Bisoños Usuarios de GNU/Linux de Mallorca y Alrededores | Bergantells Usuaris de GNU/Linux de Mallorca i Afegitons

Cap.1: Introducción GnuPG
Necesidad y guía rápida de 7 pasos

Per **René Mérou**, ***H*** (http://h.says.it/)
Creado el 10/02/2003 22:17 modificado el 10/02/2003 22:17

*Este artículo es una introducción para conocer el **por qué es necesario proteger la privacidad** y una guía rápida para preparar en unos pocos minutos nuestro ordenador para poder usar nuestro GPG, solo, o con nuestros clientes de correo.*

Cap.1: Introducción GnuPG

Necesidad y guía rápida de 7 pasos

Introducción: Esto es una introducción para saber por qué es necesario proteger la privacidad y una guía rápida para para preparar en unos pocos minutos nuestro ordenador para poder usar nuestro GPG, solo, o con nuestros clientes de correo.

Índice

Este documento es la primera entrega de tres que estamos escribiendo y contiene los dos bloques principales que a continuacións ponemos con enlaces.

Necesidad

Para hablar de la problemática de la privacidad he dividido el problema en los peligros de siempre y en los peligros nuevos.

Peligros Históricos

Desde el principio de las civilizaciones se ha deseado influir lo que piensa el pueblo. Los Acadios, el primer imperio, ya inventaron el primer sistema para difundir sus mitos y sus propagandas. Eran unos rodillos que al pasar sobre barro dejaban marcadas unas figuras que representaban a los dioses y a los reyes y sus cortes dentro de unos roles que mantenían la estructura sociopolítica. Poco futuro podría tener quien se opusiese a la versión oficial y "pretendiese corromper al pueblo" diciéndoles que el Rey no estaba refrendado por Dios o que éste no existía. Recordemos que la condena a Sócrates era por la acusación de pervertir a los jóvenes y negar los dioses cuando en realidad lo que intentaba era examinar todo y a todos bajo su rigurosa crítica.

Tales de Mileto[8], considerado el primer científico y el primero en la lista de los 7 sabios de la antigüedad, estuvo a punto de ser acusado de brujo por predecir un eclipse. Este hombre dejó una idea para la posteridad que iba a cambiar el mundo: la naturaleza no obedece al capricho de los dioses sino a leyes eternas que podemos entender. Lo extraño no es que no lo juzgasen por brujo sino que no lo matasen o algo peor. Menos mal que Grecia era algo muy especial en aquella época.

Al otro lado del mar unos siglos después, el último de los sabios de la biblioteca de Alejandría, que era mujer, Hypatia, fue despellejada viva con conchas por los cristianos seguidores del obispo Cyrilo que es considerado santo pues se le canonizó pocos años después.

Dentro del saber popular, a medida que pasaron los siglos, se fue generando la idea de que es un escaso bien el decir la verdad a la gente. Tanto que si rastreamos palabras importantísimas en los vocabularios y creencias de las gentes de hace más de 200 años encontramos ese desprecio al engaño y la propaganda. Por ejemplo la palabra Mártir en su origen griego y su equivalente Shahid de origen árabe comparten una idea clave: decir la verdad. En realidad ambas palabras designan algo más que aquel hombre que muere en manos de los enemigos de su fe y que alcanza por ello el paraíso. Las dos palabras traducidas directamente significan testigo. Martirio y Shahada, es la muerte dando testimonio de fe, y a la vez, la muerte testificando la verdad. Muhammad Ibn Abdullah (Mahoma) dijo: "El mayor Yijad es decir la verdad ante una autoridad injusta" (Yijad, literalmente esfuerzo, entendido como una entrega a Dios de hasta la propia vida)

Llegó la inquisición y no se libraron de ella ni los libros. Copérnico esperó a poco antes de morir para publicar un libro que describía las órbitas de los planetas en torno al sol porque sabía lo que le supondría. Lutero más tarde dijo de él: "un astrólogo advenedizo que pretende probar que es la Tierra la que gira, y no el cielo, el firmamento, el Sol o la Luna (...). Este loco echa completamente por tierra la ciencia de la astronomía, pero las Sagradas Escrituras nos enseñan que Josué ordenó al Sol, y no a la Tierra, que se detuviese".

Ibn Rushd[9] (Averroes, nuestro famoso médico, matemático, astrónomo, jurisprudente y filósofo musulmán de la Córdoba del siglo 12) también tuvo que sufrir ser proscrito y ver quemados sus libros. Más tarde resultó ser la inspiración que dio origen a la separación entre la filosofía y la verdad religiosa en los escolásticos. Fue así aunque él no dijese sino que la filosofía era la cumbre de la religión y esta última, más adecuada y sencilla para los no filósofos, para el pueblo; lo que realmente era llegar muy lejos. Imaginaros alguien de sus tiempos, religión y oficio (juez civil) diciéndolo, hay que tener coraje. Este hombre reabrió la puerta a la especulación griega gracias a su "hablar libremente con los verdaderos filósofos".

Galileo, católico creyente, enviaba libros por contrabando a Holanda para que se los publicasen. Incluso a Kepler, protestante pero igual de creyente, con quien mantenía una profunda amistad, le enviaba cartas con mensajes cifrados. Por ejemplo cuando descubrió que Venus también tenía fases como la luna le envió una carta con un mensaje cifrado que nadie podía leer, para poder demostrar más adelante que el era quien lo había descubierto. Sí, Galileo juzgó útil cifrar su mensaje, y con razón me atrevería a afirmar. No olvidemos que a Miguel Servet[10] se le había quemado vivo igual que a Giordano Bruno[11].

De Darwin[12] dijeron de todo y le atacaron cuanto pudieron, menos mal que ya eran otros tiempos. Pero todavía hay gente que lo insulta como una forma de defender sus propias creencias religiosas. Porque claro, o Darwin y buena parte de la ciencia actual están profundamente equivocados (hoy en día es tal la evidencia que le apoya que es absurdo afirmarlo) o no hay ya, otra forma razonable de defender la veracidad del creacionismo de casi todas las religiones.

Sobre los anteriores científicos o inclusos sabios y sus aportaciones, se puede decir que lo mucho que dieron a la humanidad, lo pudieron dar por no tener un policía 24 horas al día controlando y vigilando. Éstas personas no hubiesen podido publicar sus grandes ideas sin encontrar al menos algún resquicio de privacidad para poder producirlas y enviarlas. Y por tanto, es razonable decir que el derecho a la privacidad es aun más básico que el de la libertad de

expresión la precede y condiciona. En una frase: **Sin privacidad no hay libertad**.

Intolerancia, integrismo, sectarismos y persecuciones se dan en todo, porque el origen no es una religión, el origen en mi opinión, somos nosotros mismos cuando nos falta formación personal en los correspondientes valores. En el siglo XX la Unión Soviética, un estado bastante ateo, también tuvo sus persecuciones y no sólo contra las religiones. En los juicios de Stalin se acuso de traidores a los que le pudieran hacer sombra políticamete hablando. El Integrismo, la intolerancia y el sectarismo es especialmente dañino cuando llega al poder para imponer su forma de ver la vida a los demás y, aunque no siempre, suele ir de las manos de alguien que va a solucionar los problemas mostrando mucho carácter y vehemencia. Ya lo decían los latinos “ubi dubitum ibi libertas” (donde hay duda hay libertad), demasiada falta de dudas es muestra de intolerancia.

Acercándome ya a nuestros tiempos, es interesante el recordar que hasta la policía del dictador Franco, tenía listados de personas con su historial personal. Cuando al fin acabó la dictadura, no faltó quien quiso publicarlas para dar a conocer lo odioso y repugnante de tales prácticas completamente arbitrarias. Y especialmente lo rechazable que es elaborar listas de personas que participan en actividades mal vistas por el régimen. Listas que pudieran ser objeto de revisiones en momentos en que se solicite algo oficialmente, como un permiso de construcción o una publicación o un visado. Estas prácticas provocan la desaparición de la igualdad ante la ley. Para evitarlas se redactaron en la Constitución Española claras protecciones[13] contra este tipo de abusos, tanto de empresas como de gobiernos. Pero, claro, pasado el tiempo y olvidado el peligro, la propia constitución se vuelve papel mojado y hasta al Rey le han grabado sus conversaciones telefónicas.

Peligros Actuales

Actualmente nadie planea poner un policía vigilando cada puerta o a cada persona pero ahora la tecnología permite entrometerse en lo que una persona escribe por correo electrónico a otra. Leerlo, retardarlo, hacerlo desaparecer o incluso manipularlo sin que se note.

Todos estas posibilidades entrañan peligros que pueden venir desde la competencia empresarial (que quiere conocer nuestras estrategias o nuestros secretos) hasta nuestro propio gobierno o incluso desde otros que no tengan impedimentos legales con los derechos de los ciudadanos extranjeros. No me meto ya en si los gobiernos pactan para compartir esos datos, que legalmente no pueden obtener, con sus aliados, lo que es un evidente desprecio a las propias leyes e instituciones y al propio pueblo.

Esos peligros, se pueden evitar con el uso de herramientas informáticas como el GnuPG que protegen nuestras comunicaciones.

Muchos piensan que lo que hay que hacer contra los ataques a nuestra privacidad, como el de la red Echelon[14] (que básicamente es una red que engulle millones de emails buscando palabras clave en busca de terroristas y otros elementos “no deseados”) es añadir al final de los correos palabras como: Bomba, terror, asesinar, matar, judíos, *Allah*, *Jihad*, goma 2, CIA, FBI, Pentágono, *Bin Laden* y otras que puedan levantar la sospecha de los programas que registra los correos. Piensan que si mucha gente lo añade inundarán de ruido al programa volviéndolo inútil.

Ese sistema, que dudo que pueda ser tan útil como sus partidarios defienden, me da pie a nombrar un importante peligro. Si se rastrean los emails y se obtienen listas de sospechosos con este sistema. ¿Qué se hará con esa lista de sospechosos? ¿Se mantendrá la presunción de igualdad ante la ley? ¿Se les tratará ? No, no son bromas, recordemos que los presuntos miembros de *Al Qaida* no tienen los derechos elementales que da la ley americana como el derecho a un juicio justo. Esa igualdad es lo más importante que dejaron como legado Washington y sus compañeros.

La actualidad trae noticias frescas continuamente de lo poco que valoran nuestra privacidad nuestros gobiernos y sobretodo nuestras paranoicas agencias de seguridad. Véase como ejemplo el extraño interés del gobierno en que se guarde toda la información de nuestras comunicaciones durante una año. La desafortunadamente famosa LSSI[15].

Dos ejemplos actuales, extraídos de las noticias más votadas de Yahoo[16] (primer y tercer puesto), de lo que viene desde fuera y contra lo que no protestará nuestro gobierno a pesar de que nos afecta:

1. Primero asoma un empeoramiento de las limitaciones a la privacidad levantadas a partir del 11S: El nuevo Patriotic Act[17] Información que parece que se les ha escapado de las manos. O será quizás una prueba para ir viendo si ya es hora de dar una vuelta más a la tuerca, según la reacción popular.

2. Y la otra que parece un broma pero no lo es: Bush planea aumentar la violación de nuestra privacidad con algo que ha llamado la TIA[18]. No se trata de Mortadelo dando el cambiazo de una radio de coche por un loro, se trata del presidente de los USA y pretende cambiar privacidad por "seguridad".

Esta clase de peligros de origen político, también son evitables con el uso del GnuPG. Los gobernantes no pueden encontrarse con una situación de facto donde una gran cantidad de gente utiliza el cifrado en su correo personal (o en sus comunicaciones) e intentar imponer una ley en contra. De hecho el uso del cifrado en los mensajes personales suele conllevar un reconocimiento sobre lo importante de proteger el derecho a la intimidad. Hay no obstante otro importante motivo para el uso del cifrado, es una herramienta muy útil en las transacciones económicas y eso quizás sea una presión más importante para los gobiernos, como el Francés que tenía prohibido el uso de sistemas de cifrado.

En países con serias limitaciones a la libertad como Guatemala o China, organizaciones como la American Association for the Advancement of Science's Cryptography, Scientific Freedom, and Human Rights[19] entrenan a activistas de los derechos humanos para que puedan usar los sistemas de cifrado de emails. Los activistas que son perseguidos y torturados usan estas tecnologías para poder enviar información peligrosa a sus colegas.

En mi opinión, y en la de mucha gente más valor y saber, igual que nadie envía un extracto del libro de cuentas de una empresa en una postal de correo, porque todo el mundo podría leerlo; **los emails como las cartas deben ir firmados y cerrados.**

Eso resulta muy sencillo actualmente si se siguen unos pocos pasos, como a continuación se verá.

La guía rápida de los 7 pasos

Introducción

Primero quiero dar una muy ligera idea de cómo funciona y después dar los pocos pasos que se necesitan para tener el sistema en pleno funcionamiento, compartiendo claves públicas con amigos y usando servidores de claves del programa GnuPG.

Utilizaremos el GnuPG por que es el programa más utilizado por la comunidad del Software Libre y el más instalado en las distribuciones del Gnu/Linux y no necesitaremos la ayuda de programas que lo faciliten con entornos visuales sencillos. Así sirve de base como capítulo de introducción de la serie y se ve mejor lo que realmente está sucediendo.

Pero si se desean las máximas facilidades existen entornos de usuario más sencillos y disponibles también para windows. Se pueden encontrar en la web del GnuPG[20] o la propia de Zimmerman[21] donde distribuye el programa PGP.

Cómo funciona (muy escuetamente)

Se crea un par de claves con las que se establece la comunicación, la pública (candado) y la privada(llave). Las claves son intercambiables lo que produce otras interesantes posibilidades que no comentaremos en este artículo. Dejamos para la continuación en otros dos artículos el profundizar en las posibilidades del GnuPG y en su fundamentación algorítmica y matemática.

Entonces, cuando se desea enviar un mensaje a alguien **lo que hace el programa de correo es utilizar su clave publica para cifrarlo, y gracias al algoritmo,** que es seguro según nos garantiza el tiempo que hace que es de código abierto sin que nadie le haya encontrado ninguna debilidad, **sólo la clave privada puede abrirlo**.

Los programas de correo normalmente también nos permiten firmar un mensaje para asegurar quién es el autor y que nadie lo ha modificado.

Y al grano: Los 7 pasos.

1- Generar

Supuesto que tenemos instalado el GnuPG con la versión 1.0.7 o superior. (Comprobable usando gpg --version)

gpg --gen-key

Entonces tendremos que responder a una serie de preguntas:

-¿Tipo de clave? Elige la opción predeterminada, la **1**.

-¿Longidud de la clave? Yo pongo 4096, pero se recomienda la de 2048. (Si la sobrepasas te pide confirmación del tamaño, se dice que sí, y listos.)

-¿Caducidad? Pon 1y (un año), que es lo aconsejado y más si es tu primer par de claves. Si sólo es para probar un momento, con poner un dos, que significa dos días, irá bien.

-¿Nombre? Si pones tu nombre bien, cuando des el fingerprint (luego lo comento) podrás identificarse mostrando tu DNI. (No pongas el DNI ni ningún dato privado, porque luego es información accesible públicamente.)

-¿Email? No te preocupes si tienes más de uno, que luego ya podrás ir añadiéndolos y no cometas el error típico de añadir texto para evitar el spam.

-¿Comentario? No pongas demasiado texto. Luego confirma que los datos que te muestre sean correctos.

-¿Frase de contraseña? Te aconsejo una que tenga al menos 4 palabras (no todas presentes en el diccionario) y que te resulte cómica, será más fácil luego recordarla.

Normalmente para seleccionar una clave se pone el email pero en caso de que haya varias con los mismos datos, para saber tu uid pon gpg --list-keys.

Lo que te mostrará una lista de claves que empiezan con algo como esto:

pub 1024D/**AA8E6A57** 2002-09-01 H.says.it (Sin privacidad no hay libertad) <list@@ono.com>

Si corresponde con tus datos la zona que he marcado en verde es tu uid, en mi caso es **AA8E6A57**. (He añadido una @ en el email para evitar publicidad no solicitada que busque correos en Bulma. Pero vosotros no lo hagáis.)

2-Certificado de revocación

Créate un certificado de revocación por si lo necesitas más adelante. (En vez de poner al final mi uid pon el tuyo, recuérdalo para todo el documento.)

gpg --output cert_revoc_arch.asc --gen-revoke -armor aa8e6a57

Te preguntarán el por qué revocas la clave, mi respuesta: El 3, clave que ya no se usa, y en el texto he indicado "certificado por si pierdo la clave o el password." Después te pide el password y te responde "ASCII armored output forced." "Revocation certificate created."

Si más adelante se necesita activar definitivamente la revocación, sólo entonces habrá que importarla (**gpg --import cert_revoc_arch.asc**) y luego enviarla al servidor (**gpg --send-keys aa8e6a57**).

3-Enviar la clave publica al servidor

Primero editamos el fichero el fichero ~/.gnupg/gpg.conf (o el ~/.gnupg/options en las versiones anteriores al gpg 1.2.2) y buscamos la línea donde está el keyserver que probablemente esté comentada, tiene que quedar así:

keyserver hkp://subkeys.pgp.net (antes usaba pgp.rediris.es en España, pero me dejo de funcionar)
Ya que estamos, es un buen momento para instalar el gnupg-agent (apt-get install gnupg-agent) y añadir (o descomentar) dentro de gpg.conf la línea la siguiente:

use-agent

Y ahora ya podemos ponernos en contacto con el servidor de claves para enviar la clave:

gpg --send-keys aa8e6a57

4-bajarse la clave de alguien

Es tan sencillo como poner: (con el uid de quien buscas, si tienes su fingerprint son las últimos 8 caracteres)

gpg --recv-keys aa8e6a57

5-Fingerprint

Para conocer el fingerprint o huella digital de una clave basta con poner:

gpg --fingerprint aa8e6a57

Debemos hacer eso con las claves que recibamos para comprobarlas antes de firmarlas y con la propia para obtener el texto que luego podemos dar en mano impreso en un pequeño papel.

6-Firmar una clave

Si quieres poder enviar un correo cifrado te conviene firmar la clave del destinatario. ATENCIÓN, no puedes hacerlo si no tienes la completa seguridad de que es suya y recibirla mientras chateáis por Internet no da esa seguridad. Que te la dé en mano o su fingerprint y tras asegurarte de que es quien dice que es (si hace falta le miras el DNI) y de que el fingerprint corresponde con el de la clave que te has bajado, entonces si puedes firmarle la clave así:

gpg --sign-key aa8e6a57

No hay que olvidar enviar las claves firmadas para que la firma pueda servir al dueño. Con gpg --send-key uid-firmado o con caff (del paquete signing-parties)

Problema: Él está en Madrid y yo en Canarias y necesito enviarle un email cifrado hoy mismo, no hay tiempo de que me pase en persona (o lea por teléfono) el fingerprint. Solución: Fírmale de forma que no se exporte la firma. Se trata de firmar la clave con gpg --edit-key aa8e6a57debes poner lsign (de local, esa no se exportará a los servidores.) Ese modo también te permite firmar como antes con un sign.

7-Clientes de correo

Una vez que hemos enviado nuestra clave al servidor y nos hemos bajado las de algunos amigo ya podemos enviarnos correos cifrados o firmados. Os indico como configurar algunos clientes, el Kmail, el Evolution y el Mutt para con un clic cerrar los emails a los ojos mal educados tras firmarlos.

Evolution:

En Herramientas/setings/eligiendo una cuenta de correo/editar/ en la etiqueta de security hay que poner el uid. Y la cuenta de correo debe ser la misma que se indicó al crear la clave o una añadida posteriormente editándola y seleccionando adduid. Mejor tener seleccionado el “siempre cifrarme a mí mismo cuando envíe correo cifrado”

Kmail:

Configurar Kmail/identidades/modificar pestaña cifrado donde pone clave OpenPGP poner el uid. También ponerla en clave de cifrado OpenGPG para cifrar a uno mismo. Luego en Configurar Kmail, en seguridad, seleccionar OpenPGP y si teneis s/mime también, dejar dentro todo por defecto creo que va bien.

Mutt:

Hay que editar el archivo .muttrc para añadir la siguiente línea (el 0x del principio es necesario):

set pgp_sign_as="0xaa8e6a57"

Otros:

Hay 19 clientes de correo más que pueden usar el PGP y sería muy extenso incluirlos aquí todos. También hay múltiples utilidades, podéis encontrar más información de todo ello en el apartado Interfaces de Usuario[22] de la web del GnuPG.

Conclusión

La privacidad no es un derecho por el que se preocupa un grupo de pirados, su importancia es evidente del hecho de que se creyese necesario reflejarlo en la Constitución Española y en muchas otras.[23] Es porque es algo muy importante que necesita ser protegido activamente. Y no me extrañaría que muchas veces se incluyese en las constituciones porque además de ser de lo más importante es un peligro que puede venir de malos gobiernos que cambian o reinterpretan las leyes con demasiada facilidad. No hay más que acudir a la historia para ver lo mucho que se ha deseado controlar las comunicaciones y lo mucho que ha luchado la democracia (y la ciencia) para impedir que se limiten.

La seguridad no es un estado, es un proceso. Es mejor no dejar de lado demasiado tiempo este interesante tema. Una vez que se tiene el sistema funcionando necesita, de vez en cuando, ser mantenido (con gpg --refresh-keys y gpg --check-trustdb) y siempre hay consejos sobre las claves, conocimientos sobre el algoritmo, funciones desconocidas, nuevas aplicaciones que las implementan... La criptografía es apasionante.

Por último quiero remarcar estás dos frases que, en la época que nos ha tocado vivir, están muy relacionadas.

- **Sin privacidad no hay libertad**.
- **Los emails como las cartas deben ir firmados y cerrados.**

Referencias

Sobre la privacidad

Base de Datos Políticos de las Américas. (1998) Privacidad personal y familiar. *Análisis comparativo de constituciones de los regímenes presidenciales* [Internet]. Georgetown University y Organización de Estados Americanos. En: http://www.georgetown.edu/pdba/Comp/Derechos/privacidad.html[23]. 8 de febrero 19103.

Carnivore FAQ[24] En español.

Nautopía[13] Acerca de lo que dice nuestra constitución sobre la privacidad.

Total Information Awareness (TIA) System.[25] En inglés.

Bush Database Plan Raises Privacy Concerns[18]. En inglés.

El nuevo Patriotic Act.[17] En inglés

Kriptopolis (ciberderechos).[26] En español

Electronic Frontier Fundation.[27] En inglés.

Sobre el uso del GnuPG

La completa, el man. En el Konqueror y otros navegadores en lugar de http:.... poner man:gpg[28] que es más o menos lo mismo que poner **gpg --help**.

Una web muy interesante para ver estadísticas y caminos para tener confianza entre una llave y otra: PGP pathfinder & key statistics[29]

Generador de gráficas GPG[30] Artículo de Celso en Bulma

GPG. Preguntas y respuestas rápidas.[31] Otro Artículo de Celso.

El sitio oficial del GnuPG: GnuPG.org[32]

Y en especial su apartado Interfaces de Usuario[22] donde se enlazan 22 clientes de correo que pueden usar el PGP además de dar otras interfaces como clientes de mensajería instantánea o programas para plataformas windows y mac.

Privacidad en correos electrónicos con GPG.[33] En español.

Texto muy breve, que muestra como generar llaves, administrarlas, ...[34] de rkc.

Mutt y GPG en 5 minutos.[35] Artículo también de Celso en Bulma

Integración de PGP y Mutt.[36] Muy interesante y completo (tanto esa página como la siguiente sobre macros).

muttrc-> Command formats for gpg. (This version uses gpg-2comp)[37] (en inglés) Lo he encontrado muy completo.

Relacionados

Este artículo ha sido citado en la web de LinuxBCN[38] aquí[39] por Joan.

Comentarios

Por último, pediros que si encontráis algún error (aunque sea un simple fallo tipográfico) me enviéis un email para que lo corrija.

Lista de enlaces de este artículo:

1. http://bulma.net/body.phtml?nIdNoticia=1684&nIdPage=2
2. http://bulma.net/body.phtml?nIdNoticia=1684&nIdPage=3
3. http://bulma.net/body.phtml?nIdNoticia=1684&nIdPage=4
4. http://bulma.net/body.phtml?nIdNoticia=1684&nIdPage=5
5. http://bulma.net/body.phtml?nIdNoticia=1684&nIdPage=6
6. http://bulma.net/body.phtml?nIdNoticia=1684&nIdPage=7
7. http://bulma.net/body.phtml?nIdNoticia=1684&nIdPage=8
8. http://www.geocities.com/gflaubert/cas/hist001.htm
9. http://www.geocities.com/hisfilos/averroes.html
10. http://perso.wanadoo.es/icsalud/servet.htm
11. http://www.agongen.com/OF-Bruno.htm
12. http://www.agongen.com/OF-Darwin.htm
13. http://nautopia.coolfreepages.com/articulo18.htm
14. http://www.noticias.com/noticias/2001/0109/n01090651.htm
15. http://bulma.net/body.phtml?nIdNoticia=1581
16. http://personal.news.yahoo.com/us/news/categories/901/index.html
17. http://story.news.yahoo.com/news?tmpl=story&u=/ap/20030207/ap_on_re_us/anti_terr

18. http://story.news.yahoo.com/news?tmpl=story&u=/pcworld/20030206/tc_pcworld/10925
19. http://www.aaas.org/spp/crypto/
20. http://gnupg.org/
21. http://web.mit.edu/prz/
22. http://www.gnupg.org/(es)/related_software/frontends.html
23. http://www.georgetown.edu/pdba/Comp/Derechos/privacidad.html
24. http://amsterdam.nettime.org/Lists-Archives/nettime-lat-0109/msg00084.html
25. http://www.darpa.mil/iao/TIASystems.htm
26. http://www.kriptopolis.com/index.php?id=C0_1_1
27. http://www.eff.org/br/
28. http://man:gpg
29. http://www.cs.uu.nl/people/henkp/henkp/pgp/pathfinder/
30. http://bulma.net/body.phtml?nIdNoticia=2138
31. http://bulma.net/body.phtml?nIdNoticia=1483
32. http://www.gnupg.org/(es)/index.html
33. http://www.xtech.com.ar/articulos/gpg/html/node21.html
34. http://www.buanzo.com.ar/linux/70s-gpg.htm
35. http://bulma.net/body.phtml?nIdNoticia=1062
36. http://andressh.alamin.org/linux/Mutt-GnuPG-PGP-Como-6.html
37. http://security.dsi.unimi.it/~lorenzo/misc/mutt/gpg.mutt.html
38. http://www.linuxbcn.com/
39. http://www.linuxbcn.com/nuke/article.php?sid=496

E-mail del autor: ochominutosdearco _ARROBA_ gmail.com
Podrás encontrar este artículo e información adicional en: http://bulma.net/body.phtml?nIdNoticia=1684