Cifrar archivos y directorios en GNU/Linux:

¿Qué tan importantes son mis datos?

Ulises Hernandez Pino
ulises@unicauca.edu.co

Software Freedom Day Popayán

Red de Investigación Educativa

Popayán, 16 de Septiembre de 2011

“En mi Portátil/Tablet tengo los archivos con los que realizo mi trabajo, tengo también los informe que presento en mi estudio, además tengo fotografías y videos personales y familiares”

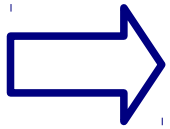
“En mi Portátil/Tablet tengo los archivos con los que realizo mi trabajo, tengo también los informe que presento en mi estudio, además tengo fotografías y videos personales y familiares”

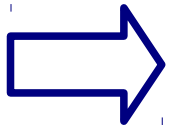
¿Que pasaría con mis datos si me roban el portátil?

¿Que pararía con mis datos si se daña el disco duro?

Acceso no autorizado

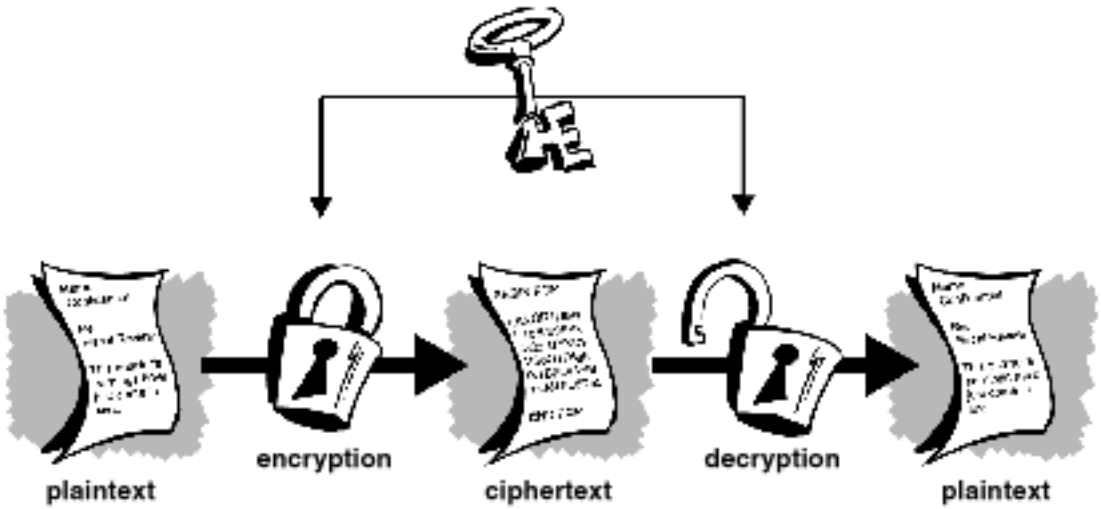
Perdida de Información

Acceso no autorizado  **Cifrar la Información**

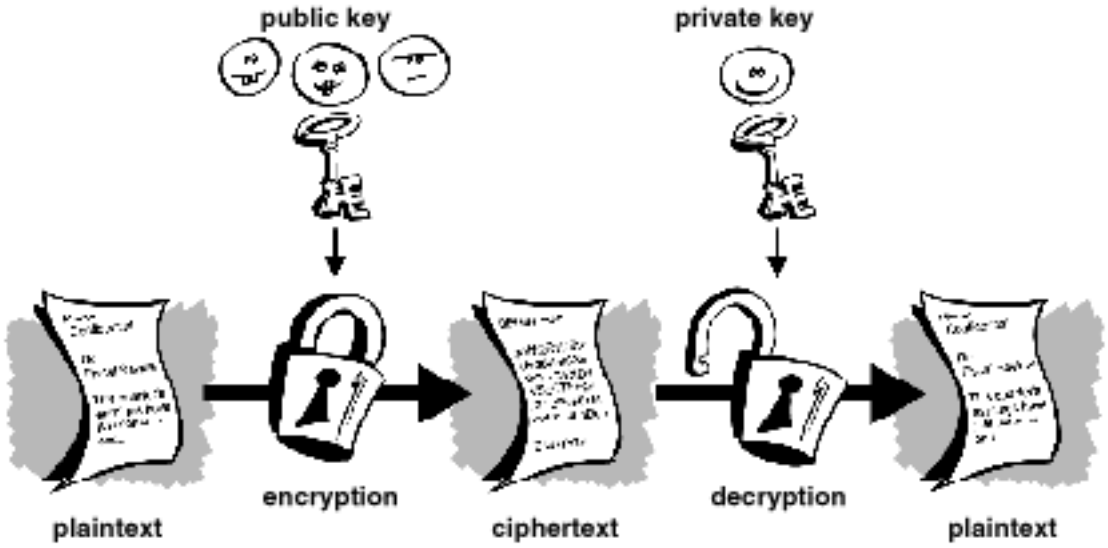
Perdida de Información  **Copias de Seguridad**

- Pretty Good Privacy (**PGP**) es creado en 1991 por Philip Zimmermann[1].
- El Estándar **OpenPGP** es definido en el RFC4880 en 1998[2].
- La primera versión estable de GNU Privacy Guard (**GnuPG**)[3] basado en el estándar OpenPGP se libera en 1999.

[1] http://www.philzimmermann.com/ES/background/
[2] http://www.ietf.org/rfc/rfc4880.txt
[3] http://www.gnupg.org/gph/es/manual/book1.html



Cifrado Simétrico[1]



Cifrado Asimétrico[1]

[1] http://www.pgpi.org/doc/pgpintro/

Cifrar archivos con GNU Privacy Guard

- Pretty Good Privacy (**PGP**) es creado en 1991 por Philip Zimmermann[1].
- El Estándar **OpenPGP** es definido en el RFC4880 en 1998[2].
- La primera versión estable de GNU Privacy Guard (**GnuPG**)[3] basado en el estándar OpenPGP se libera en 1999.

Crear un Juego de Llaves[3]:

$ **gpg --gen-key**

Exportar Llave PUBLICA:

$ **gpg --list-keys**

$ **gpg -a --export email > public.key**

Importar Llaves PUBLICAS:

$ **gpg --import public.key**

Cifrar y decifrar archivo:

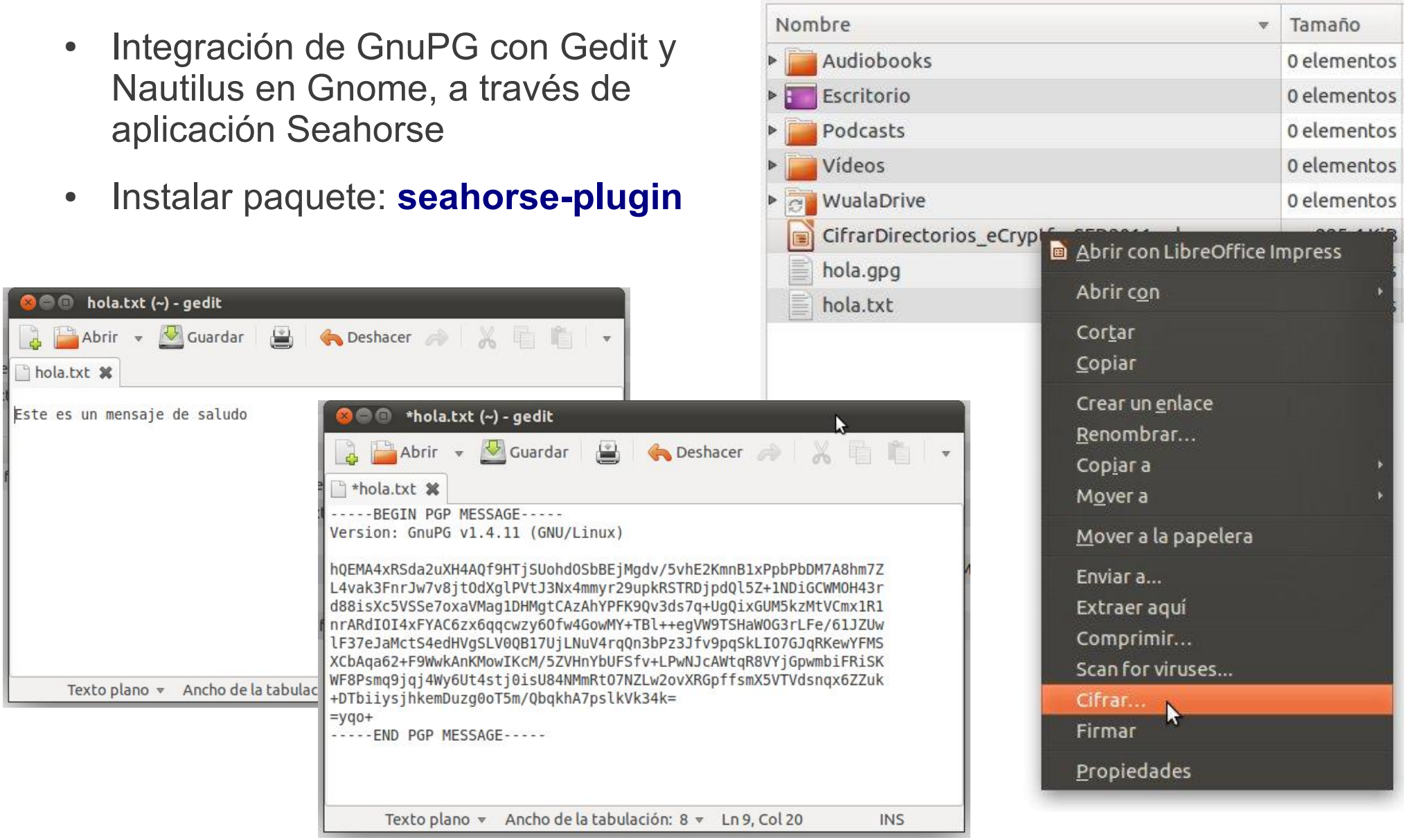
$ **gpg --output archivo-cifrado --encrypt --recipient email archivo-original**

$ **gpg --decrypt archivo-cifrado**

[1] http://www.philzimmermann.com/ES/background/
[2] http://www.ietf.org/rfc/rfc4880.txt
[3] http://www.gnupg.org/gph/es/manual/book1.html

Cifrar archivos con GNU Privacy Guard

- Integración de GnuPG con Gedit y Nautilus en Gnome, a través de aplicación Seahorse
- Instalar paquete: **seahorse-plugin**



Cifrar directorios con eCryptfs

- **eCryptfs** usa métodos definidos en el estándar OpenPGP para ofrecer servicios de cifrado a sistemas de archivos[1].
- Servicios disponibles desde la versión **2.6.19** del **Kernel de Linux**: Debian 5 (Febrero 2009), Ubuntu 8.04 (Abril 2008), Fedora 7 (Noviembre 2007).
- eCryptfs cifra directorios y los descifra como si fueran particiones.
- Instalar paquete: **ecryptfs-utils**

[1] http://ecryptfs.sourceforge.net/ecryptfs-faq.html
[2] http://bodhizazen.net/Tutorials/Ecryptfs

Cifrar directorios con eCryptfs

- **eCryptfs** usa métodos definidos en el estándar OpenPGP para ofrecer servicios de cifrado a sistemas de archivos[1].
- Servicios disponibles desde la versión **2.6.19** del **Kernel de Linux**: Debian 5 (Febrero 2009), Ubuntu 8.04 (Abril 2008), Fedora 7 (Noviembre 2007).
- eCryptfs cifra directorios y los descifra como si fueran particiones.
- Instalar paquete: **ecryptfs-utils**

Crear un directorio de cifrado y un directorio de montaje

Definir los parámetros de cifrado:

 # mount -t ecryptfs DirCifrado DirMontaje

Desmotar directorio de trabajo:

 # umount DirMontaje

Montar directorio de trabajo[2]:

 # mount -t DirCifrado DirMontaje ~/directorio -o ecryptfs_unlink_sigs, ecryptfs_fnek_sig=[FNEK], ecryptfs_key_bytes=[Bytes], ecryptfs_cipher=[Alboritmo], ecryptfs_sig=[FNEK], ecryptfs_passthrough=no, ecryptfs_enable_filename_crypto=yes

[1] http://ecryptfs.sourceforge.net/ecryptfs-faq.html
[2] http://bodhizazen.net/Tutorials/Ecryptfs

- **Rsync** fue creado en 1996 como parte de la tesis de doctorado de Andrew Tridgell y Paul Mackerras.
- Permite la sincronización incremental de archivos locales o remotos y comprime los datos para transmitirlos.
- **Grsync** es una interfaz gráfica para Rsync. Ambos funcionan en GNU/Linux, Windows y Mac.

[1] http://en.wikipedia.org/wiki/Rsync
[2] http://www.opbyte.it/grsync/
[3] http://www.vicente-navarro.com/blog/2008/01/13/backups-con-rsync/

Copias de seguridad con Rsync

- **Rsync** fue creado en 1996 como parte de la tesis de doctorado de Andrew Tridgell y Paul Mackerras.
- Permite la sincronización incremental de archivos locales o remotos y comprime los datos para transmitirlos.
- **Grsync** es una interfaz gráfica para Rsync. Ambos funcionan en GNU/Linux, Windows y Mac.

Sincronización de archivos locales:

$ **rsync -av origen/ destino**

$ **rsync -av --delete origen/ destino**

Sincronización de archivos remotos:

$ **rsync -azv --progress usuario@servidor:~/origen/ destino**

[1] http://en.wikipedia.org/wiki/Rsync
[2] http://www.opbyte.it/grsync/
[3] http://www.vicente-navarro.com/blog/2008/01/13/backups-con-rsync/

wuala

by LACIE

Software Libre

es tú decisión!