



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

Disponible la nova versió de GnuPG (6099 lectures)

Per **Carlos Cortes Cortes**, [carcoco](http://bulma.net/~carcoco/) (<http://bulma.net/~carcoco/>)

Creado el 03/05/2002 22:45 modificado el 03/05/2002 22:45

S'acaba de lliberar la versió **1.0.7** de **GnuPG**, este programa es un criptosistema que substitueix completament a **PGP**, de forma que permetix realitzar entre altres coses comunicacions segures i almacenatge segur de informació. Sent ideal per a escriure i enviar e-mail's segurs, xifrats i signats, verificar claus, ...

"The GNU Privacy Guard (GnuPG) is GNU's tool for secure communication and data storage. It is a complete and free replacement of PGP and can be used to encrypt data and to create digital signatures. It includes an advanced key management facility and is compliant with the proposed OpenPGP Internet standard as described in RFC2440. This new release has a lot of features beyond OpenPGP which will be included in a soon to be published RFC2440 successor."

Característiques de **GnuPG**:

- Reemplaça totalment a PGP.
- No utilitza algoritmes patentats.
- Llicència GPL, codi font disponible.
- En alguns aspectes es millor que PGP i té algunes millotes en seguretat.
- Molt utilitzat per tot el mon. (es practicamente un estandard **de facto**).
- Es pot gastar com a programa de filtrat.
- Implementació total del [OpenPGP](#)⁽¹⁾.
- Desxifra y verifica missatges de PGP 5.x.
- Implementa els següents algoritmes: ElGamal, DSA, 3DES, Blowfish, Twofish, CAST5, MD5, SHA-1, RIPE-MD-160 i TIGER.
- Fàcil implementació de nous algoritmes utilitzant mòduls d'extensió.
- L'identificador d'usuari es genera amb el format estandar.
- Implementació de data caducitat.
- Suport per al castellà, rus, portugués, polaco, italià, alemany, francès i anglès entre altres.
- Complet sistema de ajuda
- Receptors opcionals de missatges anònims.
- Suport integrat per a servidors de claus **HKP**
- ...

La llista de **novetats** i de **bugs** que soluciona esta nova versió es realment impresionat, per el que es molt recomanable l'actualització a la nova versió **GnuPG 1.0.7**

[Announce] **GnuPG 1.0.7 released**: <http://lists.gnupg.org/pipermail/gnupg-announce/2002q2/000251.html>⁽²⁾

GnuPG es multiplataforma i hi ha informes de que funciona perfectament en el següents sistemes operatius i plataformes (encara que segur que funciona perfectament en moltíssimes més ;-):

- **Linux** x86, alpha, sparc64, m68k, i/o PowerPC.
- **FreeBSD**
- **OpenBSD**
- **NetBSD**
- **HPUX** v9.x y v10.x con UCP HPPA
- **IRIX** v6.3 con UCP MIPS R10000



- **OSF1** V4.0 con UCP Alpha
- **OS/2** versión 2.
- **SCO UnixWare/7.1.0.**
- **SunOS, Solaris** para Sparc y x86
- **USL Unixware** v1.1.2
- **Windows 95 and WNT** con UCPs x86.

En principi **GnuPG** s'utilitza a través de la línia de consola, però existixen un munt de [frontends](#)⁽³⁾ gràfics que simplifiquen notablement l'ús del **GnuPG**, com el potent [GPA - The GNU Privacy Assistant](#)⁽⁴⁾. **GnuPG** moltes vegades el trobareu escrit com a simplement **gpg**.

Credits

GNU Privacy Guard ha sigut desenvolupat per l'equip de **GnuPG**: Matthew Skala, Michael Roth, Niklas Hernaes, Rémi Guyomarch, y Werner Koch. Gael Queri, Gregory Steuck, Janusz A. Urbanowicz, Marco d'Itri, Thiago Jung Bauermann, Urko Lusa, i Walter Koch es van encarregar de les traduccions. Mike Ashley està treballant en el Manual de GnuPG.

Les següents persones van ajudar molt suggerint millores, testejant, corregint errors, donant recursos, i altres faenes importants: Allan Clark, Anand Kumria, Ariel T Glenn, Bodo Moeller, Bryan Fullerton, Brian Moore, Brian Warner, Caskey L. Dickson, Cees van de Griend, Charles Levert, Christian von Roques, Christopher Oliver, Christian Recktenwald, Daniel Eisenbud, Daniel Koenig, David Ellement, Detlef Lannert, Dirk Lattermann, Ed Boraas, Enzo Michelangeli, Ernst Molitor, Fabio Coatti, Felix von Leitner, Frank Heckenbach, Frank Stajano, Gaël Quéri, Greg Louis, Greg Troxel, Gregory Steuck, Geoff Keating, Harald Denker, Hendrik Buschkamp, Holger Schurig, Hugh Daniel, Ian McKellar, Janusz A. Urbanowicz, James Troup, Jean-loup Gailly, Jens Bachem, Joachim Backes, John A. Martin, Johnny Teveßen, Jörg Schilling, Jun Kuriyama, Karl Fogel, Karsten Thygesen, Katsuhiko Kondou, Kazu Yamamoto, Lars Kellogg-Stedman, Marco d'Itri, Mark Adler, Mark Elbrecht, Markus Friedl, Martin Kahlert, Martin Hamilton, Martin Schulte, Matthew Skala, Max Valianskiy, Michael Roth, Michael Sobolev, Nicolas Graner, NIIBE Yutaka, Niklas Hernaes, Nimrod Zimmerman, N J Doye, Oliver Haakert, Oskari Jääskeläinen, Paul D. Smith, Philippe Laliberte, Peter Gutmann, QingLong, Ralph Gillen, Rat, Reinhard Wobst, Rémi Guyomarch, Reuben Sumner, Roland Rosenfeld, Ross Golder, Serge Munhoven, SL Baur, Stefan Karmann, Stefan Keller, Steffen Ullrich, Steffen Zahn, Steven Bakker, Susanne Schultz, Thiago Jung Bauermann, Thomas Roessler, Tom Spindler, Tom Zerucha, Tomas Fasth, Thomas Mikkelsen, Ulf Möller, Urko Lusa, Walter Koch, Wim Vandeputte i Gerlinde Klaes.

Este programa ha sigut possible gràcies al treball anterior de gent com: Chris Wedgwood, Jean-loup Gailly, Jon Callas, Mark Adler, Martin Hellmann Paul Kendall, Philip R. Zimmermann, Peter Gutmann, Philip A. Nelson, Taher ElGamal, Torbjorn Granlund, Whitfield Diffie, alguns matemàtics desconeguts del NSA, i tots aquells que han treballant molt dur per a crear sistemes operatius complets i lliures.

GnuPG (GNU Privacy Guard)

<http://www.gnupg.org/>⁽⁵⁾

Enllaços relacionats amb **GnuPG**:

- GnuPG documentation project (incluix el [Manual de Privacidad de GNU](#)⁽⁶⁾ (en castellà))
<http://www.gnupg.org/gph/es/>⁽⁷⁾
- "GNU Privacy Guard" (GnuPG) Mini Como
http://www.dewinter.com/gnupg_howto/spanish/⁽⁸⁾
<http://www.insflug.org/COMOs/GPG-Mini-Como/GPG-Mini-Como.html>⁽⁹⁾
- Substituir PGP 2.x por GnuPG
<http://www.gnupg.org/gph/es/pgp2x/t1.html>⁽¹⁰⁾
- Mutt-i, GnuPG y PGP Como (de **Andrés Seco**)
<http://andressh.alamin.org/linux/Mutt-GnuPG-PGP-Como.html>⁽¹¹⁾



- Como configurar Pine y GnuPG (gpg) en cipres (de **Rolando Abarca**)
<http://cipres.cec.uchile.cl/~rabarca/gnupg-cipres.html>⁽¹²⁾
- Comunicación Segura en Linux con GnuPG
<http://www.gacetadelinux.com/es/lg/issue60/sharma.html>⁽¹³⁾
- miniGuia de instalación/uso de GnuPG: firma y cifrado de clave pública
<http://perso.wanadoo.es/manel3/chuletas/I-gnupg>⁽¹⁴⁾
- Using GnuPG with Pine for Secure E-Mail
http://www.linuxsecurity.com/feature_stories/feature_story-83.html⁽¹⁵⁾
- Gnu Privacy Guard tutorial, part 1 (kuro5hin)
<http://www.kuro5hin.org/story/2000/5/1/17058/47630>⁽¹⁶⁾
- Gnu Privacy Guard tutorial, part 2 (kuro5hin)
<http://www.kuro5hin.org/story/2000/5/9/193916/2290>⁽¹⁷⁾
- Documentació de GnuPG
<http://www.gnupg.org/docs.html>⁽¹⁸⁾

--

\$ alias **carcoco**="echo Carlos Cortes"

http://bulma.net/todos.phtml?id_autor=132 ⁽¹⁹⁾

Lista de enlaces de este artículo:

1. <http://www.gnupg.org/rfc2440.html>
2. <http://lists.gnupg.org/pipermail/gnupg-announce/2002q2/000251.html>
3. <http://www.gnupg.org/frontends.html>
4. <http://www.gnupg.org/gpa.html>
5. <http://www.gnupg.org/>
6. <http://www.gnupg.org/gph/es/manual/book1.html>
7. <http://www.gnupg.org/gph/es/>
8. http://www.dewinter.com/gnupg_howto/spanish/
9. <http://www.insflug.org/COMOs/GPG-Mini-Como/GPG-Mini-Como.html>
10. <http://www.gnupg.org/gph/es/pgp2x/t1.html>
11. <http://andressh.alamin.org/linux/Mutt-GnuPG-PGP-Como.html>
12. <http://cipres.cec.uchile.cl/~rabarca/gnupg-cipres.html>
13. <http://www.gacetadelinux.com/es/lg/issue60/sharma.html>
14. <http://perso.wanadoo.es/manel3/chuletas/I-gnupg>
15. http://www.linuxsecurity.com/feature_stories/feature_story-83.html
16. <http://www.kuro5hin.org/story/2000/5/1/17058/47630>
17. <http://www.kuro5hin.org/story/2000/5/9/193916/2290>
18. <http://www.gnupg.org/docs.html>
19. http://bulma.net/todos.phtml?id_autor=132

E-mail del autor: carcoco_ARROBA_gmail.com

Podrás encontrar este artículo e información adicional en: <http://bulma.net/body.phtml?nIdNoticia=1300>