web. De esta manera, aunque indirectamente, nos ahorramos algunas de las cookies de las web donde estamos, entorpecemos el rastreo y además, que da mucha rabia abrir un enlace y que te salgan diez páginas de pornografía o mierdas que quieran venderte.

Para las que uséis Linux, especialmente Kubuntu, ya que es el que uso yo, soy fan de KDE, dentro de la misma distro está "Rekonq" que es realmente rápido y configurable hasta el punto que creo que puede dar sorpresas a Firefox a la larga. Es solo una opinión...

SEAMONKEY

SeaMonkey es una suite de internet conformada por un navegador web, cliente de correo electrónico, libreta de contactos, editor de páginas web (Composer) y un cliente de IRC (ChatZilla). En esencia, es un proyecto que continúa del desarrollo de Mozilla Aplication Suite, siendo el desarrollo realizado y controlado enteramente por su comunidad de desarrolladores y usuarios a través de The SeaMonkey Council, entidad apoyada sobre todo en cuanto a recursos técnicos por la Fundación Mozilla.

Seamonkey, al formar parte de la familia Mozilla, tiene unas ventajas en cuanto a seguridad que destacan por encima de cualquier suite de internet que estén dentro de Microsoft.
Realmente es muy similar a Firefox y su gestor de correos es

casi idéntico a Thunderbird. Cabe resaltar de este proyecto el hecho de que no sólo es un buscador y un gestor de correo todo junto, sino que además, cuenta con la posibilidad de un editor de texto HTML, un Chat IRC entre otras herramientas que ya se escapan un poco del propósito de la guía, pero que para algunas de vosotras seguro serán muy útiles.

Para instalar Seamonkey en Windows hay que ir a la página principal del proyecto.
http://www.seamonkey-project.org/releases/, descargar el .exe y seguir los pasos habituales. Para Linux también podéis usar el mismo link para su descarga. Como suele ocurrir en Linux, es posible que lo encontréis en los repositorios, pero en el caso de que no esté, en otro enlace sale otra manera de instalarlo agregándole PPA.

De todos modos lo habitual para la instalación de Seamonkey, es descargarlo del enlace anterior. Ahí descargaréis un paquete *.tar.bz2*.
Para instalarlo bastará con ir a la carpeta de *Descargas*, y ahí lo descomprimiremos haciendo clic derecho encima del paquete y seleccionando *Extraer – Extraer comprimido aquí, autodetectar subcarpeta*. Aparecerá un directorio con toda la información de Seamonkey. Accederemos a la carpeta aparecida y haremos clic encima del archivo ejecutable que dice *seamonkey*.

Para instalarlo desde la línea de comandos es preciso acceder a la terminal y ahí teclear:

```
cd Descargas && cd seamonkey
```

Con esta sintaxis estaremos dentro de la carpeta descomprimida y para ejecutarlo escribiremos:

```
./seamonkey
```

Con esto ya tendremos instalado este software y podremos disfrutarlo desde este mismo momento. Existe la posibilidad de que en cuanto lo instalemos y exploremos un poco su interior, en el momento de querer entrar a la sección del correo, desde la opción *Ventana – Correo y Noticias* nos aparezca una ventana preguntando si queremos importar todos los datos de cuentas que tengamos almacenados en otro gestor, ya sea Outlook o Thunderbird. En una sección próxima mostraremos que no debemos usar nunca Outlook Express y se enseñará cómo usar Thunderbird como alternativa real y segura.

Ventajas que tiene Seamonkey:

Es de la Fundación Mozilla y da la seguridad de que el "anonimato" o la "privacidad" están más garantizadas que con otros buscadores.
En la ventana de *preferencias* encontraremos un sinfín de opciones destinadas a tener una configuración muy personalizada en cuanto a cookies, historiales, ventanas emergentes, contraseñas, SSL, certificados, etc...
Incluso desde el mismo panel de configuración del buscador se puede configurar las preferencias del correo o el editor web.

Desventajas de Seamonkey

No todos los complementos de Firefox son compatibles con él, aunque de todos modos una gran cantidad de ellos se adaptan completamente.
La interfaz no es muy elegante que digamos, por lo menos para mí, pero sobretodo el problema es que está un poco recargada y no es tan intuitiva como Firefox.

En cuanto al gestor de correo comentar que el complemento Enigmail es compatible, con lo que la mensajería cifrada es totalmente posible y es cierto que este gestor tiene algo que, aun siendo exacto a thunderbird, lo hace especial. Probadlo y decidid vosotras.

De todos modos no está mal completar un paquete de buscadores en vuestro PC con esta suite. Es probable que si tienes Firefox y Thunderbird, a la mayoría no le hará falta, pero básicamente tienen un nivel de seguridad similar y cada persona se adapta mejor a unos programas que a otros.

Anonimato

Hay un montón de usos para las etiquetas RFID, pero ninguno de ellos, dicen, te debe preocupar en relación a tu privacidad. Tu nevera podrá enviar su contenido al supermercado para que lo tengan en cuenta a la hora de estudiar los "stocks", y tu televisión podría programarse para que retransmita publicidad según el contenido de tu despensa...

... Todo es muy cómodo. Nunca debemos olvidar tomar nuestro soma.

Algo que debe saber cualquier persona que desea navegar sin dejar rastro, es que hacer de la navegación algo totalmente privado es imposible. Este es un concepto que debe quedar claro ya que aun usando todas las herramientas que a continuación se explicarán, nadie debe de creer que por ello, podrá escaparse a la mirada de la máquina.

De todos modos cuando hablemos durante esta guía del hecho de navegar de la mejor manera posible, lo haremos diciendo que es anónima. Aunque pueda parecer que es una contradicción, va a ser una forma en la que nos entenderemos.

Para aprender cómo podemos llegar a viajar por la red intentando no dejar rastro, hay varios conceptos que deben quedar claros, ya que son estos los que deberemos evitar. Lo primero que hay que saber es que cuando navegamos por la red, lo hacemos llevando "encima" nuestro una IP (en el siguiente artículo se entenderá mejor qué es). Otra manera en la que podemos ser rastreadas es mediante las cookies (estas ya hemos visto en la sección de Firefox como podemos evitar almacenarlas).

Antes de explicar cómo funciona el rastro que deja una persona cuando navega por internet hay que entender bien qué es y cómo funciona una cookie.
Una cookie es información que un sitio web almacena en tu ordenador mediante el uso de un navegador o explorador de internet. Una cookie permite que los sitios web registren tus actividades de navegación en internet – como por ejemplo, cuáles son las páginas y contenidos que has estado mirando, cuándo los visitaste, qué buscaste, y si hiciste clic sobre algún anuncio. Los datos recolectados por las cookies se pueden combinar para crear un perfil de tus actividades en internet.

Si alguna persona no entendió muy bien por qué se tenía que configurar el buscador Firefox, o cualquier de ellos, para estar en navegación privada, suponemos que con esta aclaración habrá quedado claro que hay que evitarlas siempre que se pueda. Aun así como ya se ha comentado, nada es seguro, y para mostrar un ejemplo, el periódico Wall Street Journal destapó un escándalo en el que estaba inmerso Google, en el que se demostró que este buscador hizo una instalación fraudulenta de cookies en el explorador de internet Safari de Apple, es decir, en cualquier dispositivo iphone, ipad o mac. El problema más grave de este escándalo reside en que Google uso códigos que trucaron el software del explorador Safari, instalando las cookies incluso a usuarios que habían optado por la opción de no compartir las cookies de terceros (third-party cookies).

Ahora vamos a ver parte un artículo encontrado en la red donde se explica bastante bien el tema de las IP, para entender mejor los programas que aparecen en las próximas páginas.

"Muchas personas piensan que Internet es impersonal y que con borrar el historial de navegación de nuestro navegador hemos conseguido no dejar rastro en Internet de lo que hemos hecho. Nada más lejos de la realidad. Veamos dónde se va quedando el rastro de lo que hacemos por Internet.

Todas las peticiones que lanzamos a Internet desde nuestro ordenador, ya sea navegar por una página web, conectarnos a un ftp o intentar conectarnos a un messenger, deben salir con una dirección IP de origen, dirección indispensable para que los paquetes puedan localizar nuestro ordenador a la vuelta de la petición y entregarnos lo que solicitamos.

La dirección IP es como nuestro d.n.i. en la red, ya que si existiera un solo duplicado, ambas máquinas con la misma IP estarían incapacitadas para utilizar la red (el enrutamiento de la red no sabría a cuál de las dos máquinas enviar los paquetes de datos). La IP es un número del tipo 88.31.165.165

Si nos conectamos desde un ordenador con IP pública fija (la máquina siempre tiene la misma IP), todo lo que hacemos queda almacenado en los servidores destino.

Si por contra, nos conectamos desde casa, nuestro proveedor nos ofrece una IP dinámica en cada conexión. Hoy tenemos una IP pero mañana podemos tener otra. Parece más anónimo, ya que una administradora en Internet no sabría qué máquina exactamente tenía esa IP en ese momento, pero no lo es, ya que las proveedoras mantienen el archivo de todas las IPs que se han ido entregando a cada usuaria en cada momento.

Por otro lado, cuando navegamos no sólo se queda almacenada la IP de nuestra máquina, sino también datos de nuestro

Sistema Operativo, tipo de máquina y navegador utilizado, la fecha y la hora de la petición y las páginas que hemos pedido.

Todas las máquinas de cualquier oficina o incluso en nuestra pequeña red doméstica, mantienen una IP privada a pesar de que todas ellas naveguen a través de una IP pública, por lo que consultando el log del punto de acceso a Internet se puede saber qué personas de una determinada red navegaron por qué páginas, qué p2p o messenger utilizaron y demás datos confidenciales."

TOR

Dentro del entorno activista, Tor es el programa más conocido para el anonimato en la red... Tiene algo bueno y es que está diseñado por activistas y dirigido a activistas, por lo que nos da la seguridad de que nos ponemos en las manos de gente que está por lo mismo que nosotras.

Pero, aunque como hemos dicho tiene cosas buenas, también tiene otras, no tan buenas (para una servidora que por supuesto nadie tiene que coincidir con esta opinión). No es muy rápido y si lo que queréis es hackear, ya sea inyecciones SQL, hacer ataques DDOS o lo que os dé la gana, con esta herramienta estáis bastante limitadas y yo no aconsejaría usarla para esos fines, ya que Tor crea una navegación anónima del buscador, pero no del ordenador en sí mismo. Pero para lo que se diseñó, tal como hacer búsquedas en internet de manera segura. Lo hace muy bien.

Tor está diseñado para incrementar el anonimato de tus actividades en Internet. Este disfraza tu identidad y protege tus actividades en línea de las diversas formas de vigilancia en la red. También puede ser utilizado para eludir los filtros

en Internet. Es de código abierto y software Libre, así que no estaremos colaborando con corporaciones.

Para su instalación en Linux. Lo podemos encontrar para descargar en
https://www.torproject.org/download/download-easy.html

Seleccionamos el idioma que queramos y descargamos el paquete de *Tor Browser Bundle for GNU/Linux*. Habremos descargado un archivo .tar.gz, que una vez descargado lo guardaremos donde queramos y lo abriremos cuando necesitemos.
Este paquete que habréis descargado es un portable con lo que nos ahorra instalaciones, facilitando su uso.

Para ejecutarlo deberemos ir al directorio donde lo guardamos, lo descomprimiremos y únicamente tendremos que presionar sobre el icono que dice:

start-tor-browser

Cuando hagáis clic encima del archivo aparecerá una ventana donde el programa solo, intentará conectarse a la red Tor. Cuando haya terminado se abrirá un Firefox anónimo donde trabajaremos con Tor. A parte de este firefox, si lo deseamos, podemos abrir nuestro propio Mozilla para trabajar más rápido, pero teniendo en cuenta que este no será tan fiable como el de la red Tor.

La facilidad de esta herramienta junto al buen resultado que ofrece, son buenos motivos para usarlo, siempre y cuando respetemos lo que anteriormente comentábamos acerca de los usos que le queramos dar.

Para la instalación en Windows el proceso es el mismo. Entramos en el mismo enlace de descarga, pero esta vez descargaremos el paquete destinado a la distribución de

Windows. Una vez descargado el paquete, hay que hacer clic encima de este y el resultado de la extracción será una carpeta donde habrá un .exe que será la aplicación.
Durante estos últimos años Tor ha hecho un gran trabajo de configuración ya que anteriormente había que hacer la instalación de tres paquetes para poder navegar con él, mientras que con este programa portable, no hace falta ninguna instalación.

Además de que el uso del proxy (más adelante veremos qué es un proxy) de Tor es utilizado por otros programas destinados a la navegación anónima, como por ejemplo Proxychains, que está disponible para Linux únicamente y del que a continuación veremos cómo funciona.

TAILS

Recién acabamos de hablar de Tor. Ahora nos toca hablar de Tails, un Live CD que como veréis tiene bastante que ver con el anterior software.

Tails es un Live CD aislado que se encargará de conectarse anónimamente a la red, y lo hará desde la red Tor. Una de las características de Tails es que trabaja sin dejar rastro, a menos que se indique explícitamente, en los discos duros que puedan haber en el ordenador donde se introduzca. ¿El motivo? Poder trabajar en un entorno seguro en el que la conexión sea lo más privada y anónima posible. Otra de las ventajas de Tails es que está basado en Debian GNU/Linux, pero a la hora de empezar a trabajar con el Live CD, os pedirá si queréis trabajar en el entorno camuflado de Windows XP, con lo que una vez seleccionada esta opción, tanto el fondo de escritorio como el entorno, son idénticos a XP. Y tal como explican en su página web, uno de los motivos por los que se creó Tails, es para

trabajar en un local comercial, por ejemplo un locutorio de internet, y con el entorno creado por Tails nadie distingue si se está trabajando con un Live CD o con el mismo sistema del propio local, apartando así, cualquier sospecha de personas que pasen a vuestro lado.

Además de que Tails, no dejará ningún rastro en el ordenador anfitrión de que se ha trabajado con otro sistema.

Y por si esto fuera poco, Tails tiene otras herramientas de seguridad, como LUKS, el estándar de Linux para cifrar USB o discos duros. Cifra las conexiones con HTTPS, tiene en su software aplicaciones de correo o mensajería instantánea en las que se puede usar complementos de cifrado como OpenPGP o OTR (Off The Record) respectivamente. Además de que cuenta con Nautilus Wipe para el borrado y sobreescritura de archivos.

Hay algo que cualquiera que use Tails deberá saber. Cuando navegamos con Tails, estamos navegando en la red Tor, a no ser que no queramos. De este modo la conexión es semi-anónima, pero el rastro que dejamos en la red muestra que estamos usando Tails, e incluso que estamos usando Tor. Este concepto no es que sea negativo, pero sí algo a tener en cuenta.

Algo que para algunas de nosotras sí es algo negativo, o por lo menos a tener muy pero que muy en cuenta, es que en Tails colaboran varios proyectos entre los cuales está Lightweight Portable Security (LPS). Este programa que colabora con Tails es un programa realizado por el Laboratorio de la Fuerza Aérea de Investigación, Anti-Sabotaje - Iniciativa de Protección de Software (ATSPI) Oficina de Tecnología, creado para proteger la propiedad intelectual (software de aplicación), de la piratería, el sabotaje y las amenazas contra el estado americano.
A quien le dé un poco de grima esto, mejor busque alternativas para trabajar de esta forma, aunque hay que tener en cuenta

que casi todo el mundo usa Windows, y pocos software colaboran tanto con las autoridades como él, aunque usar una distribución que directamente colabora con un proyecto como ese no apetece mucho, verdad? La verdad es que es un buen software. Que cada una haga lo que crea necesario...
También Tails forma parte del proyecto de Ubuntu Privacy Remix (UPR), del que hablaremos más adelante, y del que no puedo confirmarlo, pero espero que no colabore con LPS ya que como se mostrará en el capítulo dedicado a UPR, es el mejor método para manejar información realmente sensible, y si LPS estuviera en medio de UPR, generaría sospechas acerca de la seguridad y eficacia de Ubuntu Privacy Remix.

Como alternativa a Tails, existe "AnonymO.S. Live CD", que funciona de la misma manera que Tails, navegando a través de Tor, cambiando si queremos la dirección MAC (una especie de código de serie, único, de cada red), incluso podemos usarlo con el entorno de Windows XP.

A continuación seguirá una pequeña guía de Tails para hacer un primer y básico uso de esta distribución, mostrando de manera sencilla (lo más sencilla que podamos) como conectarse a la red o enviar un comunicado (por ejemplo).

Para más información sobre Tails, así como para descargarlo deberéis entrar en https://tails.boum.org/.

Para empezar a trabajar con este Live CD, deberemos introducir el DVD/CD o el USB booteable con Tails, reiniciamos el ordenador y deberemos entrar en la BIOS del ordenador, para a continuación seleccionar el arranque desde el dispositivo que contenga Tails (esto depende del ordenador, pero a no ser que este sea muy antiguo podréis hacerlo sin problemas). Una vez el software ha empezado el arranque, aparecerá una pantalla donde en el panel inferior podremos cambiar el idioma a aquel que deseemos. Con el idioma cambiado deberemos escoger si

queremos que el programa nos muestre más opciones o que arranque ya mismo. Escogeremos la opción de *Más opciones*. Aparecerá una nueva ventana y en ella deberemos decidir una contraseña para poder trabajar como root y así poder configurar más herramientas de Tails tales como el uso o desuso de los discos duros del ordenador, o la configuración de llaves para encriptar. En esta misma ventana marcaremos la casilla *Activar camuflaje de Microsoft Windows XP*.

Una vez Tails ya está corriendo y de pronto parece que estemos trabajando en una máquina con XP esperaremos un rato que vaya cargando (hay que tener en cuenta que si lo hemos cargado en un DVD/CD o un USB irá más lento) y aparecerá la ventana principal de Iceweasel, que es el navegador por defecto y con el que trabajaremos de forma anónima a través de la red Tor. En el caso de que no apareciera deberíamos ir a *Start – Internet – Iceweasel* y ya estaríamos navegando con Tor.

Como ejemplo para este primer inicio con Tails vamos a imaginar que queremos mandar un comunicado de una acción o una convocatoria cualquiera y que la información de esta la tenemos guardada en un archivo de texto dentro de un USB (ahora mismo da igual que esté encriptado el USB, el texto o que no lo estén), hemos ido a un locutorio de internet, hemos puesto el Live CD de Tails y hemos arrancado en modo camuflaje Windows XP, con lo que estamos pasando desapercibidas en un ordenador cualquiera de los que hay.

Una vez hecho estos pasos anteriores, a continuación deberemos dirigirnos a *Start – Lugares – My computer* y en la ventana que aparece seleccionaremos el dispositivo donde se encuentre el texto, lo buscaremos, abriremos y lo mandaremos donde queramos como si hubiéramos estado en nuestra casa haciendo esto (esto último por favor no lo hagáis nunca). Lo mejor de todo es que no habremos dejado ningún rastro (más que en las posibles cámaras que hubieran en el local) en esa máquina, salvo en la memoria RAM (esta se eliminará en el

momento de apagar el ordenador o cerrar Tails). Si hemos trabajado en modo XP no aparecerá, pero si hemos trabajado desde el entorno original de Debian, en el momento de apagar veremos que aparece un aviso mencionando que el software se está encargando de eliminar esta dichosa memoria. Para mayor seguridad en la eliminación de RAM, ver el capítulo "secure delete (sdmem)".

En el caso de que el USB donde guardamos el texto estuviera cifrado con Truecrypt (TC) deberéis llevar otro USB con el programa dentro de él para extraerlo y descifrar el USB del archivo (también podríais descargarlo directamente de su web y extraerlo ahí mismo, pero mejor estar poco rato en el locutorio). Para más información sobre este uso de TC debéis mirar en el capítulo de Truecrypt: sección "cifrar USB".

Además de este uso que acabamos de mostrar y del que podemos estar bastante relajadas en cuanto a un poco de seguridad y anonimato, Tails también tiene otras aplicaciones, como la herramienta de *contraseñas y claves de cifrado*, que podréis usar para gestionar y configurar vuestras claves OpenPGP. Para sobreescribir archivos y dificultar su recuperación se puede usar Wipe, que en el momento de clicar con el botón derecho sobre un archivo aparecerá una opción que dice *Wipe* y que servirá para eliminar los datos. Si la seleccionamos deberemos clicar en la nueva ventana *Options – 38* y marcar la casilla *Last pass with zeros instead of random data*.

PROXYCHAINS

Proxychains es un programa disponible solamente para GNU/Linux y Unix que nos permite crear cadenas de proxies, "ocultando" así nuestra IP pública real en todo tipo de conexiones (HTTP, FTP, SSH, etc...). Esto se traduce en que

podemos navegar por Internet o realizar cualquier operación en la red de redes sin descubrir nuestra identidad real.

¿Cómo funciona esto? ¿Es realmente posible? ¿Podría ocultar mis pasos en Internet?

Para poder conocer la respuesta a estas preguntas es necesario tener una mínima noción de lo que es un proxy en la jerga informática.

¿Qué es un proxy?

Un proxy puede definirse como un ordenador o servidor en el cual está corriendo un servicio de proxy, es decir, un "programa" que permite a ese ordenador actuar de intermediario entre nuestro ordenador y el destino final. En este caso, Proxychains nos ofrece conectarnos a más de uno en cadena.
Lo que significa que cuando navegamos por la red podemos usar estos "ordenadores" y utilizarlos incluso en cadena, para dificultar el rastreo de nuestras búsquedas. De esta manera si usáramos un proxy de México y otro de la India. Si rastrearan la búsqueda tardarían en encontrarnos, sobretodo si el proxy que usamos es anónimo, que incluso podría no dar información de quien se habría conectado a él. Lo malo que tiene este sistema es que es tremendamente lento y si no tienes una conexión de esas potentes, no vale la pena.

Instalando Proxychains

Para instalar Proxychains sólo debemos abrir la terminal de Linux y escribir:

```
sudo apt-get install proxychains
```

Configurando Proxychains.

Crear una cadena de proxies con Proxychains es muy sencillo. Solo necesitaremos el programa instalado, un editor de texto plano y conexión a Internet para buscar nuestros proxies (por supuesto, si ya tienen vuestros propios proxies no la necesitarán). Una buena lista de proxies es esta:
http://www.proxies.by/proxy/?rule1

(Recomiendo tener varias páginas desde donde descargar los proxys ya que a veces no se encuentra lo que se quiere y sobretodo, nunca a la primera)

Busquemos donde los busquemos siempre tenemos que tener en cuenta que soporten el protocolo HTTPs, ya que si queremos usar los proxies para navegar por Internet lo necesitamos, o por el contrario, no podremos hacerlo.
Una vez tengamos nuestros servidores elegidos, procedemos a editar el archivo de configuración:

```
sudo gedit /etc/proxychains.conf
```

Si no lo hemos modificado anteriormente, este archivo debería constar de un pequeño manual de como configurarlo.
La mejor opción es deshabilitar "dynamic_chain", es decir borrar el # antes de la línea. Ahora, y preferentemente al final del archivo para facilitar su lectura, añadiremos las direcciones de los proxies con el siguiente formato:

```
socks5          77.91.195.16          3128
socks5          188.93.20.179         8080
socks5          216.155.139.115       3128
```

Donde socks5 es el tipo de proxy, seguido de la dirección IP y del puerto a usar. En vez de socks5, también podemos usar socks4 y http (los proxys https no se indican con "https" si no con "http").

Una vez añadidos, guardamos los cambios y cerramos el editor. A continuación para usar el programa, sólo tenemos que teclear en la terminal:

proxychains nmap, o proxychains firefox o la aplicación que sea...

Otra manera de usar proxychains

Para usar proxychains también podemos hacerlo instalando directamente proxychains + tor, de esta manera en terminal quedaría algo así:

```
sudo apt-get install proxychains tor
```

De esta manera estaremos instalando Proxychains, además de Tor (si bien no instalamos todo el programa de tor, para instalar tor es como se ha informado antes y aun teniendo instalado tor en nuestro Linux hay que pensar que "tor browser" es como un portable), y estará utilizando el proxy de Tor.

Para ejecutar de esta forma el programa deberemos abrir el terminal y la sintaxis será la misma:

```
proxychains firefox
```

Sólo que de esta forma no deberemos cambiar el archivo que antes requería modificarse.

VPN (VIRTUAL PRIVATE NETWORK)

Una red privada virtual, RPV, o VPN de las siglas en inglés de Virtual Private Network, es una tecnología de red que permite

una extensión segura de la red local sobre una red pública o no controlada como Internet. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada. Esto se realiza estableciendo una conexión virtual punto a punto mediante el uso de conexiones dedicadas, encriptación o la combinación de ambos métodos.

Desde mi punto de vista, una VPN es el mejor método para el anonimato en la red. Mi conclusión reside en el hecho de que "Anonymous" aconseja utilizarlo para el "hacktivismo". Además de que con VPN la velocidad de red es la misma o casi la misma que sin VPN, mientras que en otros métodos como Tor o utilizando proxys la velocidad se ve tremendamente afectada.

Hay dos maneras de utilizar VPN, depende del distribuidor hay de pago o gratuitas. Es cierto que Anonymous desaconseja utilizar VPN gratuitas para hackear, pero debemos tener en cuenta el uso que le quiera dar cada una.

Cuando pienses en ponerte un servicio de VPN, primero plantéate la legislación del país. Una VPN estadounidense puede entregar tus datos fácilmente ante la emisión de una orden judicial. En otros países, como Suecia o Islandia, sería improbable, pues tienen una fuerte política de privacidad, lo cual hace que sea más difícil para las agencias de la ley acceder a ellos. Además, algunos servidores no guardan logs (registros) de los usuarios. También intenta conseguir servicios de una VPN que acepte pago anónimo (para aquellos que guardan datos sobre la facturación). Lo que hace la VPN es ocultar tu IP, y tú puedes escoger entre diversas IP correspondientes a distintos países. Cuando elijas un servicio VPN asegúrate de que no sea de tu país sino de uno donde al rastrear tu IP sea difícil encontrar tu información privada como decíamos.

A continuación os dejo una lista que he extraído de la web de "hispanon". Hay gratuitas y de pago. De todos modos puede que algunas estén desactualizadas o ya no existan.
También dejaré las que seguro existen y que personalmente las he probado tanto en Windows como en Linux.

Servicios Comerciales VPN [Recomendadas]:
http://www.swissvpn.net
http://www.perfectprivacy.com
https://www.ipredator.se
http://www.anonine.se
https://www.vpntunnel.se

VPN gratuitas (No recomendables):
http://cyberghostvpn.com
http://hotsposshield.com
http://proxpn.com
https://anonymityonline.org

Personalmente he utilizado para Windows "cyberghostvpn" y no tengo ninguna queja.
Para Linux no hay tantas opciones como para Windows o incluso Android o Mac (para las que también están disponibles), pero el caso es buscar y quien busca encuentra. Hay varias opciones como por ejemplo "torvpn", pero el servicio gratuito está muy limitado en cuanto al tiempo de uso y la configuración para neófitas en Linux es bastante complicada. En cambio "Securitykiss" es muy fácil de configurar y el resultado es muy complaciente. Existe "vpnbook" pero no la he probado y personalmente no puedo decir nada de ella.

Así pues, podemos utilizar para:
Windows:
http://www.cyberghostvpn.com
http://www.hotspotshield.com

Linux
http://www.vpnbook.com
https://www.securitykiss.com
http://www.torvpn.com

No vamos a detallar como instalar una VPN, ya que eso depende de cada red que se quiera descargar e instalar. De todos modos, como siempre, en Windows y sobretodo para quien no esté muy acostumbrada a Linux, instalar las VPN es muy fácil. En Linux la cosa se complica un poco, depende de cual escojamos. Si queremos instalar Torvpn, la instalación es bastante complicada, mientras que por el contrario, la instalación de SecurityKiss es muy sencilla y no conlleva demasiados dolores de cabeza.

Aun así, como siempre se recomienda encarecidamente...

¡USAD LINUX!

PROXY WEB

Este apartado desde mi punto de vista no lo tengo muy claro ya que no lo he utilizado demasiado, pero no por ello voy a dejar de mostrarlo. Estas web se basan en que vosotras, a la hora de querer buscar información en la red de una manera "anónima", utilicéis el proxy que os ofrece la web. Así estaréis navegando de manera "segura". Para encontrar páginas de este tipo, con que busquéis en ixquick "proxy web" o algo así, encontrareis las que queráis. De todos modos dejo a continuación un para que sepáis un poco como funcionan.

http://proxyweb.com.es
http://proxyanonimo.es

Como mencionamos arriba es algo que no se ha experimentado demasiado ya que es fiarse de la buena fe de estos sitios, y por desgracia es algo que no sobra demasiado en los tiempos modernos. Así que es preferible que cada una controle lo que hace y sea una misma responsable de sus propias acciones.

HIDE IP MEGAPACK

Otro modo de navegar "anónimamente" es encontrar algún software que oculte nuestra IP. Este tipo de programas son parecidos a Tor, teniendo en cuenta que lo que deseamos con estos, es que nuestro rastro a la hora de hacer búsquedas quede camuflado.

Para encontrar alguno que nos haga navegar de manera anónima no hace falta buscar mucho, por lo menos para Windows ya que para Linux la cosa se complica, ya que escribiendo en la barra del buscador algo como *descargar navegar anónimo* salen muchos enlaces para descargarnos alguno. Cada programa de estos funcionan de una manera distinta, aunque la mayoría de ellos funcionan a base de proxys, así que con esta información sabemos que su velocidad queda diezmada a la hora de encadenar los proxys, si es que los encadenan.

En este caso voy a hablar de "Hide IP Mega Pack" y os voy a dejar el enlace para su descarga, ya que es realmente cómodo, bastante rápido, y algo debe tener, que hasta hace un par de meses que cerraron una web destinada a la información del activismo informático, había un paquete de aplicaciones para hacer "ataques DDOS" y entre estos, "Hide Ip" era el que mostraban como programa para ocultar la IP y realizar el ataque.

Link del programa y el vídeo donde se enlaza a su descarga:
http://www.mediafire.com/download/1tral8tbb1twn69/Hide+IP+Mega+Pack+Por+TheChibaldo.rar
https://www.youtube.com/watch?v=ZUfG2qFdy0E

La instalación y uso de este programa es muy fácil, además de que en el vídeo ya explican como de instala.

Conversaciones Seguras

Hablemos de ECHELON. Se trata de un software informático que busca palabras clave específicas en e-mails, faxes y mensajes telex. Las palabras clave incluyen actividades militares, tráfico de drogas, el comercio con bienes embargados o la tecnología de doble uso (esto es, productos comerciales que pueden tener también usos militares), y actividades económicas...
... Se está desarrollando la tecnología que permitirá distinguir ciertas voces de entre millones de grabaciones telefónicas....

Tal como indica el título, en el siguiente capítulo vamos a ver cómo podemos tener comunicaciones seguras, lejos de ojos que interceptan, investigan, escrutan, en fin ¡que espían!. Para ello en las próximas páginas vamos a mostrar con un par de programas, cómo hacerlo. El primer programa es Mozilla Thunderbird, un gestor de correo. Y el segundo es Pidgin, un gestor de mensajería instantánea.

Aunque cada programa utiliza herramientas distintas del otro para poder mantenernos seguras a la hora de comunicarnos, la base principal de todo ello, es la misma: CIFRAR los mensajes.

En el capítulo "Cifrado" intentaremos hacer una explicación, breve y sencilla, ya que de lo contrario se pueden escribir varios libros, y de hecho los hay, sobre el funcionamiento criptográfico y de los tipos de cifrados que hay. Así que en éste nos centraremos en intentar detallar lo mejor posible el cómo llegar a escribir mensajes encriptados y estar un poco más seguras a la hora de comunicarnos en internet.

Seguro que no es necesario, pero aun así lo repetimos: a pesar de la aparente seguridad que proporcionan estos programas, ya que hacen prácticamente imposible la lectura de un mensaje cifrado a no ser que tengáis las llaves y contraseñas necesarias, en internet nada es cien por cien seguro.

Para comprobar la fuerza de una llave y su contraseña, y entender mejor a que me refiero, no hacen falta muchos programas. Basta con escribir un pequeño texto en un mensaje y cifrarlo con una llave que su contraseña sea simple, de siete u ocho dígitos (un nombre de pila por ejemplo). Luego escribir el mismo texto y cifrarlo con una llave de la cual su contraseña sea una serie de treinta dígitos (con números, letras mayúsculas, minúsculas, símbolos varios...), y veréis que mientras el cifrado del primer mensaje es muy corto, el segundo mensaje será mucho más largo. Es muy posible que esto que acabamos de comentar no se entienda ahora mismo, pero dentro de unas cuantas páginas y un buen rato frente a vuestros ordenadores, sabréis a qué me refiero.

En la situación social actual, donde cada día aparecen datos nuevos sobre la interceptación de comunicaciones (por teléfono, internet, hasta en el lenguaje de signos!!) por parte de estados, servicios secretos, empresas privadas y demás; es de suma importancia empezar a tener una cultura de seguridad en estos temas. Desde mi punto de vista, la seguridad a la hora de comunicarnos por internet, no debe estancarse en el ámbito político, sino que debería incluirse en todas y cada una de nuestras conversaciones. Ya sea para preparar una

manifestación, quedar para ir a tomar un café o felicitar un cumpleaños.

Los datos filtrados por antiguos militares o incluso ex trabajadores de la CIA, demuestran una vez más la ética del sistema, intentando averiguar cualquier detalle sobre todas nosotras para controlar los aspectos de nuestras miserables vidas, facilitando la represión, la manipulación y absolutamente lo que se le pueda ocurrir a estas mentes enfermas que la gente sigue votando pase lo que pase.

Los problemas de la vigilancia indiscriminada o política no pertenecen sólo a los nuevos proyectos de control social como PRISMA, que el ex funcionario de la CIA Edward Snowden reveló demostrando que el gobierno de los Estados Unidos vigila constantemente a sus ciudadanas y en el que están metidas empresas de redes sociales, telefónicas o de transferencia de archivos. O proyectos como TIA (Total Information Awareness) del que se habla en el prólogo del libro. Sino que tenemos precedentes de proyectos como Echelon o COINTELPRO que se esforzaron por acabar y asesinar con cualquier resistencia que se opusiera a las medidas imperialistas de los EEUU.

Teniendo en cuenta que estos planes son sólo algunos que pertenecen a Estados Unidos, y que la vigilancia global se extiende a cualquier país, deberíamos plantearnos seriamente nuestra manera de relacionarnos con las demás, sobretodo ahora que las personas hablan sin verse, cuentan sus problemas sin conocerse, sin saber si la persona con quien hablas es quien dice ser, sin saber si lo que escribimos lo están leyendo terceras, cuartas, o quintas personas. Debemos dar por hecho que todos los países tienen proyectos similares, quizá no tan desmesurados, pero los tienen. Y que estés donde estés deberías pensar en hacer algo al respecto.

Es obvio que los estados poseen cierta tecnología que nosotras ni imaginamos, pero no por ello dejaremos de luchar. Hará diez años atrás las personas en España creían que gozaban de cierta "libertad", ya que en tiempos de la dictadura franquista podían meterte presa si te detenían pintando en la calle, mientras que ahora no acostumbra a ocurrir nada peor que una multa en este caso específico. Pero en 2013 han detenido a cinco personas y las han acusado de terroristas por opinar en redes sociales. Así que, puede que quienes leáis esto lo tengáis muy claro, pero...
¿De verdad permitiremos ponérselo tan fácil?.
Por lo menos que no puedan leer a la primera lo que decimos. Que tengan que perder el tiempo en intentar averiguar nuestras contraseñas.
Que sufran miopía y les suban sus dioptrías por estar horas frente a ordenadores "seguros"...

THUNDERBIRD

Mozilla Thunderbird es un cliente de correo electrónico que pertenece a Mozilla. Entre sus ventajas destaca el hecho de que forma parte del software libre y además nos permitirá crear llaves para poder comunicarnos con nuestras compas de manera "segura" y cifrada.

Thunderbird, para quienes no lo conozcan, es algo similar a Outlook Express, pero en vez de ser una mierda de gestor destinado únicamente a llenarnos el PC de coockies para rastrear nuestros movimientos, gustos y preferencias. Es un gestor de correo que nos permitirá tener todas nuestras cuentas con un par de clics, y con la capacidad de poder generar mensajes cifrados que sólo la destinataria podrá descifrar. Como ocurre a menudo, al final todo se reduce a lo mismo:

la fuerza de la contraseña. Pero esto ya lo desarrollaremos cuando generemos las claves y en el capítulo destinado a "Keepass", el administrador y creador de contraseñas.

Instalando Thunderbird

Como la finalidad de este libro es mostrar información sobre la seguridad y más precisamente este capítulo está destinado a hacer una guía de como poder enviar y recibir mensajes cifrados, vamos a centrarnos en ir paso a paso hasta la meta. Con esto quiero decir que no me centraré en el funcionamiento básico del programa, sino en las herramientas necesarias y como instalarlas para encriptar nuestras conversaciones.

Para ello recomiendo buscar más información al respecto, ya que gráficamente siempre se entiende mejor, pero para resumir un poco.

El cifrado de los mensajes se basa en que tú tienes 2 claves; una pública y una privada, aunque en realidad sólo verás un número de clave (0x87K52853) , o una clave. Y la persona con quien te escribes también.
Este tipo de comunicación se basa en que tú, antes de poder cifrar nada debes mandar tu clave pública a la destinataria y tener guardada su clave pública (más adelante lo explicaremos con detalle).
Una vez hayáis hecho este proceso las dos, el mensaje se encripta con la llave pública de la otra persona y la destinataria lo desencripta con la privada.

Parece un lío importante pero no es tan difícil, de veras. En realidad, aunque estés trabajando con tus dos llaves, sólo hay una contraseña para las dos. Para mayor seguridad, es totalmente imposible que le enviaras la privada en vez de la

pública por error ya que no existe una opción para ello (es imposible equivocarse).
Cuando se vea el proceso paso a paso se entenderá mejor, o no (?). jeje

Es relativamente importante seguir paso a paso la guía para hacerlo todo correctamente. Por supuesto que algunos pasos no es necesario seguirlos al detalle, pero mi consejo es que por lo menos la primera vez lo hagáis como se muestra.

Paso 1 - Descarga e instalación

En windows deberemos clicar en https://www.mozilla.org/es-ES/thunderbird/. Mientras que en Linux, desde mi punto de vista lo mejor será utilizar el centro de software ya que lo instalaremos con nuestro idioma y no tendremos que compilar nada, ni código fuente, ni cosas que a veces se complican. Si al instalarlo en Linux hubiera algún problema, sobretodo con el idioma probad lo que se explica en el siguiente enlace:
http://antoniocruzgomez.blogspot.com.es/2011/06/instalar-thunderbird-en-espanol.html
A partir de descargarlo y seguir los pasos de su instalación, vayamos donde esté instalado y cliquemos en él...

Paso 2 – Descargar e instalar las herramientas de cifrado

Una vez tenemos instalado Thunderbird debemos descargar e instalar en el ordenador el programa "Kleopatra". Este programa será el encargado de gestionar las claves y sin él sería imposible cifrar los mensajes (hay otros programas que sirven para ello, pero después de pasar muchas horas delante de la pantalla. descubrimos que este funciona perfecto). Para las que utilicen Windows tenéis que descargarlo de http://www.gpg4win.org/download.html y descargar la última versión estable que se pueda. A continuación seguís los pasos típicos de instalación de cualquier programa de Windows (Aceptar, acepto, aceptar, etc...).

Mientras que las que usan Linux pueden descargarlo desde el Centro de Software (ahora las que usáis Windows os estáis arrepintiendo, no?). Una vez instalado no hagáis nada con él todavía. Aunque que aparentemente no hace falta para nada, es totalmente necesario para cifrar los mensajes. Aunque para encriptar mensajes no lo utilicemos, gestiona las llaves haciendo que estén accesibles.
En otro capítulo nos detendremos en él y contaremos más cosas sobre este gran programa.

La otra herramienta necesaria es "Enigmail". Enigmail es un complemento de Thunderbird, así que para instalarlo deberemos abrir Thunderbird y buscarlo en *herramientas – complementos*. Aquí es importante decir que cuando abráis Thunderbird por primera vez os aparecerá una o dos pantallas, las cerráis y listo.
Una vez cerradas haced clic con el botón derecho arriba de todo de la pantalla del programa, y en el cuadro que sale teclear en *barra de menú*. Ahora ya tenéis el menú y podéis encontrar la pestaña *herramientas*. Dentro de los complementos, donde dice *Buscar herramientas* poned "Enigmail", lo instaláis y reiniciad Thunderbird. A partir del reinicio ya veréis que en la barra de menú hay una pestaña nueva que dice *OpenPGP*.

Paso 3 – Crear las cuentas

Las cuentas en Thunderbird, tienen algunas "dificultades" que dependen del administrador de la cuenta. Si es hotmail (nunca recomendable) en Linux no habrá problema pero en Windows casi seguro que algo raro ocurre (a mí me ha pasado 9 de cada 10 veces que lo he instalado), así que mejor haceos una cuenta en gmail por lo menos (además de que **con hotmail no se pueden cifrar mensajes**, así que no vale para nada).
Para instalar la cuenta gmail en Thunderbird, antes de nada hay que abrir la cuenta en Firefox y clicar en *herramientas – configuración – reenvío y correo POP/IMPAP* y marcar la casilla de *habilitar IMPAP*.

Guardad los cambios, cerrad la cuenta en Firefox y listo. Ahora podemos abrir de nuevo Thunderbird.
Cuando abrimos Thunderbird, creo que sale un cuadrado con algunas cosas (*¿Le gustaría tener una nueva dirección de correo?*), pero no le hacemos caso y lo cerramos seleccionando *saltarse esto y usar mi cuenta existente* (cada vez que creéis la cuenta en Thunderbird os saldrá este cuadrado (por lo menos en los últimos dos años ha estado ahí siempre el cuadradito...). En el caso que no salga, dais en *crear una nueva cuenta* y seguid los pasos para crearla. Debéis poner la contraseña y todo lo normal de la cuenta que ya teníais anteriormente.

Igual es tontería que lo diga, pero la cuenta se debe crear antes de descargar Thunderbird, o sea que es la que usáis a diario u otra creada para tal fin. No os agobiéis si a la primera no sale ya que siempre pasa algo raro cuando instalamos solas este programa, lo digo por experiencia. Pensad si la contraseña es la correcta, o el correo, o lo que sea. Aceptáis a todo y listo. A continuación tendréis en la pantalla izquierda vuestra cuenta con sus mensajes y todo eso (vuelvo a decir que si es con hotmail no saldrá ningún mensaje de la bandeja de entrada ni nada o quizás sí, mientras que si es gmail o riseup -Por supuesto que ya estáis tardando en pasaros a riseup!- os saldrán todos los mensajes que tenéis...

Paso 4 – Generar las claves

Para generar las claves debéis ir a *OpenPGP – Administración de claves*. En el cuadro que sale, lo primero debe ser marcar la pestaña que dice *Mostrar por defecto todas las claves*.

A continuación hay que hacer clic en *Generar – Nuevo par de claves*. Sale un cuadro nuevo, y en él seleccionáis la cuenta que os interesa donde dice: "Cuenta / ID usuario".

Poned la contraseña que creáis más segura, ya que debe ser muy pero que muy segura (para ella lo mejor quizás sería

usar Keepass para crearla, aunque cada vez que recibáis un mensaje cifrado o enviéis uno deberéis escribir la contraseña, con lo que hay que tener Keepass abierto todo el rato...).

A continuación, personalmente marco la pestaña de *la clave no expira*, buscad la pestaña de *avanzadas* y ahí poned el tipo y tamaño que queráis de la clave. Cuando esté todo listo haced clic en *Generar clave* (si la contraseña es potente y el tamaño también tardará unos minutos).
Cuando estén generadas las claves os saldrá un cuadro diciendo que hagáis el certificado de revocación, yo personalmente clico en C*ancelar* ya que si algún día quiero dar de baja la clave lo haré entonces... Con esto ya tendremos el par de claves. Aunque durante todo este proceso hablan de "clave", la realidad es que acabamos de generar el "par de claves".

Paso 5 – Configuración de las cuentas

Una vez tengamos las claves creadas, cerraremos todas estas ventanas y tocará configurar la cuenta para poder cifrar. Estamos en la ventana principal. En Windows marcamos *herramientas – configuración de las cuentas*, en Linux marcamos *Editar – configuración de las cuentas*.

Aparecerá una ventana de configuración y lo primero que veremos es la *Configuración del servidor*.
En principio, sobre este tema, sobretodo si trabajáis en Linux, no hay que tocar nada. Pero por si acaso escribiremos la información que debéis escribir. Si algo no coincidiera deberíais poner lo que escribimos en esta guía.

A la izquierda de la ventana que sale, vemos las cuentas con opciones de configuración y a la derecha las configuraciones posibles.

Hasta el momento, debería estar todo así:

Riseup

Servidor de entrada IMAP: imap.riseup.net
Puerto: 993

Gmail

Servidor de entrada IMAP: imap.googlemail.com
Puerto: 993

Para comprobar el "Servidor de salida SMTP", que se encuentra en la parte inferior-izquierda de la ventana (debajo de las cuentas), Hay que clicar en *Servidor de salida* y las cuentas deberían estar:

Riseup

Nombre del servidor: mail.riseup.net
Puerto: 465
Seguridad: SSL/TLS
Método de identificación: Contraseña normal

Gmail

Nombre del servidor: smtp.googlemail.com
Puerto:465
Seguridad: SSL/TLS
Método de identificación: Contraseña normal

Debajo de cada cuenta, en sus respectivas opciones, hay que seleccionar *redacción y direcciones* y deshabilitaremos la pestaña de *redactar mensajes en formato HTML*.

Lo más importante en este paso es ahora, debemos hacer clic en *Seguridad OpenPGP* y habilitar la pestaña de *Activar el soporte OpenPGP para esta identidad – usar un ID de clave específico* y seleccionamos la clave específica de esta cuenta.

Con esto ya queda menos para cifrar los mensajes. Aceptamos y listo.

Paso 6 – Intercambio de llaves

En la ventana principal, clicad en *Redactar*, os saldrá una ventana para redactar un mensaje. Escribís a quien vosotras queráis, que deberá ser alguien que tenga claves o esté haciendo lo mismo que vosotras.

Donde dice *De* seleccionad la cuenta en cuestión (hay detalles que escribo que parece que sean una tontería pero lo típico es mandar el mensaje y que sea con otra cuenta y cosas por el estilo, y hasta que no lo descubres pueden pasar días). En *asunto* lo que os dé la gana y en el mensaje también. Aquí lo importante es que debéis clicar en *OpenPGP* (en el de la barra de menú, no en el que tiene el candado dibujado) – *Adjuntar mi clave pública*. Es posible que no salga nada en el cuadrado de los adjuntos pero tranquilas que seguro que lo manda. Saldrá cuando se esté enviando. Lo enviáis y listo, una cosa menos.

Si cuando habéis instalado la cuenta en Thunderbird habéis seleccionado que no guarde la contraseña de la cuenta, cada vez que enviéis un mensaje o encendáis Thunderbird os pedirá la contraseña de la cuenta.

Cuando mandéis mensajes cifrados os pedirá la contraseña de la cuenta y la de la clave, por separado en dos ventanas distintas. Deberéis leer bien cual os pide en cada momento; la del servidor SMTP (de salida) o PGP (.asc). Esto lleva a muchas confusiones...

Cuando recibamos la clave de otra persona, en la ventana principal saldrá que tenéis un mensaje nuevo. Doble clic encima de este y saldrá la ventana del mensaje recibido. Debajo del mensaje aparecerá como archivo adjunto la llave de quien os la envía, que como hemos comentado antes son una serie de números y cifras (0xJ6H786G).

Clicamos con el botón derecho encima del adjunto y seleccionamos *Importar clave OpenPGP*. En el momento que hagamos esto la llave pública de nuestra compa estará en el "administrador de claves" y si queremos podemos comprobarlo seleccionando *OpenPGP – Administración de claves*.
En esa ventana debería salir el correo de la persona junto con su nombre de la cuenta y el ID de clave.
En las opciones de las claves podemos configurar como queramos las claves, podemos darle confianza y subir nuestra clave pública al servido de claves, por si alguien busca nuestra clave pública teniendo únicamente nuestro correo. También podemos buscar la clave de algunas web como "lahaine" o "biteback" u otras que puede que hayan subido su clave pública a alguno de los servidores de claves...

Paso 7 – Enviar y recibir mensajes cifrados

Ahora ya viene lo bueno y para lo que habéis estado un buen rato enpantalladas por un poco de seguridad e intimidad en vuestras conversaciones.

Personalmente aconsejo usar este método para cualquier correo que enviemos, sea de comprar el pan o pedir dinero a una amiga.

Como sabréis muchas de vosotras, los correos son muy fáciles de hackear por gente novata en el arte del hack, imaginaos que puede hacer el estado si va a por alguna de nosotras.

Para **enviar**, en la ventana principal seleccionamos *Redactar*, escribimos el mensaje y como ya es lógico escribiremos la cuenta para mandar el mensaje de alguien del que poseamos su clave pública (ya que es con lo que se va a cifrar) y seleccionaremos *OpenPGP* (cualquiera de los dos que hay) – *Cifrar mensaje*.

Hay que tener en cuenta un consejo que doy. Mejor seleccionad también *firmar mensaje*, ya que vuestra clave firmará el mensaje y quedará demostrado que sois vosotras. La diferencia es que si usáis esta opción al enviar el mensaje os pedirá la contraseña de vuestra clave y la de la cuenta, mientras que si no la seleccionáis únicamente os pedirá el pass del servidor de salida (SMTP) que es el de la cuenta. Lo expongo así ya que hay un momento en que se convierte la cosa un poco técnica y está bien conocer estos conceptos.
Para **recibir**, en la ventana principal veréis que os ha llegado un mensaje. Cuando lo seleccionéis aparecerá una ventana con el mensaje, que consta de una serie enorme de números y cifras, pero a la vez saldrá otra ventanilla que os dirá algo como *Por favor, escriba la frase de paso OpenPGP o el PIN de su tarjeta inteligente*. Estará pidiendo la contraseña de vuestra clave.

Desde mi punto de vista hay que tener en cuenta un par de detalles, y que se traducen en leer bien qué es lo que pide en cada momento, ya que es muy fácil confundir qué clave o qué cuenta estáis usando.

Hasta aquí hemos llegado en el capítulo de Mozilla Thunderbird, uno de los pilares principales en la comunicación segura e íntima.
El programa en sí tiene muchas más opciones y recomiendo que cada una las investigue por su cuenta, para de este modo usarlo con cabeza y responsabilidad.

Y ahora, que nadie os espíe!!!

PIDGIN + OTR

Pidgin es un cliente gratuito y de código abierto que te permite organizar y administrar tus distintas cuentas de Mensajería Instantánea (MI) utilizando una única interfaz. El complemento Off-the-Record (Fuera de Registro) (OTR) diseñado para ser utilizado con Pidgin garantiza comunicaciones autenticadas y seguras entre usuarios de Pidgin.

Por desgracia no he podido probar demasiado, en realidad no lo he probado con nadie, ya que al ser un gestor de mensajería instantánea te ves obligada a comunicarte con alguien que use Pidgin y en mi caso no tenía a nadie con quien compartir una experiencia Pidgin.

Lo que sí puedo decir es que su instalación es muy simple en Windows y en Linux y desde la misma página principal se descarga para los dos sistemas operativos. Como ya he comentado, al no tener experiencia en este software, lo que haré será dejaros algunos enlaces para su descarga, instalación y como configurarlo para enviar mensajes cifrados.

Para instalarlo en Linux también lo encontramos en los repositorios, y lo podremos descargar desde el Centro de Software, o bien escribiendo en un terminal:

```
sudo apt-get install pidgin
```

Como algunos de los programas que salen en esta guía, Pidgin está recomendado por el colectivo de "Security In A Box", y para quien quiera información sobre esta gente, debe saber que lo forman dos colectivos destinados a "satisfacer las necesidades de seguridad digital y de privacidad de activistas y defensores de derechos humanos".

Seguridad Local

Golpe represivo contra el movimiento libertario catalán
15 de Mayo de 2013 (caso contra las 5 de Barcelona)

...También se le incautaron varios ordenadores que se están analizando en estos momentos para determinar su grado de implicación en una organización terrorista anarquista con la que se le vincula...

Europa Press - 9 de Febrero de 2007 (caso contra Nuria Pórtulas)

Contraseñas

Hablemos ahora de Carnivore.
Carnivore es un "analizador de paquetes" o "sniffer" adherido a los ordenadores de las compañías de servicios de internet para que grabe datos acerca del tráfico de e-mails. Digamos que eres una sospechosa. Carnivore puede grabar los nombres de las que te han enviado o a las que has enviado e-mails, al igual que el contenido de estos. Puede compilar el historial de las páginas web que has visitado... El FBI está desarrollando un virus "Linterna Mágica" que permita a Carnivore recopilar contraseñas de los ordenadores.

Es bien sabido que dentro de la seguridad informática, la piedra angular que decidirá si estamos seguras o no, si obtendrán pruebas contra nosotras o si se van a tener que comer sus denuncias y represión, es la capacidad de crear contraseñas adecuadas, fuertes y seguras.

Siempre se comenta que no debemos poner fechas de nacimiento, nombres de familiares y cosas por el estilo que puedan delatarnos a la primera y que no les sea difícil descifrar. Es cierto que la tecnología que disponemos para nuestra seguridad es muy efectiva en lo que respecta a este tema, pero siempre es mejor pensar que ellas están un paso

por delante nuestro. De esta forma nos mantendremos en guardia en todo momento.

Esto siempre ha sido así, la policía y el estado puede fallar tantas veces como quiera en cogernos, pero nosotras no podemos fallar nunca. Al mínimo error o despiste, la represión estará ahí para recordarnos que si luchas contra la máquina esta hará lo que pueda por vengarse.

Por este motivo las contraseñas deben ser seguras y fuertes. ¿Qué significa esto? Que sean largas (de 25 caracteres por lo menos), que tengan mayúsculas y minúsculas, que usemos números, símbolos y todo lo que se nos ocurra. Siempre he leído que para crear contraseñas pensemos en refranes, textos que no tengan nada que ver con nosotras, o sea que no valdría "Viva la Anarquía", y que juguemos con estos poniéndoles comas o puntos, intercambiar mayúsculas, etc...

Por ejemplo: Una contraseña débil sería una que fuese muy corta o que fuese la predeterminada, o una que pudiera adivinarse rápidamente al buscar una serie de palabras que es posible encontrar en diccionarios, nombres propios, palabras basadas en variaciones del nombre de la usuaria. Una contraseña fuerte debe ser suficientemente larga, al azar, o producirse sólo por la usuaria que la eligió, de modo tal que el 'adivinarla' requiera un largo tiempo. Ese tiempo 'demasiado largo' variará de acuerdo al atacante, sus recursos, la facilidad con la que la contraseña se pueda descubrir, y la importancia de ésta para el atacante. Por lo tanto, una contraseña de una estudiante quizás no valga la pena para invertir más de algunos segundos en la computadora, mientras que la contraseña para acceder al control de una transferencia de dinero del sistema de un banco puede valer varias semanas de trabajo en una computadora.

'Fuerte' y 'débil' tienen significado solamente con respecto a tentativas de descubrir la contraseña de un usuario, ya sea

por una persona que conoce al usuario, o una computadora que trate de usar millones de combinaciones. En este contexto, los términos pueden tener una precisión considerable. Pero nótese que una contraseña 'fuerte' en este sentido puede ser robada, o extraída del usuario ya sea mediante la extracción del historial de un teclado, grabada mediante aparatos de comunicación o copiada de notas dejadas por olvido.

Tengamos en cuenta que normalmente el intento de adivinar una contraseña, ya sea por parte de la policía o quien sea, suele hacerse por "fuerza bruta" (un software con uno o varios diccionarios va probando combinaciones hasta dar en el clavo), pero hay ocasiones que han reconocido que para ciertos casos necesitarían años para que un súper ordenador llegara a conseguirla. El FBI estuvo un año intentando conseguir abrir unos volúmenes creados con Truecrypt en un caso de mafias y corrupción en Brasil y finalmente se dio por vencido, así que todavía no está todo perdido. También debemos pensar que cada año mejoran considerablemente sus herramientas (y las nuestras), reduciendo el tiempo necesario para descifrar las contraseñas.

De todos modos generar una contraseña fuerte y ahora viene lo bueno, recordarla!! es muy difícil. Por eso mismo el siguiente programa que mostraremos es un generador y administrador de contraseñas.

KEEPASS

Debo reconocer que nunca me he fiado de este tipo de software, siempre he intentado hacer yo las contraseñas y pensaba que eran robustas, hasta que instalé Keepass y vi que las que yo creaba, a nivel de fuerza eran una mierda. Ahora me veo en la obligación de cambiarlas todas.

Ya que el motivo de que lo haya descubierto, ha sido la intención de añadirlo en la guía debo reconocer que no he tenido mucho tiempo para ver todo lo que esconde este programa, pero aquí vamos a mostrar los usos básicos de crear y configurar contraseñas. De todos modos Keepass es bastante intuitivo y con las explicaciones que daré a continuación no será muy difícil que os hagáis amigas de la aplicación.

La ventaja que tiene este software es que después de tener varias cuentas de correo, llaves para cifrar mensajes, carpetas y archivos encriptados... Y todo esto protegido con contraseñas, lo único que tendremos que recordar es un par de estas. La importancia reside en su robustez y fortaleza, ya que lo que protegerán, es precisamente el resto de la seguridad de nuestro PC.

Instalación

Para instalar en Windows se accede a http://keepass.info/download.html, descargáis el .exe y su instalación es simple y rápida, además de que en esta versión ya viene incorporado el idioma español con lo que facilita las cosas.

Para su instalación en Linux (recordemos que en toda la guía estamos refiriéndonos a Ubuntu y derivados) debemos abrir la consola y teclear en esta:

```
sudo add-apt-repository ppa:jtaylor/keepass
sudo apt-get update
sudo apt-get install keepass2
```

Para instalar el idioma español deberemos ir a http://keepass.info/translations.html, descargar el paquete y una vez lo tengamos en nuestra carpeta de descargas (por ejemplo), lo descomprimimos, lo copiaremos a la carpeta */usr/lib/keepass2* y le daremos permisos de ejecución.

En cuanto abramos el programa, iremos a *view – change language* y seleccionaremos el español.

Para hacer esta secuencia iremos a la consola:

```
cd Descargas && ls
unzip KeePass-2.22-Spanish.zip
sudo cp Spanish.lngx /usr/lib/keepass2
chmod 777 spanish.lngx
```

Y listo. A disfrutarlo en castellano!!

Configurar la llave maestra

Esta llave maestra es lo que deberemos recordar sí o sí. Para ello la esconderemos, la memorizaremos o lo que sea, pero no la olvidemos jamás. Una buena opción puede ser guardarla en un volumen oculto de Truecrypt con lo que únicamente deberíamos recordar la de este volumen.

Empezar

Se pulsa sobre el botón *Nuevo* y aparecerá una ventana para crear la llave maestra. La ventaja de esta ventana es que cuando estamos intentando crearla justo debajo nos muestra la cantidad de bytes que pesa esta, con lo que nos hacemos una idea de lo fuerte que puede ser.
Otra opción que hay es que la hagamos con el generador de contraseñas. En este caso pasamos a otra ventana y mientras esta la genera debemos mover el ratón aleatoriamente en el recuadro gris que hay para darle más fuerza.
También podemos usar las dos opciones a la vez y si algún día nos intervienen el ordenador, el policía de turno que tenga que descifrar nuestro ordenador va a pasarlo mal con nosotras.

Lo que deberemos hacer cuando hayamos modificado todas nuestras contraseñas con este programa será abrir keepass,

nada más encender el ordenador ya que dependeremos totalmente de él.

Este es uno de los motivos por los que aun viendo las ventajas de keepass, soy un poco reacia a usarlo como método para todas las contraseñas. Pensad que si un día el disco duro se estropea, podemos perder mucha información, y en el caso que hagamos copias de seguridad de las contraseñas estaremos debilitando nuestra seguridad. Quizás lo mejor sea ir apuntando en un papel las contraseñas y tenerlo a buen recaudo, pero esto no deja de ser una debilidad en la seguridad.
Que cada una haga lo que mejor le convenga. Si usáis este programa estudiadlo bien ya que es de gran utilidad y podemos sacarle mucho provecho.

Generar y administrar las contraseñas

Una vez hemos creado la clave maestra, volveremos a estar en la ventana principal y veremos que habrá aparecido una carpeta denominada general y con varias subcarpetas. Esto que tenemos podremos editarlo, borrarlo o añadirle nuevas entradas. También veremos que hay un par de contraseñas por ahí, son un par de ejemplos y mejor será eliminarlos para no hacernos un lío.

Para terminar vamos a mostrar como haremos una contraseña para una cuenta de correo, por ejemplo.

Vamos a teclear encima de la carpeta que pone *eMail*. Una vez seleccionado nos desplazamos a *herramientas – generar contraseña*. Nos saldrá una nueva ventana con varias opciones sobre cómo queremos que sea, incluyendo los caracteres, algoritmo, si queremos que emplee un patrón específico o recolectar una entropía adicional. En varios tutoriales de la red muestran esta parte de otra forma. Según los que he leído, en el momento de estar en la ventana principal, seleccionan

añadir entrada y rellenan el nombre o lo que queráis poner para identificarla. Yo prefiero la otra forma ya que como hemos visto primero podemos modificar la configuración de la contraseña para que sea más difícil descifrarla.

También podemos usar keepass como administrador de las contraseñas que tengamos, añadiéndolas como entradas a la sección que queramos.

Algo que me gusta mucho de este programa es, que para ver si las contraseñas que usamos hasta ahora son lo suficiente buenas, basta con escribirlas cuando las añadimos como "nueva entrada", y veremos que en realidad no eran tan buenas como pensábamos.

KEEPASSX

Keepassx, aunque el nombre sea casi idéntico al software que acabamos de mostrar, es otra aplicación. Su trabajo es el mismo que Keepass y su interfaz gráfica es casi idéntica. En un principio no se iba a añadir al libro, ya que con Keepass había suficiente, pero posteriormente hemos descubierto que Keepassx está en todos los repositorios de Linux, además de poder instalarlo en Windows, y esto hace que sea más compatible con todos los sistemas que Keepass.
No hace falta cambiarle el idioma en Linux, ya que se instala directamente con el idioma de nuestra distribución.

El funcionamiento es casi exacto a Keepass, así que no haremos una explicación de cómo usarlo.
Lo que sí haré es mostrar su web para que las usuarias de Windows puedan descargarlo:
www.keepassx.org/downloads

Para las usuarias de Linux bastará con escribir en la terminal:

```
sudo apt-get install keepassx
```

Tenemos estas dos opciones. Cada una que utilice la que mejor le convenga.

Cifrado

La privacidad y la seguridad son peor que las falsas esperanzas, son distracciones. Ya han tirado de la cadena, y por las tuberías hacia las cloacas bajan las preocupaciones ecológicas y sociales, así que esa seguridad no existe. Y la privacidad nunca existió excepto en las fantasías de aquellas que se veían a sí mismas como disgregadas del resto de la población

El cifrado es un método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para descodificarlo

En criptografía un **cifrado**, es un procedimiento que utilizando un algoritmo (**algoritmo de cifrado**) con cierta clave (**clave de cifrado**) transforma un mensaje, sin atender a su estructura lingüística o significado, de tal forma que sea incomprensible o, al menos, difícil de comprender, a toda persona que no tenga la clave secreta (**clave de descifrado**) del algoritmo que

se usa para poder descifrarlo (**algoritmo de descifrado**). Por tanto tenemos dos algoritmos (el de cifrado y el de descifrado) y dos claves (clave de cifrado y clave de descifrado). Estas dos claves pueden ser iguales (criptografía simétrica) o no (criptografía asimétrica).

No vamos a detenernos mucho explicando exactamente cómo funciona la criptografía, ni cuantos tipos de claves hay, ya que daría para mucho y es realmente complicado entender todo esto (por lo menos para mí). Lo que sí haremos es mostrar una breve explicación sobre los tipos de cifrado que podemos encontrar en los programas que usaremos en esta guía.

Para empezar, ya que hemos hablado anteriormente de Thunderbird y OpenPGP, vamos a mostrar qué tipos de clave se utilizan para cifrar mensajes.
Cuando hemos creado nuestro par de claves con OpenPGP, hemos visto que podíamos escoger entre los tipos de clave "RSA" y "DSA y El Gamal".

RSA es el primer algoritmo de cifrado creado y el más utilizado con el que se puede cifrar y firmar digitalmente.
La seguridad de este algoritmo radica en el problema de la factorización de números enteros. Los mensajes enviados se representan mediante números, y el funcionamiento se basa en el producto, conocido, de dos números primos grandes elegidos al azar y mantenidos en secreto. Actualmente estos primos son del orden de 10 elevado a 200, y se prevé que su tamaño crezca con el aumento de la capacidad de cálculo de los ordenadores.
Se cree que RSA será seguro mientras no se conozcan formas rápidas de descomponer un número grande en producto de primos.

DSA y Elgamal se refiere a un esquema de cifrado basado en problemas matemáticos de logaritmos discretos. Como RSA es capaz de cifrar y firmar mensajes.

Hasta el momento el algoritmo ElGamal de cifrado/descifrado puede ser considerado un algoritmo efectivo. Un adversario con la habilidad de calcular logaritmos discretos podría ser capaz de romper un cifrado ElGamal. Sin embargo, en la actualidad, el algoritmo de computación de logaritmos discretos es subexponencial con una complejidad de $\lambda = 1/3$, la misma que la de factorizar dos números primos, y por tanto, incapaz de realizar tal tarea en números grandes en un tiempo razonable.

Estos dos tipos de algoritmos son los utilizados para cifrar mensajes y como hemos comprobado su efectividad es más o menos la misma. A continuación veremos los algoritmos usados por TrueCrypt, y que hasta el momento son los más utilizados en criptografía.

Tanto en TrueCrypt como en otro software de cifrado, el algoritmo más utilizado y normalmente por defecto es el algoritmo AES (Advanced Encryption Standard), que es un algoritmo estandarizado incluso por el gobierno de Estados Unidos. En 2003, la NSA declaró que este podía ser usado para información clasificada del gobierno y esta era la primera vez que el público utilizaba un software aprobado por la NSA. Hasta el 2005 no había podido ser descifrado a pesar de las pruebas de ataque realizadas por las investigadoras. No tengo nuevos datos, así que nos quedaremos con la idea, de que aunque nunca haya sido atacado con éxito, no por ello vamos a fiarnos hasta el fin de este algoritmo o cualquier otro.

En TrueCrypt encontraremos también otras opciones de cifrado que incluso se complementan a éste: AES, Twofish, Serpent, AES-Twofish, AES-Serpent, Twofish-Serpent, Serpent-Twofish-AES. De los cuales al parecer el más efectivo, según un comentario en elhacker.net sería Serpent-Twofish-AES, y eso sin tener en cuenta que lo dirá más por lógica que por otra cosa. Lo que sí he leído bastante es que con AES tenemos más que suficiente. Aquí el tema es el de siempre. ¿Qué va a hacer

que no puedan entrar en tu volumen TrueCrypt encriptado? TU CONTRASEÑA!!

Existen otros algoritmos: de cifrado, de hash... Pero con esta pequeña presentación sobre los algoritmos más utilizados ya tendremos una pequeña idea de lo que estamos haciendo y podemos pensar con más información acerca de nuestra seguridad en la red o en el ordenador.

KLEOPATRA

Kleopatra es un software de código abierto destinado a encriptar archivos y correo electrónico.

En el capítulo donde se explica detalladamente como cifrar mensajes para una comunicación privada y segura, hemos visto que lo único que hacíamos con Kleopatra era descargarlo, instalarlo y listo. En ningún momento lo hemos usado y puede que a algunas les haya pasado por la cabeza que quizás no era necesario. Digo esto porque a mí me pasó.
El motivo de que no lo usáramos es que aunque no haga falta abrirlo, en realidad es él quien gestiona el cifrado de los mensajes. Del mismo modo que cuando estamos en Thunderbird y abrimos el administrador de llaves vemos las claves públicas y privadas que tenemos guardadas, si abrimos Kleopatra vemos que también las tenemos ahí, además de que podemos crear nuevas llaves públicas y privadas, importar nuevas claves o buscar certificados en los servidores de llaves.

En este caso vemos que es muy similar a Enigmail en cuanto a herramientas y utilidades. Debemos pensar que aunque no tuviéramos Enigmail podríamos enviar mensajes cifrados.

Bastaría con abrir un archivo de texto como LibreOffice Writer, cifrarlo y mandarlo como adjunto en un correo normal sin cifrar.

Básicamente es lo que vamos a mostrar en este capítulo.
Debo reconocer que mis conocimientos sobre informática y más detalladamente en estos temas son muy limitados. Es por este motivo que para mandar un archivo adjunto cifrado, lo que hacemos con Thunderbird, al no haber indagado acerca del cifrado tipo S/MIME, utilizo Kleopatra para poder hacerlo. Seguro que hay otras formas, pero os mostraré la que conozco y que es bastante fácil.

No vamos a explicar cómo se instala ya que lo hemos visto en el capítulo de Thunderbird, pero sí vamos a ver cómo enviar esos adjuntos. Lo único que debemos tener en cuenta es que para cifrar un archivo y mandarlo debemos encriptarlo con la llave pública de nuestro destinatario de igual modo que si se tratara de un mensaje... Ya que cómo hemos visto antes la comunicación cifrada se basa en: Se cifra con la llave pública del destinatario y se descifra con la privada de quien recibe el mensaje.

Para cifrar un archivo, seleccionamos este en el directorio donde se encuentre, pulsamos encima con el botón derecho y seleccionamos *acciones – cifrar archivo*. Emergerá una ventana con varias opciones, entre ellas si queremos comprimirlo (esto nos permitirá poder mandar un directorio y no tener que comprimirlo antes), cifrarlo, firmarlo y si queremos eliminar el archivo original después de cifrar. Esta opción depende de lo que queramos, ya que si queremos mantener el original después de mandarlo, debemos tener en cuenta que desde el momento que lo ciframos con la llave de otra persona nunca más podremos abrirlo ya que no dispondremos de su llave privada para descifrarlo.

Clicaremos en *Siguiente* y escogeremos el certificado (llave) con el que encriptar el archivo. Marcaremos *Cifrar* y ya lo tendremos cifrado y listo para mandar.

Veremos que la extensión del archivo es .gpg, mientras que las extensiones de las llaves son pub.asc si es pública, o pub. sec.asc si es el par de llaves pública y secreta.

Con Kleopatra también podemos de esta forma, cifrar archivos dentro de nuestro PC y tenerlos guardados con la confianza de que nadie los pueda ver, siempre y cuando la contraseña sea buena (aunque a estas alturas ya lo serán, no?)

Una pequeña desventaja que tiene Kleopatra, es que Enigmail permite crear los pares de llaves con mayor cantidad de bits. En Enigmail llega a 4096 bits, mientras que Kleopatra alcanza 3072.

En Linux también existe Kgpg, normalmente viene incluso por defecto en algunas distribuciones y se encuentra en los repositorios. Lo podemos descargar del Centro de Software y tiene las mismas utilidades que Kleopatra. Como siempre utilizo Kleopatra no me he parado mucho con Kgpg, pero supongo que si no son idénticos, casi lo serán.

AESCRYPT

Aescrypt es un programa que se encuentra disponible para Windows y Linux, y que encripta archivos y carpetas con el sistema avanzado Advanced Encryption Standard "AES". Por lo visto, algunos de los archivos que Wikileaks filtró y que le supusieron el cierre junto con todo el circo mediático que acompañó a las historias que destapó, fueron cifrados con este programa.

Si no con este, de todos modos se podrían descifrar bien con Aescrypt.

La descarga, instalación y desarrollo del programa son distintos como suele suceder, en Windows o en Linux.
Para descargarlo deberéis acceder a http://www.aescrypt.com/download/ y allí encontraréis las distribuciones para los dos sistemas que usamos en esta guía.

Para instalarlo en Windows seguiréis los pasos habituales y una vez instalado, para encriptar el archivo deseado, solo hay que hacer clic con el botón derecho encima del archivo, seleccionar *AES Encrypt*, y aparecerá una ventana que pedirá la contraseña. Esta será la que vosotras queráis. A partir de ahí el programa se encargará de cifrarlo con este sistema. Para descifrarlo haréis lo mismo, con la diferencia que haréis clic en *AES Decrypt*, de nuevo la contraseña y listo.

En la versión de Linux hay que descargar el "install.gz". Una vez descargado iréis a la carpeta donde se habrá alojado y lo descomprimiréis, le daréis permisos de ejecución y después lo instalaréis. Para hacer esto deberéis hacer unas cosas en el terminal y otras en modo gráfico.
Una vez estáis en la carpeta que tiene el programa. Hacéis clic derecho encima del archivo comprimido y seleccionáis *Extraer – Extraer aquí, autodetectar subcarpeta*. Aparecerá un solo archivo que termina con la sintaxis "install". Ahora abriremos el terminal y nos dirigiremos a la carpeta donde está, por ejemplo Descargas.

```
cd Descargas && ls
```

(con "ls" aparecerán todos los archivos que estén dentro de *Descargas*)

```
chmod +x AESCrypt-GUI-1.0-Linux-x86-Install
sudo ./AESCrypt-GUI-1.0-Linux-x86-Install
```

Con esta última línea procederemos a instalar el programa en nuestro Linux. A partir de aquí se abrirá una ventana que os preguntará el idioma y esas cosas típicas como si fuera un programa de Windows.

Una vez lo tengamos instalado, para encriptar archivos deberemos hacerlo desde la línea de comandos, o desde el modo gráfico. Primero lo explicamos desde el terminal y luego pasaremos a hacerlo en su alternativa gráfica.

Si abrimos un terminal y escribimos `aescrypt`, nos aparecerá en modo de ayuda, la sintaxis que se debe utilizar para cifrar o descifrar archivos.
Esta es:

```
usage: aescrypt {-e|-d} [ { -p <password> | -k
<keyfile> } ] { [-o <output filename>] <file> |
<file> [<file> ...] }
```

Como veis es un lío, así que mostraremos una manera un poco más sencilla. Pongamos que el archivo que se quiere cifrar está en la carpeta /home/Manual/Escritorio/cifrados, y el archivo se llama acab.doc (ya nos dice que mejor no esté muy a la vista, no?), y la contraseña bastardxs (muy original).
La sintaxis para encriptarlo sería:

```
cd /Escritorio/cifrados && ls
aescrypt -e -p bastardxs acab.doc
```

Una vez cifrado el resultado sería un archivo al lado del anterior que se denominaría acab.doc.aes. Como habréis observado el funcionamiento de esta herramienta es de lo más fácil y no requiere demasiadas complicaciones.

Hay que tener en cuenta un dato muy importante, y es que con AesCrypt NO podremos cifrar carpetas, así que si queremos cifrar varios archivos de una sola vez, deberemos

comprimirlos antes para posteriormente cifrarlos. Podremos comprimir en .zip, .rar, o lo que os dé la gana

NOTA: Pensad que el archivo original no desaparece. Cuando hemos visto la opción de cifrar con Kleopatra donde el resultado sería acab.doc.gpg, nos pregunta si queremos eliminar el archivo original después de cifrarlo. Con Aescrypt no ocurre esto. Si queréis eliminar definitivamente el archivo original deberéis hacerlo con alguna de las herramientas que se encuentran al final de la guía y que se encargan de eliminar completamente los archivos.

Para descifrar el archivo la sintaxis sería:

```
aescrypt -d -p bastardxs acab.doc.aes
```

Para cifrar y descifrar desde el modo gráfico, lo que se debe hacer es ir hacia el archivo en cuestión, hacer clic derecho encima de éste y seleccionar *Abrir con – Otros*. Aparecerá una ventana con la que navegaremos hasta *Utilidades – Aescrypt* y aceptaremos. Una nueva ventana nos pedirá un par de veces la contraseña que queremos dar y automáticamente aparecerá el archivo cifrado. Para descifrarlo haremos lo mismo, pero el resultado es el archivo descifrado.

Es un programa muy útil, sobretodo si creamos una contraseña fuerte que impida que se pueda descubrir con un ataque de fuerza bruta. Por lo que estamos comprobando, el protocolo de cifrado AES es realmente bueno, pero hay herramientas muy potentes capaces de hackear contraseñas y acceder a la información deseada por quien dirija el ataque, así que hay que pensar bien qué es lo que hacemos.

Para las que tengáis dudas sobre qué programa utilizar para cifrar archivos, entre este o Kleopatra, mi consejo es que utilicéis éste para cifrar archivos personales y que uséis Kleopatra para cifrar archivos que a posteriori se mandarán

por correo. Pienso que es mejor así ya que en el caso contrario hay que mandar la contraseña del archivo a la destinataria, con lo que siempre es un fallo de seguridad, y de esta manera enviando un cifrado con Kleopatra lo mandaremos con la llave de la destinataria y ni siquiera nosotras tendremos la contraseña.

CCRYPT

Ccrypt es un programa que está disponible para un montón de distribuciones, entre ellas Linux y también en Windows 95, 98, 2000 y NT. La verdad es que sólo lo he usado en Linux y no creo que esté disponible para Windows 7 o estas últimas distribuciones de Microsoft.

Es un programa que hace lo mismo que el anterior, cifra con el mismo sistema AES y funciona de la misma manera, con algunas pequeñas diferencias.

Vamos a hacer la explicación de su instalación y funcionamiento en Linux que es para lo que creo que lo podréis usar. Para instalarlo bastará con abrir el terminal y escribir:

```
sudo apt-get install ccrypt
```

Para ejecutarlo bastará con escribir:

```
ccrypt -e archivo_en_cuestión
```

Nos preguntará la contraseña de seguridad un par de veces y aparecerá el archivo cifrado en la carpeta correspondiente.

Para descifrarlo:

```
ccrypt -d archivo_en_cuestión.cpt
```

NOTA: Podréis observar que una de las diferencias con Aescrypt es que aquí la terminación es ".cpt", además de que ahora el archivo original ha desaparecido. Una vez lo descifréis volverá todo igual que estaba al principio.

Para cifrar o descifrar una carpeta:

```
ccrypt -eR nombre_de_la_carpeta
ccrypt -dR nombre_de_la_carpeta
```

Tened en cuenta que la carpeta no se cifra. Lo que hace es cifrar su contenido. Por estos motivos personalmente prefiero Aescrypt a la hora de trabajar con archivos cifrados, pero cómo para gustos, colores. He querido dejar la información sobre este programa.

TRUECRYPT

Y aquí llega la gran estrella de esta guía. Truecrypt es el software de encriptación por excelencia. Su reputación se la ha ganado a pulso y hasta el FBI ha cedido ante su sofisticación. En los anexos hay un artículo sobre como el FBI intentó durante un año descifrar Truecrypt y después de que sus hackers lo intentaran sin resultado alguno, se dio por vencido.
Tal es su reputación que incluso hay ciertos rumores que dicen que la CIA podría haberlo manipulado y que Truecrypt tuviera una puerta trasera. También encontraréis el artículo acerca de estos rumores, para que tengáis toda la información al respecto y podáis tomar la decisión que más os complazca.

Yo sin duda, confío plenamente en este software que hasta el momento es el programa de criptografía más fácil de usar, intuitivo y "seguro" que he encontrado, además de que por muchos rumores, no encontraréis ninguna noticia real de alguien que haya encontrado la manera de atacarlo con éxito. Cabe reconocer que son demasiadas facilidades y que este mismo hecho es el que crea la primera sospecha. -¿Cómo puede ser que sea todo tan bueno?-, se pregunta una mente realista. -Pues hasta el momento es así.

Hay que tener en cuenta que los rumores sobre posibles puertas traseras y demás vienen motivadas porque hace un tiempo, en el programa OpenBSD (un software de seguridad), se descubrió que la CIA había colado un backdoor (puerta trasera) hasta que alguna usuaria experimentada se dio cuenta y saltó la voz de alarma .

Al parecer, en EEUU se está intentando que por ley, este tipo de software destinado a proteger nuestros datos, lleve incorporada una puerta trasera y que según la CIA y el FBI; "sólo la utilizarán en los momentos que sea estrictamente necesario, como en casos de terrorismo". -Sí claro, claro...!! Y sois vosotras quienes decidiréis además cuando es necesario, verdad?.
-Increíble…

También es cierto que en España, por ejemplo, se ha vinculado con un titular algo sensacionalista que ETA usaba este software, con lo que ya es hora de que se empiece a controlar estos programas que solo lo usan terroristas, verdad?

De todos modos mi consejo es que cada cierto tiempo, quien esté interesado en Truecrypt y sus impresionantes posibilidades, que eche un vistazo en internet a ver si alguien ha conseguido descifrarlo o aparece alguna noticia similar.
Hasta este momento he podido constatar que hay personas que dedican mucho tiempo a intentarlo, así que algún día

llegará un crío de 14 años y casi sin querer lo logrará y nos quedaremos todas sin la seguridad que nos proporciona este software.

¿Qué características podemos encontrar en Truecrypt?

-Puede crear un disco virtual cifrado dentro de un archivo, montándolo como si se tratase de un disco real.
-Permite cifrar una partición completa e incluso todo un dispositivo de almacenamiento, como un disco duro o una memoria USB. Puede cifrar una unidad, o una partición, donde esté instalado Windows.
-El cifrado se produce de forma automática, en tiempo real y de forma transparente.
-Ofrece diferentes niveles de denegación, en caso de vernos obligados a revelar la contraseña: Volúmenes ocultos (se tiene un volumen TrueCrypt dentro de otro volumen TrueCrypt). O sistema operativo oculto.
-Los volúmenes de TrueCrypt no pueden ser identificados, ya que no se diferencian de los datos aleatorios.
-Soporta diferentes algoritmos de cifrado como AES, Blowfish, CAST5, Serpent, Triple DES, y Twofish o una combinación de los mismos.

Estas son las principales funciones de Truecrypt y si os habéis dado cuentan básicamente lo que hace Truecrypt es encriptar, por resumir un poco e ir al grano. Encripta volúmenes (directorios), encripta usb, los usuarios de Windows tienen la posibilidad de cifrar el sistema entero, y una de las mejores características es que encripta volúmenes ocultos.

Vamos a entrar a detallar un poco más cada una o varias de estas opciones, su descarga e instalación, tanto para Windows como para Linux, pero antes vamos a comentar esto de los volúmenes ocultos.

Como veremos más adelante, un volumen cifrado por Truecrypt, no es más que una carpeta cifrada con un algoritmo que usa para que nadie, excepto quien tenga la contraseña, vea lo que hay en su interior. En esta carpeta guardamos todo lo que queramos o nos quepa, depende del tamaño que le hayamos asignado. Pues bien, dentro de esta carpeta podemos crear otra carpeta de la que según parece, y digo esto porque al no ser informática (y siendo algo pragmática) no puedo asegurar nada que no haya podido demostrar yo misma, no hay ningún rastro. Lo único que podremos comprobar es que si observamos la capacidad de almacenamiento de la carpeta, los MB usados y los MB restantes, vemos que no hay ninguna prueba evidente de que dentro de ella, haya otra carpeta oculta con su tamaño correspondiente. Por ejemplo, si el volumen es de 100 MB y el oculto es de 50 MB, en principio debería verse esos 50 MB por ahí que faltan, pero nada, no hay rastro. Además, aunque algún hacker policial pudiera intuir que está esa carpeta, Truecrypt no guarda ningún registro (y eso sí he leído que hay gente que ha buscado algún registro como locos y nunca lo han encontrado), con lo que tampoco podrían creer durante mucho tiempo que sí existe ese volumen. En este caso todo serían suposiciones.

Hay ciertas diferencias desde la versión de Windows a la de Linux, hay algunos cambios que no suelen haber en los programas y que no imaginas que pudieran estar en este. Es cierto que Linux tiene un nivel muchísimo mayor que Windows en cuanto a seguridad y cifrado, ya que puedes cifrar desde el momento de la instalación del sistema operativo todo el contenido o particiones. Pero aun así se agradecería que Truecrypt pudiera cifrar la distribución entera, aunque imagino que si no lo hace es porque no se debe poder.

El último comentario que hago por ahora, que también es una desventaja para las usuarias de Linux, es que no intentéis buscar el paquete de idioma español ya que, mientas que lxs que utilicen Windows bastará con descargar el paquete

correspondiente y guardarlo en el directorio de la ubicación del programa para poder cambiar a éste, las que usen Linux no podrán. Es una manera de que aprendamos inglés, o sea, es una ventaja más de Linux. O no?

Descarga e instalación

Para descargar Truecrypt, tanto si es para Windows o Linux deberéis ir al siguiente enlace:
http://www.truecrypt.org/downloads
Aquí simplemente deberéis escoger vuestra distribución y descargarla.

Para instalar Truecrypt en Windows bastará con clicar un par de veces en el paquete descargado y seguir la instalación como siempre se hace con cualquier paquete.

La instalación de Linux es algo distinta. Por un lado podéis descargar el código fuente y compilarlo vosotras mismas, pero es algo para usuarias experimentadas.
Para las que hayáis escogido el paquete "standard-32bits" habréis descargado un archivo .tar.gz. Para instalar deberéis ir a la carpeta de descargas o donde lo hayáis guardado y clicar con el botón derecho y seleccionar *extraer aquí, autodetectar subcarpeta*.

Una vez esté descomprimido, clicáis sobre el archivo que aparezca con el botón derecho de nuevo y esta vez teclearéis *propiedades – permisos,* habilitaréis la pestaña *es ejecutable* y después *aceptar*. Una vez hecho esto pulsad encima del archivo y aparecerá una ventana del terminal que os pedirá si queréis instalar el programa o extraer el archivo. Pulsad el 1 y os mostrará los términos y condiciones del servicio. Cuando os aparezcan, con la tecla de la flecha dirigida hacia abajo del teclado descenderéis hasta que os aparezca la frase de aceptar los términos. Una vez aceptados se habrá acabado la instalación y Listo! Truecrypt instalado.

Es posible que por el motivo que sea no podáis usar esta manera de instalarlo, o que prefiráis utilizar la terminal para hacerlo. En este caso abrís el terminal:

cd Descargass (o donde esté descargado)
tar xzf truecrypt-7.1a-linux-x86.tar.gz (o la distribución descargada)
chmod +x truecrypt-7.1a-setup-x86
./truecrypt-7.1a-setup-x86

Una vez que el programa está instalado, las usuarias de Windows tenéis la posibilidad de cambiar Truecrypt al idioma que queráis. Para pasar el programa a español, basta con descargar de este enlace:
http://www.truecrypt.org/localizations el paquete que necesitéis, lo descomprimís en el directorio donde se ubica el programa *Archivos de programa – TrueCrypt* y una vez hecho este paso, ejecutaréis el programa y es posible que ya haya cambiado el idioma. En el caso contrario clicaréis en *Settings – Language* y seleccionáis el que queráis.

Antes de meternos en faena quiero aclarar que las explicaciones sobre el uso de truecrypt las he extraído de la red, más explícitamente de una página que encontraréis al final del manual. He decidido hacerlo así y no explicarlo yo misma, ya que excepto algunas aclaraciones que irán saliendo, está explicado de manera muy sencilla.
Otro motivo por el que se ha decidido hacer, casi, un corta y pega, es que dada la importancia de este programa no quiero obviar ni olvidar nada que pudiera pasarme por alto.

De todos modos recomiendo utilizar otras fuentes, disponibles en el libro, ya que en ellas hay imágenes, lo que seguro hará más agradable la instalación y aplicación del programa

Crear un volumen cifrado

De momento vamos a ver cómo crear un volumen o archivo contenedor cifrado, pero sencillo. Más adelante veremos cómo crear uno oculto para mayor seguridad de nuestros datos.

Después de instalar el programa tendréis Truecrypt en alguna parte del ordenador. Seguramente en Windows lo tendréis en el mismo escritorio y el Linux lo tendréis en *Aplicaciones – Utilidades*.
Una vez localizado deberemos ejecutarlo y aparecerá la ventana principal del programa.

Para crear un nuevo contenedor, debes hacer clic sobre el botón *Create Volume*. Verás que aparece una nueva ventana con un asistente que te guiará a lo largo de todo el proceso. Para empezar, debes asegurarte de que tienes seleccionada la primera opción: *Create an encrypted file container*. A continuación, sólo tienes que hacer clic en el botón *Next*.
Lo siguiente que debes decidir es si tu contenedor será estándar u oculto. De momento, creo que debemos conformarnos con el primero. Por lo tanto, te aseguras de que está seleccionado *Standard TrueCrypt volume* (que es el valor por defecto) y haces clic en el botón *Next*.

En el siguiente paso, debes decidir dónde ubicas tu archivo contenedor. Puedes optar por escribir directamente en el cuadro de texto, incluyendo la ruta completa y el nombre del archivo, o puedes hacer clic en el botón *Select File …* para obtener una ventana que te simplifique la elección de la ruta. Si has hecho clic en el botón, te aparece una ventana, donde puedes escribir el nombre del archivo y elegir el lugar donde se creará, en la lista desplegable o eligiendo *Buscar otras carpetas.*
En cualquier caso, el resultado será el cuadro de texto de la ventana anterior debidamente relleno. Sólo quedará hacer clic de nuevo en el botón *Next*.

Se supone que el siguiente paso es el más importante, ya que en él puedes elegir el método que se aplicará para cifrar la información dentro del archivo contenedor. Sin embargo, para usos normales, pienso que cualquiera de ellos es más que suficiente. Cuando te hayas decidido por uno (o por una combinación de ellos), sólo tienes que hacer clic en *Next* para seguir.

Según algunas fuentes cómo por ejemplo, http://foro.elhacker.net/criptografia/cual_es_el_mejor_algoritmo_de_encriptacion_de_truecrypt-t358949.0.html, el mejor algoritmo de cifrado de truecryt es "AES-Twofish-Serpent"

El siguiente paso consiste en establecer el tamaño del contenedor. Basta con escribir el número y elegir en la lista la unidad de medida. Como puedes leer en la misma ventana, hay que tener en cuenta que el tamaño mínimo de una unidad FAT es de 275 KB y el de una partición NTFS es de 2829 KB. Una vez establecido, debes hacer clic de nuevo en el botón *Next*.
A continuación deberás escribir tu contraseña. Recuerda que este es el paso más delicado y que, según tu elección, tus datos serán más o menos vulnerables. En esta ventana se pueden leer, además, las recomendaciones típicas para elegir una buena contraseña (utilizar varias palabras, mezclar caracteres no alfanuméricos, etc)

La contraseña debe escribirse dos veces por precaución (para prevenir posibles errores tipográficos). Cuando termines, haz clic en el botón *Next*.

El siguiente paso consiste en elegir el sistema de archivos con el que se formateará el contenedor. Si vas a utilizarlo en diferentes sistemas operativos, una forma de asegurar la

compatibilidad es elegir FAT, pero hay que tener en cuenta que el formato FAT sólo acepta archivos de menos de 4 Gb, así que si queréis crear un archivo de 8 Gb o 10 Gb deberéis usar NTFS, o bien ext4 si estubiérais en Linux. Una vez elegido el sistema de archivos, debes hacer de nuevo clic sobre el botón *Next* para continuar.

En la siguiente ventana se calculan los valores aleatorios que se utilizan como base para cifrar los datos. Para conseguirlo, se utilizan como referencia los movimientos del ratón. Después de mover el ratón durante algo de tiempo y de la forma más aleatoria posible, puedes hacer clic sobre el botón *Format*.
Cuando acabe, aparecerá una ventana informando de la situación. Aquí sólo hay que hacer clic en *Aceptar.*
Por último, obtenemos un mensaje que nos indica que el volumen se ha creado satisfactoriamente y que está listo para usarlo. Si queremos repetir el proceso y crear un nuevo contenedor, podemos hacer clic en el botón *Next*. Si no es así, pulsaremos el botón *Exit.*

Antes de ver cómo utilizar el volumen, hay que aclarar que la opción de crear el volumen cifrado es casi idéntica en Linux o en Windows, así que no hace falta hacer otro manual con la creación del volumen en Windows. Realmente se va a usar un ejemplo en cuestión, ya sea de Windows o Linux para demostrar cómo funciona el programa. Dadas las similitudes entre la manera de hacerlo con un sistema u otro, sería demasiado largo y redundante hacerlo de las dos maneras.

Utilizar el volumen

Para utilizar el contenedor que hemos creado en el punto anterior, sólo hay que ejecutar TrueCrypt y, en la ventana inicial del programa, hacer clic en el botón *Select File.* Si conoces la ubicación de tu archivo contenedor, puedes escribirla en el cuadro de texto que hay junto al botón.

Utiliza la ventana que aparece para buscar tu archivo y, una vez localizado, selecciónalo y haz clic sobre el botón *Abrir*.
De vuelta en la ventana principal, sólo queda montar la nueva unidad. Tienes que seleccionar un Slot (por ejemplo el uno) y hacer clic en el botón *Mount*.
Lógicamente, antes de montar la nueva unidad, TrueCrypt debe pedirnos la contraseña que introdujimos al crear el contenedor. Una vez escrita, sólo tienes que hacer clic en el botón *Aceptar*.
Una característica que a mí me resulta un poco molesta es que, para montar una unidad, también necesita privilegios de administración (en Linux). Por ese motivo, TrueCrypt también solicita la contraseña de root.
Si las contraseñas son correctas, verás que el contenedor aparece en el Slot 1.

Desmontar el volumen

Esto parece una tontería, pero hay que tener siempre muy presente que cuando se quiera cerrar el programa y que los datos vuelvan a estar bien cifrados, después de cerrar la ventana de "dolphin", "nautilus" o "windows", hay que pulsar siempre encima de *Dismount*. De esta forma los datos quedarán bien guardados y seguros. De lo contrario sería más fácil, aunque reiniciáramos el ordenador, acceder a la información ya que quedaría un registro hecho por el ordenador, aunque Truecrypt no lo hubiera hecho.

Cifrar una partición o un USB

A continuación vamos a ver cómo cifrar una partición (por ejemplo /home en Linux) o un pendrive. Antes de seguir hay que recordar que la partición que se vaya a cifrar se va a formatear con lo que deberéis hacer una copia de seguridad de los datos o guardarlos en otro lugar de momento.

Para comenzar, desde la ventana principal del programa, el primer paso consistirá en hacer clic sobre el botón *Create Volume*.
Verás que aparece una ventana donde puedes elegir entre *crear un archivo contenedor encriptado* o *crear un volumen dentro de un dispositivo o de una partición*. Esta segunda opción es la que nos interesa hoy, luego, hacemos clic sobre ella y a continuación en el botón *Next*.

En el siguiente paso, el programa te ofrece la posibilidad de elegir entre un *volumen estándar* o un *volumen oculto*. De momento nos interesa la primera opción, quizás otro día dediquemos nuestra atención a la segunda. Por lo tanto, debes hacer clic sobre ella y, a continuación, de nuevo en *Next*.
Debes elegir el dispositivo que vas a cifrar. Puedes escribir el nombre del dispositivo en el cuadro de texto, pero, para evitar errores, te recomiendo que hagas clic en el botón *Select Device*.

Después aparece una ventana con todos los dispositivos de almacenamiento que tenemos conectados a nuestro ordenador. Debes tener cuidado, un error al elegir el dispositivo puede hacer que pierdas toda la información que contenga. Recuerda que el dispositivo elegido va a formatearse. No obstante, si te fijas en el directorio de montaje, es muy fácil identificar el dispositivo correcto. Al volver a la ventana del asistente, verás que ya está seleccionado el volumen adecuado. Como de costumbre, para seguir, sólo hay que hacer clic en el botón *Next*.

Bueno, creo que si has llegado hasta aquí, el mensaje que te muestra ahora Truecrypt está un poco de más. En él, encontramos una recomendación para usuarias inexpertas donde nos sugiere que, en lugar de cifrar un dispositivo completo, creemos un contenedor. Si optamos por esta segunda opción, podremos tratarlo como a cualquier otro archivo y el resto de archivos de nuestra unidad no correrían ningún tipo de peligro. Si estás seguro de continuar, haz clic en *Sí*.

En el siguiente paso, Truecrypt nos recuerda que la unidad que hemos seleccionado se va a formatear y que este paso implica la pérdida de todos los datos que contenga actualmente. Desde luego, si perdemos algún archivo, no podremos culpar al programa. Si aún estás seguro de seguir adelante, debes hacer clic en el botón *Sí.*

Los siguientes pasos son idénticos a los vistos en el artículo anterior. Para empezar, debemos seleccionar el algoritmo de cifrado que vamos a utilizar. Las opciones son *AES, Blowfish, CAST5, Serpent, Triple DES, y Twofish*, además de algunas combinaciones entre ellos. Puedes hacer clic en *More information on…* para obtener más detalles sobre el algoritmo que elijas. Cuando hayas tomado una decisión, debes hacer clic en el botón *Next* para continuar.

A continuación, escribiremos la contraseña que usaremos más adelante para acceder a nuestra memoria USB. Debemos de escribirla dos veces para estar seguros de que no cometemos ningún error tipográfico al escribirla.
En el siguiente paso elegimos el tipo de sistema de archivos que utilizaremos en el formateo de nuestra unidad. Si piensas utilizar tu memoria USB sólo en sistemas Linux, puedes utilizar ext3, pero si también piensas acceder a ella desde sistemas Windows, es muy recomendable que utilices FAT. En cualquier caso, después de hacer tu elección, haz clic sobre *Next* para continuar.

En la siguiente ventana se calculan los valores aleatorios que se utilizan como base para cifrar los datos. Para conseguirlo, se utilizan como referencia los movimientos del ratón. Después de moverlo durante algún tiempo y de una forma lo más aleatoria posible, puedes hacer clic sobre el botón *Format* para seguir.

Ahora sí. El sistema ya está dispuesto para comenzar el formateo de la unidad. Ya no habrá más posibilidades de

arrepentirse. Por eso, a riesgo de parecer pesado, Truecrypt vuelve a preguntarte si estás realmente seguro de perder cualquier cosa que tengas en el PenDrive. ¿Estás realmente seguro de que no tienes datos importantes en tu PenDrive que no hayas copiado en otro soporte? ¿Seguro?. Pues ya puedes hacer clic en el botón *Sí* para iniciar el proceso de formateo.
A continuación, verás una barra de progreso que te indica el avance del formateado.
Cuando llegue a su fin, Se muestra una ventana informando de que el proceso ha concluido. Sólo queda hacer clic en el botón *Aceptar* para empezar a disfrutar de nuestro PenDrive protegido a prueba de curiosos.

Esta manera de cifrar una partición o pendrive, está explicada sobre el sistema de Linux. La verdad es que en Windows por desgracia no lo he probado y no sé si será muy distinta, aunque imagino que no. En el caso de que las usuarias de Windows os encontréis con algo raro, seguid a vuestra intuición y trabajad con cautela, no perdáis información importante.

Utilizar la partición o USB

Una vez que hemos cifrado la unidad, ya sólo podremos acceder a ella desde Truecrypt, después de escribir la contraseña adecuada. Así que para utilizarla abriremos el programa y en su ventana principal, hacer clic sobre el botón *Select Device…*
En la ventana que aparece, seleccionas la unidad cifrada y haces clic sobre el botón *Aceptar*. Observa que ahora no aparece directorio de montaje, porque aún no está montada.
De vuelta en la ventana principal de TrueCrypt, debes hacer clic en uno de los Slot que tienes disponible, por ejemplo en el primero y después sobre el botón *Mount*. Y a partir de aquí funcionamos igual que si quisiéramos abrir un volumen cifrado normal.

Crear volumen oculto

En la creación del volumen oculto hay algunas diferencias entre Windows respecto de Linux. Mientras que en Windows existe la posibilidad de hacerlo de dos maneras, creando el volumen oculto directamente dentro de un volumen cifrado ya creado anteriormente, o crear el oculto y el normal a la vez, Linux solo te deja crear los dos volúmenes a la vez, de manera que si tienes otras carpetas cifradas no puedes añadirles una oculta. Tiene sus inconvenientes, pero por algún motivo se hará así. La manera de hacerlo en Linux seleccionando la opción *Hidden TrueCrypt volume*, se basa en que primero crearemos el volumen normal y siguiendo los pasos crearemos más tarde el oculto.

Para esta explicación no vamos a detallar paso por paso como en los ejemplos anteriores ya que es exactamente lo mismo que antes sólo que añadiendo unos pasos más para crear el oculto. De manera que:
Abrimos Truecrypt y seleccionamos *Crear Volumen*. En la siguiente seleccionaremos *Crear un contenedor cifrado – Volumen oculto Truecrypt* y a partir de aquí en Windows nos preguntará si queremos hacerlo del modo directo o el modo normal (éste es el modo que usaremos para explicar y es el modo que utiliza la distribución de Linux).
Una vez seleccionado la opción, pasaremos a crear el volumen exactamente igual que se ha detallado antes creando el contenedor normal.

Nota: Toma en cuenta el tipo de documentos, su cantidad y tamaño que necesitan ser almacenados. Deja cierto espacio para el Volumen Común. Si seleccionas el tamaño máximo disponible para el Volumen Oculto, no serás capaz de colocar ningún archivo nuevo en el volumen Común original.
Si tu Volumen Común es de 10 Megabytes(MB) de tamaño y tú especificas un tamaño de Volumen Oculto de 5MB, tendrás dos volúmenes (uno oculto y el otro común) de aproximadamente

5MB cada uno.
Asegúrate que la información que almacenas en el Volumen Común no exceda los 5MB que has fijado. Ello debido a que el programa TrueCrypt no detecta, por sí mismo, en forma automática la existencia del Volumen Oculto, y podría accidentalmente sobre-escribirlo. Te arriesgas a perder todos los archivos almacenados en el volumen oculto si excedes el tamaño previamente establecido. Para evitar esta situación intentad ir sobradas de espacio para los dos volúmenes.

Haremos todos los pasos igual que antes y terminada la creación de éste seguiremos adelante para generar el oculto. Los pasos para crear este último, son los mismos que los anteriores. Cuando hayamos terminado el proceso de creación de los dos volúmenes accederemos a la ventana principal de Truecrypt.

Utilizar el volumen

Para utilizar cualquiera de los dos volúmenes hay que tener en cuenta que para un mismo archivo, carpeta o volumen (o como queramos llamarlo), tendremos dos contraseñas, a cada cual más potente y segura, pero esto siempre puede llevar a confusiones u olvidos.

Para ingresar al directorio oculto seguiremos los pasos normales para ingresar a cualquier volumen cifrado de truecrypt y guardaremos en él lo que queramos.
La importancia de esta característica de Truecrypt es sobretodo algo que debemos intentar que no se nos olvide, sobretodo cuando tengamos los volúmenes ya llenos de archivos y datos. Y es que cuando queramos abrir el volumen normal, en el momento que nos pide la contraseña deberemos acceder a *Opciones* que aparece en la ventana. Esta se abrirá y habilitaremos el cuadrado de *Proteger el volumen oculto cuando se monta el otro*, y pondremos debajo la contraseña del oculto. De esta manera nos ahorraremos la situación que se comenta

un poco más arriba acerca de sobreescribir los datos del otro volumen.

Keyfiles (Archivos Llave)

Truecrypt, por si con lo anteriormente mencionado no hubiera suficiente seguridad, nos ofrece la posibilidad de crear "archivos llave" o usar cualquier archivo como llave para acceder a los volúmenes. Estos archivos llave nos serán de gran ayuda sobretodo para aquellos casos en los que la contraseña no sea lo suficiente fuerte, y darán una mayor seguridad a nuestros contenedores cifrados.
Desde mi punto de vista lo realmente bueno de estos archivos llave, es que a la hora de crear un volumen podremos usar cualquier archivo (ya sea una película, una imagen o lo que nos dé la gana) para bloquear el acceso al volumen. Esto significa que en el momento de querer entrar en el contenedor deberéis poner la contraseña y el susodicho archivo.

Para crear un archivo llave. En la creación de un volumen, cuando estéis en la ventana en la que hay que decidir la contraseña, pulsaréis en la opción que dice *Keyfile* y una vez en la otra ventana clicaréis en *Generate Random Keyfile*. Aparecerá otra ventana donde deberéis mover el ratón para dar mayor fuerza al algoritmo y a la seguridad del archivo. Cuando estéis listas clicaréis en *Generate and save Key*, con lo que ahora deberéis decidir donde guardar el archivo y el nombre que queráis.

Desde mi punto de vista es mejor, ya que en principio no habrá ningún registro ni rastro de su nuevo uso, utilizar cualquier archivo que tengamos en el ordenador para usarlo como archivo llave. Para ello, en la misma ventana de la contraseña, clicaréis en *Keyfiles* y en la siguiente ventana pulsaréis en *Add files*. En este momento decidiréis qué archivo escoger para usarlo de llave y después *Ok*.

Ahora ya habremos escogido o creado un archivo de llave y lo único que queda es saber que cuando queramos montar el volumen, en el momento que nos pida la contraseña, clicaréis en *Keyfiles* y bastará con seleccionarlo.
No he comentado en la explicación que para usar estas llaves deberemos habilitar la casilla de *Use Keyfiles* en el momento de decidir usarlas, ya que se sobreentiende. Si alguien tiene algún problema que compruebe antes si estaba habilitada la opción de usarlas.

Hasta aquí esta explicación de los archivos llave. Creo que como mayor seguridad puede ser muy útil ya que el archivo lo podemos guardar donde queramos. Eso sí, habrá que tener cuidado de no perder ese archivo ya que sino no podremos entrar a nuestro volumen. Deberemos pensar siempre en hacer copias de seguridad de este archivo.

Hacer de TrueCrypt un programa Portable

Esta opción es de gran utilidad aunque la usemos en pocas ocasiones, si por ejemplo queremos ir a un locutorio y nos encontramos en él con un USB que hemos cifrado por completo con TrueCrypt en nuestra casa. Dado que la única manera de poder acceder a la información que contiene el pendrive sería descifrándolo con TrueCrypt, tendríamos la posibilidad de descargarlo en el mismo locutorio, instalarlo y usarlo, pero esto sería un poco engorroso, sobretodo porque estaríamos dejando rastros de nuestro paso por el local.

Cuando nos disponemos a instalar el programa, ya sea en Windows o en Linux, nos pregunta antes de efectuar la instalación, si queremos instalarlo o extraerlo. Esta es la característica de hacerlo portable.

En Linux, una vez extraído el programa, éste se guardará temporalmente en la carpeta *tmp* y para entrar en ella deberemos ser superusuarias. Esta carpeta contendrá dos

subcarpetas y dentro de la que dice *bin* encontraremos el archivo ejecutable *Truecrypt*.

Otras funciones

Como se ha dicho ya, Truecrypt tiene más características, como la de cifrar el disco duro entero (opción para Windows). Particularmente esta función es realmente útil, pero depende de varias especificaciones que debe cumplir la usuaria, como que el ordenador no tenga arranque dual (tener dos sistemas operativos en un disco duro), u otras características que harían que esta guía sobre seguridad informática para la activista se convirtiera en un manual exhaustivo acerca de este software.

De todos modos mi consejo es que exploréis al máximo este programa y que, hasta que no se conozca nadie capaz de hackearlo, tenedlo presente en vuestra seguridad.

Limpieza

Los Planeadores de Control Doméstico (DCHD) están diseñados para planear a unos 15 metros de altura, pero pueden llegar hasta los 160 metros. Pueden mantenerse en el aire unas tres horas sin repostar, y pueden desplazarse a 80 Km./h. Pueden controlarse por satélite o desde vehículos en tierra. Se ofrecen en un elegante color negro mate para su uso nocturno y en blanco mate y azul cielo para aquellos días en los que te sientas más alegre. Son, por supuesto, casi del todo silenciosos, tanto que no pueden escucharse a menos de tres metros...
… También tienen micrófonos (rabiosamente modernos, claro, capaces de escoger una conversación entre muchas a más de 400 metros de distancia), y transmisores para que las que dirigen el aparato puedan hablarte directamente. Pueden decirte que te pares, que te acerques al aparato. Pueden pedirte que muestres tu identificación en frente de la cámara. ..
… Y si te niegas, el Aparato Planeador de Control Doméstico está equipado con un arma paralizante.

Para entender el porqué de este capítulo, hay que tener en cuenta un par de conceptos. El primero es que para que un ordenador funcione bien, este debe estar limpio de registros, de virus, la memoria RAM debe estar siempre lo más accesible posible para que el sistema sea más veloz, pero además si trabajamos con información sensible deberemos limpiarla con seguridad. El segundo concepto se refiere más al próximo capítulo de esta guía, y es que cuando borramos un archivo cualquiera y lo mandamos a la papelera de reciclaje, éste sigue en el disco duro. Estos dos conceptos nos ayudarán a entender el motivo por el que añadimos a la guía algunos programas que no son cien por cien seguridad informática,

pero desde mi punto de vista es igual de importante tener a buen recaudo nuestra información, que eliminar todo el rastro que esa información haya dejado por la PC.

En este caso vamos a diferenciar los programas de Linux de los de Windows, ya que para cada sistema en esta guía serán distintos.

BLEACHBIT

Bleachbit es una herramienta multiplataforma (tanto Windows como GNU/Linux) que nos permite realizar un borrado seguro evitando dejar algunos rastros. Cabe resaltar que aunque existan este tipo de herramientas, siempre la informática forense estará un paso adelante descubriendo hasta los más mínimos detalles de aquellos rastros que son imposibles de borrar.

Esta herramienta escaneará nuestro ordenador y será capaz de eliminar de forma irrecuperable la información que le digamos que elimine. Desde Thumbs.bd, hasta archivos basura, registros e historiales.
En realidad es una aplicación muy sencilla de usar y no hace falta extenderse demasiado para mostrar cómo funciona. Lo más importante de mencionar es que para que Bleachbit sobreescriba la información deberéis habilitar la opción en *Editar – Preferencias*, o la primera vez que lo uséis, ya que en su primer arranque aparecerá una ventana con varias opciones, entre ellas estará la que deberemos seleccionar: *Sobreescribir archivos para ocultar su contenido.*

Otra información importante es, que para mandar a Bleachbit que elimine los datos que pertenezcan al propio sistema deberéis entrar como superusuario.

Y para ello deberéis entrar en el terminal de Linux y escribir:

```
sudo bleachbit
```

Para instalarlo lo podréis encontrar en el Gestor de Software o instalarlo desde los repositorios con la terminal.

```
sudo apt-get install bleachbit
```

Una vez instalado el programa podremos localizarlo en *Aplicaciones – Sistema* y cuando lo ejecutemos apareceremos en la ventana principal del programa, ahí escogeréis las opciones que deseéis escanear y eliminar, antes de que Bleachbit empiece el trabajo.
Cuando lo hayamos instalado y encontrado el icono del programa en *Sistema,* veremos que justo al lado hay otro icono que se llama "Bleachbit as root". Si antes hemos mostrado como arrancar el programa en modo superusuario desde la terminal, es debido a que a veces falla al intentar ejecutarlo desde el icono mencionado. Cuando ocurra eso lo haremos desde la terminal (tanto si es modo superusuario como si es modo normal).

Es muy posible que después de haber ejecutado Bleachbit, o mientras está realizando la limpieza, empiecen a aparecer avisos de fallos en el sistema. No os preocupéis. En realidad se está "equilibrando" el sistema y aunque Linux es quizás la mejor manera de trabajar con ordenadores, a menudo tiene algunos detalles inestables. Este es uno de ellos pero para nada preocupante. En cuanto termine de realizar la limpieza, con reiniciar la máquina estará todo como nuevo, mejor que nuevo.

SECURE DELETE

Las herramientas Secure Delete, son un conjunto de herramientas muy útiles que usan avanzadas técnicas para borrar de forma permanente archivos. Estas se encuentran también en los repositorios de Ubuntu, con lo que para instalarlo desde terminal:

```
sudo apt-get install secure-delete
```

El paquete Secure-Delete, está constituido por cuatro herramientas:
-srm utilizado para borrar archivos o directorios que se encuentran en tu disco duro
-sdmem utilizado para limpiar restos de información en la memoria de tu máquina (RAM)
-sfill utilizado para limpiar los restos de información del espacio vacío de tu disco duro
-sswap utilizado para limpiar los restos de información de la partición swap

La herramienta srm, encargada de eliminar archivos o directorios de manera irrecuperable la explicaremos en el capítulo destinado a la eliminación permanente de datos, por lo que ahora detallaremos las otras opciones que están más en connivencia a este capítulo.

sdmem

A pesar de que al apagar tu máquina se vacía la memoria RAM, siempre quedan restos de información. Sobre todo con las actuales memorias SDRAM, que al igual que suceden en los discos duros, hasta que esta información es sobrescrita repetidas veces, queda residente. Esto significa, que es relativamente fácil, utilizando las herramientas adecuadas, averiguar qué tuviste en la memoria RAM, desde el contenido de archivos importantes, la actividad de internet, o lo que

quiera que hicieras con tu máquina. El proceso de borrado es similar al de srm, y también se basa en el Método Gutmann, pero con ligeras modificaciones:

1 pasada con 0×00
5 pasadas aleatorias. Si está disponible se empleará /dev/urandom
27 pasadas con los valores especiales definidos por Peter Gutmann
5 pasadas aleatorias. Si está disponible se empleará /dev/urandom

El uso de sdmem es el mismo que srm, aunque es significativamente más lenta. Hay opciones para acelerar el proceso, pero la reducción de la velocidad, se realiza en base a realizar menos pasadas, con lo que el proceso es evidentemente más inseguro:

-f, no se emplea /dev/urandom.
-l, solo dos pasadas, la primera y la última aleatorio
-l, con dos -l solo se realizará una pasada

sfill

Sfill, sigue la misma metodología que srm, pero se utiliza para "limpiar" el espacio libre de tu disco duro, donde en un pasado existieron archivos. Esto es especialmente útil, si en un momento determinado, decides deshacerte de un disco duro. En ese caso, la operación será arrancar el sistema con un LiveCD, borrar todo el contenido del disco, y entonces utilizar sfill para asegurarte que no se pueda recuperar nada. Es necesario que tengas derechos de administración para utilizar esta herramienta.
El uso es:

```
sfill puntodemontaje/
```

sswap

Esta herramienta, está desarrollada para limpiar tus particiones de intercambio "swap", que almacenan la información de los programas en ejecución cuando la memoria RAM está "llena". Por tanto, por la misma razón que realizas una limpieza de tu memoria RAM, tienes que realizarla de tu memoria de intercambio. El método de limpieza es muy similar al de sdmem, si bien, antes de poder utilizar esta herramienta, es necesario, inhabilitar la partición "swap". Para saber qué particiones de intercambio tienes montadas, ejecuta el siguiente comando:

```
cat /proc/swaps
```

En mi caso la partición que tengo montada es /deb/sdb2. Lo primero es inhabilitar esta partición, para ello ejecutamos la siguiente instrucción:

```
sudo swapoff /dev/sdb2
```

Una vez inhabilitado, podemos limpiar la partición de intercambio, que en mi caso lo haré con

```
sudo sswap /dev/sdb2
```

Una vez terminado el proceso de limpieza que es largo, tienes que volver a activar la memoria de intercambio:

```
sudo swapon /dev/sdb2
```

CCLEANER

Para Windows tenemos ciertas herramientas capaces de limpiar concienzudamente nuestro sistema. Con pasear un poco por la red encontraréis muchos programas dirigidos a tal fin, sin embargo hay un programa entre todos estos que desde hace tiempo se convirtió para muchas personas, en el programa por excelencia para limpiar nuestro ordenador. Este es Ccleaner.

Después de estar durante años utilizando esta herramienta, descubrí al final que, a pesar de que eliminaba muy bien información delicada, también se ha podido demostrar que quizás es demasiado duro a la hora de escanear y limpiar.
Parece ser que Ccleaner a la hora de limpiar registros, datos antiguos o historiales, termina por eliminar de una zancada el directorio al completo y al final ralentiza nuestro PC o ha llegado a perder información valiosa para el sistema, con lo que en alguna ocasión se ha tenido que reinstalar de nuevo el sistema operativo.

En contrapartida a Ccleaner, después de estar tiempo buscando un substituto, al final alguien recomendó Registry Mechanic, y una vez instalado y probado hay que reconocer que cumple su función al detalle.

Creo que se pueden tener los dos programas instalados y utilizar cada uno cuando mejor convenga. La dureza de Ccleaner no tiene por qué ser algo totalmente malo. La opción puede ser, cuando queráis limpiar el ordenador usar Registry Mechanic y cuando se quiera hacer una limpieza total y exhaustiva usar Ccleaner.

Con Ccleaner podréis analizar y eliminar, eliminar puntos de restauración, limpiar el registro de Windows, desinstalar programas o quitar programas del inicio.

Dado que esta guía está destinada a la seguridad y este capítulo está dedicado a la limpieza del PC, explicaremos el funcionamiento de las opciones para *limpiar el registro* y *analizar y eliminar*.

Para descargar Ccleaner deberéis acceder a su página proveedora y descargarlo,
https://www.piriform.com/ccleaner/download

Una vez descargado la instalación es una serie de pasos típicos de Windows y cuando estéis listas ejecutaréis la aplicación para efectuar la limpieza del ordenador.

Una vez abierto Ccleaner y estéis en la ventana principal, lo primero será dirigirse a *Opciones – Configuración – Borrado seguro de archivo*. De esta manera haréis que los archivos borrados sean totalmente irrecuperables. Entre las opciones podréis llegar a utilizar el borrado de archivos "Método Guttman" que hace 27 pasadas para eliminar los archivos.

Cuando hayáis hecho esto volveréis al limpiador y en la ventana si os fijáis hay dos subventanas, una que dice *Windows* y otra que dice *Programas*. Allí podréis escoger todo aquello que queráis que Ccleaner analice y elimine.

No es recomendable marcar todas las casillas ya que como hemos comentado antes Ccleaner hará un barrido que podría suprimir algo importante. Usad el programa con cabeza y si tenéis alguna duda sobre cualquier opción buscad información antes de habilitarla.

Para limpiar el registro de Windows deberéis dirigiros a la opción de *Registro* y marcar aquello que deseéis que se limpie. Se puede decir que así como las opciones de la limpieza general es algo insegura, en el registro no, con lo que podéis habilitar todas las casillas sin miedo a perder información valiosa para el sistema.

Una vez hecho esto empezará la limpieza y preguntará si queréis hacer una copia de seguridad de los cambios. Cada una que escoja lo que quiera, y una vez terminado deberemos revisar las operaciones. Presionad en *Reparar todas las seleccionadas* y ya habremos terminado con la limpieza del registro de Windows.

REGISTRY MECHANIC

Como hemos comentado antes, Registry Mechanic es similar a Ccleaner en cuanto a limpieza del ordenador. Desde mi punto de vista es más fino a la hora de limpiar, con lo que para la fluidez del ordenador sería mejor escoger este programa.

Por desgracia este programa no es de código libre, con lo que no puedo poner un sitio de descarga gratuita, pero no porque esté prohibido, sino porque no vale la pena descargarse la versión de prueba. Recomiendo encarecidamente que a la hora de querer descargarlo pongáis en el buscador algo como, "*descargar registry mechanic gratis full*" o algo así.

Después de buscar un rato lo encontraréis, aunque seguramente debáis descargaros unos cuantos antes de encontrar alguna versión que valga la pena.

De momento he encontrado este enlace que todavía se puede descargar de alguno de los link que hay. Como ya sabréis cada vez es más difícil descargar de internet y cuando estéis leyendo esto puede que el enlace no siga activo. Si es así, seguid buscando...
http://www.luchoedu.org/descargas/pc-tools-registry-mechanic-11-1-0-214-multi/

La contraseña para extraer el archivo de la descarga está en la página desde donde descargarlo.

Una vez descargado deberéis instalarlo según os lo indique el archivo destinado a tal fin, que esté dentro de vuestra descarga con su crack, su serial o lo que hayáis encontrado. Seguid los pasos y llegaréis a la ventana principal en la que, cómo este programa va cambiando de diseño cada cierto tiempo, cada una de vosotras deberéis estudiarlo un poco para trabajar con él y limpiar bien vuestro ordenador.

No vamos a detallar su funcionamiento debido a que, aun siendo cada versión muy parecida, puede modificar algún paso importante y que la guía no valga de mucho.
De todos modos su uso es muy fácil e intuitivo y seguramente no necesitaréis más de cinco minutos para saber cómo limpiar vuestro ordenador.

Esperamos que con estas aplicaciones tengáis vuestros PC en perfectas condiciones para usarlos como mejor creáis en la lucha contra la opresión hacia las Humanas, las Animales y la Tierra.

Rastros

El control que las poderosas quieren ejercer (y que las que no tienen quieren obedecer) se extiende no solamente a las pocas tierras salvajes que quedan, sino sobre todo a las más íntimas zonas de nuestros cerebros y corazones. Si el conocimiento es poder, tal como lo propaga el cliché de la Era de la Información, y como DARPA sostiene, entonces si nos conocen nos pueden controlar...
… Cuando una entidad "externa" controla la información que recibo, entonces controla mi experiencia sobre el mundo. Y dado que mi experiencia sobre el mundo controla mis acciones, cualquiera que controle mi experiencia del mundo me controla a mí

Para entender este capítulo debemos tener claro un concepto que nos acompañará durante las siguientes páginas: **¡Aun utilizando un programa de borrado seguro de archivos, se pueden recuperar los datos de estos archivos!**

En un principio este capítulo no se iba a incluir en la guía por un simple motivo. El desconocimiento total de la información que hay en él.

Podemos afirmar que casi todas las personas que tienen un ordenador saben que los archivos, al mandarlos a la papelera

de reciclaje se pueden recuperar fácilmente.
Lo siguiente pues, esa conocer programas que eliminen definitivamente estos archivos. El sistema empleado para ello se basa en la sobre-escritura y su posterior eliminación.

Hasta aquí perfecto. En el próximo capítulo íbamos a ver (y de hecho lo veremos) varias herramientas para la eliminación de archivos y carpetas que usan el sistema anteriormente mencionado, y todas contentas. Pero gracias a nuevas informaciones leídas en el nuevo fanzine "Rastros: Cómo golpear y no caer en el intento", todo ese concepto de la sobre-escritura se ha ido al traste (por lo menos en parte). A pesar de la innegable eficacia de estos programas, con información muy técnica y detallada demuestran cómo se puede recuperar rastros de datos en nuestro ordenador. Da igual lo que hagamos: sobre-escribir 50 veces el archivo, romper un CD o un disco duro... Siempre hay posibilidades. con programas y software específico como un microscopio de fuerza magnética, de extraer la información.

En este manual se ha repetido que en el mundo de la informática nada es seguro del todo, pero cuando aprendes los métodos para posibilitar estos hechos, piensas en que hay que tomarse muy en serio nuestra seguridad.

El contenido de la fuente que se utilizó para elaborar el mencionado fanzine, del cual recomendamos su lectura completa, es una serie de artículos aparecidos en la revista autónoma PRISMA de Alemania y vio la luz en 2010. Por desgracia es imposible referenciar el fanzine ya que quienes lo editaron no dan ninguna información para contactar, además de que no está (todavía) en Internet.

El capítulo que menciona las técnicas de reconstrucción de datos en medios de memoria muestra una extensa y variada serie de argumentaciones del porqué y cómo se pueden recuperar los datos. El artículo es tan interesante y valioso

para el tema que estamos trabajando en esta guía que si intentáramos hacer un resumen del mismo, no sería justo ni beneficioso para el concepto de seguridad que queremos difundir aquí. Así que en las próximas páginas veréis el artículo tal cual aparece en el fanzine.

Como veremos, toda la información que pase por nuestros discos duros queda registrada en ellos, así que la alternativa pasa por arrancar el ordenador con un Live CD y desconectar los discos. Para ello se ha creado "Ubuntu Privacy Remix Live CD" y del que detalla rigurosamente el artículo.

EL PROBLEMA DE ELIMINAR DATOS CON SEGURIDAD

La mayoría de nosotras sabe que simplemente borrar datos en un ordenador (por ejemplo mandándolos a la papelera de reciclaje y después vaciándola) no es definitivo en ningún sistema operativo (Windows, Linux, Mac, etc). El contenido de los datos es accesible. El espacio donde se encuentran los datos aparece en una tabla como vacío y liberado para el uso siguiente. Aunque se formatee el disco duro los datos siguen estando ahí, accesibles.

Muchas veces se utilizan programas que sobre-escriben con letras y símbolos sin sentido, archivos sensibles, directorios o unidades de discos duros enteros, lápices de memoria... Un método muy preciso sobre-escribe los datos con hasta 35 plantillas de bits diferentes (estáticas y casuales), que modifican de la forma más duradera posible, datos originales con procesos de codificación. Este método se usa, por ejemplo, en el programa srm (secure remove), accesible con el LiveCD (Ubuntu Privacy Remix (explicado más adelante).

Escribir sobre un archivo para eliminar datos del disco duro o del lápiz de memoria no es suficiente, porque:

1. Los programas de texto (entre otros) dejan normalmente copias de seguridad temporales. Éstas no se borran de forma definitiva, se quedan en el disco duro o el lápiz de memoria.

2. Por razones de espacio, el sistema de usuaria almacena automáticamente bloques de datos no visibles para el usuario de la memoria del ordenador (RAM) a un disco duro de un archivo provisional (SWAP), para luego llevarla otra vez a la memoria. Si el archivo borrado se redactó y se modificó en vuestro ordenador, normalmente queda una copia en algún lugar de ese gran espacio del SWAP en vuestro disco duro.

Esto lo saben muchas usuarias de ordenadores. Pero, en el supuesto que pudiéramos descartar el punto 1 y 2, que no sólo sobre-escribiéramos los espacios libres del archivo mismo sino también del disco duro en un procedimiento que dura horas, "de forma segura", ¿los medios de memoria limpios serían realmente limpios en el sentido que no se podría restaurar el archivo original y sus copias involuntarias "con seguridad"? ¡NO!

La reconstrucción de rastros de datos en medios de memoria
- Medios magnéticos (discos duros, disquetes)

El Defense Security Service (DSS) del Ministerio de Defensa de EEUU, advierte en su estándar de seguridad de 2007 que los métodos de software para borrar datos de medios magnéticos no son suficientes. Discos Duros magnéticos "muy sensibles" tienen que ser destruidos físicamente. Nosotras describimos a continuación algunas circunstancias, efectos y peligros de la sobre-escritura en medios magnéticos. Lo que explica la gran desconfianza de los supuestos programas de eliminación seguros.

Los datos se graban en secuencias de bits, es decir, secuencias de ceros y unos. En un portador de datos magnéticos estos ceros y unos lógicos se codifican físicamente como cambio de la dirección de micro imanes. Un campo magnético local direcciona muchos de estos micro imanes en el entorno al escribir algo. Después de escribir quedan regiones de una magnetización diversa en un rastro del disco duro. Un cabezal de lectura pasa por encima de este rastro y puede testear con cierta precisión estas plantillas magnéticas y leer así los datos.

Amortiguadores molestos entre medio

Borrar datos de los discos duros sobre-escribiendo varias veces significa simplemente que muchos de estos micro imanes se giran varias veces, así se escriben secuencialmente varias plantillas de datos en el lugar del archivo para borrar. La memoria caché es una especie de amortiguador en medio del disco duro. Si el disco duro prevé nuestro intento de escribir varios archivos secuencialmente en el mismo lugar, "optimiza" esta operación y escribe (con la caché activa) sólo la última plantilla de los datos. Los archivos sensibles serán sólo sobre-escritos y no borrados como pensamos y fácilmente recuperables. Los programas de eliminación intentan eliminar la memoria caché antes de la sobre-escritura. Pero no todos los discos duros pueden hacerlo. Las usuarias de ordenador no tienen ningún control (depende del disco duro y el sistema de archivos utilizado).

Sectores defectuosos

Existen discos duros modernos que copian datos de sectores defectuosos a otras partes del disco duro. Estos sectores defectuosos a partir de este momento ya no son accesibles para rutinas de eliminación. Sólo se sobre-escriben los datos en el espacio nuevo, pero no los originales. La usuaria del ordenador no se dará cuenta. Si el disco duro cae en manos de los maderos, por ejemplo en un registro, estos podrán quitar

este disco del imán del disco duro y (con cierto esfuerzo) leer estos sectores defectuosos.

Bits móviles

La fabricación de discos duros tiene que tener en cuenta que los límites entre los dominios magnéticos más pequeños con polarizaciones distintas de los micro imanes antes descritos, pueden moverse con el tiempo en el disco (varios micrómetros). También en ciertas circunstancias se pueden mover regiones de magnetización distinta, las que se usan para la grabación de datos.

Los discos duros se construyen de tal manera que el movimiento de estos bits (cuyas plantillas de magnetización se expanden o se mueven con el tiempo) se podrán compensar automáticamente a través de ajustar los cabezales de escritura; estos datos todavía se podrán leer. Pero este rastreo de los cabezales puede llegar a que las plantillas de los datos, las que se escribieron antes de esta corrección de posición en el disco, no se sobre-escribirán (completamente) en el software. Puede ser bastante efectivo para los maderos un análisis del área de amortiguación entre los rastros. Este área sirve para evitar la influencia magnética entre las plantillas de los rastros.

Después de cierto tiempo las plantillas magnéticas de los rastros entran en el área de amortiguación, el efecto es parecido al de copia continua de cintas viejas. La reconstrucción de estas plantillas y así de los supuestos datos sobre-escritos se puede hacer con la ayuda de microscopios de fuerza magnética con cierto esfuerzo. Estos microscopios son más precisos que un cabezal de lectura en una lectura forense. Este análisis funciona solo con el disco duro original, no con una copia.

Destrucción con trampas

Los materiales magnéticos cuando superan cierta temperatura (la temperatura de Curie) pierden sus propiedades magnéticas. Todos los datos desaparecen para siempre. La temperatura de Curie de la placa fina magnética del portador de datos (aleación de óxido de hierro o cobalto) está entre 800 y 1000º C; y se funden a más de 1500º. La placa magnética está montada encima de un disco fuerte de aluminio (temperatura de fundición a 660º C) o vidrio (sin fundición, pero denso a partir de 1000º C) en los discos duros. Estas temperaturas no se consiguen normalmente con una estufa de leña, ni tampoco con un soplete de camping gas, aunque su llama llegue a 1800º C, el material expuesto no supera los 700ºC (por dispersión de calor)...

… No es fácil ni barato borrar la información de un disco duro. Romper las placas en pedazos no es fiable; incluso las piezas pequeñas pueden contener muchos megabytes de datos bajo un microscopio de fuerza magnética. ¡El método más fiable es mantener los discos duros lejos de información sensible!.

- Memorias flash (tarjetas de memoria, lápices USB)

Es un tipo de almacenamiento usado en todas las tarjetas de memoria, los lápices USB, las tarjetas SD, multi-media (MMC), mini y micro SD, Compact Flash. Las smart Media (SM), y los nuevos discos duros SSD. Las unidades de estado sólido SSD no usan el principio magnético para grabar como los discos duros convencionales, sino que usan memoria flash, manteniendo su contenido también sin conexión eléctrica. Con estos dispositivos ocurre lo mismo que con los discos duros magnéticos, que se obstaculiza la eliminación segura a través del software de sobre-escritura: debido a los errores (todavía altos) de las células de memoria utilizadas, los espacios de memoria muchas veces atacados se copian provisionalmente a otros lugares para repartir el acceso de memoria. Así nuestros

datos sensibles pueden existir varias veces en el USB stick. Sobre-escribiendo el archivo varias veces, solo pillamos, probablemente, una de muchas copias.

Los chips de memoria son bastante resistentes. Quemarlos con fuego no siempre resulta y no todo el mundo tiene acceso a una trituradora industrial.
Si utilizamos un lápiz USB para grabar provisionalmente datos sensibles tendríamos que grabarlos encriptados y después de usarlo tirarlo sin dejar rastros.

- La memoria del ordenador (RAM)

En la memoria principal de ordenador los datos "pasajeros", aun sin alimentación eléctrica, no desaparecen. Tanto en los componentes semiconductores de la memoria estática (SRAM) como en la memoria dinámica (DRAM) se consiguen ver los cambios dependiendo de los datos grabados anteriormente.
Los datos más recientes de la memoria se reconstruyen completamente poco después de apagar el ordenador. Si los componentes están a temperatura ambiente el contenido se puede recuperar durante unos pocos segundos; si los chips se enfrían es posible recuperar la información horas e incluso días más tarde. Los maderos lo utilizan cuando registran un ordenador recién apagado o que todavía está encendido.

Pero a diferencia de otros tipos de memoria, el uso de la memoria interna del ordenador es inevitable, por lo que hay que limpiarla en seguida.

Sobre-escribiendo en la memoria RAM el proceso es distinto que en los portadores de datos magnéticos, no es importante un continuo cambio de plantillas, sino la duración de la memoria; cuanto más antiguo es un archivo, más arraigado está en la memoria.

- Medios ópticos

Con los CD y DVD (regrabables o no) la única forma de eliminar la información es destruyéndolos. No basta con romperlos, es mejor quemarlos. Están compuestos de policarbonato que se funde entre 220º y 230º C; se destruya a partir de 350-400º C y con 520º C salen llamas. El soplete de camping gas más barato es suficiente para fundir o quemar el disco de policarbonato, la placa fina de aluminio y la capa protectora de acrílico. Con mucha paciencia se puede usar la llama de una vela. Durante el proceso se emiten vapores inaguantables. Por eso no es aconsejable (aunque muy útil y en pocos segundos) "tostarlo" en el micro-onda.

Hacer desaparecer datos de forma PERMANENTE es muy difícil, por lo que se aconseja trabajar sin disco duro. Ya se ha mencionado que para ver como trabajamos con información sensible lo haremos con Ubuntu Privacy Remix Live CD (UPR), que creará un entorno seguro y aislado donde podremos trabajar sin ninguna conexión de internet ni con ningún disco duro que haya en nuestro ordenador.

UBUNTU PRIVACY REMIX

El objetivo es poder editar textos sensibles en un entorno de ordenador "seguro" y evitar rastros de datos, en vez de tener que borrarlos y eliminarlos posteriormente.
Para ello es necesario un sistema de usuaria en formato CD o DVD. El que vamos a utilizar en esta guía es Ubuntu Privacy Live, que lo podéis descargar de www.privacy-cd.org. Este sistema corta cualquier conexión con la red y los tipos de discos duros habituales. Para aquellas usuarias de Windows no tendréis muchos problemas para trabajar, a causa de su

interfaz simple y "parecida", además puede ser un pequeño inicio para Linux.

El concepto de seguridad

1. Ningún disco duro

Este es el punto clave para estar seguras de que evitemos los rastros en textos al ordenador. Ya que esto es tan importante, mejor confiar en nosotras y quitar el disco duro físicamente.

2. Ninguna red

Cerradura total. UPR desactiva el acceso tanto a las redes "wireless" como a las cableadas. Por si acaso mejor quitar nosotras el cable del ordenador.

3. El sistema operativo no se puede modificar (en CD o DVD)

Significa que el sistema operativo no se puede modificar externamente, los maderos tampoco puede instalar un software de forma duradera. Aunque un parásito entrara en el sistema, éste desaparece después de apagar el ordenador.

4. Aplicación del software de encriptación

Para poder editar textos hay que grabarlos en un lápiz USB nuevo (sin huellas dactilares). Para mayor seguridad, conviene hacerlo encriptado. En los Live CD está instalado el software aplicable (TrueCrypt, pgp).

El Live CD de Ubuntu Privacy Remix evita que el ordenador active los discos duros habituales de tipo ATA y S-ATA (ni leer ni escribir), pero no sirve para los discos duros SCSI (bastante poco habituales).

En este punto de la operación no confiamos en la documentación de los sistemas operativos complejos, ni en nuestro medio conocimiento en su aplicación. Entonces, evitamos la puesta (defectuosa) de lectura y escritura en las particiones del disco duro y no permitimos al ordenador extender cualquier dato al disco duro quitándolo manualmente en el ordenador. En los portátiles se quita el disco duro normalmente aflojando unos tornillos. En los ordenadores de torre hay que abrir la carcasa y quitar para cada disco duro el cable de datos o el de conexión a la red, es decir, el de la alimentación eléctrica.

Es imprescindible que el ordenador pueda iniciarse sin el disco duro conectado, sólo con el CD o DVD. La mayoría de los ordenadores pueden hacerlo automáticamente, otros necesitan que se cambie la configuración de la BIOS, para que el ordenador use la unidad CD para la secuencia de arranque del sistema.

A continuación describiremos el uso habitual de Ubuntu Privacy Remix, en un ejemplo de lo que sería editar textos sensibles.

1. Desmontar o desconectar el disco duro del ordenador, quitar la conexión de Internet, conectar la impresora con el ordenador.
Cuidado: ¡Según el tipo de impresora, después de utilizar la memoria se quedan datos grabados! Por eso no debería haber huellas encima de la impresora. El cabezal de la impresora puede ser reconocido en la impresión por sus características específicas. Por ello es importante que no tenga huellas y se deseche por separado.

2. Arrancar el Live CD en la unidad (esperar a que esté completamente subido).
No es extraño que el sistema funcione más lento. Todas las funciones y programas suben desde el CD o DVD y esto tarda más que un disco duro habitual.

3. Encender e instalar la impresora. Normalmente la impresora se reconoce automáticamente. Lo podéis comprobar en *Sistema – Sistema y mantenimiento – Imprimir*. Si no la reconoce, deberéis dirigiros a *Sistema – Sistema y mantenimiento – Imprimir* y clicar en *Nuevo* para configurarla.

4. Redactar e imprimir un escrito de prueba. Para asegurarse de que la edición de texto (por ejemplo con Open Office) trabaja sin problemas habrá que hacer una impresión de prueba.

5. Escritorio. Tened en cuenta que vuestro texto desaparecerá para siempre si apagáis el ordenador. Así que para textos más largos deberéis grabarlo encriptado (con TrueCrypt o pgp) en algún lápiz USB y guardarlo a buen recaudo sin huellas dactilares ni demás rastros. Mejor hacer copias de seguridad en otros lápices USB encriptados, por si acaso. Además, los lápices USB baratos tienen muchos fallos.

6. Imprimir. Para imprimir el texto acabado tenéis que aseguraros no sólo de no dejar rastros en la impresora y su lugar, sino también en el papel y la carpeta (nueva, sin abrir) donde se transportará la impresión.

7. Bajar (Apagar). Pulsad el botón de arriba a la derecha, esperad a que el sistema esté completamente apagado y apagad el ordenador.

8. Limpieza final: eliminar rastros de la memoria del ordenador.
Encendemos otra vez con el Live CD la unidad y elegimos *testear la memoria del equipo*. Entonces se inicia el programa del Live CD, "memtest": escribe una serie plantillas de bits en la memoria RAM para deshacernos de restos de datos. Diez tests distintos corren en una cinta infinita, hasta que la paramos con la tecla "Esc", luego el ordenador se inicia de nuevo. El test 9 "Bit Fade Test" es especialmente efectivo (usa "c" para configuración, "1" para elección de test, "4 para Bit Fade Test

y “0” para continuar), porque escribe una plantilla fija cada 90 minutos en la memoria del equipo. Este test lo dejamos operar durante unas horas, lo paramos con la tecla “Esc” y apagamos el ordenador.

Borrado "Seguro" de Archivos

La propiedad no existe. No poseo la silla en la que estoy sentada ni al gato que está sentado a mi lado. No poseo la tierra en la que vivo. Estoy sentada en una silla que todas aceptamos que me pertenece, al lado de un gato que todas aceptamos que me pertenece...

... Ninguna empresa posee tierras. Todas aceptamos que las poseen. Así les permitimos destruir el medio ambiente. Eso no es muy inteligente. Es también innecesario.

Acabamos de ver que trabajar con información sensible es realmente difícil y comprometido, sobretodo si queremos eliminarla. Hemos visto que hacerlo completamente es imposible o casi, pero por supuesto no toda la información es igual de sensible o valiosa, y el hecho de que se puedan reconstruir datos de un archivo eliminado no significa que siempre vayan a conseguirlo.

A pesar de la información aparecida en el anterior capítulo, busques por donde busques, al hecho de sobre-escribir y eliminar archivos con los programas que veremos a continuación se le denomina eliminación definitiva o

eliminación segura de datos, además de que en páginas web afines o en otras de seguridad informática aconsejan el uso de estas aplicaciones para "no dejar rastro de un archivo" (véase comillas) en nuestros ordenadores.

Con todo lo recopilado debemos hacernos una idea de que tenemos que trabajar siempre con las herramientas necesarias para cada situación. Siendo conscientes y pensar qué información nos traerá más problemas en caso de ser recuperada. ¿Qué información os puede incriminar en algo y cual os puede mandar directas a prisión?

Es obvio que en la sociedad en la que vivimos y nuestra manera de adaptarnos a ella ha hecho que nos acostumbremos a trabajar con ordenadores y a almacenar grandes cantidades de información, sea sensible o no, y no vamos a poder trabajar todo el tiempo en Live CD, porque de esa forma no podremos guardar nada, a no ser que tengamos varios discos duros portátiles encriptados y bien escondidos. Por ejemplo. Algunas personas deben guardar en sus ordenadores información sobre colectivos o asambleas, y por supuesto tener a mano todos esos datos. Así que estas personas valoraran ellas mismas como aprovechar sus conocimientos.
Dado que aplicaciones como Secure Delete, Shred o Eraser son realmente efectivas en su trabajo seguiremos llamándolas, por lo menos en esta guía y a pesar de lo mencionado antes, como herramientas de eliminación segura.

El funcionamiento de la eliminación de un archivo básicamente y a grandes rasgos se basa en que se elimina la referencia que hace de él el sistema operativo, pero no el contenido del fichero que todavía permanece en el disco duro. Por este motivo, hay programas (como los que expondremos en el siguiente capítulo) que permiten recuperar archivos y documentos que se han borrado del ordenador.
La sobre-escritura de datos se basa en hacer varias pasadas sobre el archivo seleccionado, escribiendo encima de él

series de unos y ceros. El método que utilizan varios de estos programas como Eraser o Secure Delete es el método Gutmann que hace 37 pasadas encima del archivo. Otro método usado es hacer 7 pasadas sobre el archivo. Este es el que en principio usa la NASA y el gobierno de Estados Unidos, ya que el principio básico para eliminar "definitivamente" un archivo sería hacer más de 3 pasadas sobre éste. Así que si la NASA utiliza 7 pasadas, en teoría con hacer 37 son suficientes.

Más información sobre el Método Gutmann:
https://en.wikipedia.org/wiki/Gutmann_method

ERASER

Eraser es una herramienta bajo licencia GNU que permitirá borrar de forma segura nuestros archivos en Windows mediante técnicas de sobreescritura aleatoria de sectores de disco, imposibilitando (o casi) la reobtención de esos datos gracias a patrones que siguen el algoritmo definido por Peter Gutmann entre otros.
Su interfaz permite añadir archivos y directorios enteros a la opción *On Demand* para su posterior borrado seguro así como la definición de tareas programadas para su eliminación programada (genial para borrar de forma continua logs de distintas aplicaciones por ejemplo). También añade dos opciones más al menú contextual de Windows para el uso directo de Eraser y también podemos tener acceso al explorador desde el mismo programa.

Su descarga y ejecución para eliminar los archivos es de lo más facilona.
Para descargar el programa se debe acceder a su página web http://eraser.heidi.ie/download.php y una vez se elige el último paquete estable, apareceremos en la página de descarga que

está alojada en el servidor de "sourceforge", que es donde están disponibles una infinidad de programas bajo licencia abierta.

Una vez descargado lo instalamos siguiendo los pasos habituales y lo ejecutaremos haciendo doble clic en el icono que aparecerá en el Escritorio.
Lo primero que hay que hacer es configurarlo para que el borrado de archivos se ejecute con el susodicho método Gutmann. Para ello hay que seleccionar donde dice *Settings* y donde dice *Default file erasure method* elegir el método de 37 pasadas (o el que cada una prefiera).

Hay que pulsar en *Save settings* y ya estará configurado para hacer irrecuperables los archivos.
Si marcamos la casilla *Forced locked files to be unlocked for erasure*, estamos permitiendo que los archivos bloqueados se desbloqueen para su borrado por Eraser.

Eraser tiene otras opciones como eliminar el espacio libre o sin usar del ordenador y programarlo para que lo limpie cuando queramos, pero para lo que queremos en esta guía ya lo tenemos como necesitamos.

Para eliminar un archivo o carpeta bastará con hacer clic con el botón derecho sobre éste y en el menú desplegable que aparece veréis que hay nuevas opciones (si no están deberéis reiniciar) y una de ellas es *Eraser - Erase*. Pulsaréis sobre esta y el archivo se eliminará como es debido.

SHRED

Shred es una utilidad para la línea de comandos de Linux, que sobre-escribe los ficheros especificados, repetidamente,

para hacer más difícil la recuperación de los datos, incluso utilizando programas de software muy costosos.

No intentéis descargarlo de ningún lado ya que forma parte del mismo sistema (Linux). Como hemos podido comprobar está en todas las distribuciones Linux y cómo tal no necesita instalación.
Para ejecutarlo solo hay que abrir un terminal y su sintaxis básica sería:

```
shred nombre_del_archivo
```

También podemos "cargarnos" la información de particiones y dispositivos enteros con:

`shred ruta_directorio` (por ej: *shred deb/sdb1*)

Shred sobreescribe por defecto un fichero 3 veces, pero tenemos la opción de modificarlo con la opción "-n" seguido del número de veces que queramos sobreescribir. Otra cosa que debe quedar clara es que shred no elimina el fichero o archivo por defecto, si lo queremos eliminar debemos añadir "-u" a la linea de comandos para que lo remueva una vez sobreescrito.

```
shred -n30 -u -v -f -z archivo_a_borrar
```

Para entender un poco esto:

-n: Número de veces que sobreescribe el archivo (poner la cantidad que se quiera)
-u: Eliminar el archivo
-v: Ver el proceso
-f: Cambia los permisos por si es necesario para borrarlo
-z: Añade una sobreescritura con ceros al final para ocultar la propia acción de shred

Para poder ejecutar esta herramienta debemos abrir el terminal y dirigirnos a la carpeta donde reside el archivo. Por ejemplo, si el archivo estuviera en la carpeta de Descargas, deberíamos abrir el terminal y teclear:

```
cd Descargas && ls
```

"ls" lo que hará, será mostrar todo lo que se encuentre dentro de la carpeta en cuestión, mientras que "&&" sería algo así como un espacio o como si le dijéramos "además".

A continuación escribiríamos la sintaxis de Shred que hemos mostrado antes, para eliminar el susodicho archivo.

NOTA: Recomiendo usar siempre la sintaxis entera ya que una vez interiorizada en nuestra mente estaremos seguras de haber eliminado por completo el archivo en cuestión.

Para aquellas que vengan de Windows y no estén acostumbradas a que los archivos sean del estilo "nombre-del-archivo" en vez de "nombre del archivo" (véase el detalle "_"), o sea que los archivos estén separados por espacios, se debe poner comillas antes y al final del nombre del archivo, ya que es la única manera para poder trabajar desde el terminal (un archivo que se llame: guía de seguridad informática para activistas, deberá escribirse: "guía de seguridad informática para activistas", con las comillas inclusive) . Es un dato muy importante ya que cuando eres neófita en Linux no entiendes por qué no hay manera de usar la línea de comandos. La alternativa para asegurarse es desde el modo gráfico hacer clic con el botón derecho en el icono del archivo y pulsar en *Cambiar el nombre*.

Otro dato es que con Shred no se puede, o yo no he encontrado la manera de, eliminar carpetas. Y para esas existe la última herramienta de este capítulo. Que es Secure Delete y de la que ya hemos hablado durante el manual.

SOBREESCRIBIENDO EL DISCO DURO

En el capítulo llamado "El problema de eliminar datos con seguridad" hemos visto que los datos con los que trabajamos quedan almacenados en el disco duro, además de guardarse en la memoria RAM, y por ese motivo usamos los programas que acabamos de citar para sobreescribir toda esa información y dificultar así que se pueda recuperar.

Los discos duros, externos o internos, como los lápices USB, una vez queramos deshacernos de ellos y no pensemos quemarlos con un soplete, o bien queramos formatearlos para reinstalar una distribución nueva, o simplemente queremos eliminar los rastros que hayan podido quedar almacenados desde hace años. Deben ser "barridos" o limpiados con la mayor seguridad posible.

Para ello podemos utilizar un par de sintaxis en la línea de comandos de Linux. Una se ejecuta con la aplicación "dd" y la otra con el programa que acabamos de mostrar "Shred". Personalmente la primera que vais a ver no la he probado, pero con la segunda, actualmente mi ordenador lleva tres días encendido limpiándome un disco duro externo de 600 Gb y todavía le queda. No sé si será tan efectivo como incendiar el disco, pero tiene pinta de que cumpla su propósito.

```
dd if=/dev/random of=/dev/sda
```

Lo que hace es enviar fragmentos aleatorios (que coge de /dev/random) a nuestro disco en /dev/sda (OJO: aquí debemos poner lo que corresponda al disco a eliminar en nuestro caso, que puede no estar en /dev/sda).

La otra manera con la que podemos eliminar todos los datos de nuestro disco duro, antes de formatearlo o de deshacernos de él, o lo que queramos es:

```
shred -n 10 -vz /dev/sda
```

Fijaos en lo que se comenta del ejemplo anterior. Donde dice /dev/sda puede ser cualquier otro sector, podría estar el disco en /dev/sde, /dev/sdf o en otro.

Debo recordar que borrando el disco así, deberemos tener en cuenta que vuestro ordenador deberá estar encendido durante varios días, así que estad seguras del momento que utilizaréis para hacerlo.

SECURE DELETE

Una parte de esta herramienta ya se ha comentado en el capítulo sobre la limpieza del ordenador, pero nos hemos reservado la que acostumbra a ser la más usada y que hace de Secure Delete una muy buena aplicación.

La herramienta es SRM:

Esta herramienta es una versión más avanzada del comando "Shred", que hemos visto en el apartado anterior. Sin embargo, en lugar de sólo sobrescribir tus archivos con información aleatoria, emplea un sistema basado en el Método Gutmann.

Básicamente el proceso de borrado de srm consiste en:

1 pasada con 0xff
5 pasadas aleatorias. Si está disponible se empleará /dev/urandom

27 pasadas con los valores especiales definidos por Peter Gutmann
Renombrando del archivo con un valor aleatorio
Eliminación del archivo

Además se emplean medidas adicionales de seguridad para evitar que se quede información en el caché del disco.
Su sintaxis es:

```
srm nombre_del_archivo.txt
```

Y si es un directorio:

```
srm -r nombre_del_directorio
```

Con la opción -r se eliminarán todos los subdirectorios almacenados dentro del principal.

Recuperar Datos

Cuando enseñaba en la cárcel, algunas de mis estudiantes comentaban que las juezas sabían cómo tratar a la gente que robaba por avaricia, probablemente porque ellas mismas conocían esas motivaciones muy bien. Pero la gente que roba porque odia al sistema y porque quieren destruirlo confunde y asusta a las juezas, que responden dictando sentencias desproporcionadas. Esa es la clasificación panóptica en acción, y no requiere de una particular crueldad consciente por parte de policías, juezas y espectadoras circunstanciales.

Como ha ocurrido con algún capítulo anterior, este apartado no está completamente relacionado con el tema principal de esta guía, pero creo que como aporte al capítulo que precede servirá, aunque sea para comprobar si los programas anteriormente mencionados funcionan o no. Por ello no vamos a dar muchos ejemplos, pero sí un par de herramientas realmente efectivas.

Hay que tener en cuenta que no todos los archivos que hemos eliminado desde la papelera de reciclaje (sin toda la seguridad de antes) son recuperables. Ya que a veces el archivo que recuperemos estará dañado y será imposible su lectura (por lo menos con nuestras herramientas).

Como los programas anteriores, el software que utilizaremos para Windows tendrá una interfaz gráfica, mientras que los usados en Linux necesitan ser usados desde la línea de comandos.

RECUVA

Recuva, del mismo modo que Ccleaner, forma parte de la corporación Piriform. Así que su descarga puede ser de pago con soporte adicional o gratuita, que si no eres un madero o una empresa, no creemos que necesites más que esta última.

Para descargarlo iremos a:
https://www.piriform.com/recuva/download y se instalará de la manera más común y aburrida del mundo, al estilo Microsoft Windows.
-Aceptar, Acepto los términos..., Aceptar, Acepto.
Lo cual pensando un poco recuerda al documental, "Surplus"; donde se hace un montaje con Bush y su gran paranoia del terrorismo, hablando – Terrorist, terror, terror, terrorist … -

Una vez instalado hacer doble clic en el icono del escritorio y accederéis a la ventana inicial del programa, que dice *Bienvenido al asistente de Recuva*, hacer clic en *Siguiente* y lo que seguirá será elegir qué tipo de archivo se quiere recuperar.
Después deberemos decidir dónde estaban los archivos que queremos recuperar y cuando terminemos esta fase, ya estaréis listas para empezar el escaneo. Pulsar en *Iniciar* y éste empezará a trabajar. Lo bueno que tiene Recuva es que muestra en qué condición se encuentra el archivo recuperado con diferentes colores, así se puede ver si el archivo se podrá visualizar o no hay nada que hacer con él.

Como ya se ha comentado, Recuva es un gran programa que además de efectuar un escaneo para buscar archivos

borrados tiene la capacidad de sobre-escribir archivos ya borrados para dificultar su recuperación. Con lo que aquellas que hayáis borrado de manera insegura archivos, podéis intentar recuperarlos y desde el mismo momento eliminarlos definitivamente.
En el siguiente enlace, de las compañeras de "security in a box", podréis encontrar más información sobre el programa y sus utilidades.
https://www.securityinabox.org/es/recuva_principal

TESTDISK – PHOTOREC

Esta herramienta que tratamos en seguida, de las que aparecerán a continuación, es la mejor con diferencia (por lo menos para mí). En realidad a la hora de realizar la guía me he encontrado con el dilema de si incluir las dos siguientes aplicaciones, o por el contrario mostrar únicamente TestDisk. El motivo es que TestDisk es con diferencia mucho mejor. Por supuesto que en el momento de utilizarlo no llegó a recuperar toda la información que hubiera deseado, pero de todos modos recuperó varias películas, además de todos los documentos pdf, doc, txt..., que es algo que con otros software de recuperación, después de formatear (por error, vaya tela!!) un disco duro externo con 400 Gb de información en el interior, no conseguí recuperar.

Cuando hemos eliminado un archivo, o varios y queremos recuperarlos. El software de recuperación extraerá (o lo intentará) toda la información y datos del sector que nosotras mandemos que analice. A continuación el programa depositará la información recuperada en un directorio que hayamos escogido. La información que hallemos ahí, depende del tamaño que haya analizado y estará detallada por números, es decir, un libro que tuviéramos guardado que se llamara

"Maderos, cerdos, asesinos" lo podrá recuperar, pero lo normal es que este aparezca con la denominación "7676452309.pdf". Ahora imaginaos haber intentado recuperar 8 Gb de un USB que hayáis borrado y que esté lleno de libros y de documentos que pesen pocos. A la hora de recuperar la información os encontraréis con 8 Gb de documentos sin etiquetar y que deberéis clasificar si no queréis perder la información.

Pues bien, para mi sorpresa TestDisk, después de analizar el disco ha recuperado una cantidad ingente de documentos ¡Con su Nombre!. Esto hace que podamos confiar bastante en él.

Antes de seguir debemos aconsejar a todas las usuarias de Linux que guarden todos sus datos con el nombre que queramos, pero juntando las palabras con el guión bajo "_". Curiosamente los documentos que TestDisk ha recuperado con su nombre estaban etiquetados de esta forma.

Otro detalle interesante es que si alguien formatea por error un USB o un Disco Duro y quiere recuperar la información que había en él, que por ningún motivo escriba en el Disco antes de usar un programa de recuperación. Antes hemos visto que los datos ocupan el espacio del disco de una forma un poco caótica (aunque seguro que no lo es) y si guardáramos algo en él, podríamos perder mucha información que queremos recuperar.

El hecho por el que hemos incluido, a pesar de los motivos mencionados, es que a cada una le va mejor un programa y no voy a ser yo quien decida cual es mejor. Cada una de nosotras tiene sus experiencias y puede que a otra persona le funcione mejor cualquier de los otros programas.

Usando TestDisk

Esta herramienta consta de dos programas; TestDisk sirve para recuperar archivos borrados pero en especial particiones perdidas, en cambio Photorec se especializa en la recuperación de los archivos borrados (en especial archivos multimedia) y además hace otras cosillas.
Para instalar deberemos escribir en la terminal:

```
sudo apt-get install testdisk
```

TestDisk ya instala los dos programas, así que no deberemos escribir nada más (de momento).
Una vez tengamos instalado el programa, deberemos crear una carpeta para guardar los archivos recuperados y trabajar desde ahí para que la aplicación guarde ahí por defecto todo lo que encuentre. En este ejemplo lo haremos todo desde la terminal para agilizar un poco el proceso:

```
sudo su
mkdir /recuperados
cd /recuperados
```

Una vez estemos dentro de la carpeta, deberemos poner en marcha el programa y deberemos seguir el proceso que va marcando. Quien sepa de inglés lo tendrá un poco más fácil, pero de todos modos no es muy difícil. Si alguien tiene algún problema con estas explicaciones que consulte el enlace que aparece al final del libro. Ahí encontrará imágenes y será un poco más fácil...

```
sudo photorec
```

Aparece una ventana donde deberemos seleccionar el disco a analizar y pulsaremos *Proceed*, o sea Enter. La siguiente ventana nos muestra el tipo de sistema que tiene el disco (FAT, NTFS, EXT4, etc).

Ahora deberemos escoger entre *Whole* que recuperará toda la información del disco, esté eliminada o no. O en su caso *Free*, que analizará sólo el espacio libre del disco.

A partir de este momento, si estamos trabajando en la terminal, pero dentro de la carpeta creada, deberemos pulsar *c* y el programa empezará a trabajar y a recuperar la información.

Es posible que el programa no actúe exactamente del mismo modo que lo hemos mostrado en este ejemplo. Si es así no os preocupéis y leed bien lo que vaya mostrando. Sea como sea, acabaréis encontrando lo que deseáis.

FOREMOST

Foremost es un software diseñado igual que Recuva, para recuperar archivos anteriormente borrados, escanear lápices USB, Discos duros externos o internos o cualquier memoria portadora de datos que necesitéis escanear. Como muchos programas de Linux hay que ejecutarlo desde la línea de comandos. Hay que reconocer que a veces esto echa para atrás a muchas personas y que incluso a quienes nos gusta trabajar con este método, a veces se hace un poco pesado y deseamos una interfaz gráfica que nos facilite un poco las tareas. De todos modos no os preocupéis ya que para trabajar con la mayoría de estos programas basta con tener al lado una pequeña guía como esta o cualquier otra referencia para saber lo que estamos haciendo.

Foremost recupera los siguientes archivos: avi, bmp, dll, doc, exe, gif, htm, jar, jpg, mbd, mov, mpg, pdf, png, ppt, rar, rif, sdw, sx, sxc, sxi, sxw, vis, wav, wmv, xls, zip... Además de que si queremos buscarlos todos bastará con teclear "all".

Para instalarlo:

```
sudo apt-get install foremost
```

Y para ejecutarlo abriremos el terminal y escribiremos las opciones necesarias para realizar el escaneo y recuperación de ficheros. Únicamente hay que tener clara la sintaxis y a partir de ahí ya podremos empezar la búsqueda.

Las opciones son las siguientes:

-h, muestra la ayuda y sale
-T, añade la fecha al directorio donde quieres guardar los archivos recuperados
-v, muestra la salida de datos
-q, modo rápido
-Q, modo silencioso
-w, escribe solo la el fichero donde informa de lo que se puede recuperar pero sin recuperar nada
-i, la partición que queremos escanear
-o, el directorio de salida

Un ejemplo de escaneo básico sería algo como:

```
sudo foremost -v -T -t pdf,jpg  -i /dev/sdc1 -o
/home/acab/recuperados/
```

Pondríamos "sudo" por aquello de los permisos
-v para mostrar la salida
-T para poner la fecha
-t pdf,jpg" para los tipos de archivos a recuperar
-i es la partición donde realizar el escaneo
-o donde guardar los archivos recuperados

Con esto ya habremos recuperado lo que necesitamos y ahora ya podremos probar a recuperar algún archivo eliminado con

la sintaxis "shred -n700 -u -z", a ver si se puede extraer datos del archivo.

SCALPEL

El siguiente programa es Scalpel, que aunque haya comentado que no quería extenderme mucho en este capítulo, este programa es digno de mención ya que es realmente efectivo. Para mí el problema que tiene es que una vez recuperados los archivos, estos aparecen únicamente numerados como los ha ido encontrando y no con el antiguo nombre que tenía, tal como hemos comentado antes, lo que hace realmente pesado el trabajo de buscar después el archivo en cuestión que deseamos encontrar. Aun así hay una opción para facilitar el trabajo, aunque de todos modos reconozco que no apaña mucho la cosa. Eso sí, efectivo es...

Para instalarlo:

```
sudo apt-get install scalpel
```

Una vez instalado, para decidir qué tipo de archivos queremos recuperar, seguiremos en el terminal y pondremos:

```
sudo gedit /etc/scalpel/scalpel.conf
```

(donde dice "gedit" deberemos usar el editor de texto de nuestra distribución Linux)

Nos aparecerá el archivo de configuración de Scalpel y lo único que deberemos hacer es buscar el tipo o tipos de archivo que queramos escanear y borrar el símbolo # (lo cual se denomina descomentar) que hay justo delante del tipo de archivo (pdf, avi o lo que queramos) y que está al principio de la línea.

Guardaremos los cambios para volver a la línea de comandos. Para empezar a buscar y recuperar, ejecutaremos el programa:

```
sudo scalpel /dev/sda5 -o pdf_recovered
```

Con lo que "dev/sda5" será la partición donde escanear y "-o" es el nombre que le daremos a la carpeta donde depositará lo que vaya encontrando. "pdf_recovered" es el nombre que le pondremos a la carpeta donde recopilará la información extraida

Encontraréis una gran cantidad de archivos que habrá recuperado, o no, dependiendo de vuestros discos duros. Pero para poder facilitar la búsqueda la siguiente sintaxis ordenará un poco lo que encuentre. Escribiremos en la terminal (substituyendo USER por vuestro nombre de usuaria)

```
sudo chown -R USER.USER pdf_recovered
```

y listo.

Seguridad Móvil

Durante estos más de 5 años de investigación
en el denominado "caso bombas",
han sido alrededor de 60.000 mil escuchas
telefónicas a distintas personas y
sujetos criticos con el orden actual,
sumado a una indeterminada
cantidad de interceptaciones a
emails y otros medios de comunicacion.

Seguridad Móvil

No se puede ser tan inocente como para pensar que se puede escapar a la represión. Cualquier movimiento que se pretenda revolucionario tarde o temprano deberá enfrentarse a la represión del sistema que trata de destruir. La cuestión no es si es evitable o no. Sino cómo debe afrontarse y qué consecuencias tendrá para la propia actividad del movimiento...

… La represión no debe concebirse simplemente como un hecho "bélico", como un enfrentamiento entre dos grupos, sino sobre todo como un hecho "social", en el contexto de un conflicto más amplio y prolongado...

… En un conflicto vecinal, la policía puede saber quiénes son las cabecillas, pero puede ser incapaz de actuar si su detención o acoso extiende o radicaliza el conflicto.

En la nueva era tecnológica donde las herramientas cada vez son más potentes y el control social está abandonando la sutilidad para mostrarse tal como es, aunque sea tras una pantalla de frases y palabras sacadas de contexto. La libertad se ha convertido en una falacia, vendiéndose a cualquier empresa que pague por sus servicios.

La telefonía móvil es uno de los sectores donde la represión y el control alcanza sus cotas más altas. Cada vez son más los "escándalos" (¿alguien creía que no nos espiaban?) referentes a escuchas sin ninguna justificación, ni tal sólo en base a sospechas hacia personas, por parte de estados y empresas

privadas. Cuando no es el estado quien hace las escuchas, pide la información a las empresas de telefonía y rápidamente encontrarán lo que buscan.

El control a través de los móviles varía desde las escuchas de lo que decimos, en vivo o grabando todas las comunicaciones que estén a su alcance. La intrusión en las memorias de los teléfonos, el seguimiento por GPS, conexión sin permiso por Bluetooth, SMS silencioso para saber dónde estamos en un momento determinado sin que nosotras nos demos cuenta... y otras maneras de localizarnos, escucharnos y controlarnos.

Dado que los teléfonos móviles son pequeños ordenadores, vamos a mostrar algunas herramientas para tener un poco más de seguridad con ellos. No vamos a detallar todas y cada una de las maneras en cómo poder hacer que no nos espíen, ya que el libro podría ir dirigido únicamente a la seguridad o contra-vigilancia y ese no es el tema exclusivo del libro. En cambio aprenderemos a mandar correos encriptados, navegar anónimamente, cifrar una parte de nuestros móviles para guardar ahí nuestra información sensible, llamadas "encriptadas" (aquí ponemos comillas ya que no podemos asegurar cien por cien que esto ocurra), o como modificar fotografías tomadas con el móvil.

Como consejo principal creemos conveniente decir que;

¡¡NO USÉIS PARA NADA VUESTRO TELÉFONO SI TRABAJÁIS CON INFORMACIÓN SENSIBLE!!

¿Por qué? Si en el punto donde estamos hemos entendido bien este manual, habremos visto que los ordenadores, aunque usemos muchas herramientas para hacerlos más seguros, son realmente inestables y siempre habrán posibilidades de que nos lleven a situaciones no deseadas. Por supuesto los teléfonos móviles son mucho más peligrosos en cuanto se pueden perder, los pueden robar, pueden escuchar e interceptar

nuestras comunicaciones... Esto nos lleva a la conclusión que lo mejor sería no usarlos para nada. Todos nuestros contactos pueden estar ahí y en cualquier caso no querremos que otras puedan saber con quién nos relacionamos.

De todos modos, como sabemos que en algunos momentos es inevitable tener que contestar a un mensaje, buscar algo en la red, o contestar a llamadas, ahí van algunas aplicaciones que harán más seguros vuestros teléfonos.
Para mostrar esta pequeña guía, utilizaremos Android. Es con el que la gente está más familiarizada, además de ser el que usa una servidora, así que mis limitados conocimientos se reducen a esta distribución.

CORREOS CIFRADOS

1. Lo primero que deberemos hacer antes de nada es descargar las aplicaciones que serán necesarias para mandar correos encriptado. Esto, como veréis será muy parecido a lo que habíamos hecho con Thunderbird a la hora de tener comunicaciones seguras.

Las herramientas que necesitaremos son (mejor descargarlas todas primero y luego empezad con el manual): ASTRO Administrador de archivos, APG, K-9Mail.

2. Una vez estén descargadas las aplicaciones lo primero que debemos hacer es guardar en el móvil las llaves PGP que usamos para cifrar los mensajes. Para ello las guardaremos dentro del programa APG. Esta aplicación puede generar llaves públicas y privadas como lo hace OpenPGP, pero esa herramienta está en fase BETA lo que la hace un poco inestable, así que mejor será utilizar las que ya hemos creado con OpenPGP. Aunque pudiéramos crearlas con APG sería

mejor usar siempre OpenPGP ya que las creará más fuertes y con mayor algoritmo de cifrado.
Para guardarlas deberemos conectar el móvil al ordenador. Una vez esté conectado, abriremos el programa Thunderbird y nos dirigiremos a *OpenPGP – Administración de claves*. Nos situaremos encima de las claves y una por una las guardaremos en la carpeta APG que debe estar dentro de vuestro Android. Para guardarlas ahí haremos clic con el botón derecho encima de vuestro par de claves (mejor empezar por las vuestras) y seleccionaremos en la ventana que emerge *Exportar claves a un fichero – Exportar claves secretas* y navegaremos hasta la carpeta APG. Una vez tengáis todas las llaves instaladas al finalizar los procesos siguientes, por vuestra seguridad recomiendo que volváis a conectar el ordenador y eliminéis las llaves de esa carpeta con el programa Secure Delete, Shred o Eraser (lo que mejor creáis), pero no lo hagáis con alguna aplicación del móvil. Si las herramientas de los ordenadores, tal como hemos visto, pueden ser vulneradas, imaginad una herramienta del teléfono.

Una vez estén guardadas las llaves desconectaremos el teléfono de la máquina y pasaremos al punto 3.

3. Instalar las llaves. Para instalarlas en el móvil, deberemos seleccionar el programa APG. Cuando éste arranque aparecerá una ventana con cuatro opciones. No seleccionaremos ninguna de ellas, en cambio seleccionaremos *Menú – Administrar llaves privadas*. Se abrirá una pantalla que estará vacía. Volveremos a hacer pulsar *Menú – Importar llaves*. Apareceréis en una nueva ventana y seleccionaréis la carpeta que sale para navegar hasta vuestras llaves. Nueva ventana y elegís para buscar las llaves la aplicación ASTRO. Cuando hayáis hecho esto apareceréis dentro del programa ASTRO y os dirigiréis la carpeta donde tendréis guardadas las llaves (en este ejemplo APG). Seleccionáis la llave y apareceréis de nuevo en la ventana anterior. Clicáis en *Aceptar* y veréis que la llave privada ya está instalada.

Tened en cuenta que vuestra llave privada es una clave pública y secreta, sólo que el programa ha seleccionado una parte, la secreta. Para escribir y recibir mensajes cifrados deben estar instaladas las dos llaves (dos en uno como hemos visto). Así que hay que volver al principio del programa y repetir lo mismo sólo que esta vez seleccionaréis *Administrar llaves públicas*.
Hay que repetir el proceso tantas veces por cuantas llaves de contactos tengáis. Una vez terminado de instalar las claves pasamos al 4.

4. Crear y configurar cuentas en K-9 Mail. Cerraréis APG y ahora hay que abrir K-9 Mail. Cuando lo abráis el programa irá indicando cómo deberéis crear y configurar las cuentas que tengáis. Es muy fácil e intuitivo por lo que no mostraremos como se hace. A estas alturas del manual ya sabréis configurar bien las cuentas. El único consejo es que lo hagáis delante del ordenador con Thunderbird abierto y comprobad antes de terminar de crear las cuentas que la configuración del servidor de entrada y de salida sean los mismos datos, para que no haya ningún problema.

5. Una vez las cuentas estén creadas ya podremos enviar mensajes cifrados. Aquí, de la misma manera que lo mejor cuando enviamos un mensaje cifrado es firmarlo con nuestra llave, podremos hacer lo mismo.

Cuando hacemos clic en *Menú – Redactar*, en la pantalla de redacción, debajo de la casilla reservada para escribir la destinataria hay dos opciones que deberemos seleccionar para firmar y cifrar los mensajes. Mejor hacerlo cuando hayamos terminado de redactar el mensaje ya que en cuanto lo hagamos se abrirán un par de ventanas de APG. Al marcar *Firmar* se abrirá una ventana y seleccionaremos nuestra llave para firmar el mensaje. Cuando seleccionéis *Cifrar* deberéis seleccionar la llave pública de vuestra destinataria.

6. Enviar y recibir. Para enviar, una vez hayamos redactado el mensaje y seleccionado *Cifrar*, pulsaremos *Menú – Enviar*. A continuación, si habéis seleccionado *Firmar* hay que introducir la contraseña de vuestra llave y el mensaje se enviará.

Para recibir un mensaje cifrado, en el momento de abrirlo, veremos que éste está cifrado y que hay una opción que dice *Descifrar*. Escribís la contraseña de la clave y podréis leer el mensaje que os habrán mandado.

NOTA: Hay ocasiones en que no sabréis porqué, pero K-9 Mail no manda los mensajes y aparecen algunos mensajes de error. Para soluciones esto basta, normalmente, con dirigirse al control de aplicaciones de Android y reiniciar la aplicación. En alguna ocasión esto no funciona y la solución pasa por desinstalar y volver a instalar el programa, volviendo a crear las cuentas. Lo bueno de K-9 Mail, es que acepta cualquier cuenta. Si tenéis Riseup no habrá problema para trabajar con él.

ENCRIPTAR DIRECTORIO

Para encriptar carpetas en Android existen varias aplicaciones que hacen eso, pero en esta ocasión vamos a mostrar cómo hacerlo con **Cryptonite**. Esta es una aplicación que trabaja con TrueCrypt, así que nos da un poco de confianza. Está todavía en fase BETA, así que no os fiéis mucho de ella. Como hemos comentado, aun conociendo estas herramientas, mejor no guardar información delicada en el teléfono.

Cryptonite tiene tres opciones en cuanto lo abrimos: Dropbox, Local y Expert. En esta guía trabajaremos con la opción *Local*, ya que con ella crearemos una carpeta encriptada y podremos guardar información en ella.

Cuando seleccionemos *Local*, debajo de la opción aparecerán otras opciones. Seleccionaremos *Create Local Volume*, y confirmaremos. Ahora deberemos seleccionar el tipo de cifrado que queremos entre las opciones que nos muestra. Lo mejor será elegir *Paranoia* que basa su cifrado en el algoritmo AES 256 y será más seguro. En la ventana que aparecerá pulsaremos sobre la carpeta con el símbolo "+" que tiene incrustado (así crearemos una carpeta nueva. Le daremos el nombre que queramos, y después de navegar hasta ella haremos clic sobre *Use current folder*. Pondremos la contraseña que queramos para el directorio encriptado y ya tendremos una carpeta cifrada.

Para descifrarla y así guardar o extraer información, deberemos abrir el seleccionar *Local – Decrypt local folder*. Navegaremos hasta la carpeta que antes hemos creado y pulsaremos sobre *Select current folder*. Deberemos escribir la contraseña y lo tendremos a punto de guardar lo que queramos.

APLICACIONES VARIAS

A continuación veréis una lista de aplicaciones de Android y que os servirán para poder trabajar con Android un poco más tranquilas. Entre estas encontraréis herramientas para navegar por la red, llamar por teléfono o cifrar partes del móvil.

No vamos a mostrar detalladamente como utilizar cada una de estas herramientas, como hemos hecho con las distribuciones de Windows o Linux, ya que el tema principal de este manual es la seguridad en vuestros ordenadores. De todos modos, el uso de estas aplicaciones no es muy difícil y seguro que quienes se decidan por utilizarlas no tendrán demasiados problemas a la hora de trabajar con ellas.

1. Hotspot Shield VPN

Esta aplicación está destinada a navegar bajo una red VPN. En otro capítulo hemos mostrado el funcionamiento de las VPN y su efectividad a la hora de navegar anónimamente. Es gratuita, aunque tiene opción de hacerla de pago.

2 Obscura Cam

Esta aplicación se encarga de reconocer y pixelar las caras en las fotografías que tengáis guardadas en el móvil. Es una cómoda y efectiva herramienta para aquellas que acuden a las manifestaciones para hacer fotografías.

3. RedPhone

RedPhone encripta el contenido de las conversaciones que tenéis cuando hagáis una llamada. Por supuesto RedPhone, sólo será efectivo cuando las dos partes (quien llama y la receptora) tienen instalado el programa. Como idea es genial, si un programa puede encriptar las conversaciones telefónicas. Pero sinceramente no diría nada "raro" por teléfono aunque tuviera instalados cien programas como este.

4. Orbot

Este es un software de navegación anónima que pertenece al colectivo Tor. Así que es una de las pocas aplicaciones de las que nos podemos fiar. Por lo menos quienes están detrás de Tor sabemos que trabajan por generar una cultura de seguridad en la red. Para navegar es necesaria la siguiente aplicación

5. Orweb V2

Aplicación para navegar anónimo junto con Orbot.

6. Encryption Manager Lite

Esta aplicación es similar a Cryptonite. Bajo contraseña creará directorios cifrados en vuestros teléfonos.

7. Droidwall

Cortafuegos que controlará las conexiones entre el teléfono y la red. Con él podréis escoger qué aplicaciones se conectarán y cuales no.

8. Crypt Haze

Aplicación para mandar mensajes cifrados. Para utilizarla deberéis tener tanto quien lo envía como el destinatario, la aplicación y la contraseña de cifrado y descifrado.

9. KeePassDroid

KeePassDroid es una herramienta de fácil uso para la administración segura de contraseñas para tu dispositivo Android.

10. Gibberbot

Gibberbot permite organizar y administrar tus diferentes cuentas de mensajería instantánea (IM siglas en inglés) usando una única interface. Utiliza software OTR para las comunicaciones autenticadas y seguras entre clientes incluyendo Gibberbot, ChatSecure, Jitsi, y Pidgin. Gibberbot puede añadir una capa para el anonimato y proteger tus comunicaciones de muchas formas de vigilancia en internet ya que se conecta con Orbot.

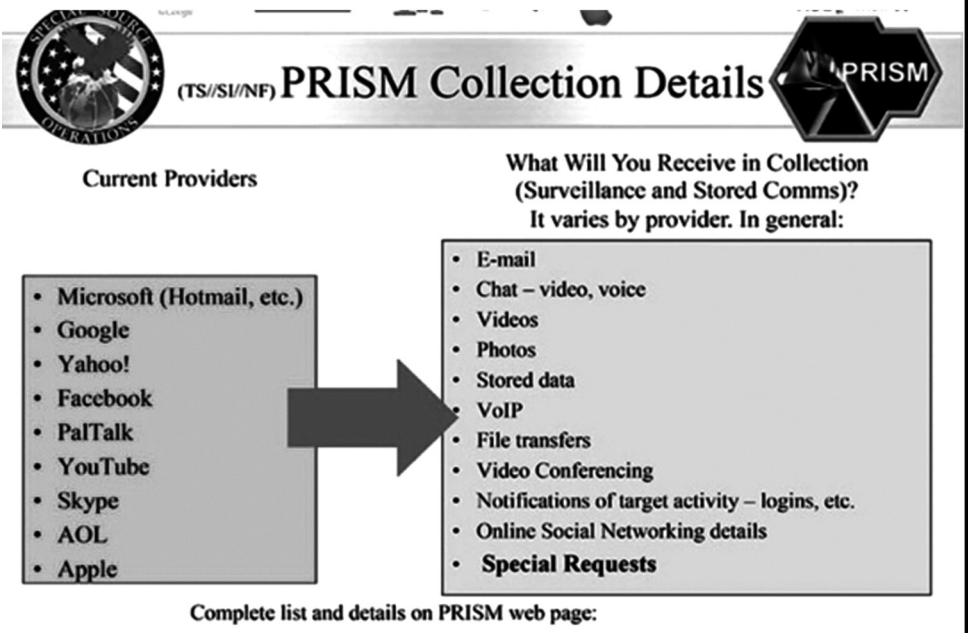
11. TextSecure

TextSecure es una aplicación para plataformas móviles de Android que encripta mensajes de texto (SMS) a la hora de su envío o mientras están en tu teléfono.

NOTA: Para instalar, configurar y utilizar estas herramientas (casi todas) encontraréis información al respecto en la página web del colectivo Security in-a-box.
https://securityinabox.org/es/seguridadportatil

Misceláneo

Las empresas que el documento menciona son: Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, Youtube y Apple, ordenadas según cuál accedió primero a otorgar su información a la NSA.
Dropbox, el servicio de almacenamiento de archivos en la nube de Google, sale mencionado con un "Próximamente".



Misceláneo

La vida no es una jungla depredadora, ni un lugar extremadamente violento como pretenden las occidentales, sino que se comprende mejor como una sinfonía de respeto mutuo donde cada jugadora tiene que jugar en una parte específica. Debemos estar en el lugar adecuado y jugar nuestro papel en el momento adecuado. Al menos en lo que respecta a los seres humamos, ya que llegamos las últimas y somos las hermanas pequeñas de las otras formas de vida.

A continuación podréis leer algunos artículos relevantes para el tema que nos ocupa: La Seguridad Informática para Activistas.

En estos textos encontraréis, seguramente, aclaraciones sobre algunos conceptos que quizás no os habrán quedado claros de las herramientas que hemos trabajado a lo largo del manual. Si hemos decidido publicar estos artículos es porque creemos conveniente que quienes hayáis tomado la decisión de trabajar por una cultura de seguridad, tengáis toda la información posible acerca de lo que habéis visto.

No se ha querido pecar de condescendientes y conformarnos con lo que leemos una primera vez, ni con lo que pensamos que está acertado. Pensamos que si cada una tiene la información necesaria, tomará decisiones acertadas, aun a riesgo de no tener todo lo que quiera.

Esta explicación se refiere básicamente a los rumores que existen acerca de TrueCrypt y su posible implicación en la CIA. Personalmente creo que de momento estamos a salvo, en lo que refiere a TC, y hasta que no llegue alguien y consiga descifrar un volumen del mismo, podremos trabajar tranquilas con él.

A modo de final, quiero agradecer a quienes hayan tomado parte de su tiempo para leer esta guía, y espero de corazón que la difusión de una cultura de seguridad sirva para crear lazos de solidaridad en una sociedad basada en el control y la vigilancia.

¿PODEMOS FIARNOS DE TRUECRYPT?

Nadie discute que hoy día el estándar de facto para cifrar discos duros / datos en un HD es TrueCrypt.

Funciona bien, es un software muy estable, y está disponible para múltiples plataformas.

Pero ¿Nos podemos fiar de TrueCrypt? ¿Es realmente un software libre de toda sospecha? ¿Podría ser un 'honeypot' de la CIA?

Hace tiempo encontré un post en el que se apuntaban ciertas partes oscuras con respecto a TrueCrypt y sobre quién está tras el proyecto. Todo lo que se expone es muy 'conspiranoico'

pero es cierto que proyecta sombras sobre el proyecto. No obstante, después de Stuxnet, Flame y amigos, la capacidad de asombro y de negación ha quedado muy mermada.

El artículo original plantea las siguientes cuestiones:
1. El dominio truecrypt.org se registró con una dirección falsa, en concreto 'NAVAS Station, Antarctica'. Esto, per se, a mí no me parece nada sospechoso, mucha gente lo hace.
2. Nadie sabe quiénes son las desarrolladoras de TrueCrypt (su identidad, se desconoce). Esto SI me parece algo a tener muy en cuenta, me parece genial que en ciertos foros donde se liberan herramientas más 'ofensivas', estas herramientas sean firmadas por pseudos o nicks, pero todo lo que tenga que ver con criptografía debe ser totalmente transparente.
3. Las creadoras de TrueCrypt trabajan gratis. Aseveración un poco discutible en mi opinión. Mucha gente trabaja 'gratis' en proyectos opensource, escribe blogs, etc etc.
4. Compilar TrueCrypt es complicado. Lo que apuntan en el post original es que, la mejor forma de incentivar la descarga de binarios pre-compilados por el equipo de TrueCrypt es hacer complicada la compilación del software. Tiene lógica.
5. La licencia de TrueCrypt no es realmente OpenSource. Bueno, tampoco indica nada en especial, es cierto que TrueCrypt ha sido rechazado de muchas distribuciones Linux (en el post citan a Fedora), pero eso no lo tiene porque hacer necesariamente sospechoso
6. El código de TrueCrypt nunca ha sido auditado. El autor del post se queja de que nadie ha publicado un estudio sobre el código de TrueCrypt, en parte tiene razón, pero resulta muy aventurado decir que nadie lo ha hecho. Lo que sí está claro es que si alguien realiza esa auditoría y encuentra algo, es su pasaporte a la fama. Cuesta creer que nadie haya puesto sus ojos en el tema. (Nota de Edición: En varios posts, los cuales no dispongo para su autenticidad, se declara que varias personas a título individual, han auditado TrueCrypt buscando puertas traseras, así que este comentario no es del todo cierto).
7. Existe censura en los foros de TrueCrypt. Parece que en los

foros de TrueCrypt no se puede hablar de otras soluciones de cifrado ni de herramientas para atacar a TrueCrypt.
No seré yo quien desacredite un producto como TrueCrypt que tantas alabanzas ha cosechado, pero del post original, tengo que decir que hay varios puntos que sí me preocupan bastante.
Lo de la identidad desconocida es bastante grave, ¿usarías un algoritmo de cifrado del que desconozcas su autoría? probablemente no, como decía más arriba, criptografía = transparencia como axioma.

Respecto a introducir un backdoor en el software, es técnicamente posible, y voy más allá: de estar ahí, puede ser REALMENTE complicado encontrarlo.

HACKERS DEL FBI FRACASAN AL INTENTAR HACKEAR TRUECRYPT

El FBI ha admitido su fracaso a la hora de romper este sistema de cifrado open source, usado para securizar discos duros incautados por la policía brasileña durante una investigación realizada en 2008.
Las autoridades brasileñas solicitaron la ayuda al FBI después de que su propio instituto de Criminología, el NIC (National Institute of Criminology) fuese incapaz de romper las contraseñas usadas por el banquero Daniel Dantas para securizar sus discos duros.

Según informes de medios brasileños, Dantas usó dos programas para cifrar los discos duros, uno de los cuales era el popular y ampliamente usado programa opensource TrueCrypt. Aparentemente, los expertos de ambos países han empleado varios meses para intentar descubrir las contraseñas usando un ataque de diccionario, una técnica que implica la

prueba de combinaciones de caracteres hasta que se encuentra la secuencia correcta.

Si se usa una contraseña compleja, por ejemplo una combinación aleatoria de mayúsculas y minúsculas con números y caracteres especiales, con una longitud grande, se necesita un tiempo de computación tan grande que en la actualidad es imposible descifrarla.

TrueCrypt también permite la existencia de volúmenes ocultos al cifrar un disco o un contenedor, por lo que un usuario que se viese forzado a montar un volumen podría ocultar la información que no quiere que sea revelada. Así, la única forma que tienen las autoridades para acceder a los datos cifrados es persuadir a los usuarios para que les proporcionen las contraseñas usadas.

ASÍ DESCIFRA LA GUARDIA CIVIL TRUECRYPT

Cada vez que las Fuerzas de Seguridad españolas o francesas detienen a algún etarra y se incautan ordenadores o 'pen drives' entra en escena el arduo trabajo de los expertos informáticos, que tratan de descifrar el contenido de archivos informáticos que poseen los pistoleros. Pero ETA ha cambiado su sistema de encriptación de documentos, lo que está dificultando la labor de la Policía.

ETA encripta sus documentos desde hace más de una década. En un principio, los sistemas que empleaban las terroristas eran relativamente precarios. Hasta diciembre de 2003, fecha de la detención de Ibón Fernández de Iradi, alias Súsper. En este golpe, la Policía halló en un cajón una hoja de papel con las claves de los archivos que almacenaba en su ordenador personal. Los expertos consiguieron acceder a

esos documentos, lo que permitió la detención de más de 150 personas relacionadas con la banda.

En ese momento, la dirección de ETA ordenó adoptar un nuevo sistema de encriptación de archivos informáticos: el 'PGP' ('Pretty Good Privacy', en inglés, o 'Muy buena privacidad'), un programa que cualquier internauta puede descargarse de la Red.

Aunque pueda parecer inexpugnable en ocasiones, los terroristas han visto cómo las Fuerzas de Seguridad descifran cada vez más documentos, lo que provoca un conocimiento más exhaustivo de los movimientos e intenciones de los 'comandos' asesinos. Por este motivo, ETA ha decidido recientemente cambiar de sistema de encriptación y pasarse al TrueCrypt. Fue el conocido como 'etarra de la bici', Ibai Beobide, quien confirmó a la Guardia Civil el dato de que ETA está empleando este "sistema operativo" de manera sistemática.

Fuentes consultadas por *El Confidencial Digital* explican el funcionamiento del sistema TrueCrypt que ahora utilizan los terroristas. Es este:
-- Se cifra el contenido completo del disco duro, en lugar de archivos particulares como hace el PGP que hasta hace pocos meses han utilizado los pistoleros. Esta diferencia plantea serios problemas a los especialistas informáticos tanto de la Guardia Civil como de la Policía francesa.
-- Se están dando casos de ordenadores y discos duros incautados a ETA que se encuentran aparentemente vacíos. Esto significa que los terroristas han encriptado los ficheros y los han convertido en ocultos. El inconveniente que surge a las Fuerzas de Seguridad es que les resulta imposible saber si existen esas unidades ocultas.
-- En definitiva, la Policía puede tener un ordenador y no saber qué cantidad de información encriptada hay en él: hay ficheros que son invisibles ya que TrueCrypt cifra el contenido

del disco duro en crudo. La única manera de acceder a esta parte oculta es introduciendo la contraseña preestablecida.

El proceso que emplean los expertos informáticos para 'atacar' los ordenadores de ETA es el siguiente (se ofrecen datos genéricos por motivos de operatividad):
-- Se diseña un programa específico para intentar averiguar la clave que 'descubre' los archivos. El objetivo es hacer que el proceso de validación de esta contraseña sea lo más rápido posible.
-- Acto seguido, se emplean diccionarios y reglas automáticas para transformar palabras, tanto en castellano como en euskera, en posibles claves. Hay que tener en cuenta que los etarras suelen utilizar frases sin sentido.
-- Con el software creado de manera específica, se hace lo que los expertos llaman un ataque de la clave "por fuerza bruta" y se espera a que el programa encuentre la clave correcta. Estos ataques son lentos ya que el barrido completo de las claves puede tardar cientos o miles de años: por ello se emplean diccionarios.

El hecho de que ETA se haya pasado al sistema TrueCrypt supone, además, que el tiempo medio que se tarda en encontrar las claves se multiplique por dos. En el caso de una búsqueda exhaustiva, explican las fuentes consultadas por *ECD*, se pasa de 1.000 a 2.000 años. Como estos tiempos no son asumibles, los diccionarios facilitan la labor policial, reduciendo los tiempos de 'ataque' de la clave.

En cualquier caso, la clave del proceso de descifrado de los ordenadores incautados a ETA reside en la creación de ese programa capaz de 'atacar' la contraseña que han introducido los pistoleros. Si se conoce que la clave es una palabra en castellano, el 'ataque' por software llevará a los especialistas sólo unos días. Si no se tiene ningún dato sobre la misma, el proceso se complica, llegándose a tardar años en poder acceder a los archivos de los terroristas.

Otro inconveniente con el que se encuentra la Policía es que el descifrado de archivos requiere, en ocasiones, costosas ampliaciones de hardware. Por ello, España y Francia ya han solicitado en al menos dos ocasiones ayuda a la Agencia de Seguridad Nacional, la NSA, estadounidense, para poder descifrar ordenadores incautados a ETA.
La información sobre los hardware y software de los que dispone la NSA es reservada, pero parece, explican las fuentes consultadas, que la agencia tiene equipos con suficiente potencia de cálculo para 'atacar' cualquier ordenador que se le ponga delante.

(Nota de Edición: Este artículo totalmente tendencioso da a entender que La GC ha llegado a descifrar un volumen de algún ordenador de ETA. ¿A quién intentan engañar? La única manera efectiva para descifrar los ordenadores según la GC es torturando a las personas hasta que alguna de ellas llega al extremo de revelar la contraseña. Intentar hacer creer a la gente que han llegado a descifrar un disco duro cifrado con TrueCrypt es ruin y manipulador).

EL FBI INSTALÓ PUERTAS TRASERAS EN EL PROGRAMA DE SEGURIDAD OPENBSD

El FBI y la CIA en el contexto de seguridad en internet, siempre se han preocupado por el uso de los cifrados por parte de las usuarias.
Si una usuaria maneja datos y los envía cifrados, ni siquiera el FBI y la CIA pueden descifrarlos, seguro que muchas de vosotras conoceréis programas para cifrar los datos como TrueCrypt (próximamente tendréis un completo manual), al cifrar estos datos con distintos tipos de algoritmos, ni siquiera el FBI con sus potentes ordenadores podrían descifrarlo

(siempre y cuando usemos claves largas para impedir o limitar los ataques de fuerza bruta).
Para atajar este problema de "seguridad nacional", y según un técnico del FBI, decidieron instalar puertas traseras en los programas de seguridad del sistema operativo libre OpenBSD, los cuales son muy usados en muchas distribuciones de Linux.
El antiguo asesor de seguridad de la Administración estadounidense, envió un e-mail al responsable del desarrollo de OpenBSD y éste lo ha hecho público para que todas que usen su código, comprueben que su seguridad y privacidad no se ha visto comprometida auditando el código fuente de OpenBSD, también ha aclarado que él no tiene nada que ver en este suceso.
Las expertas debaten la autenticidad de la historia que relata Perry. En un mensaje en Twitter, una persona que conoce los hechos asegura que el encargo existió pero que fracasó técnicamente.
Gregory Perry era director técnico de la compañía NETSEC, implicada en el desarrollo de OpenBSD. Concretamente participaba en trabajos sobre el IPSec, que aporta mecanismos de seguridad al protocolo de Internet IP (más adelante explicaremos en otro artículo en profundidad este protocolo utilizado en las redes privadas virtuales (VPN). Durante los años 2000 y 2001, el FBI habría pedido a NETSEC la instalación de estas *puertas traseras*. Perry habría participado en el encargo suscribiendo un compromiso de confidencialidad de 10 años.
El cifrado moderno dota a los archivos de un alto grado de seguridad que dificulta los intentos de descifrado.

La última propuesta del FBI con este tema de la instalación de puertas traseras, es que las empresas fabricantes las instalen y ellas se comprometen sólo a utilizarlas con una orden judicial, como en casos de terrorismo.

(Nota de Edición: Como se ha demostrado durante los últimos meses, la CIA ha investigado durante años a todas las personas que ha podido, sin órdenes judiciales, así que no les

hace falta ninguna orden para, en el caso de tener la puerta abierta a nuestros datos, vigilarnos y extraer de nosotras toda la información que puedan).

PROYECTO PRISMA – ESPIONAJE DE ESTADO

En una presentación obtenida por el Washington Post, se detallan las operaciones con las que la Agencia Nacional de Seguridad (NSA, por sus siglas en inglés) y el FBI obtienen una masiva cantidad de información directamente de algunas de las empresas más importantes de Estados Unidos y el mundo.

Mediante una conexión directa con empresas como Microsoft, Yahoo, Google y Facebook, la NSA puede acceder a correos electrónicos, documentos, audio, fotografías, videos, y hasta registros que permiten determinar los movimientos y contactos de los cientos de millones de usuarias que confían su información a las mencionadas firmas, indicó el Washington Post.

El complejo sistema encargado de reunir y clasificar esta información recibe el nombre de PRISM (prisma, en inglés), y supuestamente habría estado operando y perfeccionándose en las sombras desde el año 2007.
(Nota de Edición: Mucho antes estuvo operativo desde los años 40, el proyecto Echelon, así que nada nuevo bajo el sol).

Según menciona el post, PRISM sería la principal herramienta responsable de los informes que la NSA entrega diariamente al presidente Obama. Esto permite presumir una complejidad de operación y exactitud a la hora de recopilar y analizar datos nunca antes vista en el campo del "data mining".
Empresas consultadas, como Apple, negaron tener cualquier conocimiento de PRISM, que por otro lado habría tenido a los

pocos miembros del poder legislativo que sabían del proyecto bajo juramento para evitar que se hiciera público. Lo cierto es que en Estados Unidos aplican leyes de "inmunización legal", para las empresas que accedan a cooperar con la búsqueda de potenciales amenazas al país, todas aparecidas luego de los ataques del 9/11.

Por otro lado, existen secciones del documento que indican abiertamente la intención de dejar en secreto la participación de las compañías. "98% de la producción de PRISM está basada en Yahoo, Google y Microsoft; debemos asegurarnos de no dañar a estas fuentes", indican las notas de la presentación.

Las empresas que el documento menciona son: Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, Youtube y Apple, ordenadas según cuál accedió primero a otorgar su información a la NSA. Dropbox, el servicio de almacenamiento de archivos en la nube de Google, sale mencionado con un "Próximamente".

CLAVES DEL PROYECTO PRISMA

Las revelaciones sobre el programa de la Inteligencia estadounidense cuestiona la posibilidad de un Internet privado y seguro.

¿Qué es Prism (prisma)?
Es un programa de la Agencia Nacional de Seguridad (NSA) estadounidense destinado a recabar información masiva de comunicaciones por Internet, ya sean correos electrónicos, chat, mensajes de redes sociales o conversaciones por videoconferencia. Según distintas informaciones periodísticas, el Gobierno de Estados Unidos habría accedido a través de dicho programa a los servidores de las compañías de

telecomunicaciones, con permiso de éstas, para obtener información de millones de usuarias de todo el mundo con el pretexto de que trataba de prever acciones terroristas.

¿Cómo salta el escándalo?

Es una revelación periodística del diario británico The Guardian y el estadounidense The Washington Post. Días después, los rotativos revelan la identidad de la fuente con el acuerdo de ésta, un informático estadounidense de 29 años, Edward Snowden, quien trabajó durante cuatro años para la CIA a través de varias subcontratas.

The Guardian publicó una entrevista en video en la que Snowden afirmaba: "No tengo ninguna intención de ocultarme porque sé que no hice nada malo". El entrevistado se encuentra en Hong Kong desde el pasado 20 de mayo, intentando evitar su extradición a Estados Unidos. "Mi único objetivo es informar a la gente sobre lo que se está haciendo en su nombre y lo que se hace en su contra", aseguró Snowden a The Guardian.

¿Quién es Snowden?

Autodidacta, ni siquiera acabó la educación secundaria. Según su propio testimonio al diario 'The Guardian' se alistó en el Ejército estadounidense para luchar en Irak por elevados ideales, pero sólo duró cuatro meses al romperse las dos piernas en un entrenamiento. El mismo asegura que comenzó a trabajar en la NSA en 2004, a través de la Universidad de Maryland. En 2007 fue enviado por la CIA a Ginebra con cobertura diplomática para mantener la red de seguridad informática. De ahí pasó a ser analista de infraestructuras para las contratas de la NSA con el cargo de director del sistema de vigilancia.

¿Qué empresas están implicadas?

La Inteligencia estadounidense no dejó cabos sueltos a la hora de dirigirse a la fuente de información. Facebook, Hotmail, Yahoo, Google, Skype, PalTalk, Aol, YouTube y Gmail fueron las empresas requeridas. Destaca que la red social Twitter no aparezca en la lista de empresas "colaboradoras", lo que podría responder a que la mayoría de los mensajes que los

usuarios 'cuelgan' en la red son públicos, a excepción de los directos que se envían entre ellos.
Una de las compañías afectadas, Apple, ha hecho pública una carta que resume la posición que han adoptado todas las compañías ante el escándalo. "No ofrecemos acceso directo a nuestros servidores a ninguna agencia gubernamental, y cualquier agencia del gobierno que solicite información de nuestras clientes debe conseguir una orden judicial" dice la misiva. Otras han ido más lejos y han llegado a dar la cifra de usuarias de las que permitió la investigación, pero siempre con el argumento de que fueron casos solicitados de forma individual y con autorización judicial.
Facebook reconoce 19.000 intervenciones; Apple, 5.000. Por su parte, Microsoft admitió el viernes que durante el segundo semestre del 2012 recibió entre 6.000 y 7.000 peticiones que afectaban a entre 31.000 y 32.000 de cuentas sus usuarias.
¿Ha podido afectar a ciudadanas españolas?
Hasta el momento no ha trascendido la identidad de alguna de las millones de espiadas. La NSA asegura que se trata de ciudadanas que viven fuera de Estados Unidos, por lo que no sería de extrañar que españolas o residentes en España figuren entre las personas que se han visto afectadas. ¿Es legal?
El Gobierno de Estados Unidos se blindó ante una posible filtración y consiguiente demanda. Por ley, la NSA tiene que explicar sus métodos y objetivos a un tribunal secreto radicado en Washington. Sin más. No hacen falta órdenes judiciales concretas para cada caso de espionaje.

¿Existe algo parecido en España?

El espionaje masivo no está permitido en España. El anterior Gobierno del Partido Popular adquirió un Sistema de interceptación de las telecomunicaciones que desarrolló el ejecutivo de Zapatero. Como en el pasado, se encarga de las cuestiones operativas de las interceptaciones de móviles e Internet aprobadas previamente por un juez. El magistrado autoriza una intervención y las compañías de

telecomunicaciones abren el canal para que policías y guardias civiles tengan acceso en tiempo real a las comunicaciones. El Sistema de Interceptación de las Telecomunicaciones (SITEL) tiene una central en los 'cuarteles generales' de Policía y Guardia Civil, pero todas las instalaciones de los Cuerpos que alojan unidades de investigación tienen una sala dedicada a SITEL con monitores. El Centro Nacional de Inteligencia (CNI) tiene asignado un magistrado del Tribunal Supremo para sus intervenciones telefónicas o de Internet.

INGLATERRA AMENAZA A GOOGLE POR JUICIO POR ESPIONAJE

La Oficina del Comisionado de Información del Reino Unido (ICO, por sus siglas en inglés) amenazó este viernes con llevar a Google ante los tribunales por guardar información personal obtenida ilegalmente para su aplicación de mapas Street View.

Este organismo británico, que vela por el derecho a la información y la privacidad, anunció hoy que ha entregado al gigante de la comunicación estadounidense una orden para que elimine inmediatamente cuatro discos con información privada obtenida a través de redes inalámbricas no seguras.
Google ya había admitido en 2010 que recopiló datos privados, como claves de seguridad y correos electrónicos, en redes "Wi-Fi" no seguras mientras sus vehículos peinaban las calles para configurar sus programas de mapas.
Tras comprometerse a destruir toda esa información, la multinacional reconoció en febrero de 2012 que aún guardada, "por error", varios discos con datos privados, lo cual llevó al ICO a reabrir su investigación.
ICO señaló hoy que si la multinacional estadounidense no cumple en un plazo de 35 días con las órdenes judiciales

emitidas por las autoridades de este país, cometería un delito de "desacato".
Precisó además que esos discos adicionales han sido guardados en "celdas de cuarentena", por lo que, dijo, no se ha tenido acceso a su contenido.
Para el activista Nick Pickles, director de "Big Brother Watch", la actitud de las autoridades y, especialmente del comisionado, significa que Google se libra de las consecuencias de sus actos con un simple "azote".
"Google ha recopilado información sin derecho alguno, violado la privacidad de la gente a gran escala y dicho después que había borrado los datos, lo cual no hizo. El principio de las leyes de privacidad se basa en que las compañías no recopilan nuestra información sin nuestro permiso", afirmó Pickles.
Google vuelve así al centro de la polémica en el Reino Unido, después de que un comité parlamentario pidiese la pasada semana a Hacienda que "investigue a fondo" a esta y a otras multinacionales por entender que utilizan un régimen fiscal "muy artificial" para evitar el pago de millones de libras en impuestos.
A Google se la relaciona también con el polémico programa de vigilancia sobre internet PRISM, desarrollado por la Agencia de Seguridad Nacional estadounidense (NSA) y el FBI para recopilar en secreto información privada de las mayores empresas de internet del mundo.
Según se publicó este mes, el PRISM dio tanto a la NSA como al FBI acceso a registros de nueve de las mayores compañías de internet del mundo, entre ellas Google, Facebook, Microsoft, Apple, Yahoo y Skype.

TENEMOS QUE HABLAR DE FACEBOOK

Durante varios años, hemos estado proveyendo servidores e infraestructura de comunicación para la izquierda. Hemos

hecho todo lo que estaba en nuestras manos para mantener los servidores seguros y hemos resistido, usando varios medios, a peticiones de datos de usuarias por parte de las autoridades.

En resumen: tratamos de ofrecer una forma de comunicación liberadora dentro del internet capitalista.

Siempre hemos visto internet como un recurso para llevar adelante nuestras luchas y al mismo tiempo también como un espacio para el combate político, y hemos actuado en consecuencia con eso. Pensábamos que la mayoría de la izquierda lo veía de la misma manera. Pero desde que más y más gente de la izquierda "usan" Facebook (o Facebook las usa a ellas), ya no estamos tan seguras. Nuestro trabajo político se ha estado viendo como deficiente y agotador. La comunicación cifrada con servidores autónomos no se percibe como algo liberador, sino como algo molesto.

Disneylandia

No nos habíamos dado cuenta de que después de liberar tanto estrés en las calles y de todas esas largas discusiones en grupo, muchas activistas parecen tener ese deseo de cotorrear sin parar en Facebook sobre cualquier cosa y con cualquiera. No nos habíamos dado cuenta de que, incluso para la izquierda, Facebook es la más dulce de las tentaciones. De que la izquierda, al igual que cualquiera, disfruta siguiendo el sutil flujo de la explotación, que no parece hacer daño y, por una vez, no hace falta resistirse. Mucha gente sufre las malas consecuencias. Aunque esto les puede permitir prever las fatales consecuencias de Facebook, no parece hacerles actuar ante ellas.

¿Es realmente ignorancia?

Hagamos un esbozo del problema. Al usar Facebook, las activistas no sólo comunican de forma transparente sus

opiniones, sus "me gusta", etc., sino que las dejan disponibles para ser procesadas. No sólo eso (y esto lo consideramos mucho más importante), sino que exponen estructuras y personas que en sí tienen poco o nada que ver con Facebook. La capacidad de Facebook de barrer la web buscando relaciones, similitudes, etc. es difícil de comprender por la gente de a pie. Las luces hipnotizantes de Facebook acaban haciéndonos reproducir estructuras políticas para las autoridades y las compañías. Toda esta información puede ser buscada, ordenada y agregada no sólo para obtener datos precisos sobre relaciones sociales, personas clave, etc., sino también para hacer predicciones de las cuales se pueden deducir regularidades. Después de los teléfonos móviles, Facebook es la más sutil, barata y mejor tecnología para la vigilancia.

¿Son las usuarias de Facebook informantes involuntarias?

Siempre hemos pensado que la izquierda quiere otra cosa: continuar nuestras luchas en internet y utilizar internet para nuestras luchas políticas. De eso se trata para todas nosotras (incluso ahora). Por eso vemos a las usuarias de Facebook como un verdadero peligro para nuestras luchas. En particular, activistas que publican información importante en Facebook (con frecuencia sin saber lo que eso implica), que luego es utilizada cada vez más por las agencias que se dedican a hacer cumplir la ley. Casi podríamos ir más allá y acusar a estas activistas de colaboradores. Pero aún no hemos llegado a ese punto. Todavía tenemos la esperanza de que la gente se dé cuenta de que Facebook es un enemigo político y de que aquellas que usan Facebook la hacen más y más poderosa. Las usuarias activistas de Facebook alimentan a la máquina y de este modo revelan nuestras estructuras (sin ninguna necesidad, sin ninguna orden judicial, sin presión alguna).

Nuestro punto de vista

Somos conscientes de que hablamos desde un punto de vista

privilegiado. Para nosotras, habiendo trabajado durante años (y a veces incluso habiéndonos ganado la vida) con la red y los ordenadores, la administración de sistemas, la programación, la criptografía y muchas otras cosas, Facebook se nos presenta como un enemigo natural. Y aunque nos consideramos a nosotras mismas como parte de la izquierda, esto se une al análisis de la política económica de Facebook, donde las "usuarias" son convertidas en producto, que es vendido y eso nos vuelve a convertir finalmente en consumidoras. A esto se le llama "generación de demanda". Nos damos cuenta de que no todo el mundo vive los pormenores de internet con el mismo entusiasmo con el que nosotras lo hacemos. Pero el hecho de que haya activistas que dejan a este caballo de Troya llamado Facebook que sea parte de su vida diaria, es un signo del alarmante nivel de ignorancia que existe.

Urgimos a todo el mundo: cierra tu cuenta de Facebook! Estás poniendo a otras en peligro! Actúa en contra del monstruo de los datos!

Además: Abandona el correo de Yahoo! y similares. Abajo con Google! En contra de la retención de datos! Por la neutralidad de la red! Libertad para Bradley Manning! Larga vida a la descentralización!

Combate el capitalismo! También (y especialmente) en internet! Contra la explotación y la opresión! También (y especialmente) en internet!

Pon nerviosas a tus compañeras.

Déjales claro que alimentando a Facebook han elegido el lado equivocado!

Nadir.org, 10/2012

ENCRIPTACIÓN – ¿ES SEGURO PGP?

Una pregunta nos invade a todas las personas que utilizamos la criptografía. Cada vez que ciframos un directorio, el Disco Duro, y sobre todo cuando encriptamos nuestras comunicaciones.

Seguramente, la mayoría no decimos todo lo que queremos contar, aun cifrando los mensajes. Siempre nos queda la duda, y nos preguntamos repetidas veces, si habrá alguna manera de descifrar el contenido de los mensajes sin llegar a tener nuestra clave privada u/o su contraseña.

En este artículo intentaremos desentrañar este enigma y para ello deberemos remontarnos a uno de los primeros tipos de cifrado y con la ayuda de la evolución en tecnología criptográfica, entendiendo cómo funciona ésta y si su uso es seguro o no. Si hay quien trabaja por censurar esta tecnología o si intentan hacerla más vulnerable.

El sistema de cifrado se basa en codificar un texto claro para producir un texto secreto diferente. Esto se hace utilizando un método específico, el algoritmo criptográfico.
Actualmente los métodos más utilizados son dos, la encriptación simétrica (sólo existe una clave, y esta se encarga de cifrar y descifrar el texto) y la encriptación asimétrica (existen dos claves, una pública y una privada).
A lo largo de este artículo aparecen varios ejemplos de estos dos métodos de cifrado, pero conocer básicamente (por el momento) su funcionamiento, ayudará a entender más tarde lo que irá apareciendo.

A continuación nos remontamos a uno de los primeros tipos de cifrado, que es el llamado "Cifrado de César". El general romano, codificaba los mensajes modificando cada letra por la que le seguía en tercer lugar en el alfabeto. Es decir, "A" se convierte en "D", "B" en "E", etc...
Con la tecnología actual, sería del todo absurdo mantener una conversación segura ya que, cómo el alfabeto sólo tiene 25 caracteres, sólo habrían 25 claves y 25 combinaciones posibles. Dado que el valor de la codificación se basa en que la cantidad de claves posibles sea tan elevada, que sea imposible intentar todas estas combinaciones en un plazo razonable de tiempo, para la criptografía actual se utilizan varios algoritmos, como el uso de números primos, que hacen muy difícil, incluso para grandes ordenadores, la descodificación de las claves.

De momento, el único sistema totalmente seguro es el "cuaderno de un solo uso" (one-time pad), que se desarrolló a finales de la Primera Guerra Mundial.
Este sistema se basa en una secuencia totalmente aleatoria de letras no repetitivas. Como no utiliza ningún patrón, además de que la clave se elimina después de haberla utilizado, ningúna criptoanalista puede acceder a la clave. La desventaja de este sistema radica en que la distribución de las claves es muy limitada y la creación de grandes claves de estas características es demasiado compleja. Por lo que su uso no es muy común.

La invención del ordenador supuso un gran avance en las posibilidades y capacidades para la ejecución de complejos algoritmos de cifrado. Por ello la NSA intentó (con éxito en un principio) limitar la capacidad de estos algoritmos a 56 bits.

En este punto apareció el algoritmo DES (Data Encryption

Standard) que durante un cuarto de siglo fue la norma oficial de cifrado en los EEUU.
Este sistema, a pesar de lo que se ha publicado, no ha sido desentrañado. Incluso habiendo sido limitada la capacidad de la encriptación y que en la actualidad existen potentes ordenadores capaces de hacer un ataque por fuerza bruta.

Posteriormente apareció el "Triple DES" (de 112 bits) y más tarde el sistema que se usa en la actualidad "AES" (ya hemos hablado suficiente de él en la guía). Este es un sistema rápido y se considera seguro ya que sus creadores no han limitado la longitud de la clave.

Estos métodos mostrados forman parte del citado "Sistema de encriptación simétrica" y plantean un problema, la distribución de la clave.

¿Cómo podemos mandar a una amiga la clave para descifrar un mensaje por una vía segura?
No hay una respuesta realmente efectiva a esta cuestión y por ello apareció el sistema asimétrico.

Recordemos que este "Sistema Asimétrico" se basa en una clave pública (la que nosotras distribuiremos, que no hace falta que sea por una vía segura) y una privada (la que guardaremos nosotras como si fuera nuestro mayor tesoro).

Pero. ¿Es seguro este método?

La respuesta a esta nueva pregunta la encontramos en el "sistema RSA".
El resultado de la multiplicación de dos números primos muy elevados se convierte en uno de los elementos de la clave pública sobre la base de una función unívoca (la llamada puerta trampa).

– (Copiado tal cual, yo tampoco entiendo nada qué significa esto) –
La desencriptación sólo puede llevarla a cabo quien conozca los dos números primos utilizados. Y hasta el momento, no hay ningún procedimiento matemático que permita calcular, a partir de la multiplicación, los números primos utilizados.

Por tanto es una respuesta temporal. De momento SÍ es seguro.
El riesgo es que aparezca alguien que sea capaz de encontrar un sistema para averiguarlo, o que te detengan, requisen tu ordenador y te coaccionen (por llamarlo suavemente) para que digas tu contraseña.

La elaboración del sistema RSA (Clave asimétrica) es muy laborioso y los ordenadores normales no son capaces de crear claves lo suficientemente fuertes. Pero Phil Zimmerman tuvo la idea de asociar el sistema, que sólo podían usar grandes ordenadores, a un procedimiento simétrico más rápido e igualmente efectivo.

De este modo apareció "Pretty Good Privacy" (PGP), capaz de crear las claves con sólo un clic y del mismo modo efectuar la encriptación.

PGP es el sistema empleado a nivel usuario por todas nosotras, y el hecho de que podamos comprobar que es seguro, está asociado a que el código fuente de las primeras versiones se hizo público, por lo que se puede afirmar que no se han añadido puertas traseras (backdoors), de lo contrario se habrían encontrado durante alguna auditoría.

A pesar de que el código fuente del original PGP está a disposición de todas en la red, la empresa estadounidense NAI compró el programa. Con el ejemplo de PGP7, del

que su código fuente no ha sido publicado, podemos tener la legítima sospecha de que esa distribución no es segura.

¿Cómo podemos utilizar esta información?

Después de que se descubriera que la CIA había instalado una puerta trasera en OpenBSD, la atención se dirigió hacia Microsoft ya que éste no ha rebelado su código fuente.

Por otro lado, la realidad en la que podemos trabajar para estar "seguras" de que el software que usemos no tiene posibles "trampas", es la información. En el momento de querer descargar un programa y que éste pudiera poner en riesgo nuestra seguridad, deberemos asegurarnos de que su código fuente está accesible en su página web. Si además de esto, buscamos por la red información sobre la fiabilidad de ese programa, mejor.

Por el momento podemos confirmar que los programas relativos al cifrado que aparecen en esta guía, tales como Kleopatra (gpg4win), Enigmail, Thunderbird, AesCrypt, TrueCrypt (a pesar de los rumores), encontramos sus códigos fuente en sus respectivas páginas web y si deseamos podemos compilarlos e instalarlo en nuestros PC. Pero por encima de todo no descarguéis PGP7, ni otro software que sospechéis que pudiera ser malicioso.

Nuestra libertad puede estar comprometida. Debemos valorar nuestra seguridad y la de nuestras compañeras.

Fuentes

...El conocimiento, visto cómo parte de la
educación, viene dado de la información
que una puede y debe constatar.
La autonomía del saber hace coherente
la praxis de nuestras ideas.
Pero cuando el conocimiento se convierte en poder,
sólo queda una posibilidad, la destrucción de todo
aquello que contribuya al estado agéntico del
indivíduo frente a la prepotencia el Estado...

Fuentes

1.Ufw
http://usemoslinux.blogspot.com/2011/03/como-configurar-el-firewall-en-ubuntu.html

2. Avast
http://www.avast.com

3. Spybot Search And Destroy
http://www.forospyware.com/t10.html

4. Zemana Antilogger http://www.wadpod-ultimate.com/2013/05/zemana-antilogger-193450-final-espanol.html
http://www.mundodescargas.info/2012/04/zemana-antilogger-192941-detecta-y.html

5. Chrootkit – Rkhunter http://vijamaroylinux.blogspot.com.es/2010/06/dos-antirootkits-para-ubuntu-chkrootkit.html
http://www.taringa.net/posts/linux/12889237/Seguridad-Linux-

Rootkits---Como-Detectarlo-y-Eliminarlo.html
http://hayardillasenlared.blogspot.com.es/2011/01/antirootkits-para-linux.html

6. Riseup
https://www.riseup.net
https://www.mail.riseup.net

7. Firefox https://support.mozilla.org/es/kb/configuracion-de-la-privacidad-el-historial-de-nav

8. Seamonkey
http://www.proyectonave.es/productos/seamonkey/start/
http://paraisolinux.com/tienes-que-probar-seamonkey/

9. Tails
https://tails.boum.org/download/index.es.html

10. Proxychains
https://gnulinuxeros.wordpress.com/2011/09/22/conexiones-anonimas-proxychains/
https://es.wikipedia.org/wiki/Proxy
https://es.wikipedia.org/wiki/Proxy

11. VPN
http://hispanon.blogspot.com.es/p/eres-nuevo.html
http://www.linuxerz.org/2013/03/configurar-un-vpn-gratuito/
https://fity666.wordpress.com/configurar-vpn-para-navegar-anonimamente-en-ubuntu/

12. Thunderbird
http://www.atareao.es/ubuntu/firmar-y-cifrar-mensajes-con-thunderbird-en-ubuntu/
https://securityinabox.org/es/es/thunderbird_principal – Un poco distinto a como está explicado aquí.
https://www.mozilla-hispano.org/documentacion/Firma_y_cifrado_de_correos_electr%C3%B3nicos

13. Pidgin + OTR
https://securityinabox.org/es/pidgin_principal http://pidgin.im/download/ubuntu
https://www.pidgin.im/download
http://www.noticiasubuntu.com/cifrar-conversaciones-en-pidgin

14. Keepass
http://www.miniguias.com/miniguias/keepass-gestor-de-contrasenas-completamente-gratuito-y-sin-limites/
http://www.destroyerweb.com/manuales/keePass/keePass.htm

15. Kleopatra
www.gpg4win.org
http://gpg4win.org/download.html http://docs.kde.org/stable/es/kdepim/kleopatra/kleopatra.pdf

16. AESCrypt
http://www.gustavopimentel.com.ar/2011/01/aes-crypt-un-programa-para-encriptar-archivos-y-mucho-mas/
http://www.aescrypt.com/

17. TrueCrypt
http://www.taringa.net/posts/info/9244678/Encriptando-de-forma-muy-segura.html
https://sliceoflinux.wordpress.com/2009/03/20/ocultar-archivos-personales-en-ubuntu-810-con-truecrypt/
https://sliceoflinux.wordpress.com/2009/04/14/encriptar-el-pendrive-con-truecrypt-en-ubuntu-810/
https://securityinabox.org/es/truecrypt_volumenesocultos
http://www.kriptopolis.org/docs/tcmanual.pdf

18. Bleachbit
http://www.dragonjar.org/como-realizar-un-borrado-seguro-usando-bleachbit.xhtml
http://bleachbit.sourceforge.net/

19. Secure Delete
https://phyx.wordpress.com/2008/10/04/como-eliminar-archivos-permanentemente-y-de-forma-segura-en-linux/

20. Ccleaner
http://articulos.softonic.com/ccleaner-guia-de-uso
http://es.kioskea.net/faq/4381-tutorial-de-ccleaner

21. Registry Mechanic
http://www.pctools.com/utility/es/help/Registry_Mechanic/RM_Getting_Started.htm

22. Eraser
https://securityinabox.org/es/eraser_opciones
http://www.kriptopolis.org/eraser-borrado-seguro-windows

23. Shred
http://lamiradadelreplicante.com/2012/02/07/destruye-tus-archivos-de-forma-segura-con-shred/

24. Sobreescribiendo el Disco Duro
http://blogubuntu.com/como-borrar-completamente-un-disco-duro-en-linux

25. Recuva
https://securityinabox.org/es/recuva_principal

26. TestDisk y Photorec
http://blog.desdelinux.net/recuperar-archivos-borrados-facilmente-con-photorec-desde-la-consola/

27. Foremost
http://www.atareao.es/ubuntu/en-ubuntu-y-a-lo-csi-como-recuperar-archivos-borrados/

28. Scalpel
http://www.geekets.com/2009/03/recuperar-ficheros-con-ubuntu-kubuntu/

29. Seguridad Móvil
https://securityinabox.org/es/seguridadportatil

30. ¿Podemos fiarnos de TrueCrypt?
http://www.securitybydefault.com/2013/03/podemos-fiarnos-de-truecrypt.html

31. Hackers del FBI fracasan al intentar hackear TrueCryp
http://protegetuordenador.com/index.php/646-hackers-del-fbi-fracasan-al-intentar-hackear-truecrypt

32. Así descifra la Guardia Civil 'TrueCrypt', el nuevo sistema de encriptación de ETA: se ha pedido ayuda a la agencia de Seguridad de Obama
http://elconfidencialdigital.com/seguridad/049585/asi-descifra-la-guardia-civil-el-truecrypt-el-nuevo-sistema-de-encriptacion-de-eta-se-ha-pedido-ayuda-a-la-agencia-de-seguridad-de-obama?IdObjeto=24431

33. El FBI instaló puertas traseras en el programa de seguridad de OpenBSD
http://www.redeszone.net/2010/12/18/el-fbi-instalo-puertas-traseras-en-el-programa-de-seguridad-de-openbsd/

34. Proyecto PRISMA – Espionaje de Estado
http://tecno.americaeconomia.com/noticias/el-espionaje-de-eeuu-tambien-alcanza-9-importantes-companias-tecnologicas

35. Claves del espionaje Prisma. La red al descubierto
http://noticias.terra.es/claves-del-espionaje-prisma-la-red-al-descubierto,a593c93e2c75f310VgnVCM4000009bcceb0aRCRD.html

36. Inglaterra amenaza a Google con juicio por espionaje
http://www.blureport.com.mx/actualidad/inglaterra-amenaza-a-google-con-juicio-por-espionaje/

37. Tenemos que hablar de Facebook
http://www.nadir.org/txt/Tenemos_que_hablar_de_Facebook.html

"...AHORA SAL AHÍ FUERA Y HAZ ALGO DE LO QUE TUS ANCESTRAS Y DESCENDIENTES ESTARÍAN ORGULLOSAS..."

Rod Coronado