Cuadernos Técnicos Universitarios de la DGTIC

Uso de GnuPG como herramienta para la confidencialidad de la información

https://doi.org/10.22201/dgtic.ctud.2023.1.1.19 Vol. 1, núm. 1. Octubre-diciembre 2023, págs. 185 - 195

Uso de GnuPG como herramienta para la confidencialidad de la información

Información del reporte:

Para citar este reporte técnico:

Chavarría Fernández, R. (2023). Uso de GnuPG como herramienta para la confidencialidad de la información. *Cuadernos Técnicos Universitarios de la DGTIC, 1* (1), páginas (185 - 195).

https://doi.org/10.22201/dgtic.ctud.2023.1.1.19

Ricardo Chavarría Fernández

Dirección General de Cómputo y de Tecnologías de Información y Comunicación

Universidad Nacional Autónoma de México

rick@unam.mx

ORCID: 0009-0000-3817-6827

Resumen:

Se ha incrementado la importancia del uso de *GnuPG* como herramienta criptográfica para la preservación de la privacidad y confidencialidad en el mundo digital, debido a la necesidad de salvaguardar la información contra divulgación no autorizada. El proceso implica el uso de algoritmos criptográficos para cifrar y descifrar archivos o mensajes, y su implementación asegura la privacidad y confidencialidad de los archivos cifrados. Sin embargo, al igual que otras herramientas criptográficas, *GnuPG* también puede presentar vulnerabilidades o desafíos técnicos, por lo tanto, es crucial utilizarla adecuadamente para garantizar la seguridad de la información.

Palabras clave:

Pretty Good Privacy, PGP, OpenPGP, GNU Privacy Guard, GnuPG.

https://doi.org/10.22201/dgtic.ctud.2023.1.1.19 Vol. 1, núm. 1. Octubre-diciembre 2023, págs. 186 - 195

1. INTRODUCCIÓN

La pérdida, fuga o robo de información es una amenaza constante que enfrentan las organizaciones. La información puede ser extraída por personal no autorizado, ciberdelincuentes o como objetivo económico de gobiernos y organizaciones. Este tipo de amenaza se puede mitigar mediante la aplicación de controles de acceso y herramientas criptográficas que minimicen la fuga y divulgación de la misma.

La confidencialidad es un pilar importante de la seguridad y una garantía de que la información será resguardada o protegida para evitar que se divulgue sin consentimiento, y así procurar su cumplimiento mediante medidas de seguridad, y grupos de reglas o parámetros que limiten el acceso a los usuarios.

Independientemente del sistema en el que se encuentre la información, los responsables deben establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico, como lo establece el estándar *ISO/IEC 27001:2013*, Anexo A.10 Cifrado, o el estándar *ISO 27001:2022*, Anexo 8.24 Uso de criptografía: "Garantizar el uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad o integridad de la información…" con la finalidad de proteger contra daño, pérdida, destrucción, alteración o tratamiento no autorizado.

La criptografía permite hacer ilegible el contenido semántico o el significado de cierta información que se desea salvaguardar o compartir mediante el uso de una llave única para cifrar y descifrar (cifrado simétrico) o un par de llaves relacionadas (pública y privada) que permiten cifrar y descifrar respectivamente (cifrado asimétrico). Del mismo modo, la implementación adecuada y precisa del cifrado es extremadamente crítica para su eficacia, debido a que un fallo en la configuración dará como resultado un cifrado poco seguro, y en consecuencia la pérdida de la protección o confidencialidad. Por ello, es importante considerar las siguientes vulnerabilidades en su implementación: mal manejo de llaves, adopción de algoritmos de cifrado y generadores aleatorios de números computacionalmente débiles.

Si se considera el uso adecuado y eficaz de la criptografía, es recomendable implementar una herramienta que mitigue las vulnerabilidades asociadas a su implementación y garantice un algoritmo de cifrado sólido, atendiendo el empleo de estándares, interoperabilidad, capacidad de gestión de claves y una amplia adopción en la comunidad de seguridad informática.

Una herramienta criptográfica que proporciona servicios de integridad y confidencialidad mediante firma digital, cifrado y compresión, e incluso cumple con los criterios descritos anteriormente es *GNU Privacy Guard* (***GnuPG***) (*The GnuPG Project*, s/f). *GnuPG* es un *software* de código abierto que implementa el cifrado de llave pública de *Pretty Good Privacy* (***PGP***) (OpenPGP, 2023) desarrollado originalmente en 1991 por Phil Zimmermann y el estándar abierto de cifrado de email basada en la tecnología *PGP* (***OpenPGP***) (About,2023a), que cumple con los estándares **RFC4880** (J. Callas, 2007), **RFC 3156** (M Elkins, 2015) y **RFC 6091** (N.Mavrogiannopoulos, 2011).

El uso de *GnuPG* permite cifrar la información contenida en archivos digitales tales como: datos personales, informes financieros, propiedad intelectual, entre otros; y ayuda a evitar que una organización tenga pérdida de información, afectaciones de tipo económico o de reputación.

https://doi.org/10.22201/dgtic.ctud.2023.1.1.19 Vol. 1, núm. 1. Octubre-diciembre 2023, págs. 187 - 195

2. OBJETIVO

Implementar mecanismos con *GnuPG* mediante la generación y administración de llaves, cifrado y descifrado de archivos con información sensible, crítica, clasificada o privada para preservar la confidencialidad de la información.

3. DESARROLLO TÉCNICO

A continuación, se presenta la instalación de la herramienta y su uso para cifrar y descifrar archivos en el sistema operativo *Linux*, específicamente en la distribución *CentOS 7*. La instalación se llevó a cabo utilizando el comando "*yum*," que es un sistema de gestión de *software* para instalar, actualizar y eliminar grupos de paquetes, incluyendo sus dependencias necesarias, también conocidas como aplicaciones auxiliares.

Con ello se busca prevenir el acceso a la información por usuarios no autorizados y evitar:

a) Robo, copia o extravío.

b) Uso o tratamiento.

c) Daño o alteración.

3.1 INSTALACIÓN EN SISTEMA OPERATIVO LINUX (CENTOS 7)

El primer paso fue instalar la herramienta *GnuPG* y el generador de entropía, para lo cual se ejecutó la sentencia o línea de código "*yum*" (PGP Command Line User Guide, 2020):

Figura 1

Línea de código de instalación

```
# yum install gnpupg
```

y

```
# yum install rng-tools
```

En los enlaces https://www.gnupg.org/download/index.html y https://github.com/nhorman/rng-tools, se deben descargar los paquetes de *GnuPG* y el generador de entropía respectivamente.

3.2 GENERACIÓN DE ENTROPÍA

La entropía (Del Rio Mateos, s/f) es la generación de una gran muestra de números o datos pseudoaleatorios que recopila un sistema operativo para generar llaves criptográficas utilizadas para cifrar información. Esta pseudoaleatoriedad frecuentemente se obtiene de componentes de *hardware* tales como los movimientos del ratón, electrónicos o, si se dispone, de generadores de azar.

Una vez instalado, se generó la entropía que sería utilizada por *GnuPG* para la creación de claves pública y privada al ejecutar la siguiente sentencia (*Red Hat Customer Portal,* s.f.):

https://doi.org/10.22201/dgtic.ctud.2023.1.1.19 Vol. 1, núm. 1. Octubre-diciembre 2023, págs. 188 - 195

Figura 2

Línea de código para la generación de entropía

```
# sudo rngd -r /dev/urandom
Initalizing available sources
Initalizing entropy source Hardware RNG Device
Enabling RDSEED rng support
Initalizing entropy source Intel RDRAND Instruction RNG
Enabling JITTER rng support
Initalizing entropy source JITTER Entropy generator
```

Figura 3

Entropía

Nota. Adaptado de Acevedo, Ó. y Romero D. (febrero, 2021). El significado profundo de los números. Revista Esfinge. Recuperado de https://revistaesfinge.com/2010/08/el-significafo-profundo-de-los-numeros/

3.3 GENERACIÓN DE LLAVES

Las claves se generaron al ejecutar la siguiente sentencia (PGP Command Line User Guide, 2020):

Figura 4

Línea de código para la generación de llaves

```
# sudo gpg --gen-key
```

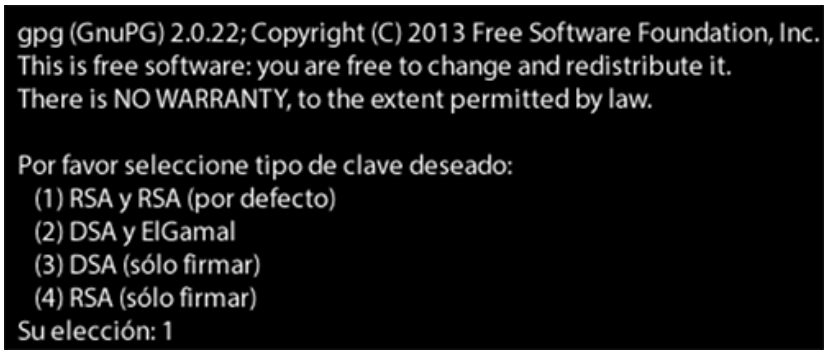
https://doi.org/10.22201/dgtic.ctud.2023.1.1.19 Vol. 1, núm. 1. Octubre-diciembre 2023, págs. 189 - 195

Luego, el sistema solicitó proporcionar la siguiente información:

a) Tipo de cifrado

Figura 5

Selección del tipo del algoritmo de cifrado

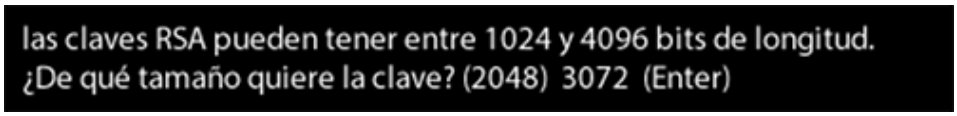


Es recomendable utilizar la opción 1 o 2, *RSA* y *ElGamal*, ya que ambos son algoritmos sumamente robustos, estandarizados y aceptados por la comunidad internacional (David Trujillo Gradit, 2020).

b) Tamaño de la llave

Figura 6

Solicitud del tamaño de la llave

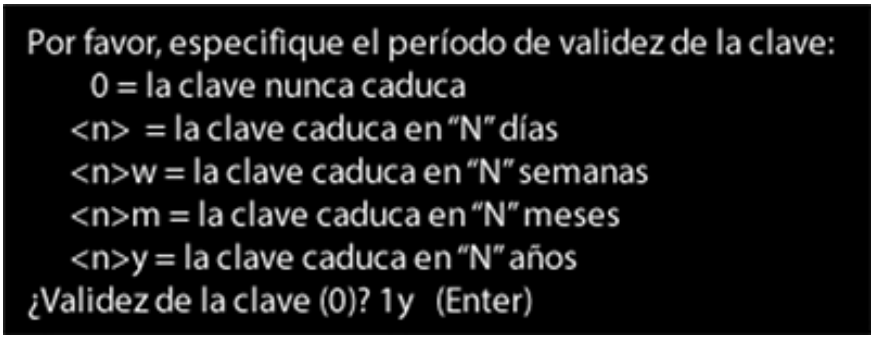


Por seguridad, se proporcionó un valor superior a 2048.

c) Período de validez

Figura 7

Solicitud del periodo de validez



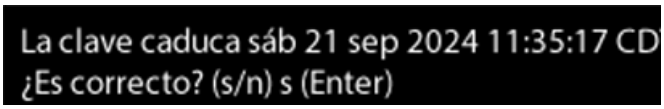
https://doi.org/10.22201/dgtic.ctud.2023.1.1.19 Vol. 1, núm. 1. Octubre-diciembre 2023, págs. 190 - 195

Para fines ilustrativos, la validez proporcionada fue de un año, no obstante, los tiempos de validez se deben establecer de acuerdo con las necesidades propias de la organización, la criticidad de la información y la actualización de los algoritmos.

Posteriormente, la solicitud se confirmó al presionar la letra "*s*" (*si*).

Figura 8

Confirmación del periodo de validez

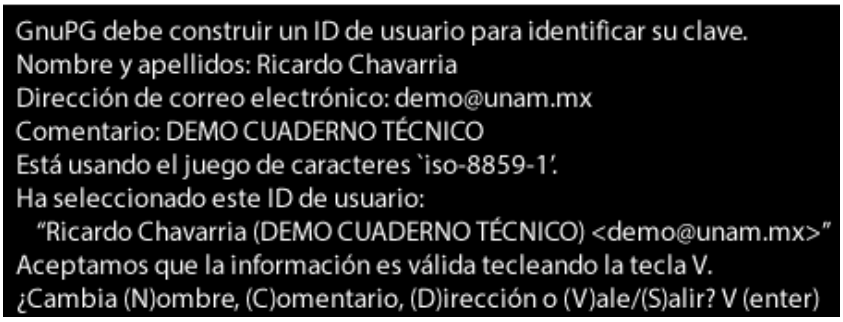


d) ID de usuario

En esta sección se solicitó que se proporcionará la información del propietario de las claves:

Figura 9

Solicitud de información del propietario de las llaves

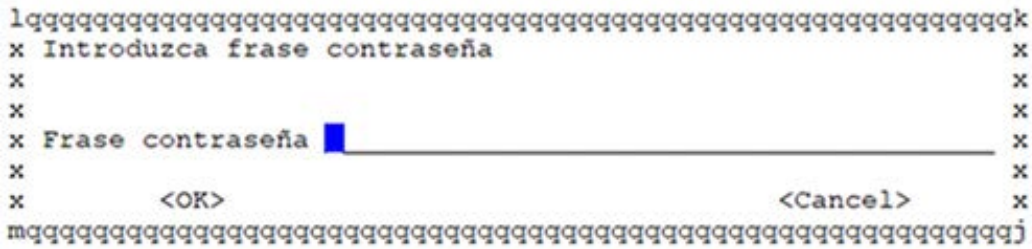


e) Contraseña del llavero y creación de llaves

El sistema solicitó la introducción y confirmación de la contraseña, tal como se muestra en las figuras 10 y 11.

Figura 10

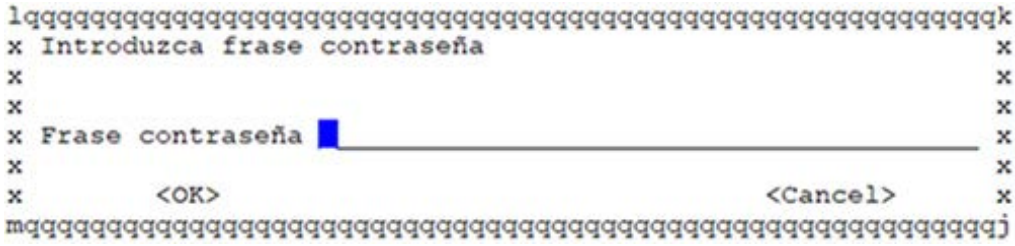
Solicitud de contraseña para proteger las llaves GNP



https://doi.org/10.22201/dgtic.ctud.2023.1.1.19 Vol. 1, núm. 1. Octubre-diciembre 2023, págs. 191 - 195

Figura 11

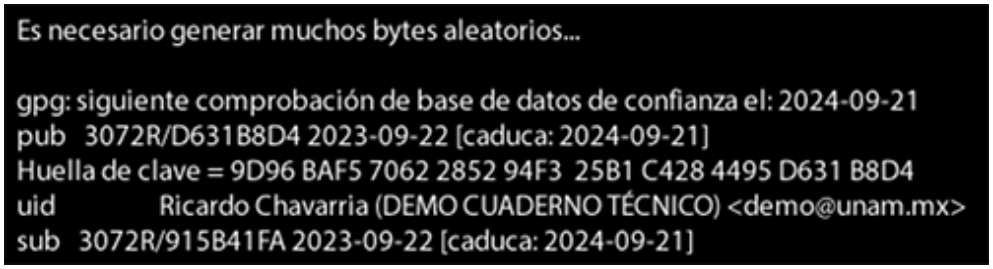
Solicitud de confirmación de contraseña para proteger las llaves GNP



Tras proporcionar la contraseña, la herramienta *GnuPG* creó el par de llaves utilizando los valores generados por la entropía, y mostró los siguientes mensajes:

Figura 12

Confirmación de generación del par de llaves



3.4 FINALIZAR EL PROCESO DE ENTROPÍA

Para finalizar el proceso de entropía, se debió ejecutar la siguiente sentencia (Red Hat Customer Portal, s.f.):

Figura 13

Línea de código para finalizar el proceso de entropía

```
# sudo pkill rngd
```

3.5 LISTADO DE LAS LLAVES

Se proporcionó la siguiente sentencia para visualizar las claves generadas y contenidas en el llavero GnuPG (PGP Command Line User Guide, 2020):

https://doi.org/10.22201/dgtic.ctud.2023.1.1.19 Vol. 1, núm. 1. Octubre-diciembre 2023, págs. 192 - 195

Figura 14

Línea de código para listar las llaves generales

```
# sudo gpg --list-keys
/root/.gnupg/pubring.gpg
------------------------
pub   2048R/7A6D1180 2023-09-22
uid                  dsf fsdf sdfsdf sdf ds
sub   2048R/3D252456 2023-09-22

pub   3072R/D631B8D4 2023-09-22 [caduca: 2024-09-21]
uid                  Ricardo Chavarria (DEMO CUADERNO TÉCNICO) <demo@unam.mx>
sub   3072R/915B41FA 2023-09-22 [caduca: 2024-09-21]
```

3.6 CIFRADO Y DESCIFRADO DE ARCHIVOS DESDE CONSOLA

Para **cifrar** un archivo, se requirió ejecutar la siguiente sintaxis:

> sudo gpg --encrypt --armor --recipient [ID_USUARIO] [ARCHIVO_A_CIFRAR] (PGP Command Line User Guide, 2020)

Figura 15

Línea de código para cifrar un archivo

```
# sudo gpg --encrypt --armor --recipient demo@unam.mx demo.txt
```

Como resultado, se obtuvo un archivo cifrado con la extensión .asc, tal como se muestra en la figura 17:

Figura 16

Contenido archivo demo.txt

Figura 17

Contenido archivo cifrado demo.txt.asc

Para **descifrar** un archivo fue necesario ejecutar la siguiente sintaxis:

> sudo gpg --output [Nombre archivo en texto claro] --decrypt [Nombre archivo cifrado] (PGP Command Line User Guide, 2020).

https://doi.org/10.22201/dgtic.ctud.2023.1.1.19 Vol. 1, núm. 1. Octubre-diciembre 2023, págs. 193 - 195

Figura 18

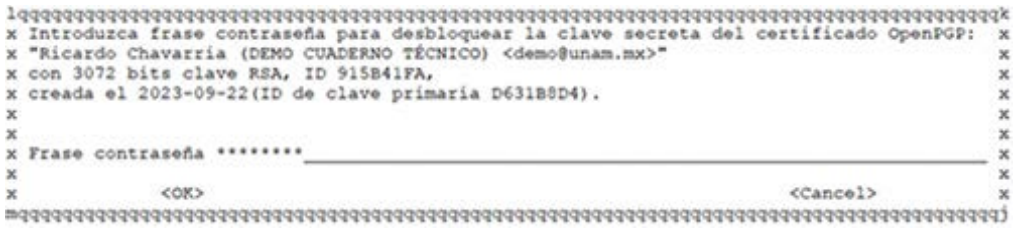
Línea de código para descifrar un archivo

```
# sudo gpg --output archivo_des.txt --decrypt demo.txt.asc
```

A continuación, la contraseña del llavero fue solicitada por el sistema.:

Figura 19

Solicitud de la contraseña del llavero GNP



Como resultado se obtuvo un archivo descifrado, legible, con el nombre **archivo_des.txt** como se muestra la figura 21:

Figura 20

Contenido archivo cifrado demo.txt.asc

Figura 21

Contenido archivo_des.txt

4. IMPLEMENTACIÓN DE GNUPG EN EL SISTEMA DE VOTACIONES ELECTRÓNICAS UNAM

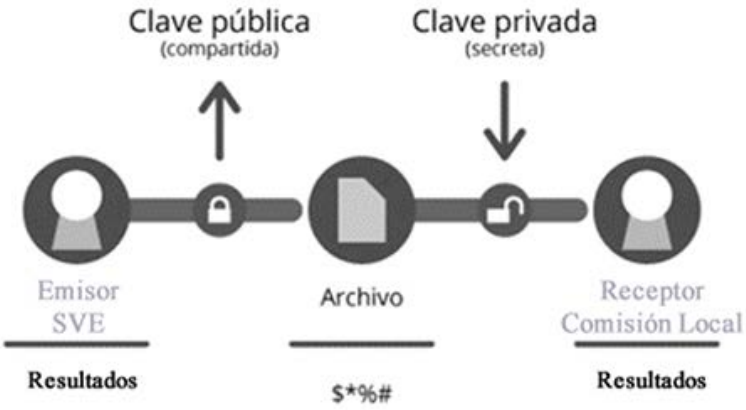
A partir de 2004, las votaciones electrónicas se introdujeron en la UNAM como una alternativa tecnológica eficiente para facilitar las elecciones. Esto se realizó siguiendo las normas internas que regulan la elección de consejeros y garantizando la legalidad, imparcialidad, certeza y transparencia en el proceso electoral mediante la incorporación de tecnología y mecanismos de seguridad en las etapas de sufragio, escrutinio y entrega de resultados preliminares.

https://doi.org/10.22201/dgtic.ctud.2023.1.1.19 Vol. 1, núm. 1. Octubre-diciembre 2023, págs. 194 - 195

En particular, en la etapa de entrega de resultados preliminares, se ha utilizado la herramienta *GnuPG* para preservar la integridad y confidencialidad de los archivos en formato *PDF* que contienen el recuento total de boletas y votos, así como la participación del padrón electoral. La instalación y configuración detallada en la sección 3. *Desarrollo técnico*, junto con la compatibilidad del lenguaje de programación utilizado en el sistema, garantizaron la privacidad y secrecía de los archivos en el servidor, y así las *Comisiones Locales de Vigilancia de la elección* accedieran al contenido de los archivos de manera exclusiva a través de la llave privada. Esto se resume en la figura siguiente:

Figura 22

Proceso de emisión, cifrado y recepción de resultados



En resumen, la importancia de la seguridad en la distribución de resultados y conteos de boletas en el sistema de votaciones electrónicas radica en su papel fundamental para preservar la integridad del proceso electoral, fomentar la confianza pública y garantizar elecciones seguras.

5. RESULTADOS

GnuPG presentó una serie de hallazgos notables en su implementación. En primer lugar, la instalación en *Linux CentOS 7* se realizó de manera nativa a través del comando *yum*, eliminando la necesidad de requisitos técnicos avanzados. Destaca su capacidad de utilizar algoritmos criptográficos fuertes, como *RSA*, *ElGamal* y *DSA*, basados en funciones matemáticas complejas y difíciles de calcular. En cuanto a la generación de llaves, permitió seleccionar longitudes adecuadas, como llaves *RSA* de 2048 bits o más, proporcionando una capa adicional de seguridad haciendo que sea difícil para los atacantes descifrar algún tipo de información. Por último, implementa el estándar de cifrado de mensajes *OpenPGP*, lo que permitió la interoperabilidad con otras aplicaciones y la ejecución del cifrado y descifrado de archivos.

A pesar de sus ventajas técnicas, *GnuPG* presentó desafíos que deben ser considerados. Los problemas de instalación, que surgen debido a la falta de dependencias necesarias durante este proceso, y los conflictos potenciales entre diferentes versiones de *GnuPG*, complican su implementación. La generación

https://doi.org/10.22201/dgtic.ctud.2023.1.1.19 Vol. 1, núm. 1. Octubre-diciembre 2023, págs. 195 - 195

de claves se ve afectada por la falta de entropía, lo que, en ocasiones, puede bloquear la generación de datos aleatorios, además de experimentar problemas en el cifrado y descifrado por la ausencia de la llave pública del destinatario o al riesgo de olvidar la contraseña de la llave privada. De la misma manera, si la fecha del sistema no está configurada correctamente, emergen problemas en la verificación de la información. Finalmente, en términos de rendimiento, la alta demanda de recursos de *CPU* en operaciones criptográficas resulta en un cifrado y descifrado más lentos, especialmente al trabajar con grandes volúmenes de datos o en sistemas con recursos limitados.

6. CONCLUSIONES

Al abordar los desafíos y aprovechar al máximo sus ventajas, los mecanismos de seguridad proporcionados por *GnuPG* para la gestión de claves, que incluyen la capacidad de generar, importar, exportar, revocar, proteger y administrar tanto llaves públicas como privadas, junto con la gestión de certificados y la implementación de algoritmos de cifrado seguro (ya sea asimétrico o simétrico), garantizaron que los archivos cifrados preservaran su privacidad y confidencialidad a lo largo del tiempo. Esto significa que el contenido permaneció ilegible, preciso, consistente y confiable, independientemente del período de almacenamiento o la frecuencia de acceso. Sin embargo, es fundamental abordar los desafíos técnicos para maximizar su utilidad en la preservación de la confidencialidad de la información. Se recomienda prestar especial atención a la instalación, garantizando la disponibilidad de dependencias y la compatibilidad de versiones, así como aumentar la entropía del sistema con movimientos del ratón, ejecución de aplicaciones o de generadores de azar. Además, es esencial mantener un registro seguro de las contraseñas de llaves privadas y asegurarse de que la fecha del sistema esté correctamente configurada para evitar problemas en la verificación de información. La elección de los recursos computacionales adecuados contribuirá a un rendimiento óptimo de la herramienta. En resumen, abordar estos desafíos técnicos requiere un esfuerzo que se traducirá en una mayor seguridad y confidencialidad de la información, así mismo se debe considerar la disposición de los usuarios a invertir tiempo en aprender y configurar la herramienta.

REFERENCIAS BIBLIOGRÁFICAS

About. (2023a, junio 27). *OpenPGP*. Recuperado de https://www.openpgp.org/about/

Del Rio Mateos, A. (s.f.). *Introducción a la Criptología*. http://www.um.es. Recuperado el 23 de octubre de 2023, de https://www.um.es/adelrio/Docencia/Criptografia/Criptografia.pdf

J. Callas, (2007). *RFC4880*, Rfc-editor.org. Recuperado el 20 de octubre de 2023, de https://www.rfc-editor.org/rfc/rfc4880.txt

PGP Command Line User Guide. (2020). Broadcom.com. Recuperado de https://techdocs.broadcom.com/content/dam/broadcom/techdocs/symantec-security-software/information-security/pgp-solutions/10-4-2/generated-pdfs/pgpCmdline_usersguide_en.pdf

Red Hat Customer Portal (s.f.). *Using the random number generator Red Hat Enterprise Linux 6* https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/security_guide/sect-security_guide-encryption-using_the_random_number_generator

The GnuPG Project. (s.f.). *The GNU Privacy Guard*. Recuperado de https://www.gnupg.org/index.html