

GUÍAS I y II DE SEGURIDAD

GUÍA I.- CONTRA LA VIGILANCIA TECNOLÓGICA

1. CAMBIA EL SISTEMA OPERATIVO DE LA COMPUTADORA.

En vez de Apple OS X, Google Chrome OS, Microsoft Windows, se aconseja a los internautas recurrir a los siguientes:

Debian es una comunidad formada por desarrolladores y usuarios que mantiene un sistema operativo basado en software libre. Los contribuidores tienen que firmar un contrato social y adherirse al manifiesto ético. Las directrices estrictas de la inclusión garantizan que sólo el software de código abierto certificado esté empaquetado en los principales repositorios.

Fedora es una distribución Linux que se caracteriza por ser un sistema estable mantenido gracias a una comunidad internacional de ingenieros, diseñadores gráficos y usuarios que informan de fallos y prueban nuevas tecnologías. El proyecto no busca sólo incluir software libre y de código abierto, sino ser el líder en ese ámbito tecnológico.

Linux Mint Debian Edition (LMDE) o **(Maya-Canela)** es probablemente los de más sencillo uso para aquellos usuarios que ‘emigran’ de Microsoft Windows.

OpenBSD se concentra en la portabilidad, cumplimiento de normas y regulaciones, corrección, seguridad proactiva y criptografía integrada.

2. ESCOGE OTRO ANDROID

En vez de los muy conocidos Google Android y Google Play, existen:

CyanogenMod es una distribución personalizada, el firmware del mercado de accesorios para varios dispositivos Android.

Replicant es totalmente gratuito y funciona sin depender de un código del sistema de propiedad.

F-droid es una alternativa libre y de código abierto a la tienda de aplicaciones Google Play para Android.

3. SISTEMA IOS, ¿LANZAR EL DISPOSITIVO A LA BASURA?

El sistema operativo iOS no tiene alternativas. Se trata del sistema operativo propietario, cuyo código no está disponible para la auditoría por parte de terceros. Usted no debe confiar ni sus comunicaciones ni sus datos a un dispositivo de fuente cerrada.

4. CAMBIA DE NAVEGADOR

Los usuarios de Apple Safari, Google Chrome y Microsoft Internet Explorer pueden pasarse a los siguientes navegadores más seguros:

Tor Browser Bundle es un navegador, quizás un poco lento, pero anónimo.

Mozilla Firefox es un navegador rápido, flexible y seguro con ecosistema vibrante y abierto.

GNUZilla IceCat es una versión de Firefox con una gran lista aplicaciones libres y buenas características de privacidad.

Orbot es una versión de Tor para el sistema operativo Android.

5. USA UN BUSCADOR ALTERNATIVO

Si no quiere ser sometido al espionaje, los tres principales buscadores, Google Search, Microsoft Bing y Yahoo! Search, debería ponerlos en cuarentena y escoger algún otro buscador alternativo:

DuckDuckGo pone la privacidad en el centro de su política, prometiendo no recabar ni compartir información sobre sus usuarios.

MetaGer es un motor de búsqueda lanzado por la organización alemana sin ánimo de lucro SUMA, que proporciona resultados anónimos de búsqueda.

Startpage es un navegador que posee clústeres de servidores en los Países Bajos y Estados Unidos y proporciona la búsqueda anónima a través de un servidor proxy gratuito.

Seeks Project es una plataforma descentralizada y abierta para la búsqueda de colaboración.

YaCy es un motor de búsqueda gratuito, totalmente descentralizado: todos los usuarios de la red del motor de búsqueda son iguales y la red no almacena solicitudes de búsqueda del usuario.

6. EXPLORA EL MUNDO CON OTROS MAPAS

Si es usuario de aplicaciones de mapas como Apple Maps, Google Maps, Google Earth, Microsoft Bing Maps, puede pasarse a las siguientes alternativas:

OpenStreetMap, un proyecto colaborativo para crear mapas libres y editables, sin costos ocultos y sin licencia limitada y con transparencia.

Marble es una aplicación de globo terráqueo virtual y de código libre.

7. CAMBIA DE REDES SOCIALES

El asunto de las redes sociales es uno de los más difíciles, ya que aquí tendrá que escoger entre la privacidad o el uso de la red que usa la mayoría. Si escoge la primera opción, en vez de Google+, Facebook, LinkedIn y Twitter, puede optar por:

buddycloud, una red social federada de código abierto.

Diaspora es una red social en la que, a diferencia de algunas otras, no tiene que usar su identidad real. Puede interactuar con la persona que elija en la forma que desee.

Friendica es una red social federada de código abierto que tiene como prioridad la privacidad.

GNU Social es una red social descentralizada que puede ser instalada en su propio servidor.

Lorea es un proyecto de desarrollo de redes sociales federadas, seguras y autogestionadas creado íntegramente con software libre. Se trata de una red virtual pensada por y para la sociedad civil y los colectivos de transformación social y política.

Movim es una red social descentralizada, completamente basada en software libre, diseñada con la motivación de poder tener el control sobre su información.

pump.io es un servidor de flujos sociales auto-hospedado.

Salut à Toi comprende un conjunto de herramientas de comunicación multipropósito, con varias interfaces.

Tent es un protocolo de la red social autónomo y libre.

RetroShare es una plataforma de compartimiento de archivos y comunicación libre y segura.

8. OJO CON LAS VIDEO-CONFERENCIAS TELEFÓNICAS

Jitsi es un cliente de mensajería instantánea totalmente libre, abierta y seguro que permite realizar llamadas de voz y videoconferencias, entre otras características.

Mumble es un chat de voz cifrado de baja latencia. <http://www.mumble.com/mumble-download.php>

CSipSimple es una configuración gratuita para recibir y hacer llamadas desde un móvil Android con Voip.

RedPhone es una configuración para hacer llamadas seguras para Android.

9. CAMBIAR DE SERVICIOS DE ELABORACIÓN DE DOCUMENTOS

Si prepara y almacena sus documentos en servicios de alojamiento de archivos, como Google Docs, Microsoft Office Web Apps o Zoho Office Suite, se le aconseja pasarse a otros más seguros:

pad.riseup.net es un servidor auto-gestionado que da servicio a multitud de movimientos sociales de todo el mundo.

etherpad es un editor web basado en la colaboración en tiempo real, lo que permite a los autores editar simultáneamente un documento de texto y ver a todos los participantes de las ediciones en tiempo real, con la posibilidad de mostrar el texto de cada autor de diferente color.

Ethercalc es un servidor de hojas de cálculo multiusuario.

10. USAR HOSPEDAJES SEGUROS PARA PUBLICAR ARCHIVOS DIGITALES

Noblogs.org es una plataforma de blogging, un lugar virtual donde cualquiera puede abrir un blog o un sitio y conocer a otras personas que comparten aficiones parecidas.

GNU MediaGoblin es una plataforma de software libre para alojar y compartir multimedia digital con el objetivo de proporcionar una alternativa extensible, adaptable, descentralizada y libre de restricciones de derechos de autor a otros servicios de internet relativos a la publicación de contenido informático.

Piwigo es una aplicación de gestión de álbumes de fotos web de código abierto.

WordPress es una plataforma auto-hospedada para álbumes fotográficos.

Zenphoto es una aplicación para publicar en Internet galerías fotográficas en línea, diseñada para ser “un simple álbum fotográfico web”.

11.- USAR CUENTAS DE CORREO SEGURAS

Servidores anónimos e independientes que ofrecen correo electrónico y otros servicios con políticas similares.

ecn.org (ECN es un lugar para relacionarse y estar en contacto con gente a la que los cambios profundos en nuestras sociedades han dispersado, un lugar donde encontrar personas que no se rinden a la uniformidad ideológica y marginalidad actual, entre personas que buscan crear un movimiento real, capaz de cambiar las cosas – Italia)

indivia.net (Listas de correo, streaming de audio, alojamiento web, IRC, correo electrónico, foros, DNS dinámico en un servidor independiente verde cuyo nombre significa “ensalada de endivias” – Italia)

oziosi.org (Oziosi.org reconoce la pereza, la lentitud y la ociosidad a la que tranquilamente pueden aspirar hombres y mujeres – Italia)

free.de (Un proyecto alemán histórico que ofrece cuentas de correo, listas de correo, y alojamiento web para activistas – Alemania)

resist.ca (El colectivo Resist! es un grupo de activista de Vancouver que trabaja para proveer servicios técnicos y comunicaciones, información y educación para la comunidad activista. El colectivo Resist! (Resist!) y el proyecto resist.ca crecieron a partir del viejo colectivo TAO – Canadá)

riseup.net (riseup.net provee de correos electrónicos, listas y alojamiento web para tod*s aquell*s trabajando en el cambio social liberador. un proyecto para crear alternativas democráticas y prácticas de auto-determinación a través del control seguro de los medios de comunicación – u.s.a.)

squat.net (squat!net es una revista internacional con las casas ocupadas como tema principal, ofreciendo servicios de internet a espacios liberados – Países Bajos)

so36.net (servidor independiente – Alemania)

nadir.org (Un proyecto en pos de una revisión de los principios de la Izquierda a través de la creación de espacios de comunicación e información – Alemania)

boum.org (servidor anónimo e independiente – colectivo radicado en Francia)

antifa.net (espacios web gratuitos para grupos antifascistas y anti-racistas – Bélgica)

freaknet.org (un laboratorio para experimentar tecnologías de la información – catania, sicilia, Italia)

interactivist.net (un esfuerzo colaborativo, un recurso de comunicación activista, un proyecto de medios independientes y un proyecto para compartir tecnologías – u.s.a.)

linefeed.org (Linefeed desarrolla plataformas tecnológicas para comunidades involucradas en proyectos socialistas del siglo XXI, así también como en aquellos

campos de la tecnología en donde las reglas sociales se están re-escribiendo rápidamente – u.s.a.)

mutualaid.org (un servidor para comunidades radicales – u.s.a.)

nodo50.org (un servidor autónomo – España)

www.r23.cc (r23 es un sistema de emisión de audio y vídeo continuo y permanente. Software libre hecho por personas invirtiendo su conocimiento y esfuerzo para establecer estilos de vida que no estén controlados ni sean corporativos – España)

tactic.org (Tactic.org es la iniciativa de un pequeño grupo radicado en Montreal. Con un espíritu de ayuda mutua, proveen algunos servicios de internet para sus comunidades locales – Canadá.

tao.ca (tao.ca es un grupo anarquista de un pequeño colectivo de área de Toronto conocido como OAT, que evolucionó desde el TAO en Toronto y está relacionado con otros grupos activistas como resist.ca e interactivist.net – Canadá)

12.- PREFIERE LA ENCRIPCIÓN DE COMUNICACIONES POR E-MAIL

USA OTRA ALTERNATIVA QUE NO SEA PGP de la empresa (**SYMANTEC**).

El programa de encriptación libre de fácil descarga se llama:

gpg4 Win.- Descargarlo. Seguir el instructivo.. Hacer copia de seguridad. Poner el nombre completo de uno y el correo para generar el código. Guardar el archivo en el disco “C” El archivo es uno de tipo (“asc”)

PARA ABRIR ARCHIVOS tipo (asc) descargar este otro programa.

Notepad++ Instalarlo seleccionar el archivo de respaldo y abrirlo, ahí aparecerán las claves públicas y privadas.

NOTA: TODO SITIO CERRADO REPRESENTA UN RIESGO, USA LIBRES. (free)

GUÍA II DE SEGURIDAD

Por Razón del Nivel de Actividad Personal o Grupal. CONTRA LA VIGILANCIA FÍSICA

ANTECEDENTES: “EL gran hermano el “ESTADO” te vigila, más que nunca antes.” En incontables maneras, la vigilancia emerge como la forma dominante en cómo el mundo se organiza a sí mismo. La seguridad es vital para el triunfo y la sobrevivencia de

cualquier movimiento social. Esto es porque tenemos un enemigo que activamente trabaja en sabotearnos, neutralizarnos y finalmente destruirnos. Fallar en lo que a seguridad personal puede ser la diferencia entre la victoria y la derrota, libertad o aprisionamiento, vida o muerte. No solo para uno mismo, sino también todos los que nos rodean.

PUNTOS DE PARTIDA

- 1.- La no colaboración con las instituciones de los agentes de gobierno es un buen punto de partida. No discutir actividades futuras en un mitin o espacio público. Mantén controlado el acceso a llaves, documentos, fondos, equipo, etc. entre las manos de los miembros confiables. Hacer duplicados de documentos/información importante, etc., y guárdalos en una locación segura y secreta. Establece un grupo con miembros de confianza evitar infiltración de personas informantes.
2. Discute directa y abiertamente con la forma y contenido de lo que haga o diga cualquiera, si es un sospechoso de ser un agente, o tiene problemas emocionales, o es simplemente iluso.
3. Mantente alerta gente que constantemente están avocando por riesgosas acciones.
4. No aceptes todo lo que escuchas o lees. Revisa con fuentes confiables la información antes de actuar. Comunicación personal entre miembros confiables pudieron prevenir o limitar muchas operaciones riesgosas.
5. No reproduzcas rumores dañinos acerca de otros- habla con amigos confiables (o miembros de grupos responsables de lidiar con intervenciones encubiertas). Evita los chismes de otros, especialmente en las telecomunicaciones.
6. Verifica y revisa varias veces todos los arreglos de hospedaje, transporte, habitaciones de reuniones, etc., para asegurarse que no han sido canceladas o cambiadas por otros.
7. Documenta todas las formas de abuso, robos, asaltos, redadas, arrestos, vigilancia, intentos de reclutar informantes, etc. para identificar patrones y objetivos. Esto también puede ser usado como reportes y defensa legal.

8. NO hables del proyecto con ningún extraño por muy amigo que quiera ser.
9. Alerta a otros similares proyectos si es que hay abusos de la autoridad. Esto hace que otros grupos estén atentos a la represión y puede limitar un abuso mayor a través de la exposición y denuncia pública.
10. Prepara a otros miembros del grupo para que sigan organizando por si se lo impiden a uno de los “líderes”, etc. Esto incluye compartir conocimientos y habilidades, contactos públicos, etc.