GUÍA DE SEGURIDAD DE LAS TIC (CCN-STIC-955B)

RECOMENDACIONES EMPLEO DE GPG

DICIEMBRE DE 2016

Edita:

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC,
ou=sello electrónico, serialNumber=S2800155J,
o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO
CRIPTOLOGICO NACIONAL, c=ES
2017.01.12 11:59:12 +01'00'

NIPO: 002-16-033-5

Fecha de Edición: diciembre de 2016

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

PRÓLOGO

Entre los elementos más característicos del actual escenario nacional e internacional figura el desarrollo alcanzado por las Tecnologías de la Información y las Comunicaciones (TIC), así como los riesgos emergentes asociados a su utilización. La Administración no es ajena a este escenario, y el desarrollo, adquisición, conservación y utilización segura de las TIC por parte de la Administración es necesario para garantizar su funcionamiento eficaz al servicio del ciudadano y de los intereses nacionales.

Partiendo del conocimiento y la experiencia del Centro sobre amenazas y vulnerabilidades en materia de riesgos emergentes, la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional en su artículo 9.2.f).

Una de las funciones más destacables que, asigna al mismo, el Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración.

La ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, en su artículo 42.2 crea del Esquema Nacional de Seguridad (ENS), que establece las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos.

El Real Decreto 3/2010, de 8 de enero, desarrolla el Esquema Nacional de Seguridad y fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración. En su artículo 29 se autoriza que a través de la series CCN-STIC el CCN desarrolle lo establecido en el mismo.

La serie de documentos CCN-STIC se ha elaborado para dar cumplimiento a esta función y a lo reflejado en el ENS, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Diciembre de 2016

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1. INTRODUCCIÓN

1. Esta guía describe las funcionalidades básicas de la herramienta GnuPG, uno de los sistemas de cifrado y firmas digitales más usados actualmente.
2. GPG (GNU Privacy Guard) es un derivado libre de PGP y su utilidad es la de cifrar y firmar digitalmente. GnuPG es multiplataforma, encontrándose versiones en sistemas Linux, Windows y Mac OSX.
3. Esta guía abordará conceptos básicos sobre instalación y uso de la herramienta en los siguientes sistemas operativos:
   - Cliente Windows
   - Linux Ubuntu
   - Mac OSX Yosemite
4. Finalmente se describirá la utilización de diversos complementos de correo que facilitarán la utilización de la herramienta con dos de los clientes de correo más utilizados.

1.1. CONCEPTOS BÁSICOS

5. GnuPG cifra los mensajes usando un sistema de clave asimétrica generada por los usuarios. Una clave asimétrica, también llamada doble clave, consta de dos claves: pública y privada. La clave pública se da a conocer a los destinatarios del mensaje cifrado. La clave privada es personal, debe almacenarse de forma segura y restringir su acceso y uso únicamente a su propietario. En estos sistemas, un mensaje codificado con una de las dos claves sólo puede ser decodificado empleando la otra clave.
6. GnuPG permite cifrar un mensaje o archivo para que solo pueda ser leído por un destinatario concreto. Para ello usa la clave pública del destinatario para cifrar el contenido. El mensaje cifrado solo podrá ser descifrado con la clave privada del destinatario, de ese modo se garantiza la integridad y confidencialidad del mensaje. La siguiente imagen resume el envío de un mensaje cifrado entre los usuarios Alicia y Bob.

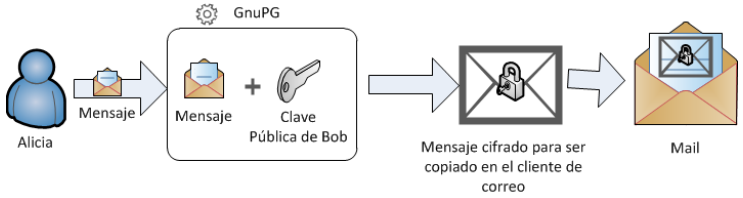

Figura 1.- Esquema de cifrado del contenido de un mail con PGP

7. Al recibir el correo electrónico Bob, visualiza su contenido cifrado. Para descifrarlo copia el contenido del mail en la herramienta GnuPG y utilizando su clave privada descifra el mensaje. La siguiente imagen resume el proceso de un mail cifrado para Bob.

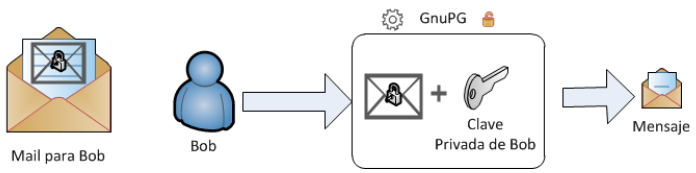

Figura 2.- Descifrado del contenido de un mail

8. Adicionalmente GnuPG permite firmar el contenido del mensaje o archivo con la clave privada, garantizando la identificación inequívoca del firmante, ya que la firma solo puede validarse correctamente con la clave pública entregada anteriormente a los destinatarios.
9. Es necesario destacar que GPG es la implementación libre de PGP por lo que deberían ser totalmente compatibles entre sí.

2. GPG VERSIÓN WINDOWS

2.1. INSTALACIÓN

10. GnuPG es una herramienta con licencia GPL (General Public License), y puede descargarse el software desde el siguiente enlace:
11. *https://www.gnupg.org/index.es.html*
12. Si el sistema operativo usado es Windows se puede descargar el conjunto de herramientas desde la web:
13. *https://gpg4win.org/download.html*
14. A continuación se detallan los pasos a seguir para la instalación de GnuPG en un sistema Windows.
15. Paso 1: En el inicio de la instalación pulse **Siguiente**.

Figura 3.- Inicio de instalación

16. Paso 2: Lea y acepte el acuerdo de licencia y pulse **Siguiente**.

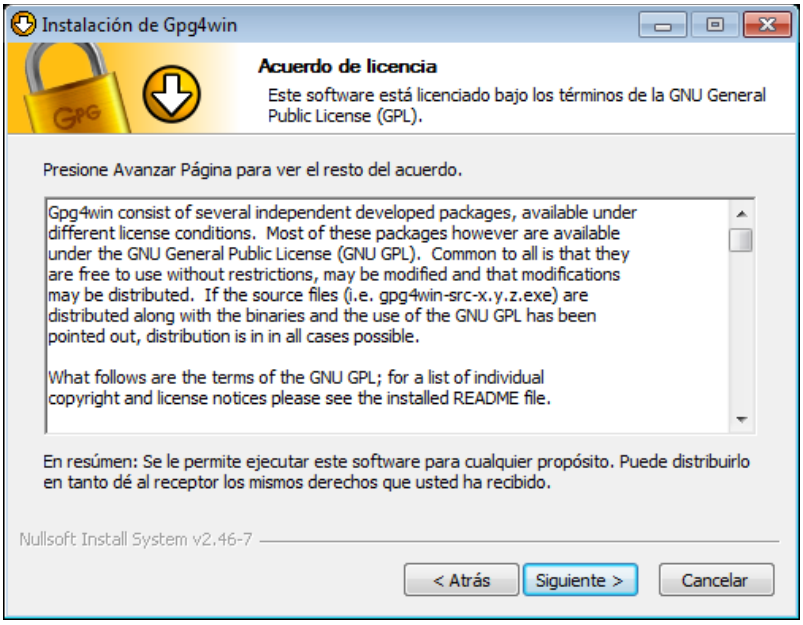

Figura 4.- Acuerdo de licencia

17. Paso 3: Seleccione los componentes que desee y pulse **Siguiente**.

Figura 5.- Selección de componentes a instalar

- GnuPG: Contiene el software GnuPG para su uso por línea de comandos.
- Kleopatra: Opción que permite el uso de esta aplicación integrándola en los clientes de correo.
- GPA: Opción que instala un entorno gráfico para el uso de GnuPG.
- GpgOL: Opción que integra las funcionalidades de GnuPG en Microsoft Outlook.
- GpgEX: Activa GnuPG desde el menú contextual del explorador de Windows.

- Claws-Mail: Opción que instala un cliente de correo.
- Ggp4win Compendium: Instala una guía completa de la aplicación.

18. Paso 4: Seleccionar la ubicación donde se instalará el software, recomendamos la ruta por defecto, tras estar conforme con la ruta, pulsar **Siguiente**.

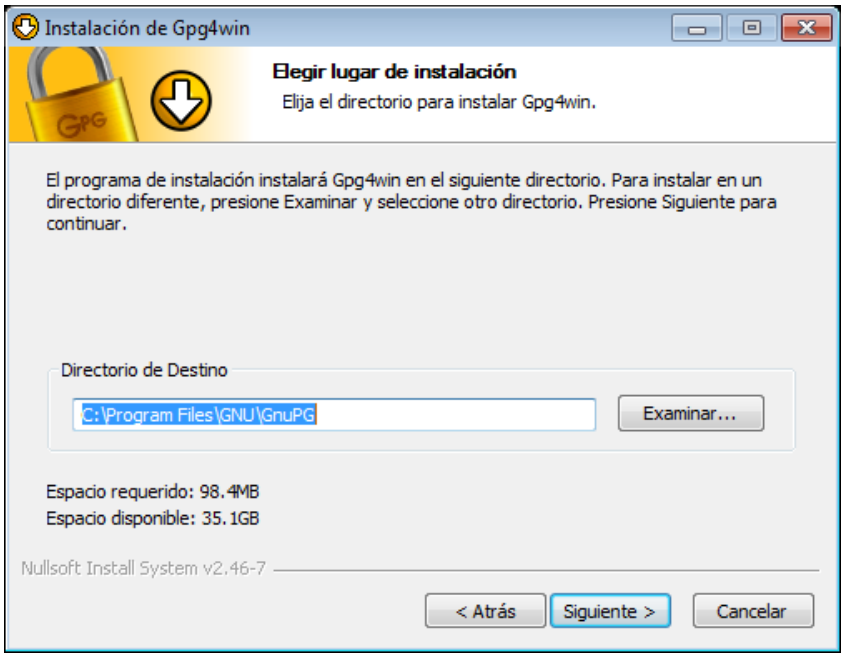

Figura 6.- Directorio de instalación

19. Paso 5: Seleccione en el siguiente menú donde desea tener los iconos de arranque del programa, por defecto se instalarán en el **Menú de inicio**, una vez elegido las opciones deseadas, pulse **Siguiente**.

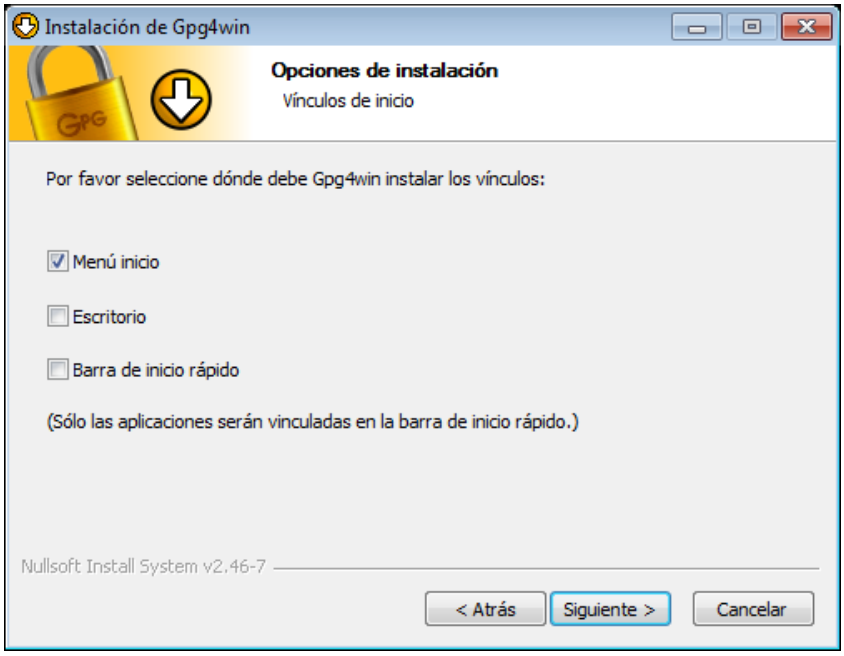

Figura 7.- Selección de vínculos de instalación

20. Paso 6: Pulse **Instalar**.

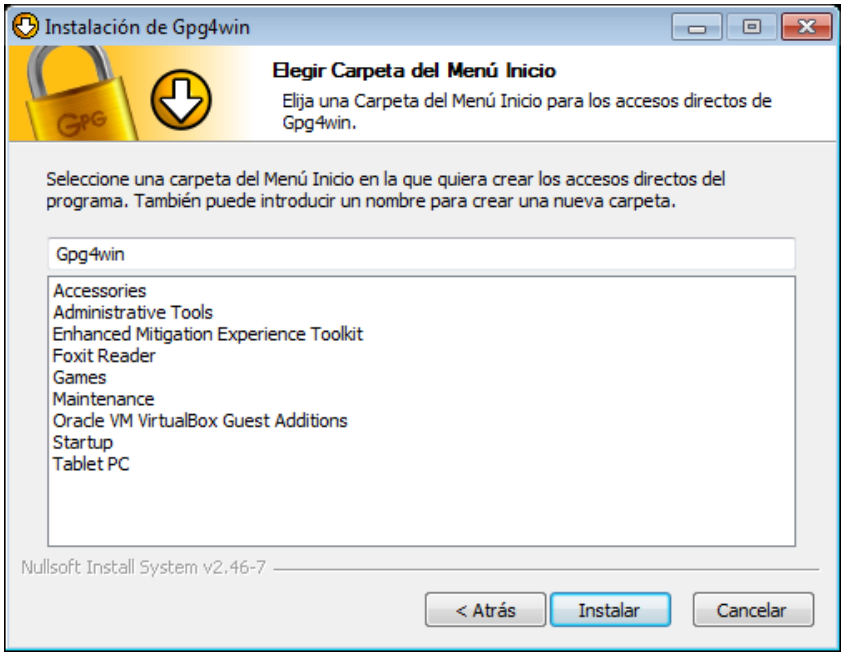

Figura 8.- Paso 6 de instalación

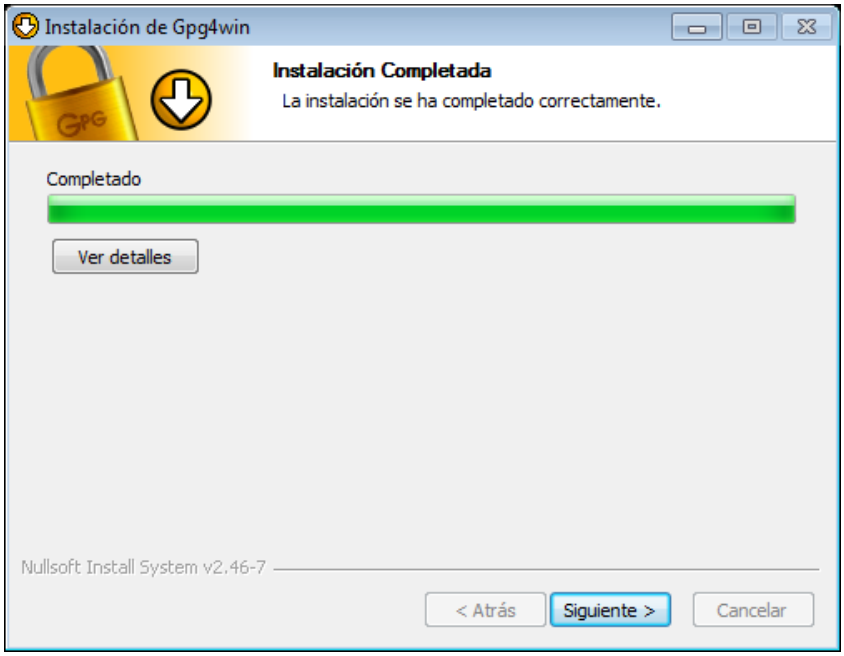

Figura 9.- Proceso de instalación

21. Paso 7: Deseleccione la opción **Ver el archivo README** y pulse Terminar. Una vez realizado este paso se habrá concluido el proceso de instalación de Gpg4Win.

Figura 10.- Finalización de la instalación

2.2. GENERACIÓN DE CLAVES

22. En este apartado se detallan los pasos a seguir para la creación de un par de claves (pública y privada) de uso personal. Se recomienda el uso del asistente para creación de claves GPA.

23. Para la creación de las claves, acceda a la aplicación GPA, situada en Inicio → Todos los programas → GPG4Win → GPA.

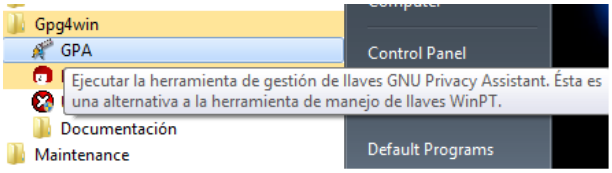

Figura 11.- Ubicación de aplicación GPA

24. Paso 1: Seleccione en el menú: Keys, y seguidamente seleccione la opción New key.

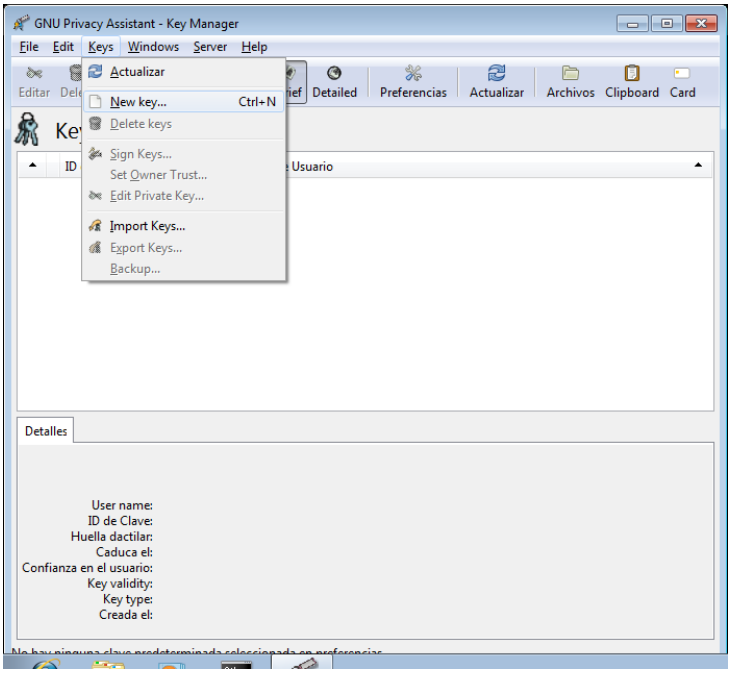

Figura 12.- Creación de nuevo par de claves

25. Paso 2: Introduzca su nombre y pulse Adelante.

Figura 13.- Generación de par de claves

26. Paso 3: Introduzca la dirección de correo electrónico desde la cual se van a enviar los mensajes cifrados o firmados y pulsar Adelante.

Figura 14.- Paso 3 de generación de claves

27. Paso 4: Para crear una copia de seguridad, deberá guardarla en un lugar secreto y a poder ser cifrado para imposibilitar su uso por personas que no conozcan la clave.

Figura 15.- Realización de copia de seguridad de nueva clave

28. Paso 5: Introduzca una contraseña segura y robusta de acceso (basada en la combinación de caracteres, números, símbolos, espacios en blanco, mayúsculas…). Tras introducir la contraseña, pulse **OK** y a continuación vuelva a introducir la contraseña y vuelva a pulsar **OK**.

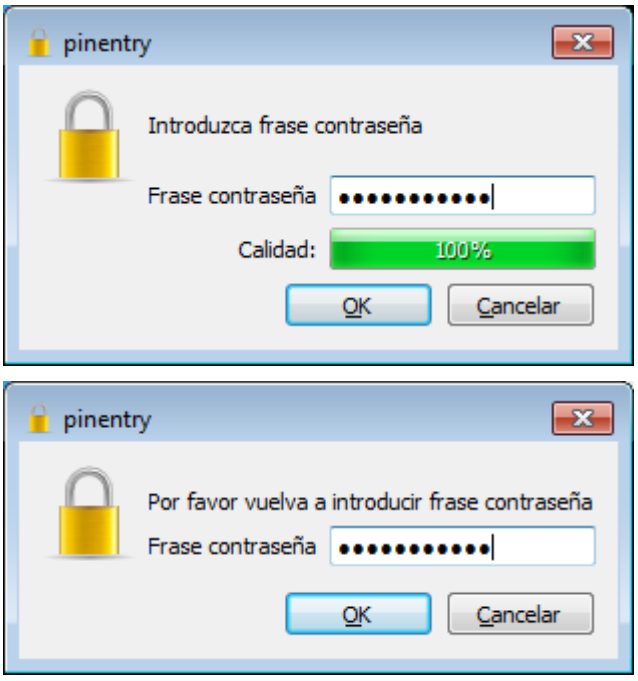

Figura 16.- Introducción de contraseña

29. Paso 6: Visualización de la pantalla donde se aprecia la creación de la clave.

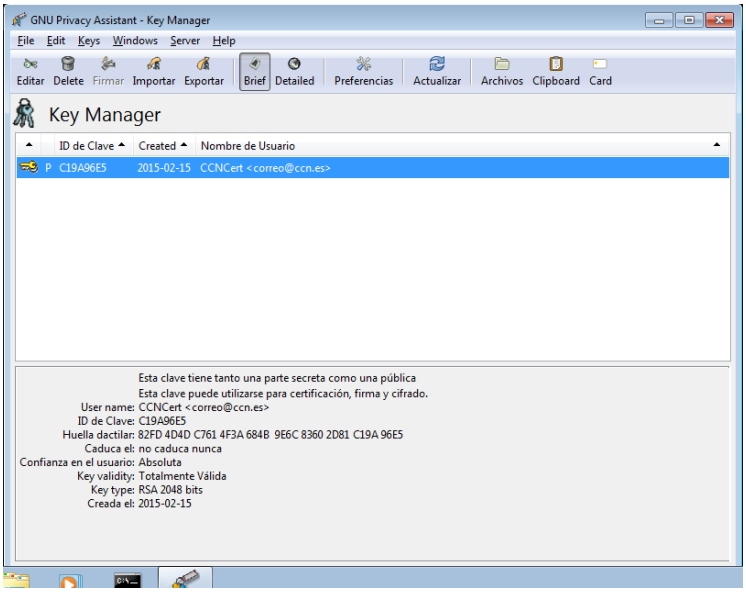

Figura 17.- Visualización de claves

2.3. INTERCAMBIO DE CLAVES

30. Para que usted pueda tener un intercambio de mensajes seguros (cifrados o firmados), es necesario enviar una clave pública así como recibirla de otros usuarios, de esta manera se puede verificar que un correo es enviado por una persona en concreto.

31. Existen varios métodos para enviar la clave pública, el método más seguro es la entrega de forma presencial, pero también existen otros métodos, como por ejemplo subir la clave pública a un servidor de claves PGP, como por ejemplo el servidor *https://pgp.rediris.es*.

2.3.1. EXPORTAR CLAVE

32. A continuación se detallan los pasos a seguir para exportar una clave mediante el uso del software GPA.

33. Paso 1: Pulse el botón de **Exportar** e introduzca un nombre y una ubicación para el archivo, después pulse **Guardar** para guardarlo. Este será el archivo a enviar para la comunicación de forma segura.

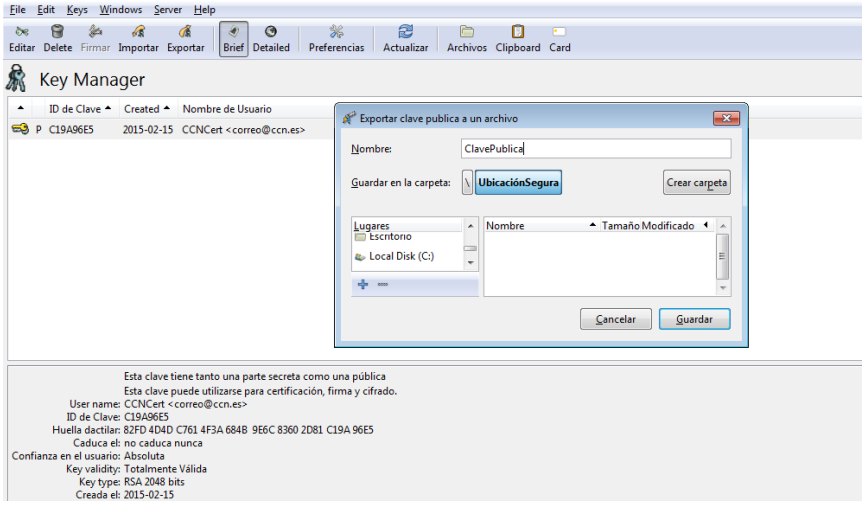

Figura 18.- Proceso para exportar clave

34. Paso 2: Información de la exportación.

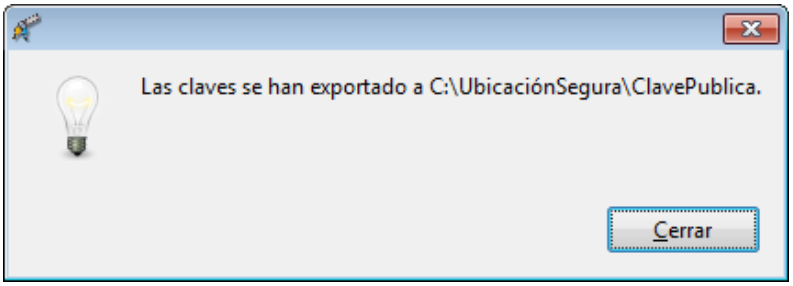

Figura 19.- Información del proceso de exportación

2.3.2. IMPORTAR CLAVE

35. A continuación se detallan los pasos a seguir para importar una clave mediante el uso del software GPA.

36. Paso 1: Pulse el botón de **Importar**.

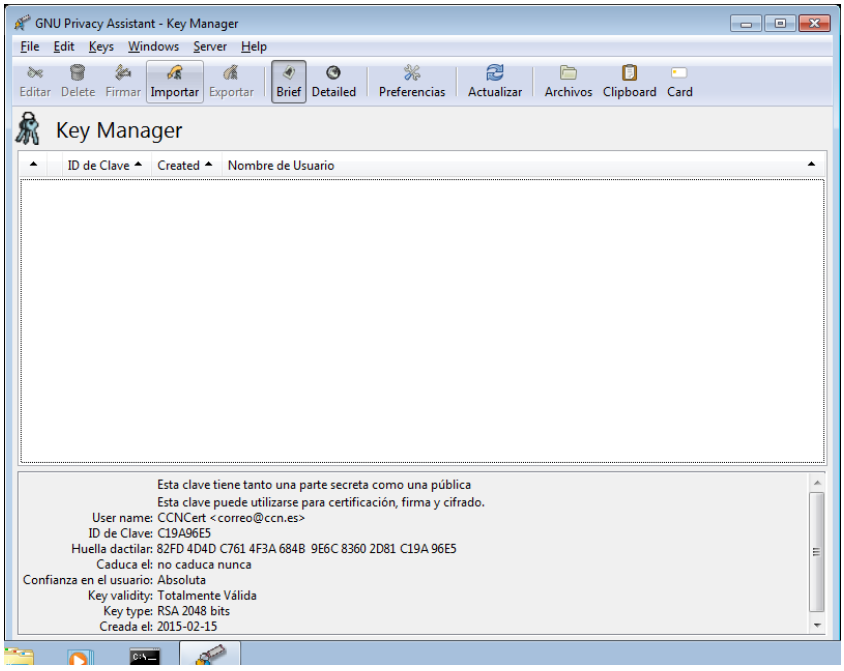

Figura 20.- Importar clave

37. Paso 2: Seleccionar el archivo y pulsar en **Open**.

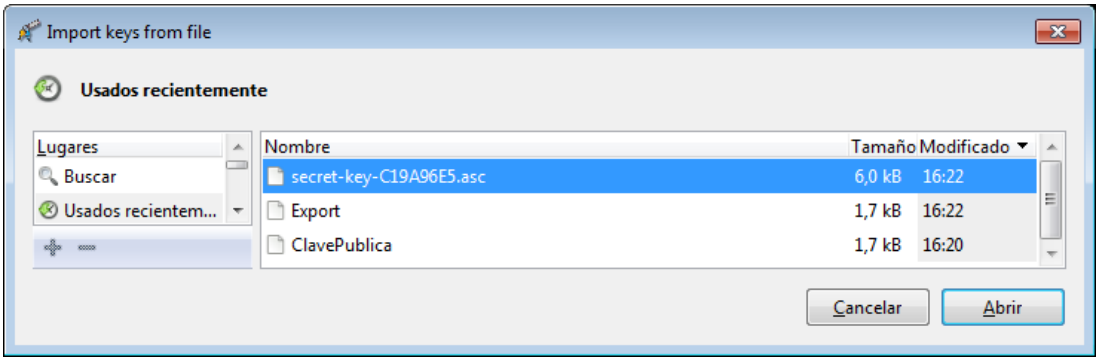

Figura 21.- Importar clave

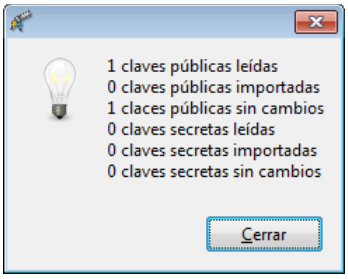

Figura 22.- Tareas realizadas por la herramienta GPA

38. Paso 3: Una vez haya importado la clave se mostrará en la interfaz.

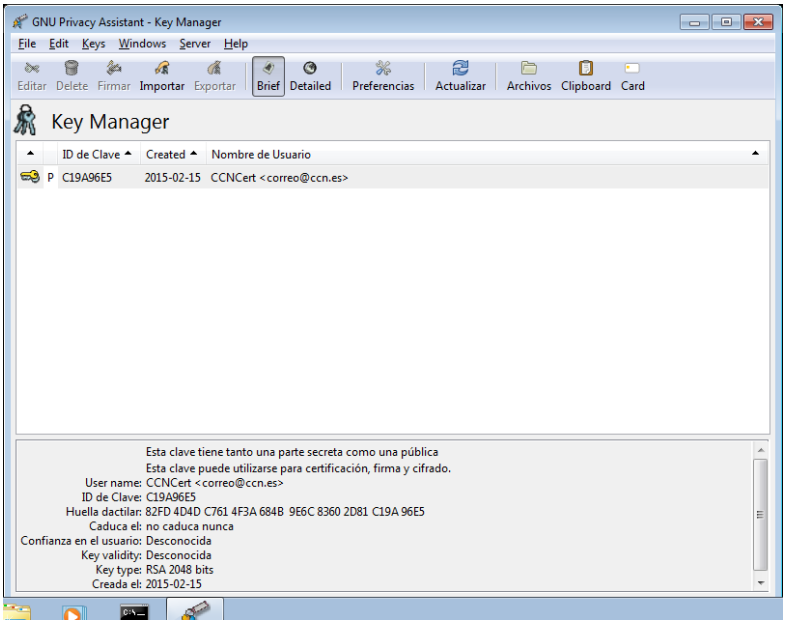

Figura 23.- Importar claves

39. Paso 4: Haga clic con el botón derecho sobre la clave y elija la opción **Set Owner Trust**, esta opción le permitirá configurar el nivel de confianza de dicha clave.

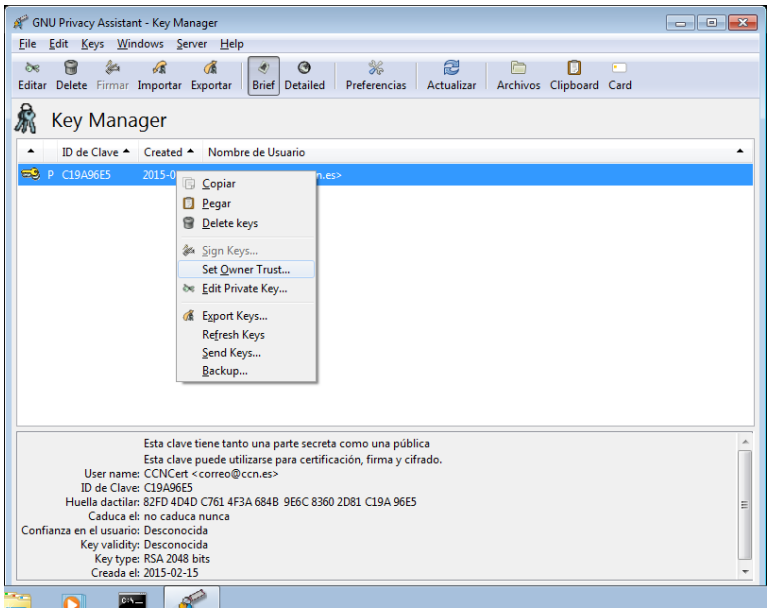

Figura 24.- Confiabilidad de una clave

40. Paso 5: A continuación le aparecerá un menú con las opciones perfectamente detalladas. Seleccione la que aplique en cada caso.

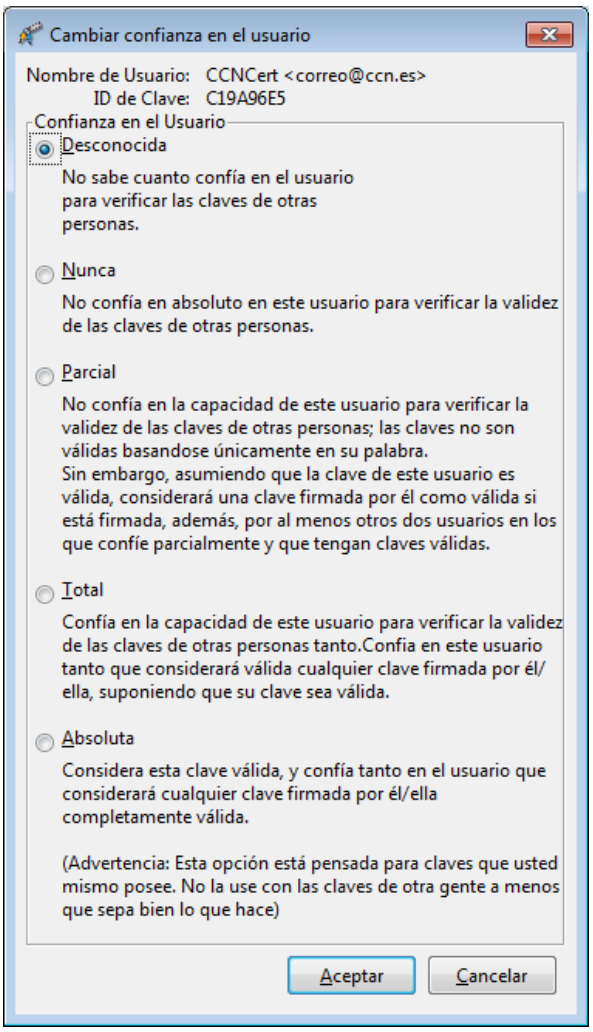

Figura 25.- Establecer confiabilidad de una clave

2.4. CIFRAR Y DESCIFRAR

41. Cada clave pública y privada tiene un papel específico en el cifrado y descifrado de documentos. Se puede pensar en una clave pública como en una caja fuerte de seguridad. Cuando un remitente cifra un documento usando una clave pública, ese documento se pone en la caja fuerte, la caja se cierra, y el bloqueo de la combinación de ésta se gira varias veces. La parte correspondiente a la clave privada, esto es, el destinatario, es la combinación que puede volver a abrir la caja y retirar el documento.

42. Dicho de otro modo, sólo la persona que posee la clave privada puede recuperar un documento cifrado usando la clave pública asociada al cifrado.

43. Con este modelo mental se ha mostrado el procedimiento de cifrar y descifrar documentos de un modo muy simple. Si el usuario quisiera cifrar un mensaje para Javier, lo haría usando la clave pública de Javier, y él lo descifraría con su propia clave privada. Si Javier quisiera enviar un mensaje al usuario, lo haría con la clave pública del usuario, y éste lo descifraría con su propia clave privada. A continuación se muestra como debería hacer esto con los archivos que se desean cifrar y descifrar.

2.4.1. CIFRAR

44. A continuación se detallan los pasos a seguir para el cifrado de un archivo:

45. Paso 1: Localice el documento o el archivo a cifrar y haga clic en él con el botón derecho. Se desplegará un menú, sitúe el cursor sobre **Más opciones de GpgEX** y a continuación seleccione **Cifrar**.

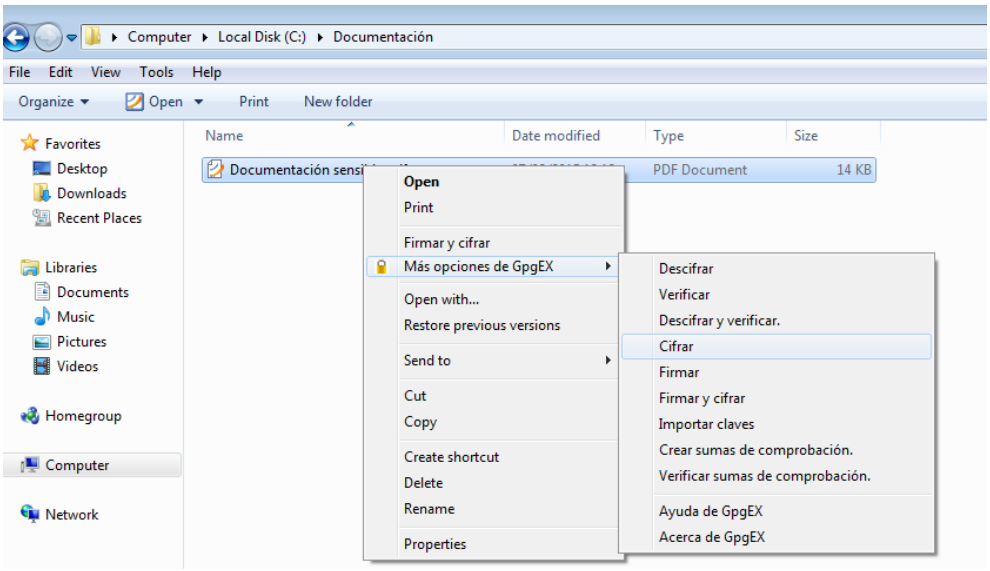

Figura 26.- Cifrar documentación

46. Paso 2: Seleccione **Next** en el siguiente menú para continuar.

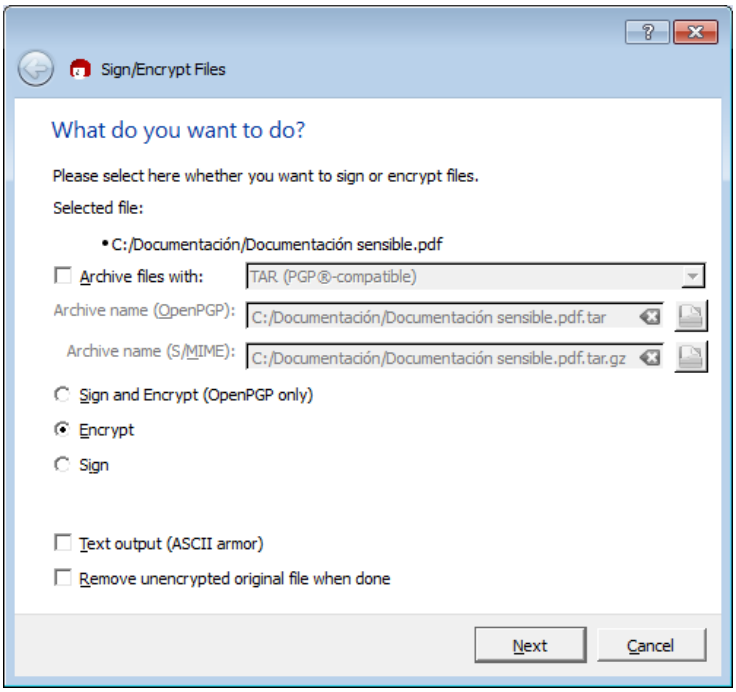

Figura 27.- Opciones de cifrado

47. Paso 3: Elija la clave o claves de cifrado en función de los destinatarios, pulsar en **Add** y a continuación **Encrypt**. Recuerde que para que usted pueda descifrar el mensaje o documento en un futuro deberá incluir su clave pública entre las elegidas.

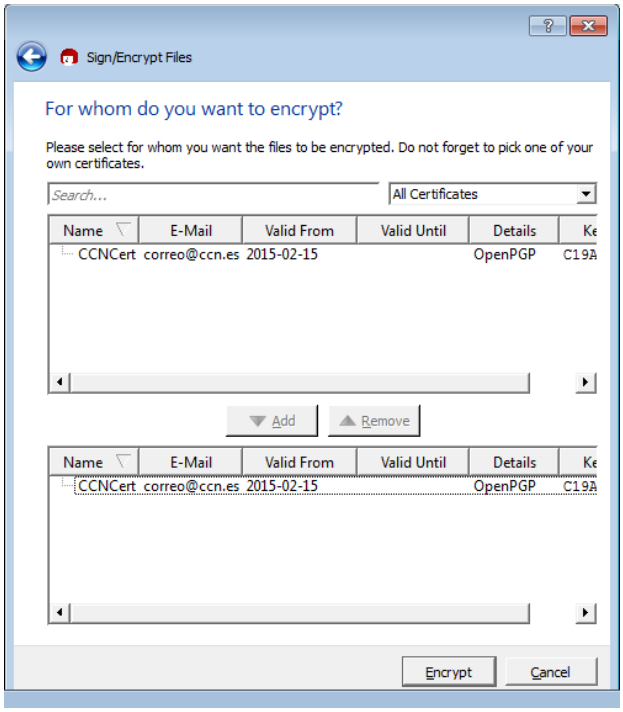

Figura 28.- Selección de destinatarios

48. Paso 4: Tras cifrar el archivo, aparecerá una ventana con los resultados y el fichero que ha generado GPG (el cual tendrá el mismo nombre, pero acabado en .gpg). Pulse **Finish** para terminar.

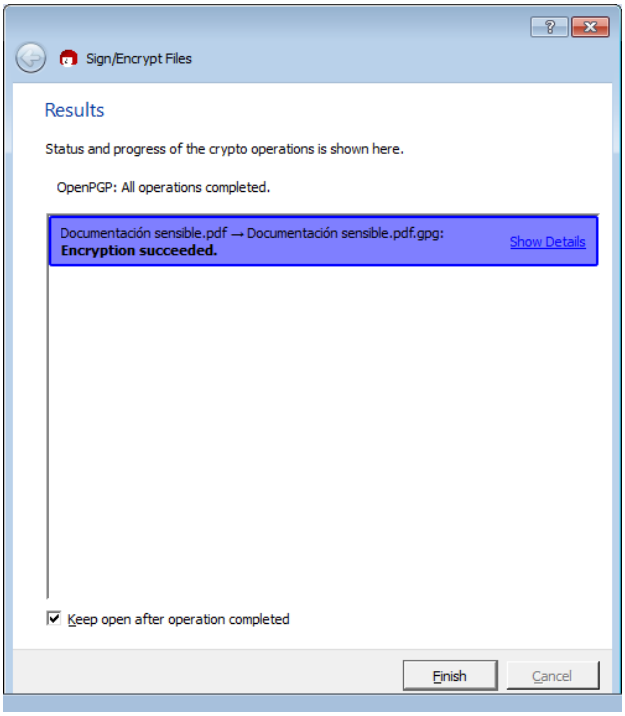

Figura 29.- Resultados de cifrado

2.4.2. DESCIFRAR

49. A continuación se detallan los pasos a seguir para el descifrado de un archivo:

50. Paso 1: Localice el archivo a descifrar y pulse con el botón derecho en el archivo. Se desplegará un menú, sitúe el cursor sobre **Más opciones de GpgEX** y a continuación pulse sobre **Descifrar**.

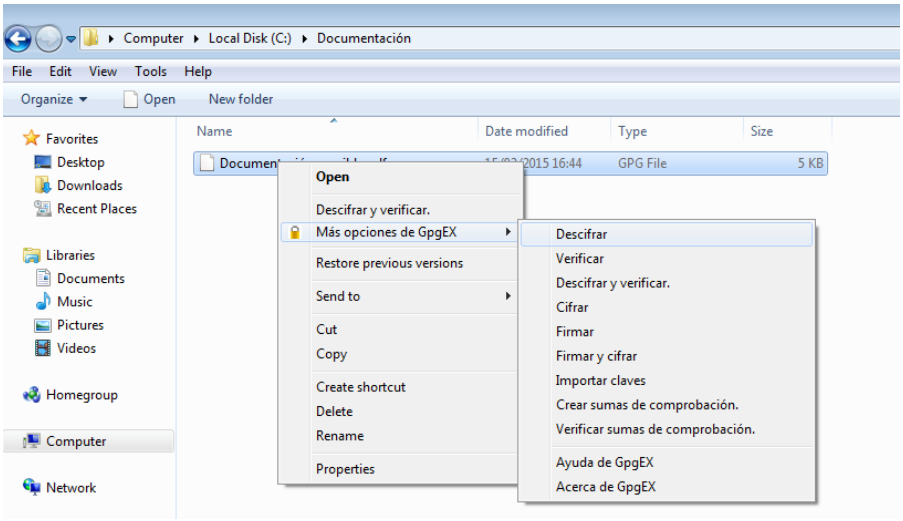

Figura 30.- Descifrar documentos

51. Paso 2: Elija la ruta de salida debajo de la opción **Create output files in a single folder**. Si no desea la ruta que le aparecerá por defecto, puede cambiarla pulsando el icono situado a la derecha de la ruta. Una vez esté conforme, continúe pulsando **Decrypt/Verify**.

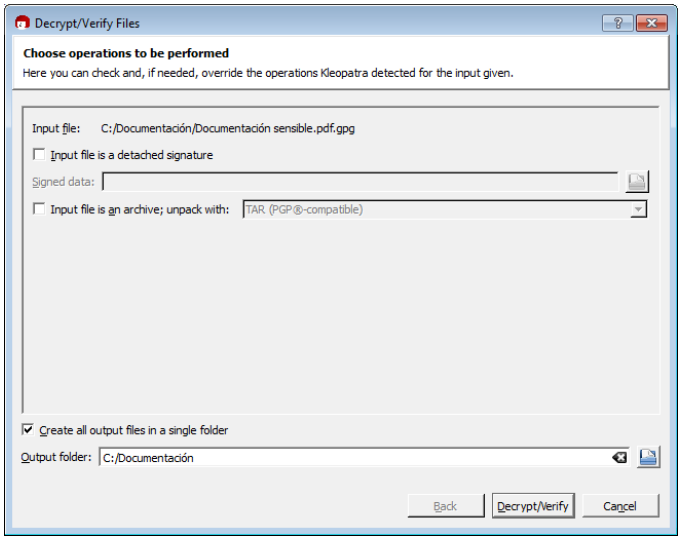

Figura 31.- Opciones de descifrado

52. Paso 3: Introduzca la contraseña.

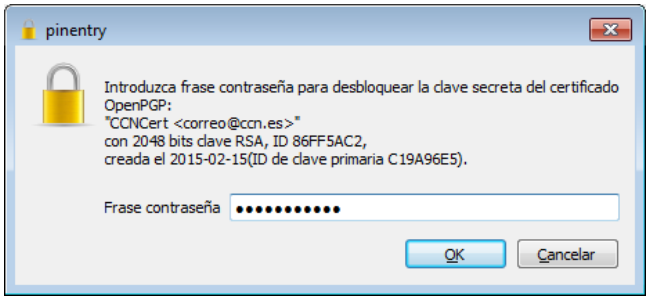

Figura 32.- Introducir la clave de descifrado

53. Paso 4: Una vez ingresada la clave correcta podrá ver el archivo descifrado en la ruta seleccionada anteriormente.

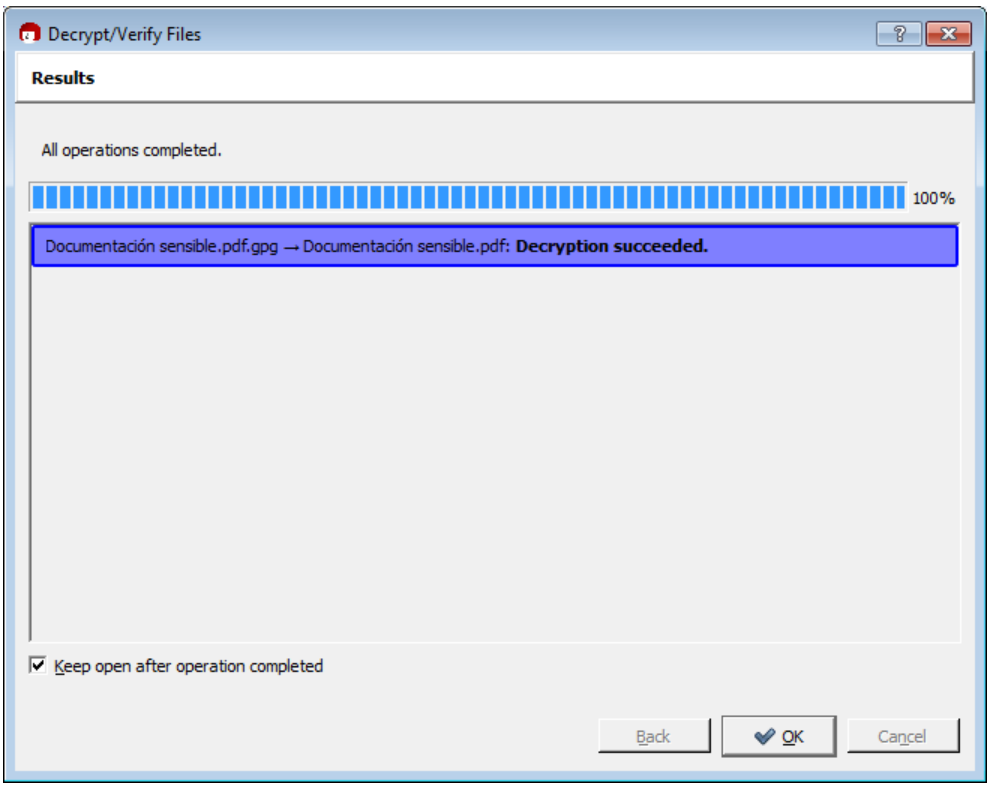

Figura 33.- Descifrado completado con éxito

2.5. FIRMAR Y VERIFICAR

54. Una firma digital certifica un documento y le añade una marca de tiempo. Si posteriormente el documento fuera modificado en cualquier modo, el intento de verificar la firma fallaría. La utilidad de una firma digital es la misma que la de una firma escrita a mano, sólo que la digital tiene una resistencia a la falsificación. Por ejemplo, la distribución del código fuente de GnuPG viene firmada con el fin de que los usuarios puedan verificar que no ha habido ninguna manipulación o modificación al código fuente desde que fue archivado.

55. Para la creación y verificación de firmas, se utiliza el par público y privado de claves en una operación que es diferente a la de cifrado y descifrado. La firma de un documento es generada con la clave privada del firmante. La firma se verifica por medio de la clave pública correspondiente. Por ejemplo, Javier haría uso de su propia clave privada para firmar digitalmente la entrega de su última ponencia a la Revista de Química Inorgánica. El editor asociado que la recibiera, usaría la clave pública de Javier para comprobar la firma, verificando de este modo que el envío proviene realmente de Javier, y que no ha sido modificado desde el momento en que Javier lo firmó. Una consecuencia directa del uso de firmas digitales es la dificultad en negar que fuera el propio usuario quien puso la firma digital, ya que ello implicaría que su clave privada ha sido comprometida.

2.5.1. FIRMAR

56. A continuación se detallan los pasos a seguir para la firma de un archivo.

57. Paso 1: Localice el archivo a firmar y pulse con el botón derecho en el archivo. Se desplegará un menú, sitúe el cursor sobre **Más opciones de GpgEX** y a continuación pulse sobre **Firmar**.

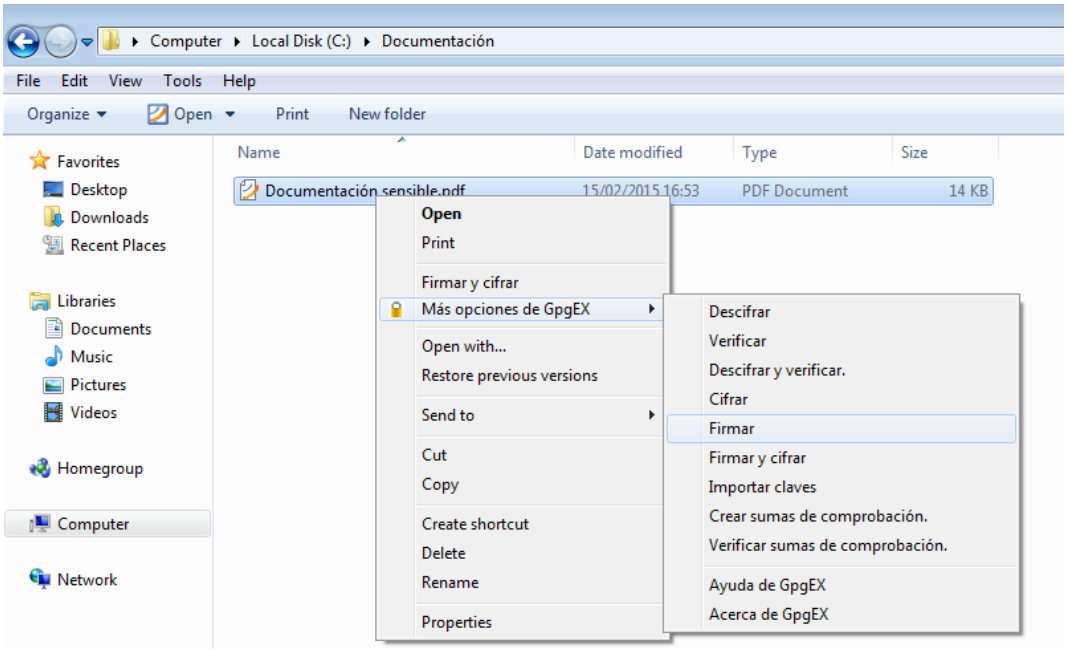

Figura 34.- Firmar documentación

58. Paso 2: Seleccione la opción **Sign**, y pulse **Next**.

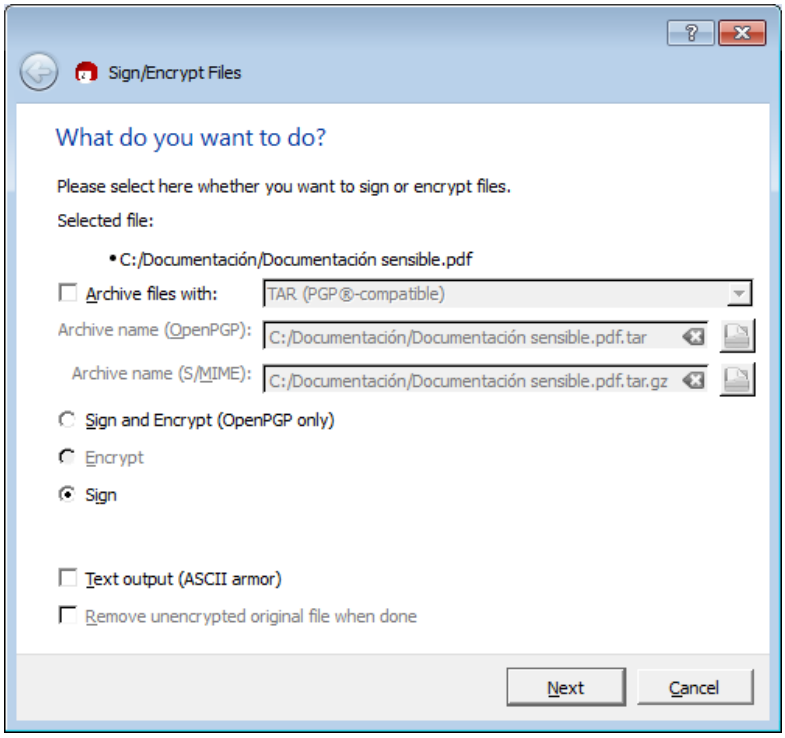

Figura 35.- Seleccionar opciones de firmado

59. Paso 3: Aparecerá un menú donde elegir el usuario con el que desee firmar. Deberá escoger uno en el menú desplegable que aparece debajo de **OpenPGP Signing Certificate**. Si desea que GPG le recuerde su elección en futuras acciones, marque la casilla **Remember these as default for future operations**. Continúe pulsando **Sign**.

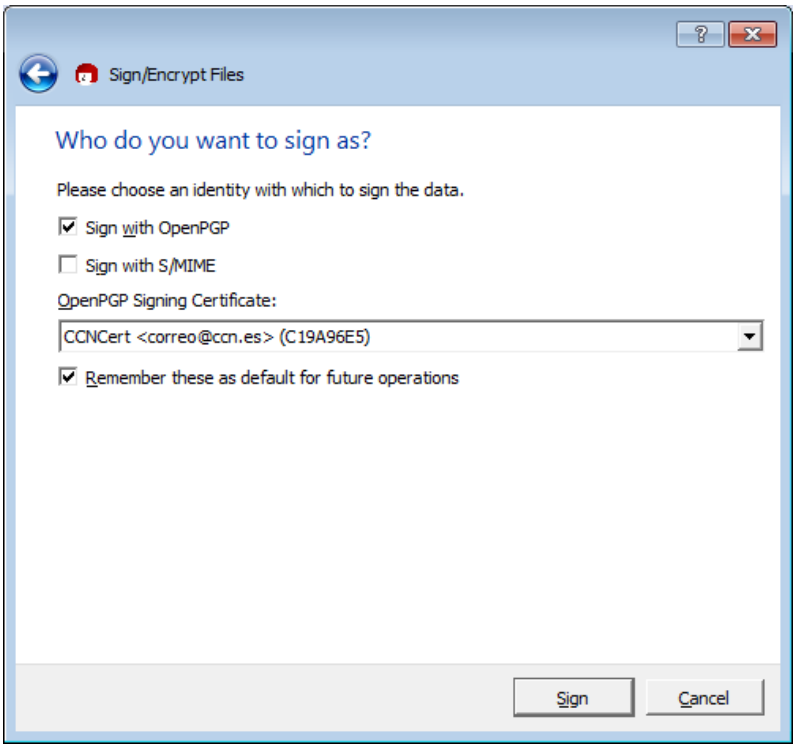

Figura 36.- Opciones de firmado

60. Paso 4: Le pedirá su contraseña, proceda a introducirla y pulse **OK**.

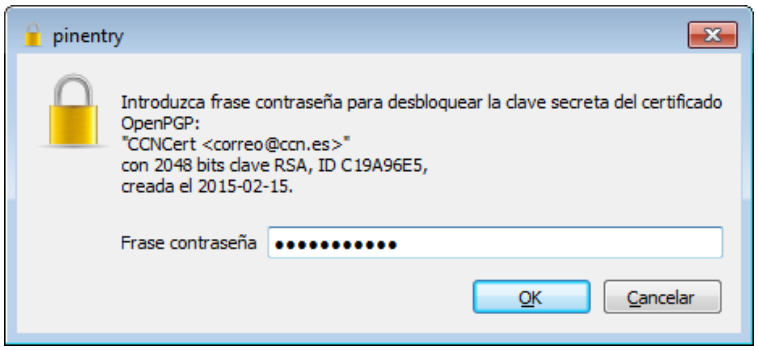

Figura 37.- Introducción de credenciales de firmado

61. Paso 5: Una vez terminado, le generará el fichero con formato .sig, en la ruta predeterminada; Pulse **Finish** para terminar.

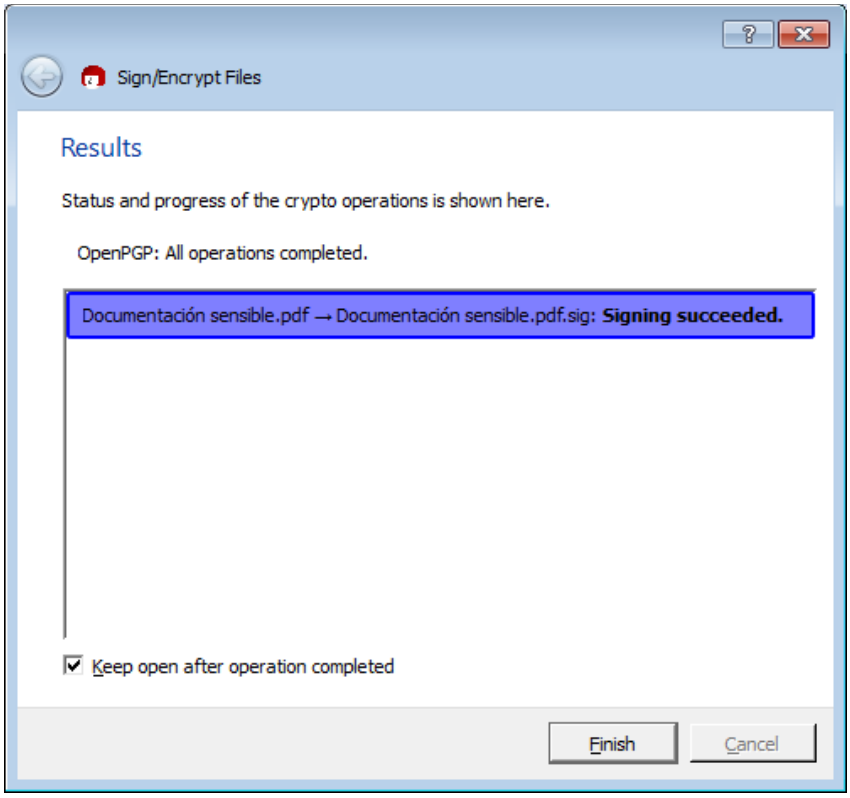

Figura 38.- Operaciones realizadas

2.5.2. VERIFICAR

62. A continuación se detallan los pasos a seguir para verificar la firma de un archivo:

63. Paso 1: Localice el archivo a verificar y a continuación pulse con el botón derecho en el archivo. Se desplegará un menú, sitúe el cursor sobre **Más opciones de GpgEX** y a continuación pulse sobre **Verificar**.

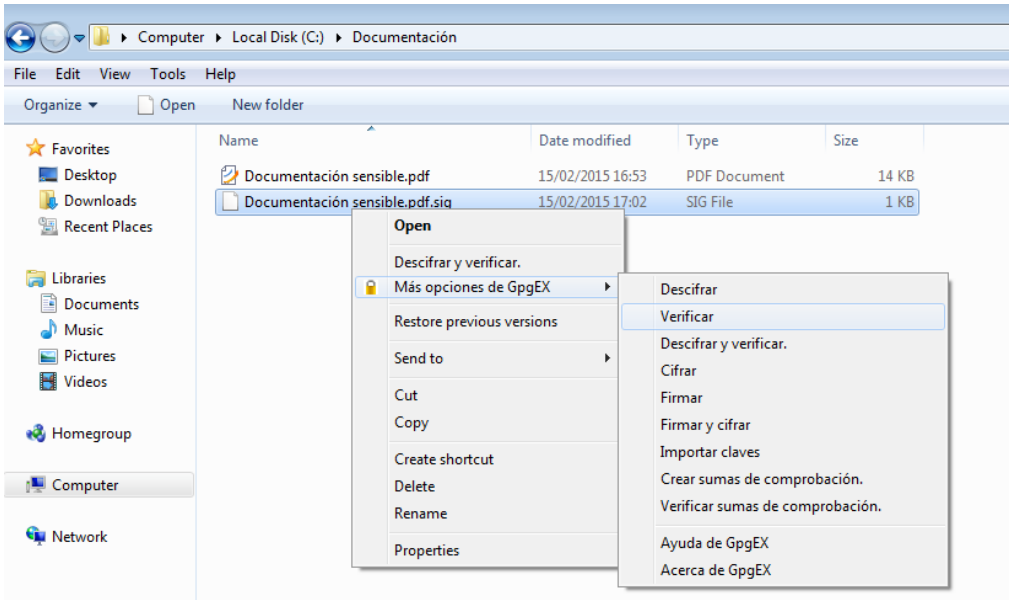

Figura 39.- Verificar documentación

64. Paso 2: Elija la ruta de salida debajo de la opción **Create output files in a single folder**. Si no desea la ruta que le aparecerá por defecto, puede cambiarla pulsando el icono situado a la derecha de la ruta. Una vez que esté conforme, continúe pulsando y **Decrypt/Verify**.

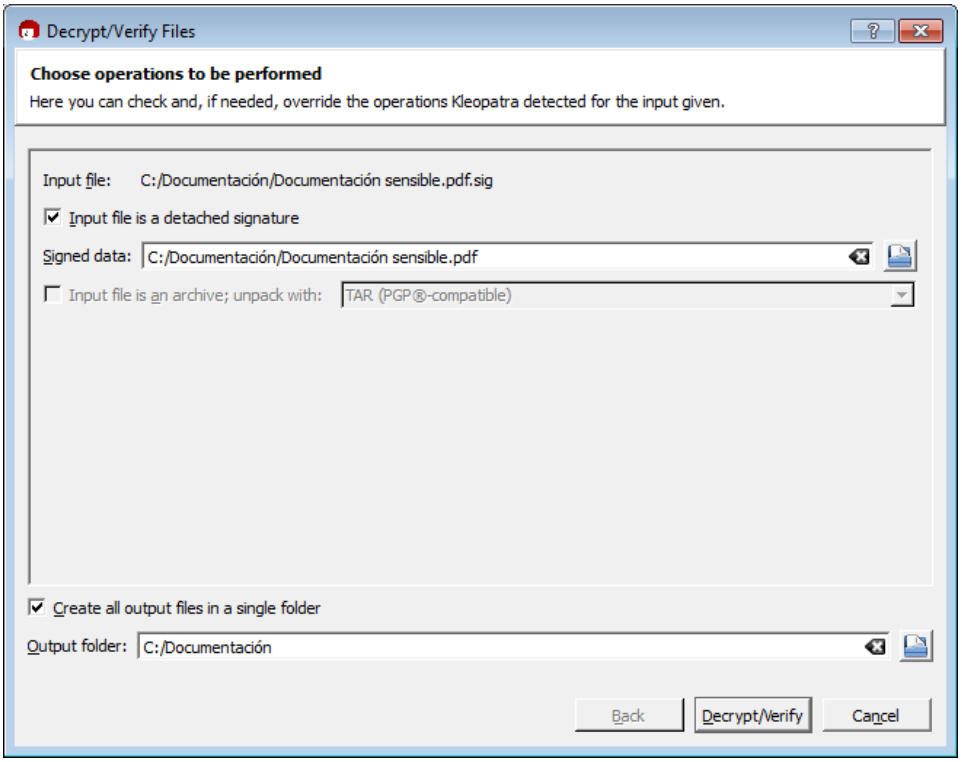

Figura 40.- Selección de operaciones a realizar

65. Paso 3: Una vez finalizada la acción, proceda a terminar pulsando **OK**.

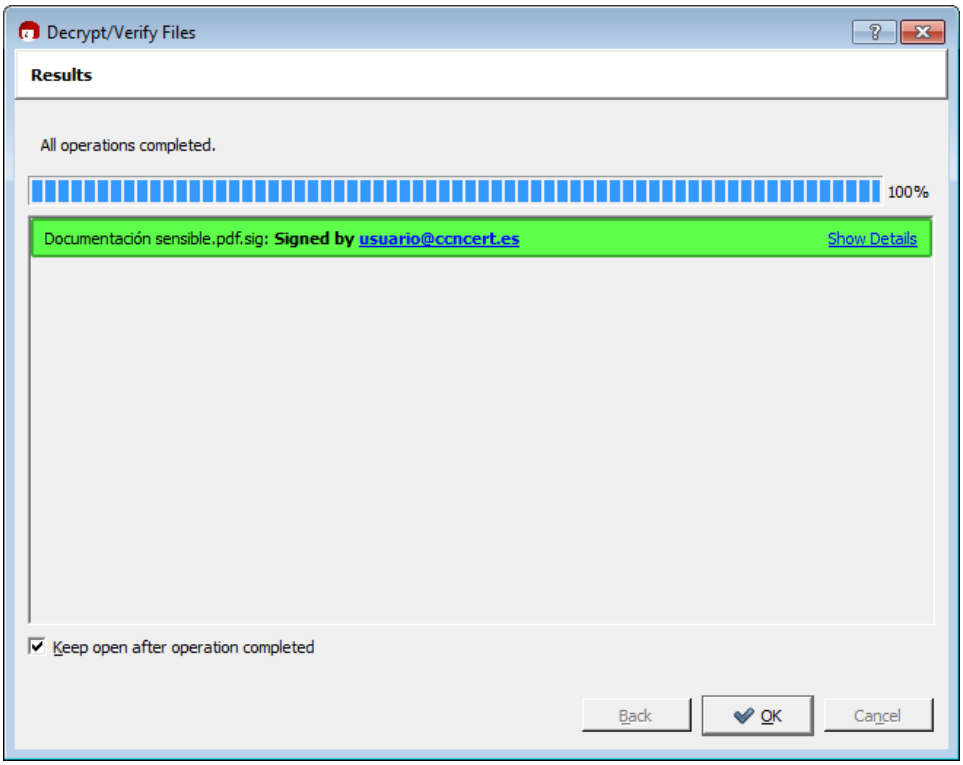

Figura 41.- Operaciones completadas

3. GPG VERSIÓN LINUX UBUNTU

3.1. INSTALACIÓN

66. GnuPG es una herramienta con licencia GPL (General Public License), y puede descargarse el software desde el siguiente enlace:
67. *https://www.gnupg.org/index.es.html*
68. Si el sistema operativo usado es Linux Ubuntu se puede descargar el conjunto de herramientas desde la web:
69. *https://www.gnupg.org/download/*
70. También es posible la instalación de esta herramienta mediante el gestor de software de Ubuntu.
71. A continuación se detallan los pasos a seguir para la instalación de GnuPG en un sistema Linux Ubuntu.
72. Paso 1: Desde el centro de Software de Ubuntu, busque la aplicación GPA. Una vez que el gestor encuentre la aplicación en el repositorio, pulse en **Instalar**.

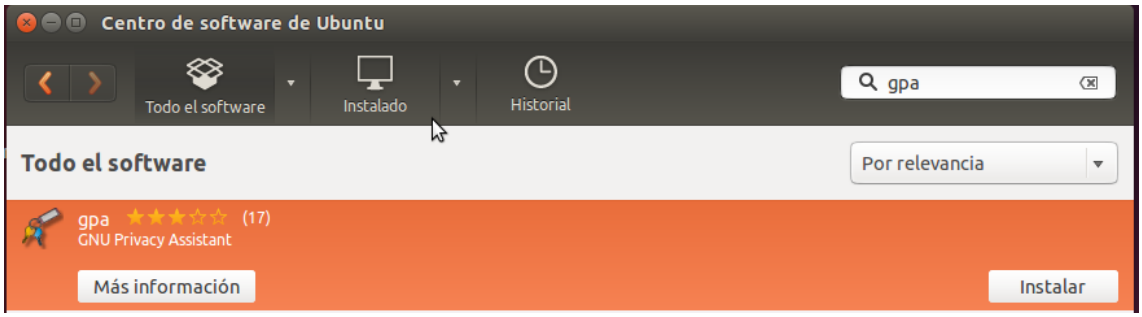

Figura 42.- Instalación a través del gestor de Software

73. Una vez realizado este único paso la aplicación se instalará y se configurará para su primer uso.

3.2. GENERACIÓN DE CLAVES

74. En este apartado se detallan los pasos a seguir para la creación de un par de claves (pública y privada) de uso personal. Se recomienda el uso del asistente para creación de claves GPA.
75. Para la creación de las claves, acceda a la aplicación GPA. Para ello puede ejecutar la aplicación desde el propio lanzador de aplicaciones o utilizar el buscador de Ubuntu.

Figura 43.- Ubicación de aplicación GPA

76. Paso 1: Seleccione el menú **Keys** y seguidamente seleccione la opción **New key**.

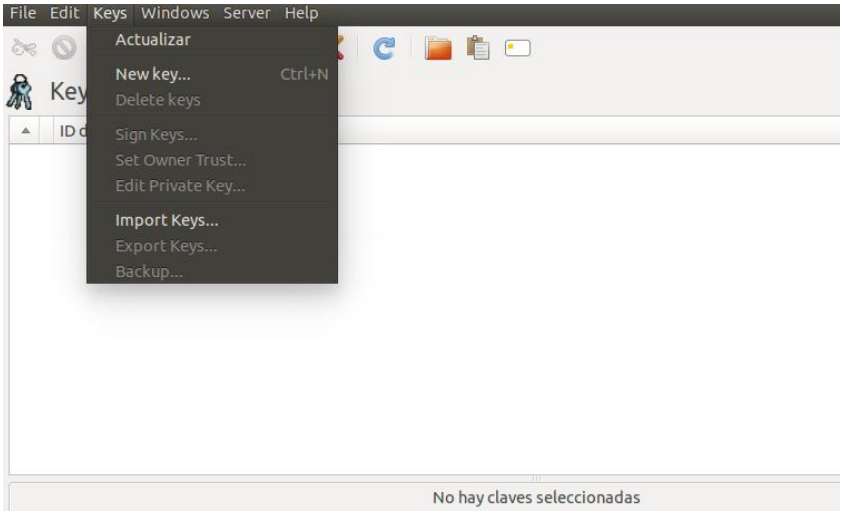

Figura 44.- Creación de nuevo par de claves

77. Paso 2: Introduzca su nombre y pulse **Adelante**.

Figura 45.- Generación de par de claves

78. Paso 3: Introduzca la dirección de correo electrónico desde la cual se van a enviar los mensajes cifrados o firmados y pulsar **Adelante**.

Figura 46.- Generación de claves

79. Paso 4: Para crear una copia de seguridad, ésta deberá ser guardarla en un lugar secreto y a poder ser cifrado para imposibilitar su uso por personas que no conozcan la clave.

Figura 47.- Realización de copia de seguridad de nueva clave

80. Paso 5: Introduzca una contraseña segura y robusta de acceso (basada en la combinación de caracteres alfanuméricos tanto en mayúsculas como en minúsculas y símbolos o en su defecto una frase de paso suficientemente larga). Tras introducir la contraseña, pulse **OK** y a continuación vuelva a introducir la contraseña y pulse de nuevo **OK**.

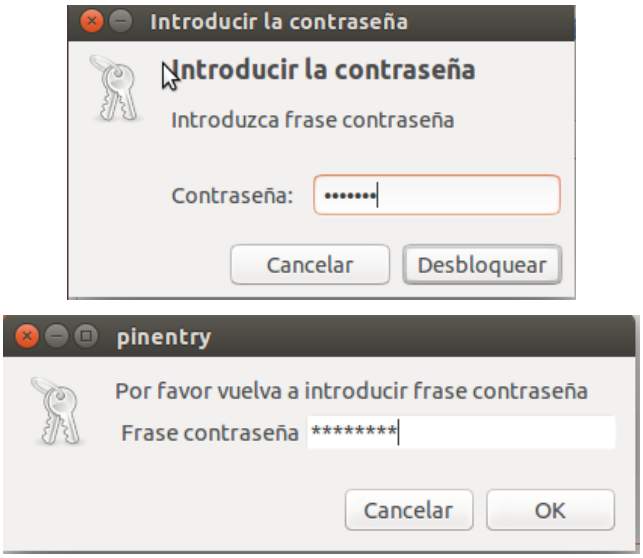

Figura 48.- Introducción de contraseña

81. Paso 6: Visualización de la pantalla donde se aprecia la creación de la clave.

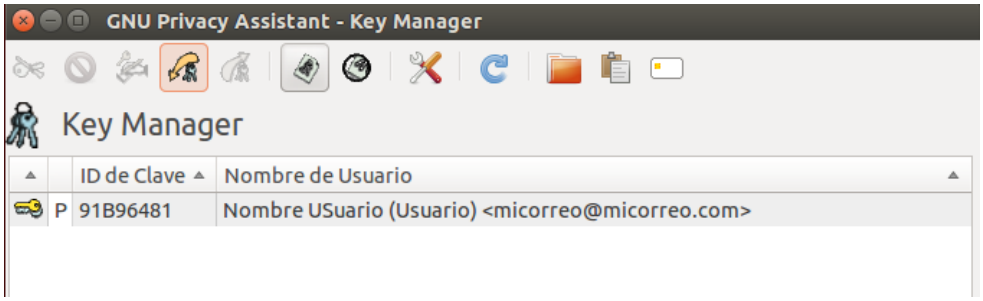

Figura 49.- Visualización de claves

3.3. INTERCAMBIO DE CLAVES

82. Para que usted pueda tener un intercambio de mensajes seguros (cifrados o firmados), es necesario enviar una clave pública así como recibirla de otros usuarios, de esta manera se puede verificar que un correo es enviado por una persona en concreto.

83. Existen varios métodos para enviar la clave pública, el método más seguro es la entrega de forma presencial, pero también existen otros métodos, como por ejemplo subir la clave pública a un servidor de claves PGP, como por ejemplo el servidor *https://pgp.rediris.es*.

3.3.1. EXPORTAR CLAVE

84. A continuación se detallan los pasos a seguir para exportar una clave mediante el uso del software GPA.

85. Paso 1: Sobre la clave que desea exportar, pulse con el botón derecho del ratón la opción **Export keys** e introduzca un nombre y una ubicación para el archivo, después pulse **Guardar** para guardarlo. Este será el archivo a enviar para la comunicación de forma segura.

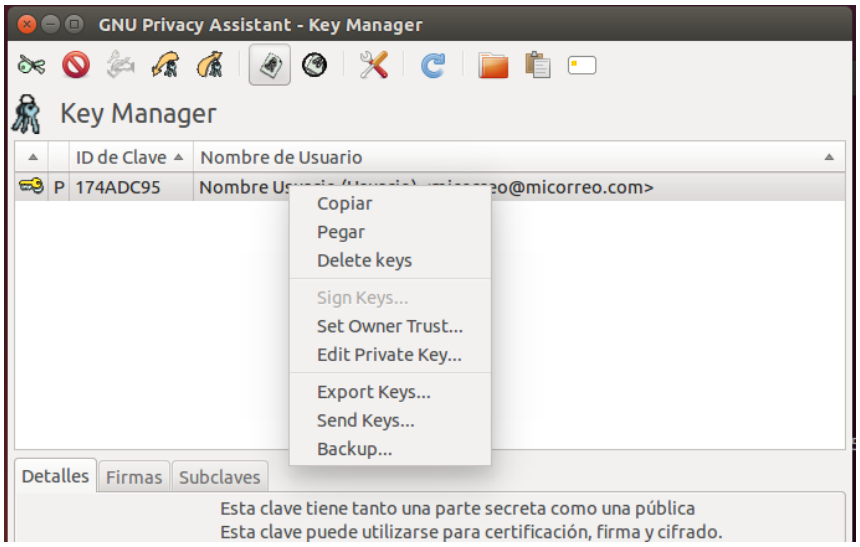

Figura 50.- Proceso para exportar clave

86. Paso 2: Información de la exportación.

Figura 51.- Información del proceso de exportación

3.3.2. IMPORTAR CLAVE

87. A continuación se detallan los pasos a seguir para importar una clave mediante el uso del software GPA.

88. Paso 1: Pulse el botón de **Keys → Import Keys**.

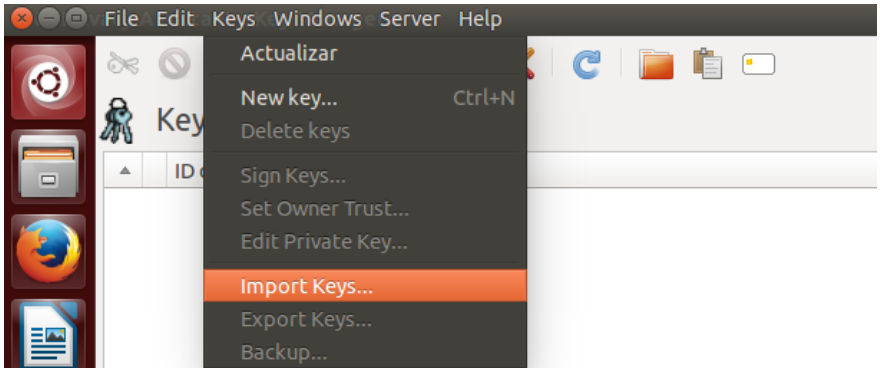

Figura 52.- Importar clave

89. Paso 2: Seleccionar el archivo y pulsar en Open.

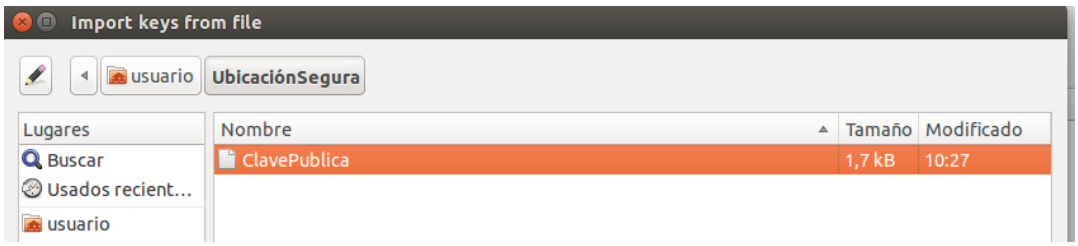

Figura 53.- Importar clave

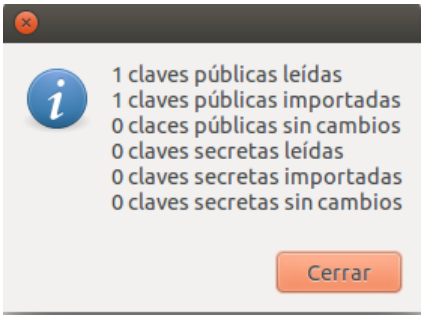

Figura 54.- Tareas realizadas por la herramienta GPA

90. Paso 3: Una vez haya importado la clave se mostrará en la interfaz.

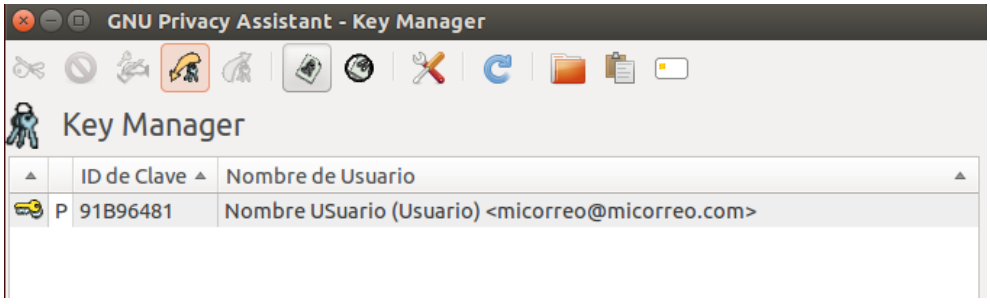

Figura 55.- Importar claves

91. Paso 4: Haga clic con el botón derecho sobre la clave y elija la opción **Set Owner Trust**, esta opción le permitirá configurar el nivel de confianza de dicha clave.

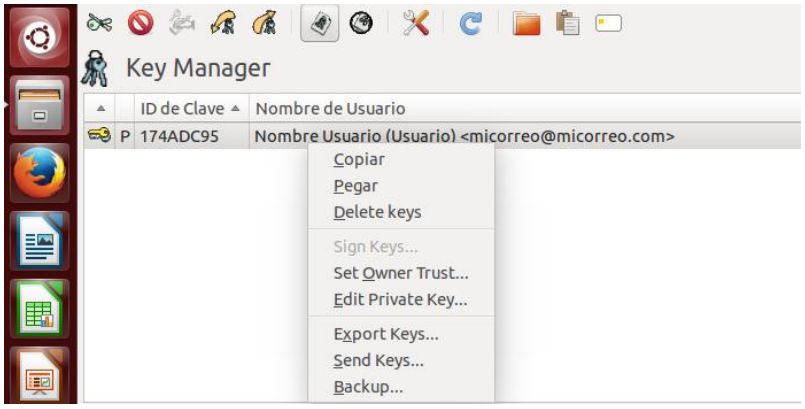

Figura 56.- Confiabilidad de una clave

92. Paso 5: A continuación le aparecerá un menú con las opciones perfectamente detalladas. Seleccione la que aplique en cada caso.

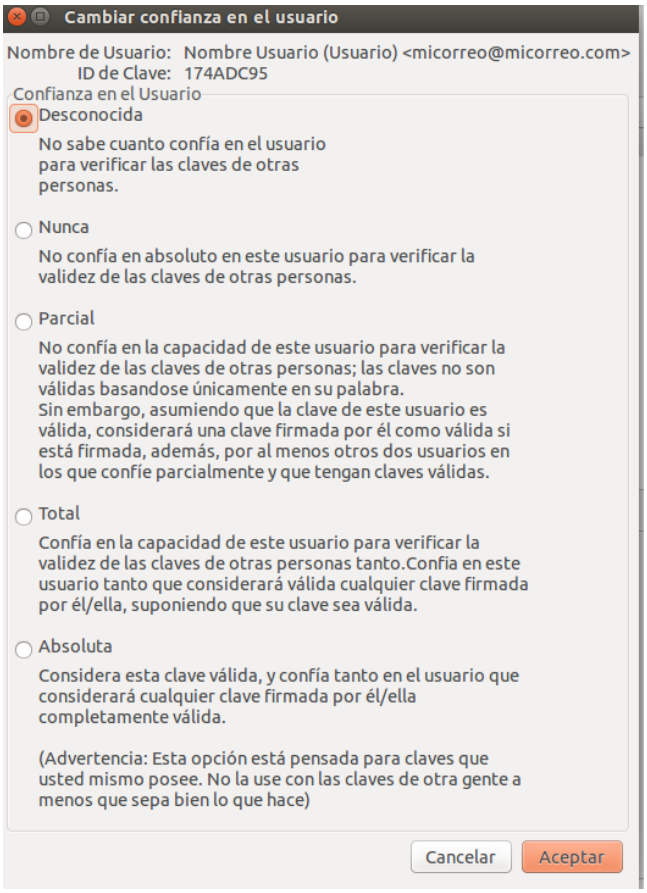

Figura 57.- Establecer confiabilidad de una clave

3.4. CIFRAR Y DESCIFRAR

93. Cada clave pública y privada tiene un papel específico en el cifrado y descifrado de documentos. Se puede pensar en una clave pública como en una caja fuerte de seguridad. Cuando un remitente cifra un documento usando una clave pública, ese documento se pone en la caja fuerte, la caja se cierra, y el bloqueo de la combinación de ésta se gira varias veces. La parte correspondiente a la clave privada, esto es, el destinatario, es la combinación que puede volver a abrir la caja y retirar el documento.

94. Dicho de otro modo, sólo la persona que posee la clave privada puede recuperar un documento cifrado usando la clave pública asociada al cifrado.

95. Con este modelo mental se ha mostrado el procedimiento de cifrar y descifrar documentos de un modo muy simple. Si el usuario quisiera cifrar un mensaje para Javier, lo haría usando la clave pública de Javier, y él lo descifraría con su propia clave privada. Si Javier quisiera enviar un mensaje al usuario, lo haría con la clave pública del usuario, y éste lo descifraría con su propia clave privada. A continuación se muestra como debería hacer esto con los archivos que se desean cifrar y descifrar.

3.4.1. CIFRAR

96. A continuación se detallan los pasos a seguir para el cifrado de un archivo:

97. Paso 1: Desde el menú principal de GPA, utilice el icono de carpeta para abrir el asistente de cifrado de archivos, tal y como se muestra en la siguiente captura.

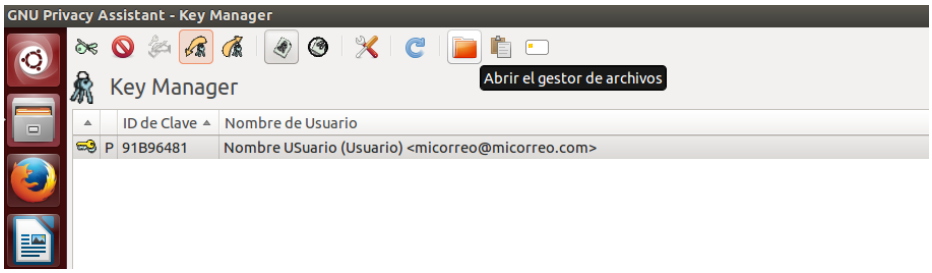

Figura 58.- Cifrar documentación

98. Paso 2: Una vez seleccionado el fichero o conjunto de ficheros, seleccione la opción **Open**. Una vez se encuentre el fichero cargado en el Gestor de Archivos, pulse el ícono relacionado con la opción de Cifrado, tal y como se muestra en la siguiente pantalla.

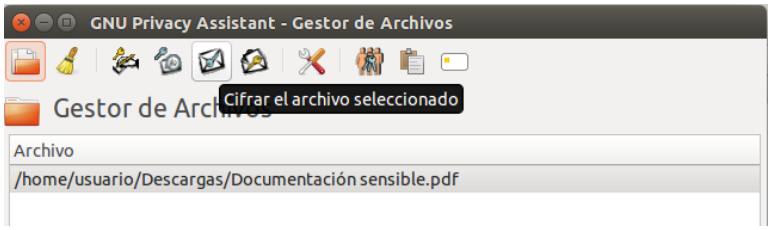

Figura 59.- Opciones de cifrado

99. Paso 3: Elija la clave o claves de cifrado en función de los destinatarios, pulsar en **Aceptar**. Recuerde que para que usted pueda descifrar el mensaje o documento en un futuro deberá incluir su clave pública entre las elegidas.

Figura 60.- Selección de destinatarios

100. Paso 4: Tras cifrar el archivo, aparecerá una ventana con los resultados y el fichero que ha generado GPG (el cual tendrá el mismo nombre, pero acabado en .gpg).

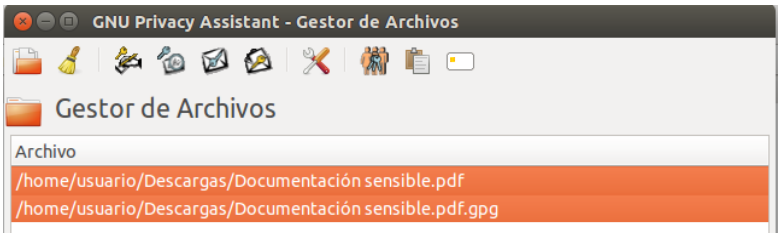

Figura 61.- Resultados del cifrado

3.4.2. DESCIFRAR

101. A continuación se detallan los pasos a seguir para el descifrado de un archivo:

102. Paso 1: Desde el Gestor de Archivos de GPA, abra el fichero que desea descifrar. Una vez localizado, pulse el ícono de descifrado, tal y como se muestra en la siguiente figura.

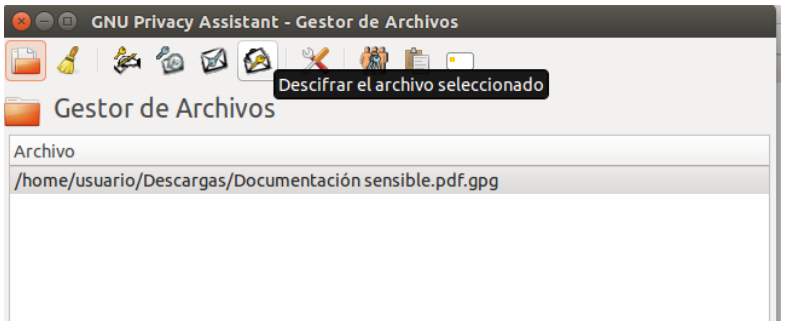

Figura 62.- Opciones de descifrado

103. Paso 2: Introduzca la contraseña.

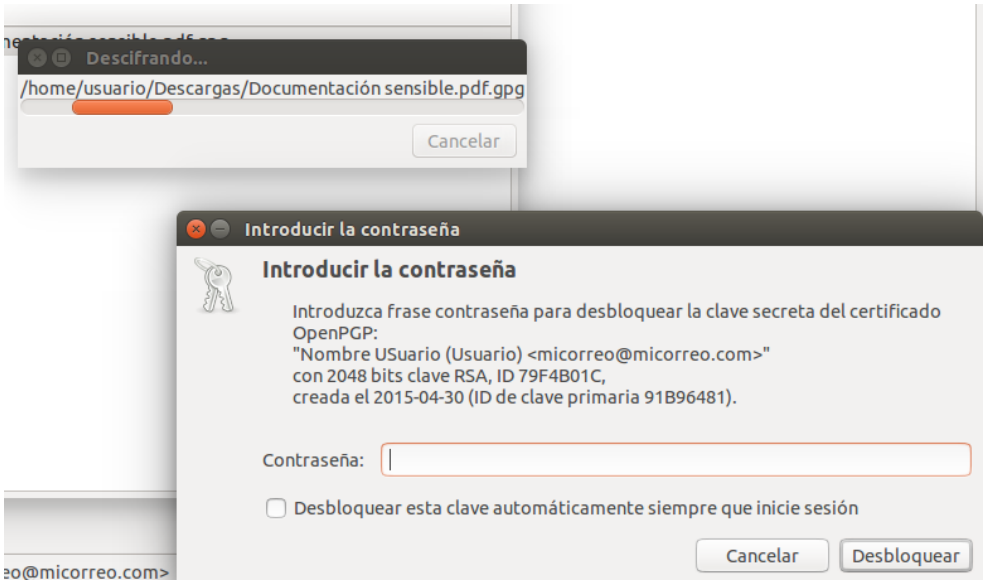

Figura 63.- Introducir la clave de descifrado

104. Paso 3: Una vez introducida la clave correcta podrá ver el archivo.

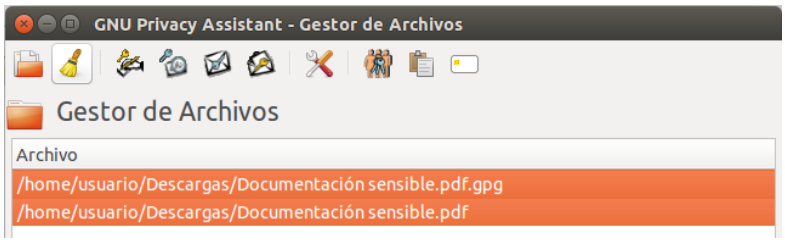

Figura 64.- Resultados del descifrado

3.5. FIRMAR Y VERIFICAR

105. Una firma digital certifica un documento y le añade una marca de tiempo. Si posteriormente el documento fuera modificado en cualquier modo, el intento de verificar la firma fallaría. La utilidad de una firma digital es la misma que la de una firma escrita a mano, sólo que la digital tiene una resistencia a la falsificación. Por ejemplo, la distribución del código fuente de GnuPG viene firmada con el fin de que los usuarios puedan verificar que no ha habido ninguna manipulación o modificación al código fuente desde que fue archivado.

106. Para la creación y verificación de firmas, se utiliza el par público y privado de claves en una operación que es diferente a la de cifrado y descifrado. La firma de un documento es generada con la clave privada del firmante. La firma se verifica por medio de la clave pública correspondiente. Por ejemplo, Javier haría uso de su propia clave privada para firmar digitalmente la entrega de su última ponencia a la Revista de Química Inorgánica. El editor asociado que la recibiera, usaría la clave pública de Javier para comprobar la firma, verificando de este modo que el envío proviene realmente de Javier, y que no ha sido modificado desde el momento en que Javier lo firmó. Una consecuencia directa del uso de firmas digitales es la dificultad en negar que fuera el propio usuario quien puso la firma digital, ya que ello implicaría que su clave privada ha sido comprometida.

3.5.1. FIRMAR

107. A continuación se detallan los pasos a seguir para la firma de un archivo.

108. Paso 1: Desde el gestor de archivos de GPA, localice y seleccione el archivo a firmar. A continuación pulse ícono relacionado con el firmado de ficheros, tal y como se muestra en la siguiente figura.

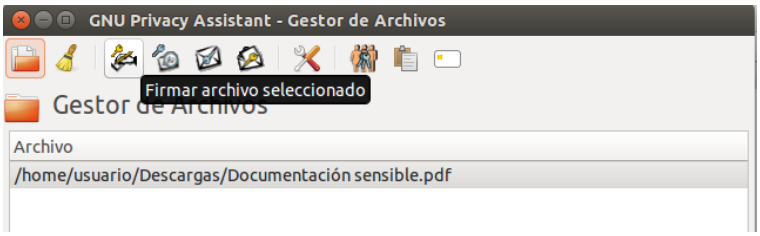

Figura 65.- Firmar documentación

109. Paso 2: Seleccione la opción **Detached Signature**, y pulse **Aceptar**.

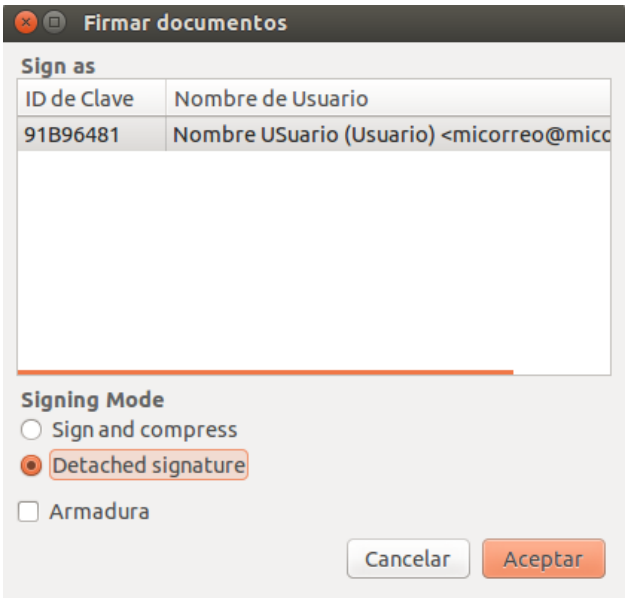

Figura 66.- Seleccionar opciones de firmado

110. Paso 3: Una vez terminado, le generará el fichero con formato .sig, en la ruta predeterminada.

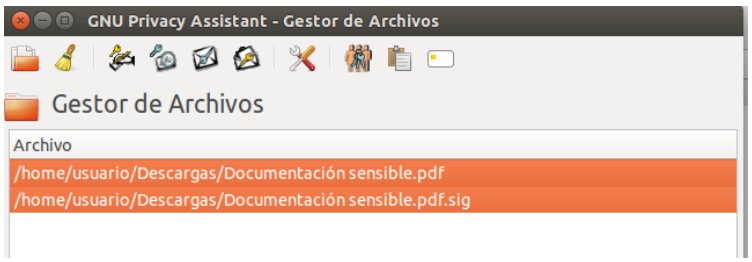

Figura 67.- Introducción de credenciales de firmado

3.5.2. VERIFICAR

111. A continuación se detallan los pasos a seguir para verificar la firma de un archivo:

112. Paso 1: Localice el archivo a verificar, y a continuación cargue el mismo en el gestor de archivos de GPA. Una vez cargado el fichero, pulse el ícono relacionado con la verificación de firma, tal y como se muestra en la siguiente figura.

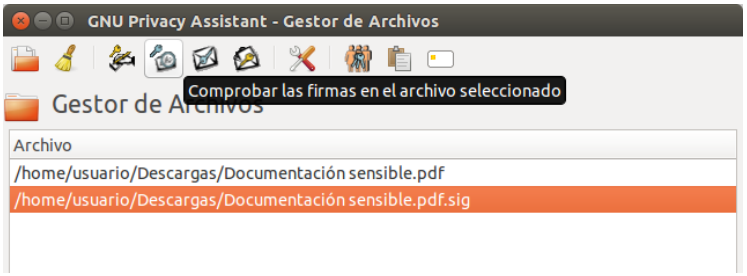

Figura 68.- Verificar documentación

113. Paso 2: Una vez pulsada la opción, la aplicación verificará la documentación junto con la firma cargada en el gestor de claves, indicando su estado, tal y como se muestra en la siguiente figura.

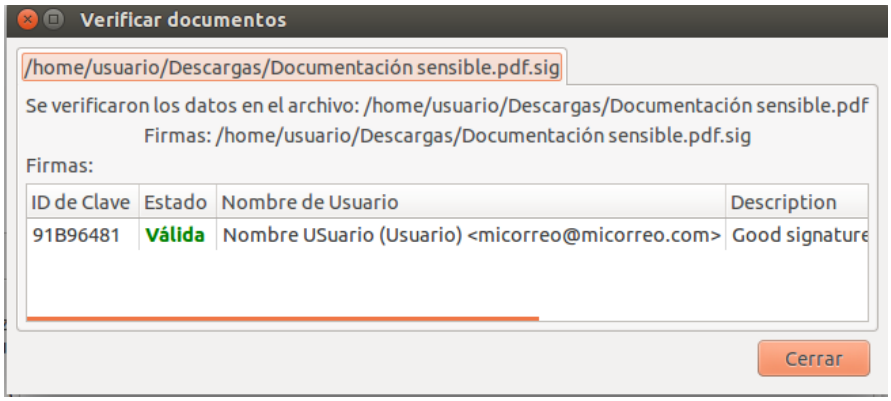

Figura 69.- Verificación de la firma

114. Paso 3: Una vez finalizada la acción, proceda a terminar pulsando **Cerrar**.

4. GPG SUITE VERSIÓN MAC OSX

4.1. INSTALACIÓN

115. GnuPG es una herramienta con licencia GPL (General Public License), y puede descargarse el software desde el siguiente enlace:

116. *https://www.gnupg.org/index.es.html*

117. Si el sistema operativo usado es Mac OS se puede descargar el conjunto de herramientas desde la web:

118. *https://gpgtools.org/gpgsuite.html*

119. A continuación se detallan los pasos a seguir para la instalación de GPG Suite en un sistema Mac OSX.

120. Paso 1: Una vez descargado y validado el software GPG Suite, ábralo y pulse la opción **Install**.

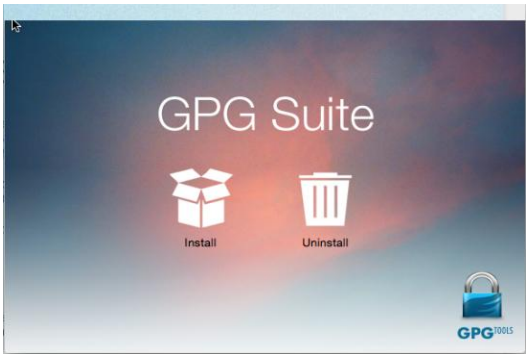

Figura 70.- Inicio de instalación

121. Paso 2: Acepte las opciones de instalación y pulse **Continue**.

Figura 71.- Opciones de instalación

- GPGMail: Opción que instala un cliente de correo
- GPG Keychain: Opción que instala un entorno gráfico para el uso de GnuPG.
- GPGServices: Opción para habilitar/deshabilitar las funcionalidades de GPG de una manera flexible y ágil.
- GPGPreferences: Cliente para gestionar las preferencias de GPG.
- MacGPG2: Software GPG.

122. Paso 3: Seleccione la ruta de instalación preferida y pulse **Continue**.

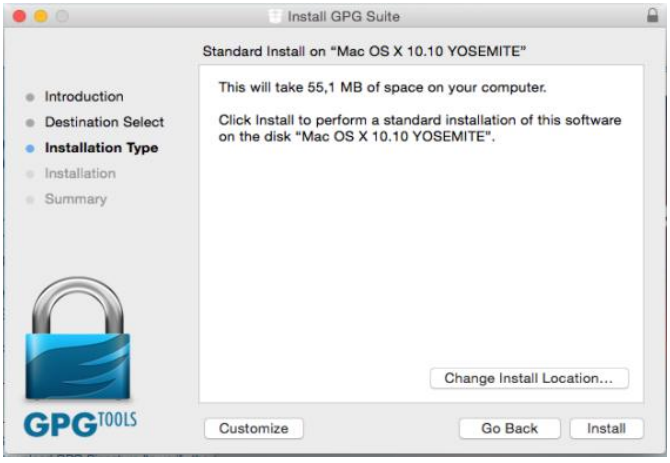

Figura 72.- Opción de cambio de ruta de instalación

123. Paso 4: Proceso de instalación.

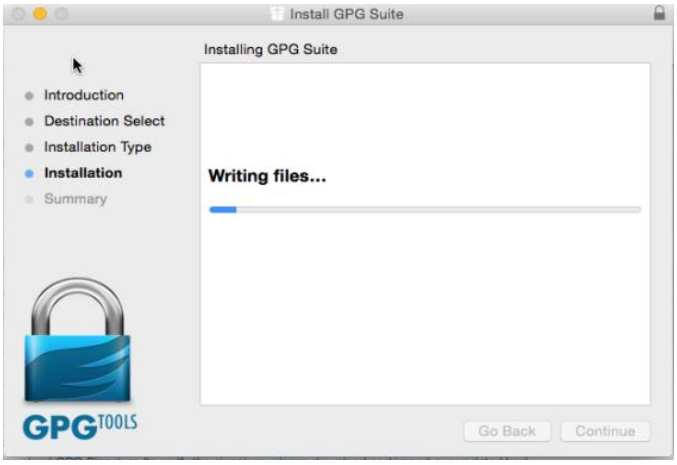

Figura 73.- Proceso de instalación

124. Paso 5: Una vez realizado este paso se habrá concluido el proceso de instalación de GPG Suite.

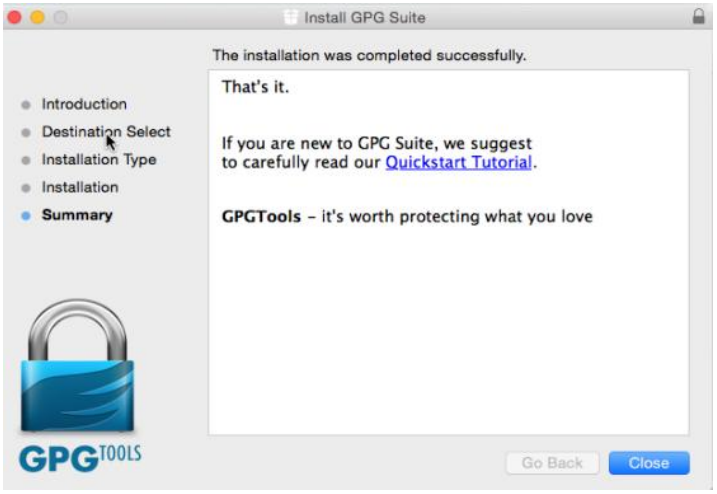

Figura 74.- Finalización de la instalación

4.2. GENERACIÓN DE CLAVES

125. En este apartado se detallan los pasos a seguir para la creación de un par de claves (pública y privada) de uso personal. Se recomienda el uso del gestor de claves **GPG KeyChain**, incluido en el software GPG Suite.

126. Paso 1: Para la creación de las claves, acceda a la aplicación **GPG KeyChain**. Para ello puede utilizar Finder de Mac, y buscar por GPG KeyChain, tal y como se muestra en la siguiente figura:

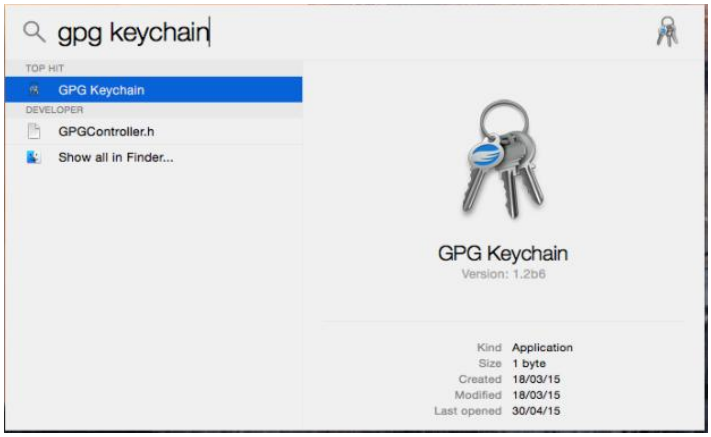

Figura 75.- Ubicación de aplicación GPG Keychain

127. Paso 2: Pulse el ícono **New**.

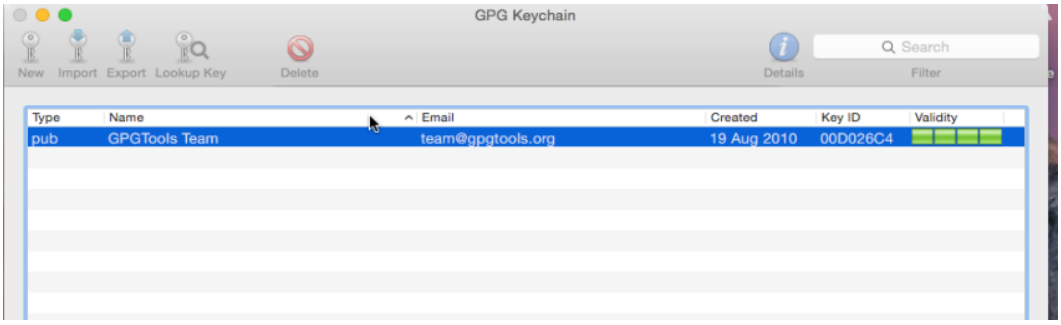

Figura 76.- Creación de nuevo par de claves

128. Paso 3: Introduzca la información solicitada en la pantalla de generación de claves. Una vez finalizado pulse el botón **Generate key**.

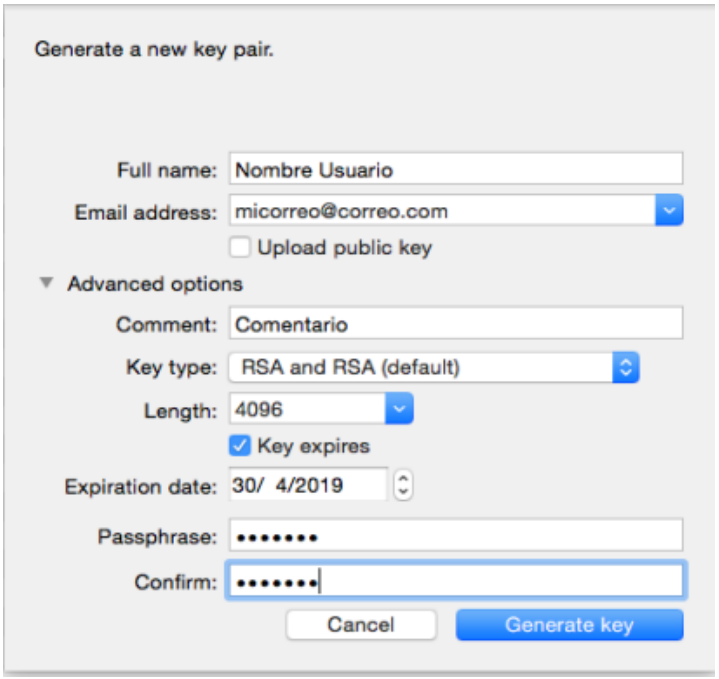

Figura 77.- Generación de par de claves

129. Paso 4: Visualización de la pantalla donde se aprecia la creación de la clave.

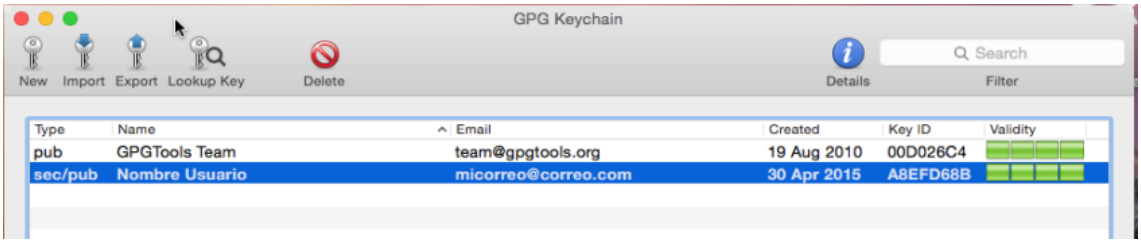

Figura 78.- Visualización de claves

4.3. INTERCAMBIO DE CLAVES

130. Para que usted pueda tener un intercambio de mensajes seguros (cifrados o firmados), es necesario enviar una clave pública así como recibirla de otros usuarios, de esta manera se puede verificar que un correo es enviado por una persona en concreto.

131. Existen varios métodos para enviar la clave pública, el método más seguro es la entrega de forma presencial, pero también existen otros métodos, como por ejemplo subir la clave pública a un servidor de claves PGP, como por ejemplo el servidor *https://pgp.rediris.es*.

4.3.1. EXPORTAR CLAVE

132. A continuación se detallan los pasos a seguir para exportar una clave mediante el uso del software GPG KeyChain.

133. Paso 1: Pulse el botón de **Export** e introduzca un nombre y una ubicación para el archivo, después pulse **Save** para guardarlo. Este será el archivo a enviar para la comunicación de forma segura.

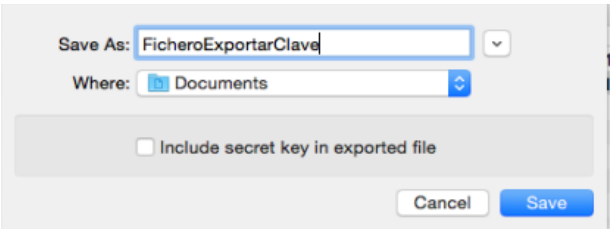

Figura 79.- Proceso para exportar clave

4.3.2. IMPORTAR CLAVE

134. A continuación se detallan los pasos a seguir para importar una clave mediante el uso del software GPG KeyChain.

135. Paso 1: Pulse el botón **Import**, situado en la esquina superior izquierda.

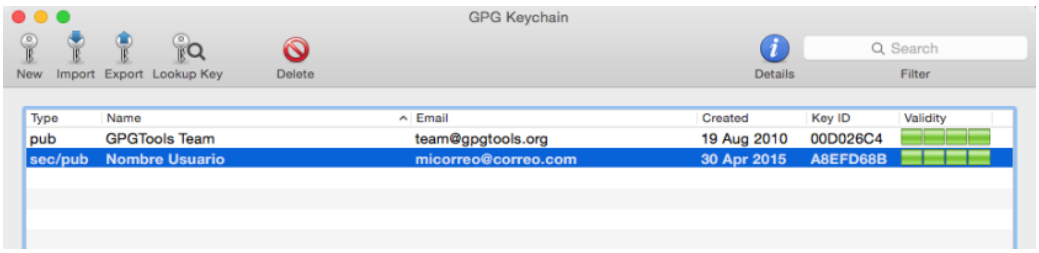

Figura 80.- Importar clave

136. Paso 2: Seleccione el archivo.

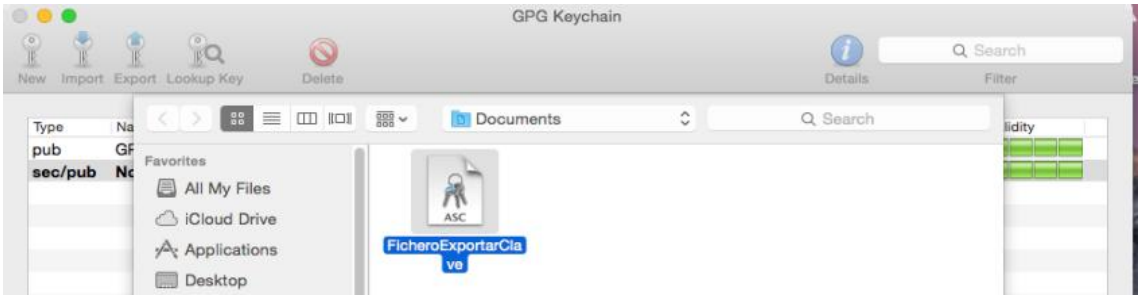

Figura 81.- Importar clave

Figura 82.- Tareas realizadas por la herramienta GPG KeyChain

137. Paso 3: Una vez haya importado la clave se mostrará en la interfaz.

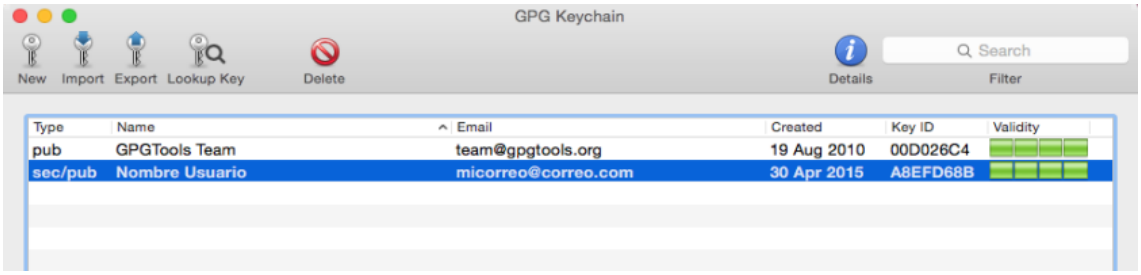

Figura 83.- Importar claves

138. Paso 4: Haga clic con el botón derecho sobre la clave y elija la opción **Details**, esta opción le permitirá configurar el nivel de confianza de dicha clave.

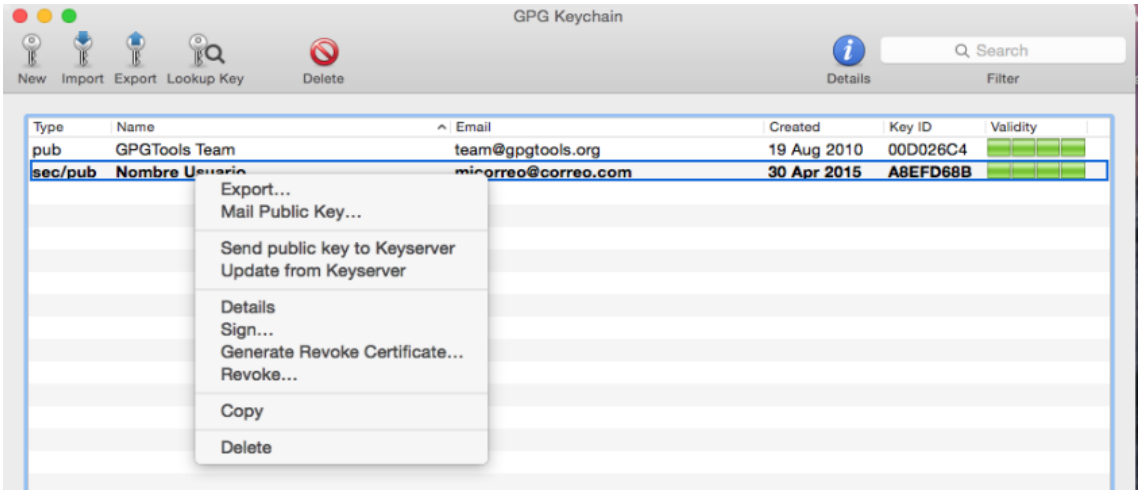

Figura 84.- Confiabilidad de una clave

139. Paso 5: A continuación le aparecerá un menú con las opciones de confianza. Seleccione la que aplique en cada caso.

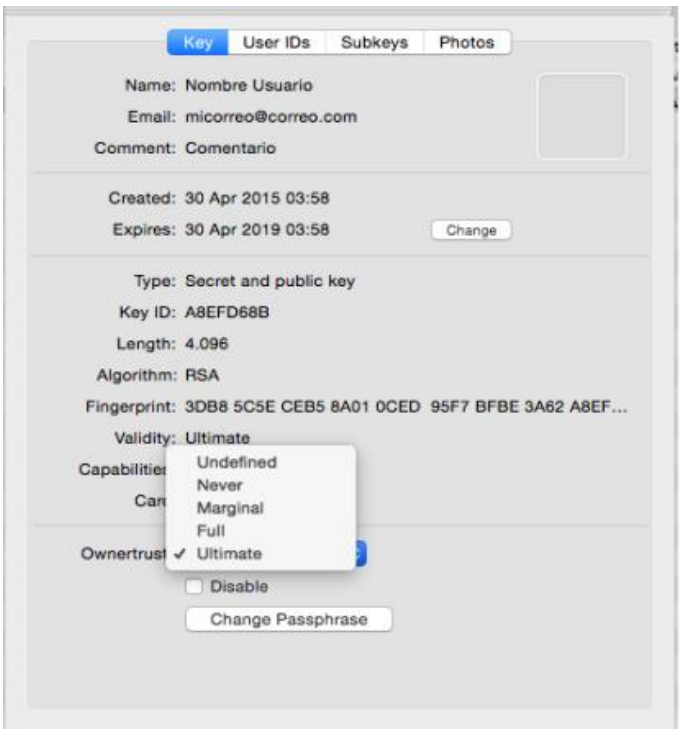

Figura 85.- Establecer confiabilidad de una clave

4.4. CIFRAR Y DESCIFRAR

140. Cada clave pública y privada tiene un papel específico en el cifrado y descifrado de documentos. Se puede pensar en una clave pública como en una caja fuerte de seguridad. Cuando un remitente cifra un documento usando una clave pública, ese documento se pone en la caja fuerte, la caja se cierra, y el bloqueo de la combinación de ésta se gira varias veces. La parte correspondiente a la clave privada, esto es, el destinatario, es la combinación que puede volver a abrir la caja y retirar el documento.

141. Dicho de otro modo, sólo la persona que posee la clave privada puede recuperar un documento cifrado usando la clave pública asociada al cifrado.

142. Con este modelo mental se ha mostrado el procedimiento de cifrar y descifrar documentos de un modo muy simple. Si el usuario quisiera cifrar un mensaje para Javier, lo haría usando la clave pública de Javier, y él lo descifraría con su propia clave privada. Si Javier quisiera enviar un mensaje al usuario, lo haría con la clave pública del usuario, y éste lo descifraría con su propia clave privada. A continuación se muestra como debería hacer esto con los archivos que se desean cifrar y descifrar.

4.4.1. CIFRAR

143. A continuación se detallan los pasos a seguir para el cifrado de un archivo:

144. Paso 1: Localice el documento o el archivo a cifrar y haga clic en él con el botón derecho. Se desplegará un menú, sitúe el cursor sobre **Services** y a continuación seleccione **OpenPGP: Encrypt File**.

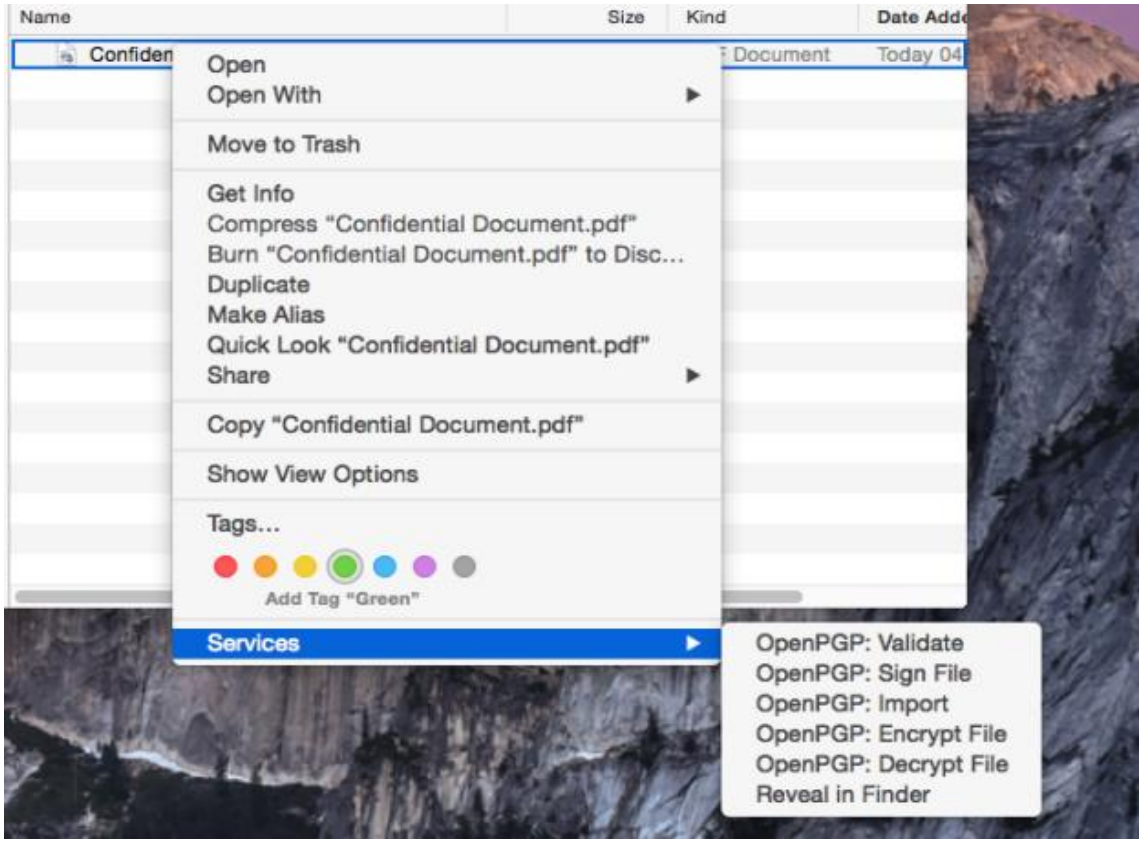

Figura 86.- Cifrar documentación

145. Paso 2: Elija la clave o claves de cifrado en función de los destinatarios, pulsar en **Ok**. Recuerde que para que usted pueda descifrar el mensaje o documento en un futuro deberá incluir su clave pública entre las elegidas.

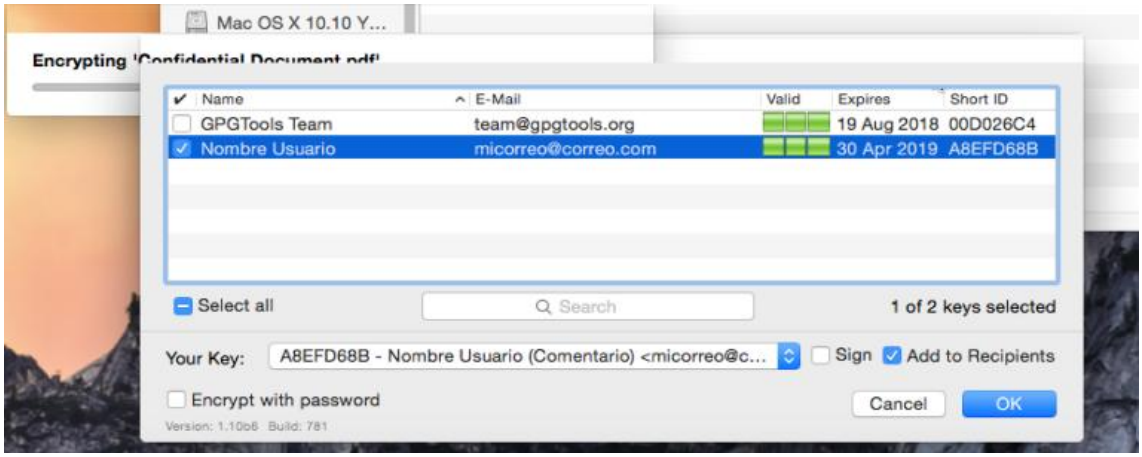

Figura 87.- Selección de destinatarios

146. Paso 3: Tras cifrar el archivo, aparecerá una ventana con los resultados y el fichero que ha generado GPG (el cual tendrá el mismo nombre, pero acabado en .gpg). Pulse **OK** para terminar.

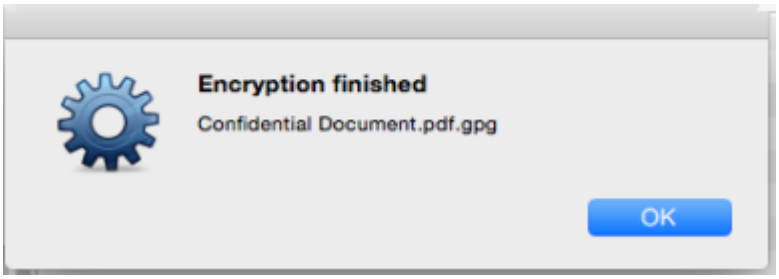

Figura 88.- Resultados de cifrado

4.4.2. DESCIFRAR

147. A continuación se detallan los pasos a seguir para el descifrado de un archivo:

148. Paso 1: Localice el archivo a Descifrar y pulse con el botón derecho en el archivo, se desplegará un menú, sitúe el cursor sobre **Services** a continuación pulse sobre **Open PGP: Decrypt File**.

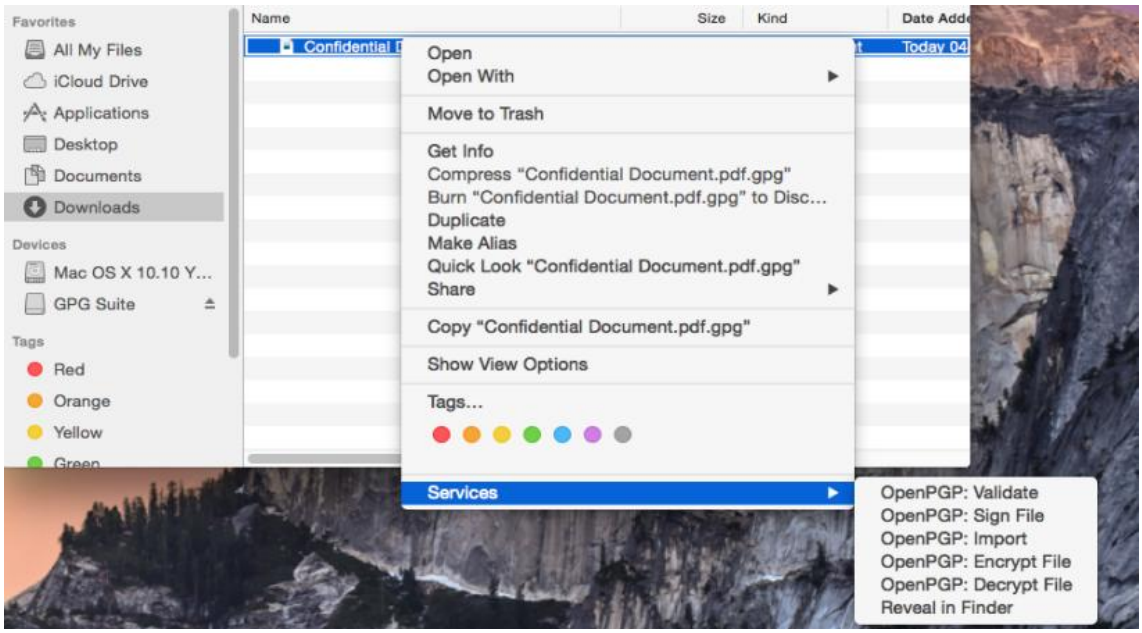

Figura 89.- Descifrar documentos

149. Paso 2: Introduzca la contraseña.

Figura 90.- Introducir la clave de descifrado

150. Paso 3: Una vez introducida la clave correcta podrá ver el archivo descifrado en la ruta seleccionada.

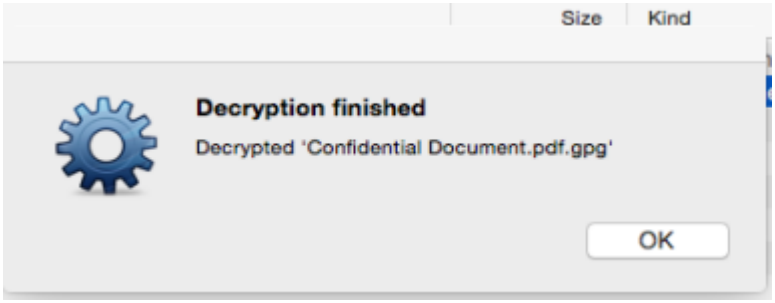

Figura 91.- Resultados del descifrado

4.5. FIRMAR Y VERIFICAR

151. Una firma digital certifica un documento y le añade una marca de tiempo. Si posteriormente el documento fuera modificado en cualquier modo, el intento de verificar la firma fallaría. La utilidad de una firma digital es la misma que la de una firma escrita a mano, sólo que la digital tiene una resistencia a la falsificación. Por ejemplo, la distribución del código fuente de GnuPG viene firmada con el fin de que los usuarios puedan verificar que no ha habido ninguna manipulación o modificación al código fuente desde que fue archivado.

152. Para la creación y verificación de firmas, se utiliza el par público y privado de claves en una operación que es diferente a la de cifrado y descifrado. La firma de un documento es generada con la clave privada del firmante. La firma se verifica por medio de la clave pública correspondiente. Por ejemplo, Javier haría uso de su propia clave privada para firmar digitalmente la entrega de su última ponencia a la Revista de Química Inorgánica. El editor asociado que la recibiera, usaría la clave pública de Javier para comprobar la firma, verificando de este modo que el envío proviene realmente de Javier, y que no ha sido modificado desde el momento en que Javier lo firmó. Una consecuencia directa del uso de firmas digitales es la dificultad en negar que fuera el propio usuario quien puso la firma digital, ya que ello implicaría que su clave privada ha sido comprometida.

4.5.1. FIRMAR

153. A continuación se detallan los pasos a seguir para la firma de un archivo.

154. Paso 1: Localice el archivo a firmar, y pulse con el botón derecho en el archivo, se desplegará un menú, sitúe el cursor sobre **Services** a continuación pulse sobre **Open PGP: Sign File**.

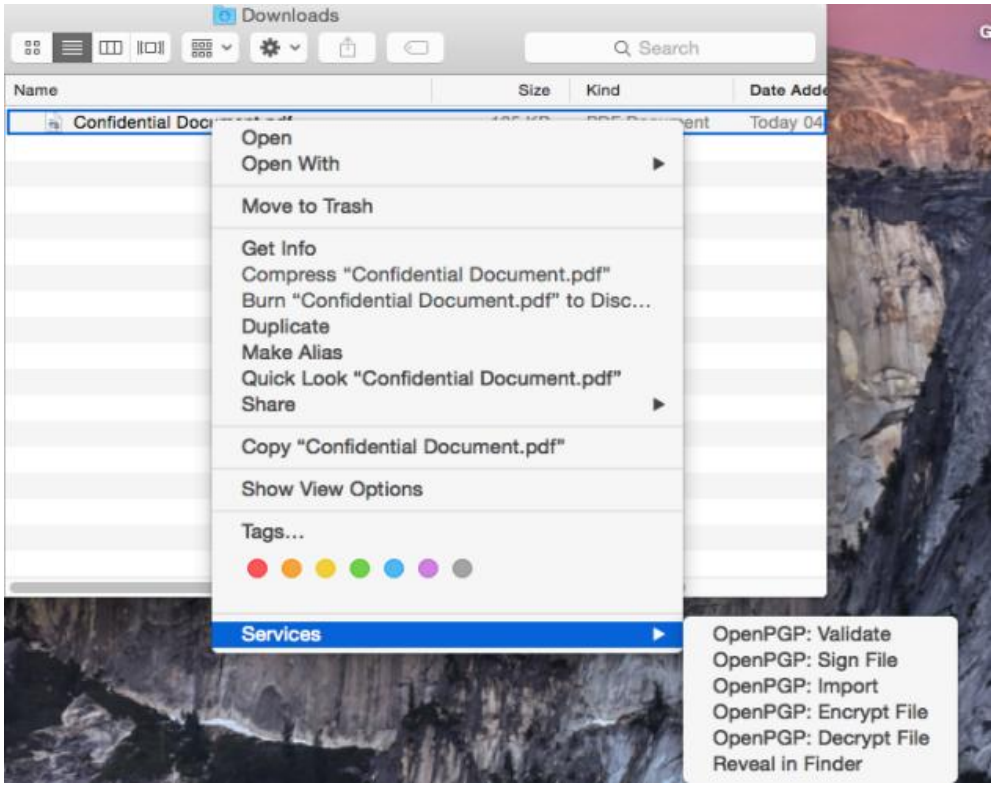

Figura 92.- Firmar documentación

155. Paso 2: Le pedirá su contraseña, proceda a introducirla y pulse **Ok**.

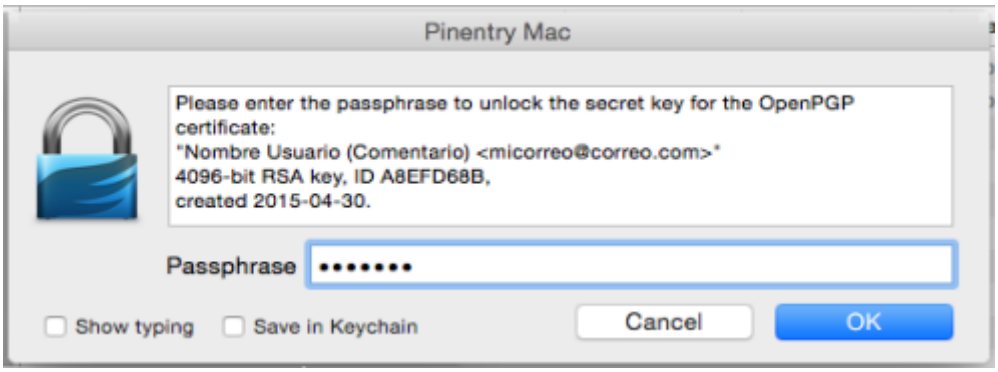

Figura 93.- Introducción de credenciales de firmado

156. Paso 3: Una vez terminado, le generará el fichero con formato .sig, en la ruta predeterminada. Pulse **Ok** para terminar.

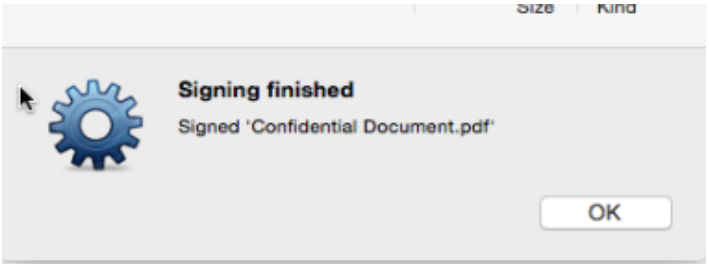

Figura 94.- Operaciones realizadas

4.5.2. VERIFICAR

157. A continuación se detallan los pasos a seguir para verificar la firma de un archivo.

158. Paso 1: Localice el archivo a verificar, y a continuación pulse con el botón derecho en el archivo, se desplegará un menú, sitúe el cursor sobre **Services** y a continuación debe pulsar sobre **Open PGP: Validate**.

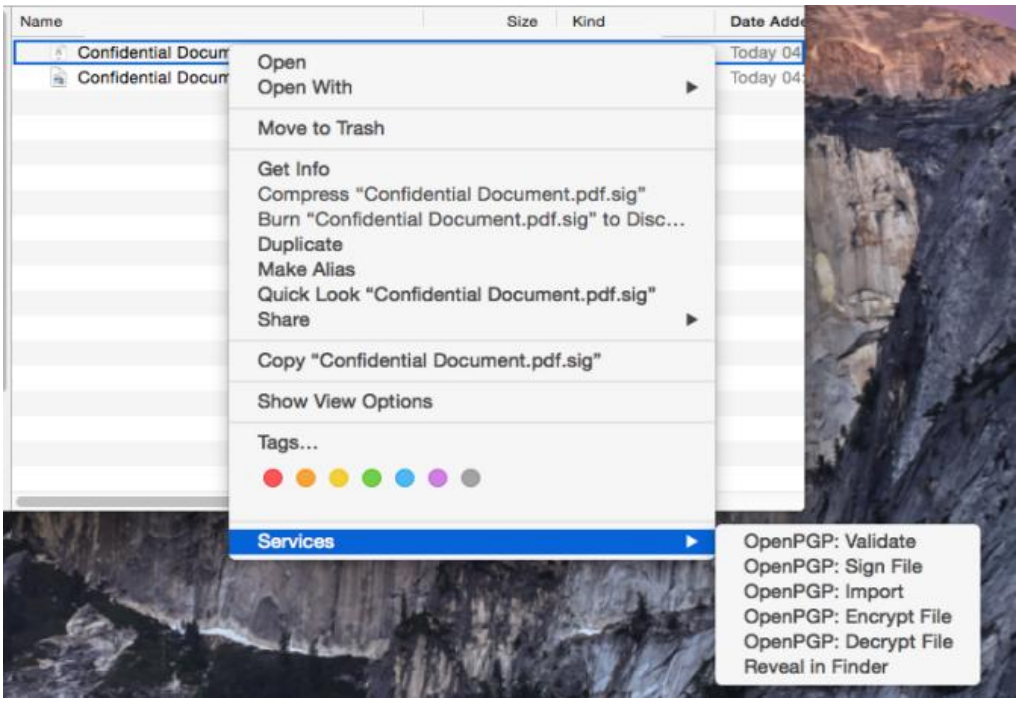

Figura 95.- Verificar documentación

159. Paso 2: Una vez marcada la acción de comprobar firma, el sistema procederá a verificar la misma.

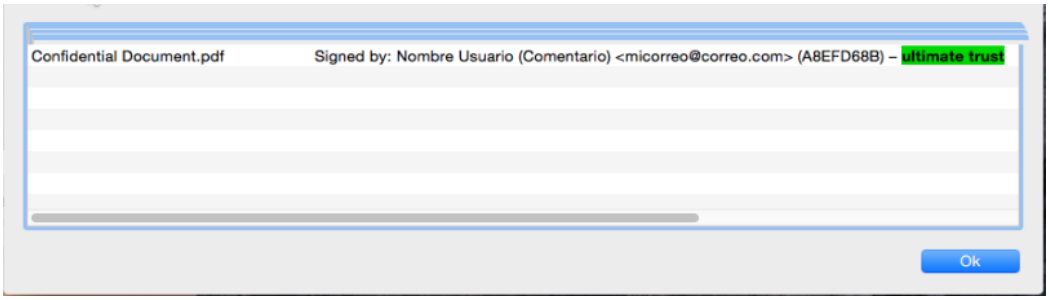

Figura 96.- Operaciones completadas

5. ENVIAR UN CORREO ELECTRÓNICO CIFRADO AL CCN-CERT

5.1. EJEMPLO DE ENVÍO DE CORREO

160. En los siguiente punto se detalla los pasos a seguir para enviar un correo electrónico a info@ccn-cert.cni.es. Se utilizará la clave pública de esta cuenta para cifrar tanto el texto del correo electrónico como los ficheros adjuntos al mismo. Ambos elementos se cifran de forma separada aunque se envíen juntos.

161. Se inicia el proceso con la obtención de la clave pública –en caso de no tenerla– desde la siguiente url: https://www.ccn-cert.cni.es/sobre-nosotros/contacto.html

162. Descargue la clave PGP pulsando en **Descargar**. A su lado se encuentra la huella digital para comprobar la correcta descarga de la clave pública.

Figura 97.- Enlace de descarga de la clave pública del centro

163. Una vez descargada la clave pública, se debe importar al repositorio de la aplicación para su posterior uso. La aplicación GnuPG, mediante su botón de **Importar** realiza la importación. Una vez pulsado el botón, se muestra una venta para la selección del fichero con la clave pública. Una vez seleccionado el fichero, se pulsa el botón **Abrir** para terminar el proceso de importación de la clave.

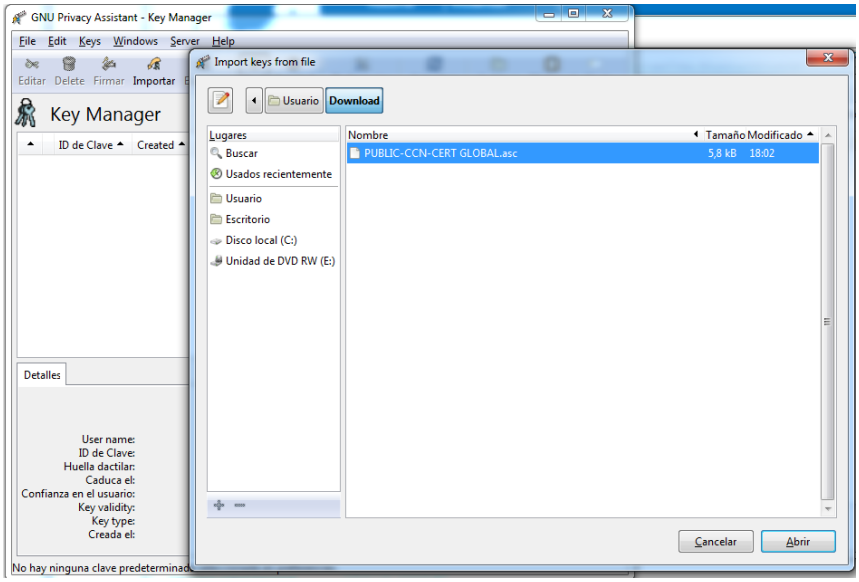

Figura 98.- Importar clave pública

5.1.1. CIFRADO DEL CONTENIDO DEL MENSAJE

164. El siguiente paso es cifrar el contenido del mensaje con la clave pública CCN-CERT GLOBAL, al ser el destinatario del correo cifrado.

165. El cifrado del contenido del mensaje se puede realizar desde el **Clipboard** de la aplicación de GnuPG, copiando el texto en la propia ventana del **Portapapeles** y pulsando los botones de **Encrypt/Decrypt** para Cifrar/Descifrar.

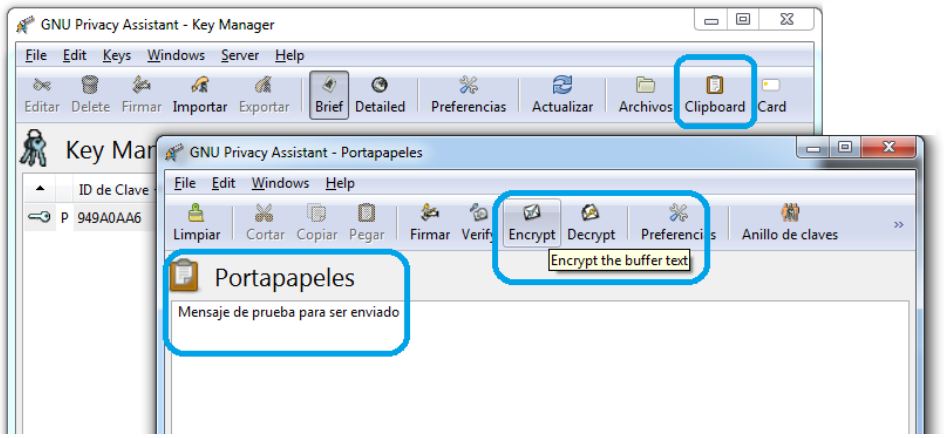

Figura 99.- Cifrar mensaje en GnuPG

166. En este caso se pulsará el botón de **Encrypt** y aparecerá la venta de selección de clave pública para ser usada en el cifrado. En esta ventana se muestran todas las claves públicas importadas en la herramienta, debe aparecer la clave pública de CCN-CERT GLOBAL, importada anteriormente.

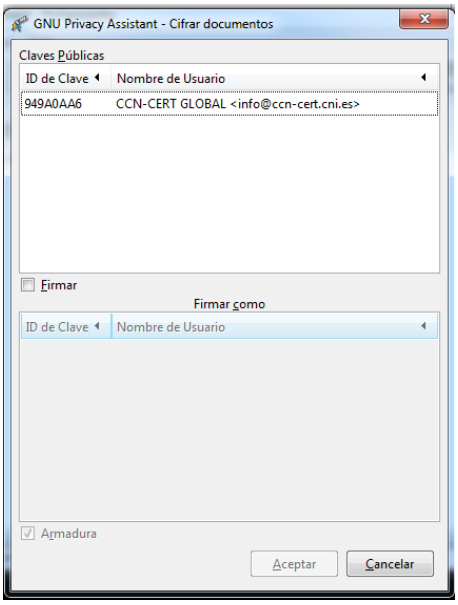

Figura 100.- Selección de clave pública para cifrar el mensaje

167. Una vez seleccionada, se marca la casilla **Armadura** y se pulsa el botón aceptar. La aplicación cifrará el mensaje y lo mostrará en pantalla. El resultado puede ser copiado en el cuerpo de un correo electrónico y enviado directamente. De esta manera el contenido del mensaje solamente será visible por el destinatario, en este caso info@ccn-cert.cni.es.

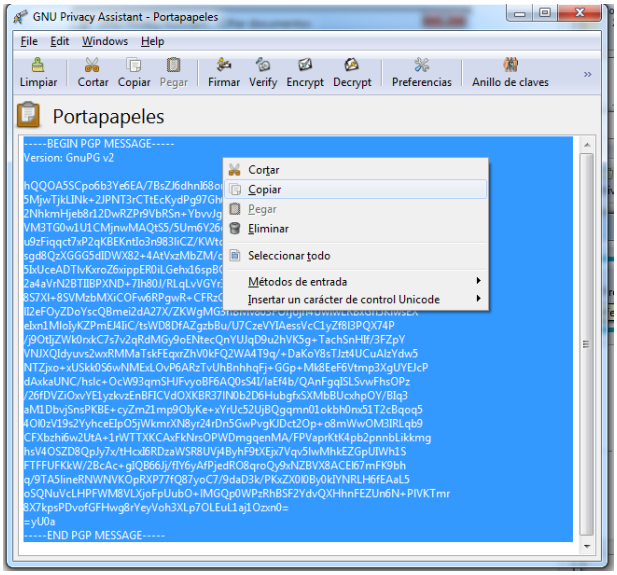

Figura 101.- Resultado al cifrar un mensaje

168. El contenido cifrado se copiará directamente en el cuerpo del mensaje electrónico en el propio cliente de correo electrónico manejado por el usuario, enviándose como cualquier otro correo electrónico.

169. Con este procedimiento se tiene listo un mensaje para su envío en un correo electrónico cifrado, manteniendo la integridad y dotándolo de confidencialidad.

5.1.2. CIFRADO DE DOCUMENTOS ADJUNTOS AL MENSAJE

170. Seguidamente se relata la manera para adjuntar un fichero de forma cifrada a un correo electrónico. El proceso es muy similar al anterior, se utilizará la herramienta GnuPG con su apartado **Archivos**. Desde esta ventana se puede cifrar ficheros del equipo, utilizando la clave pública del que será destinatario de la información.

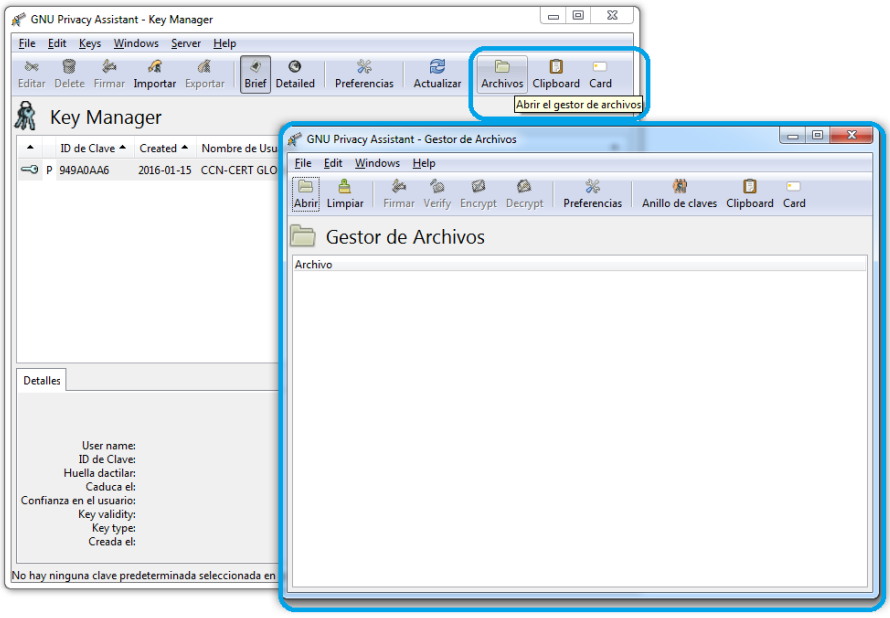

Figura 102.- Apertura del gestor de Archivos de GnuPG

171. Desde esta nueva ventana, pulsando el botón **Abrir** seleccione un fichero del ordenador. Este acceso muestra una ventana para navegar por los directorios del ordenador y seleccionar el fichero a cifrar.

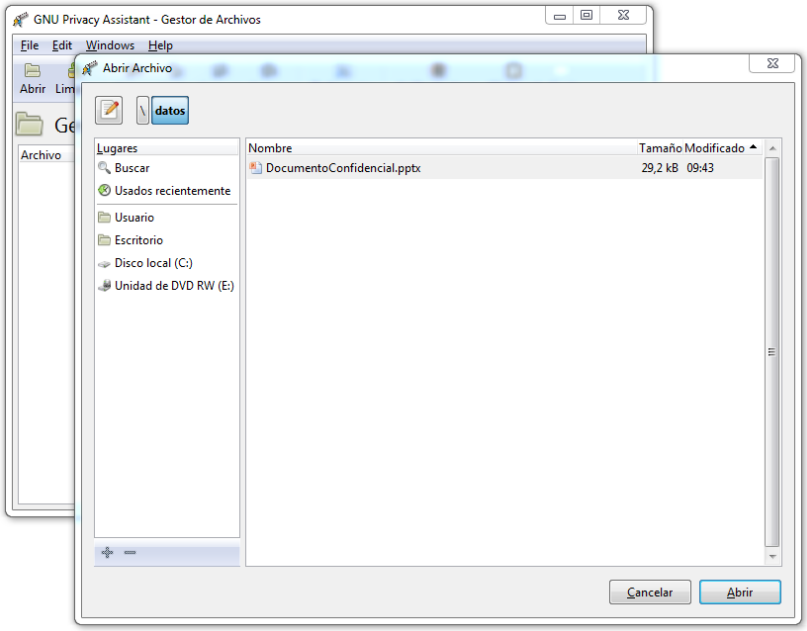

Figura 103.- Selección del fichero para cifrar

172. La aplicación nos permite seleccionar varios ficheros para ser cifrados con la misma clave. Así se agiliza el cifrado de varios ficheros, usando la misma clave pública del destinatario. El resultado serán tantos ficheros cifrados como se haya seleccionado. Los ficheros cifrados solamente se descifrarán con la clave privada del destinatario.

173. Una vez seleccionados los ficheros, en el gestor de archivos del GnuPG, se inicia el proceso de cifrado de los mismos pulsando el botón **Encrypt**.

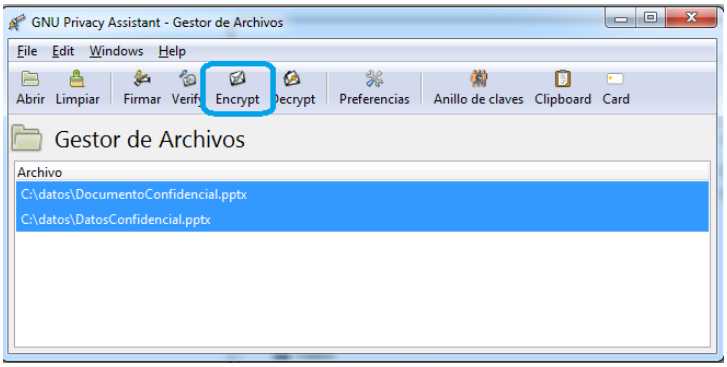

Figura 104.- Selección de ficheros para ser cifrados

174. Una vez se haya pulsado **Encrypt** aparecerá la ventana de selección de la clave pública para cifrar los archivos. Se selecciona la clave pública del destinatario, se desmarca la casilla **Armadura** y se pulsa el botón de **Aceptar**.

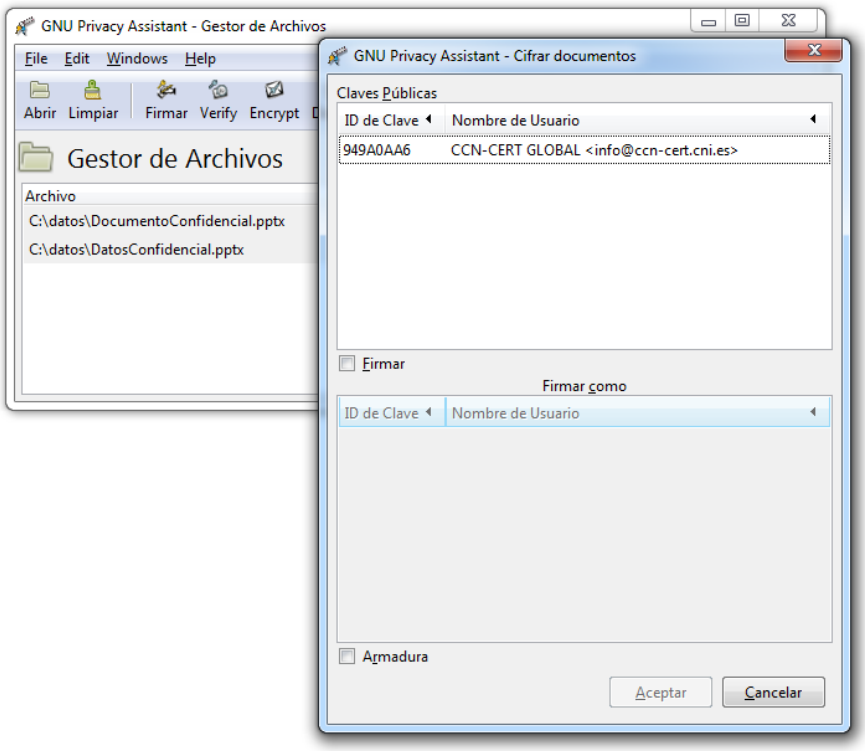

Figura 105.- Selección de clave pública para el cifrado de los ficheros

175. Una vez finalizado el cifrado de los ficheros, aparecerán los nuevos ficheros cifrados en el propio gestor de archivos, añadiéndoles la extensión "gpg". Los ficheros cifrados se guardan en la misma carpeta donde se encuentran los ficheros originales. La herramienta no elimina ninguno de los ficheros que intervienen en el proceso. El usuario debe adjuntar al correo electrónico los ficheros con la extensión "gpg".

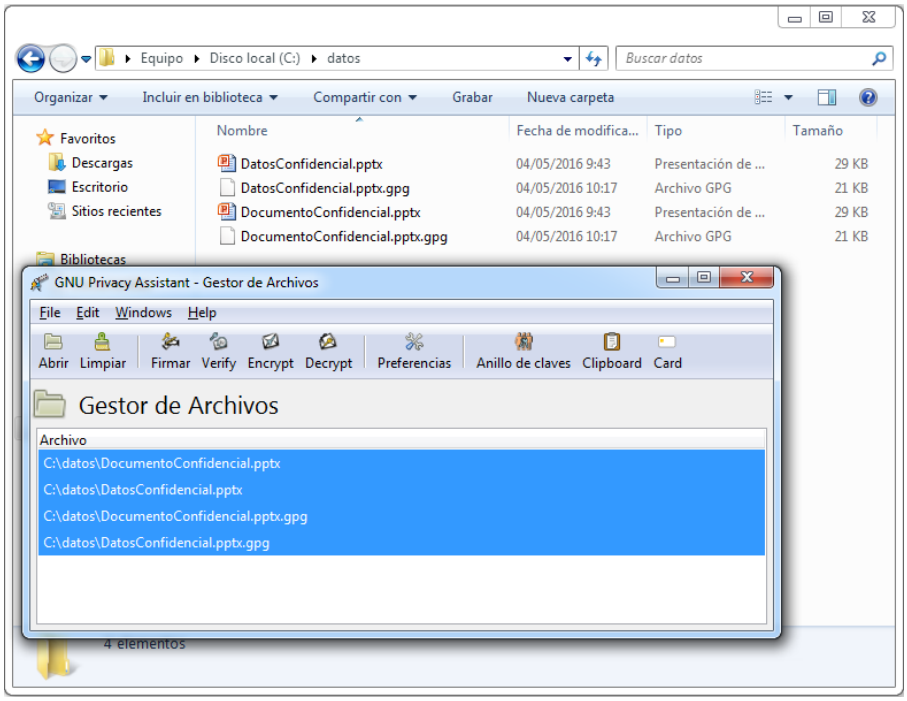

Figura 106.- Resultado de cifrar los ficheros

176. Una vez finalizados estos pasos, el usuario se encuentra en disposición de enviar un correo electrónico con el mensaje y los ficheros adjuntos cifrados con la clave pública del destinatario. Se copiaría el mensaje cifrado en el cuerpo del correo electrónico y se adjuntará los ficheros con extensión "gpg" para realizar su envío como cualquier otro correo electrónico.

6. COMPLEMENTOS PARA LOS CLIENTES DE CORREO ELECTRÓNICO

6.1. COMPLEMENTO ENIGMAIL PARA MOZILLA THUNDERBIRD

177. Enigmail es un complemento de Thunderbird que permite proteger la privacidad de los correos enviándolos de manera cifrada. Este complemento se basa en criptografía asimétrica, por lo que cada usuario debe generarse su par de claves personales (clave pública y clave privada).

6.1.1. INSTALACIÓN DE ENIGMAIL

178. Acceda al administrador de complementos del cliente de correo Mozilla Thunderbird y en **Obtener complementos** busque *enigmail*.

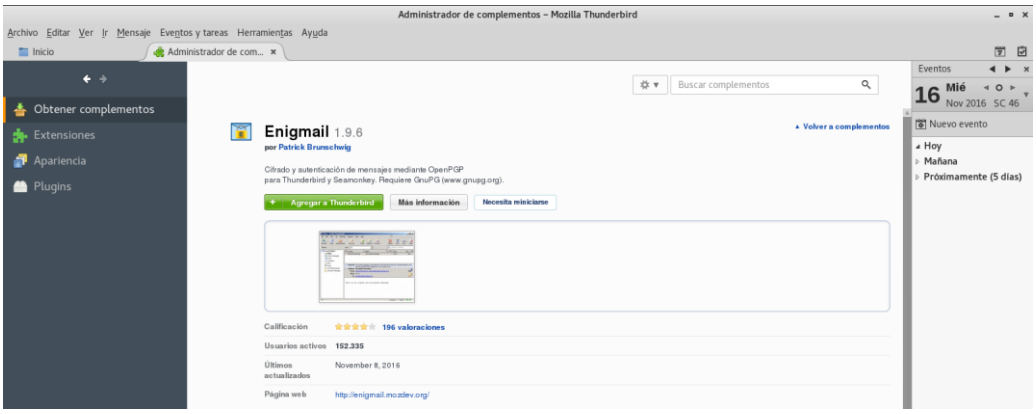

Figura 107.- Búsqueda del complemento Enigmail en Mozilla Thunderbird

179. Al pulsar sobre **Agregar a Thunderbird** comenzará la instalación y la configuración del complemento.

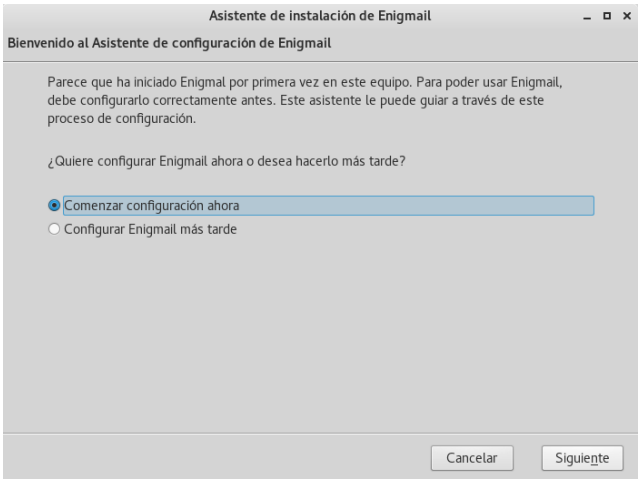

Figura 108.- Asistente de instalación de Enigmail

180. Elija el tipo de configuración que se desee (generalmente la configuración estándar).

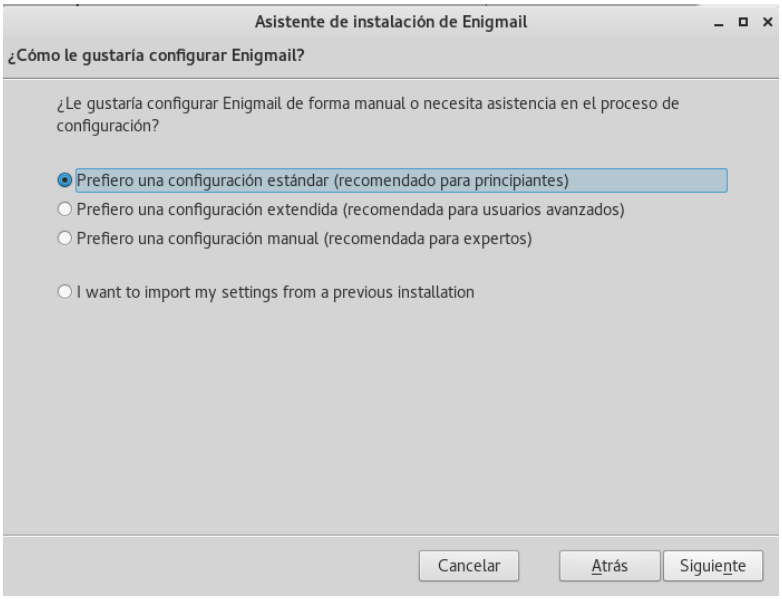

Figura 109.- Tipo de configuración de Enigmail

181. En caso de no disponer de un par de claves privada/pública la aplicación las generará en el siguiente paso, pidiéndole únicamente una contraseña para proteger la clave privada.

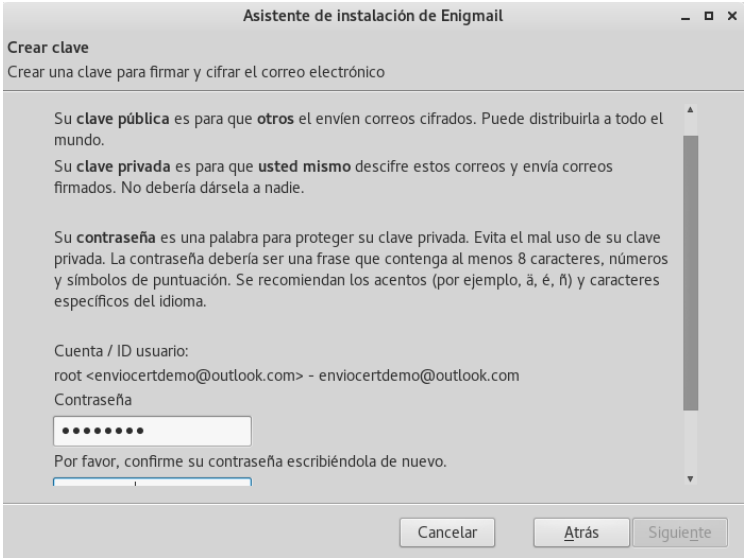

Figura 110.- Creación de una nueva clave en Enigmail

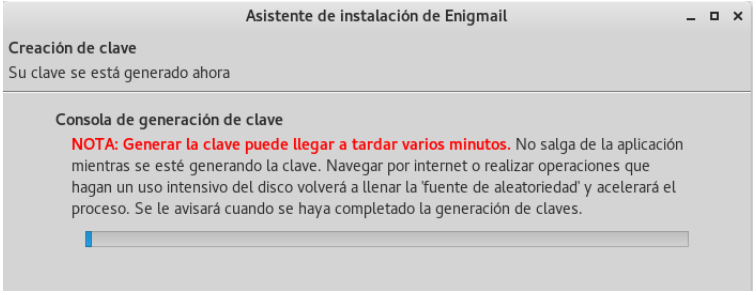

Figura 111.- Generación de una nueva clave en Enigmail

182. Para importar una clave privada propia, seleccione la opción **Administrador de claves** dentro del menú **Enigmail**.

Figura 112.- Administración de claves

183. Seleccione la opción **Importar claves desde un fichero** dentro del menú **Archivo**.

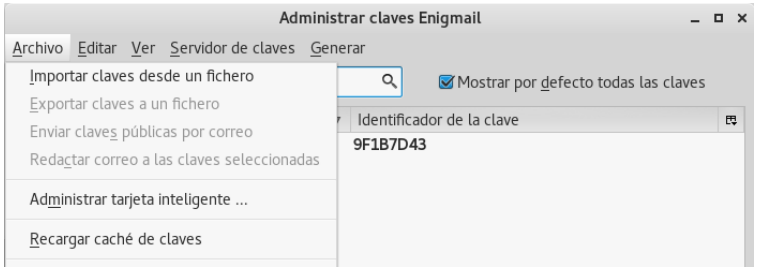

Figura 113.- Importar claves desde un fichero

184. Seleccione la clave que desee importar.

Figura 114.- Búsqueda de la clave privada a importar

185. Obtendrá una confirmación de Enigmail si la clave se ha importado correctamente.

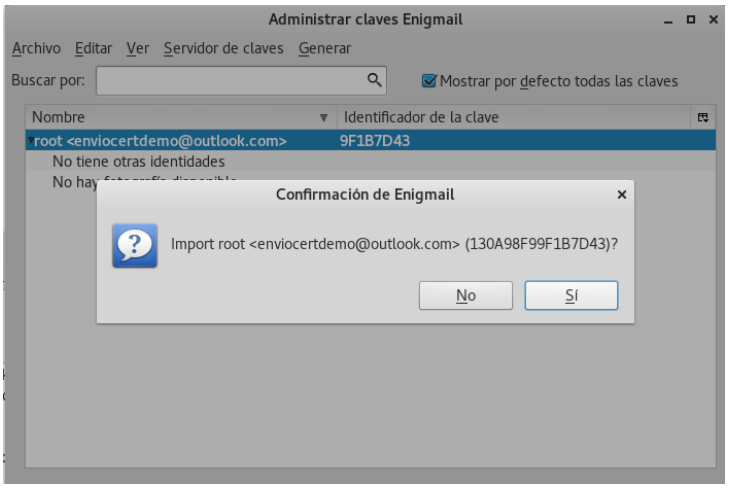

Figura 115.- Confirmación de la importación de claves

186. Una vez importada la clave privada en el sistema, será posible descifrar los mensajes que se reciban cifrados con nuestra clave pública.

187. Para poder enviar correos cifrados a otras personas es necesario importar sus claves públicas. Realizaremos los mismos pasos anteriores pero importando en esta ocasión la clave pública de las personas con las que se quiera mantener comunicaciones cifradas.

188. Tras seleccionar de nuevo la opción **Importar claves desde un fichero** dentro del menú **Archivo**, seleccione la clave pública que desee importar.

Figura 116.- Búsqueda de las claves públicas a importar

189. Obtendrá una confirmación de Enigmail si la clave se ha importado correctamente.

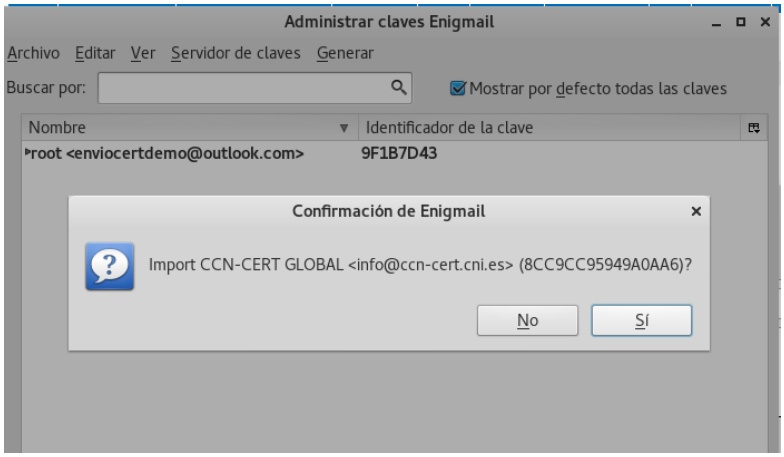

Figura 117.- Confirmación de la importación de claves

190. Si la clave ha sido importada correctamente, ésta aparecerá en el administrador de claves y estará disponible para su posterior uso en el cliente de correo.

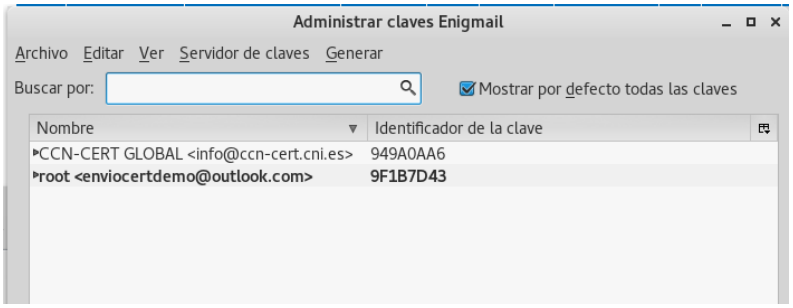

Figura 118.- Confirmación de la importación de claves

191. Es posible configurar Enigmail para que nos notifique mediante un mensaje cuándo un correo electrónico va a enviarse sin cifrar, para poder identificar en su caso el envío de información sensible en claro por error.

192. Para ello seleccione del menú de Thunderbird, dentro del submenú de Enigmail la opción **Preferencias**.

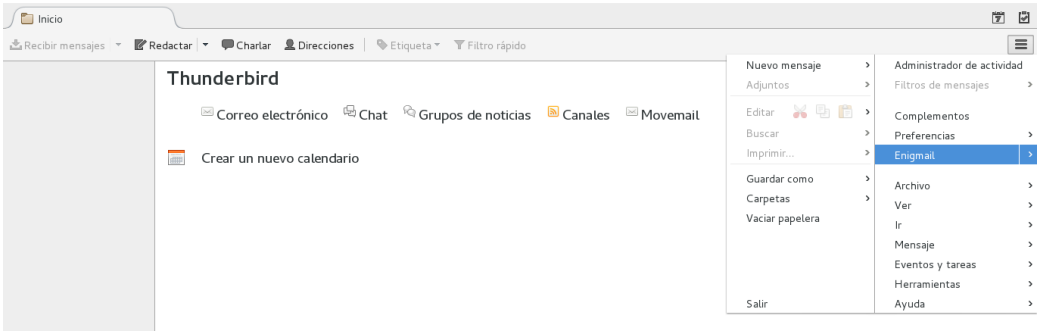

Figura 119.- Submenú de Enigmail en Thunderbird

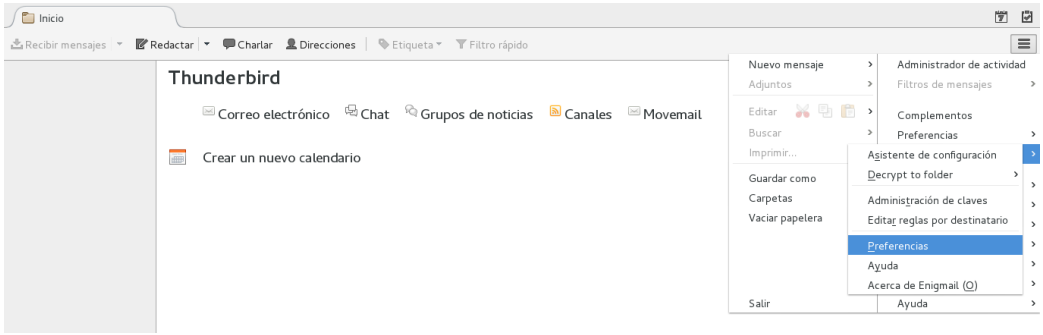

Figura 120.- Opción Preferencias de Enigmail

193. Seleccione en la ventana de **Preferencias de Enigmail** la pestaña **Enviando**.

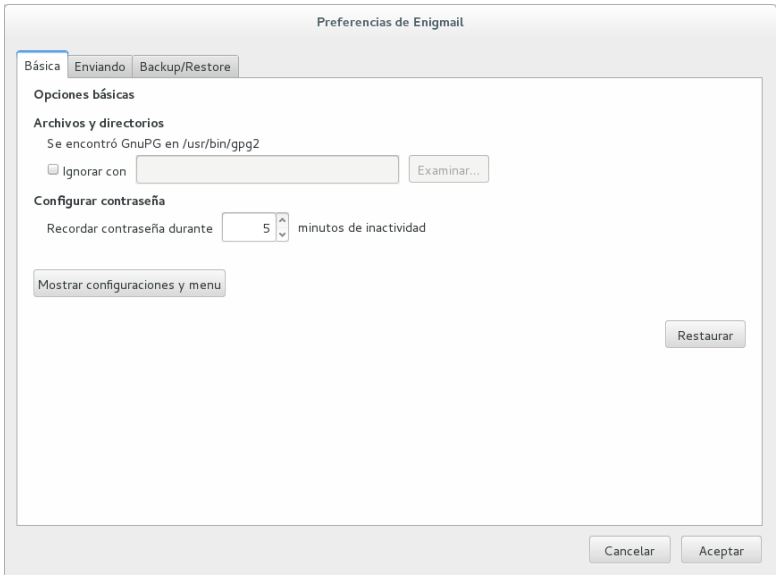

Figura 121.- Preferencias de Enigmail

194. Habilite la opción de **Configuración de envío manual** y seleccione en el apartado **Confirmar antes de enviar** la opción **Si no es cifrado**, así se tendrá una notificación cuando se intente enviar un mensaje sin cifrar.

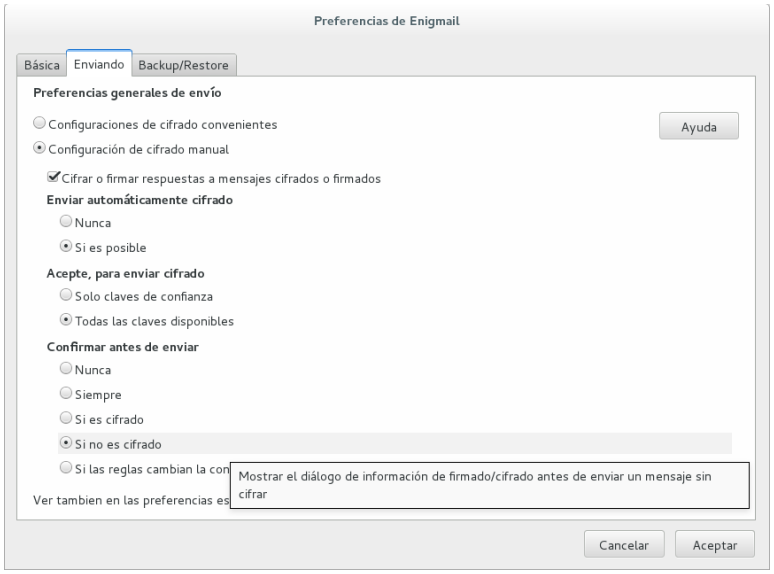

Figura 122.- Configuración de opciones de envío de mensaje en Enigmail

6.1.2. ENVÍO DE CORREO

195. Para el envío de un correo electrónico cifrado se hará uso de las opciones que ofrece el complemento Enigmail a la hora de redactar un correo electrónico. El cifrado de los correos electrónicos incluirá también cualquier documento que se adjunte al mensaje.

196. Inicie la redacción de un mensaje nuevo y escriba en el **Para** la dirección de correo del destinatario al que quiera enviar el mensaje cifrado.

197. Si la clave pública del destinatario del correo se había importado con anterioridad, Enigmail le indicará que el mensaje se enviará cifrado.

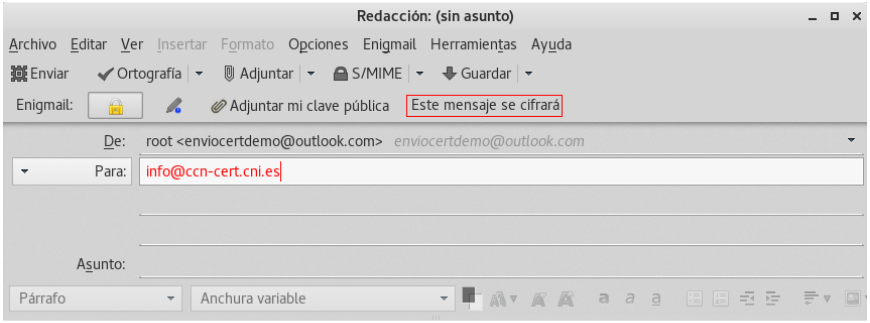

Figura 123.- Envío de correo cifrado a destinatario con clave importada

198. Para cambiar el modo de envío bastará con pulsar el símbolo del candado, deseleccionando la opción de cifrado de mensaje, que nos permitirá enviar un correo en claro a este destinatario.

199. Si por el contrario no estuviera disponible la clave pública del destinatario del correo, Enigmail indicará que el mensaje se enviará en claro mediante el mensaje *"Este mensaje no será firmado ni cifrado"*.

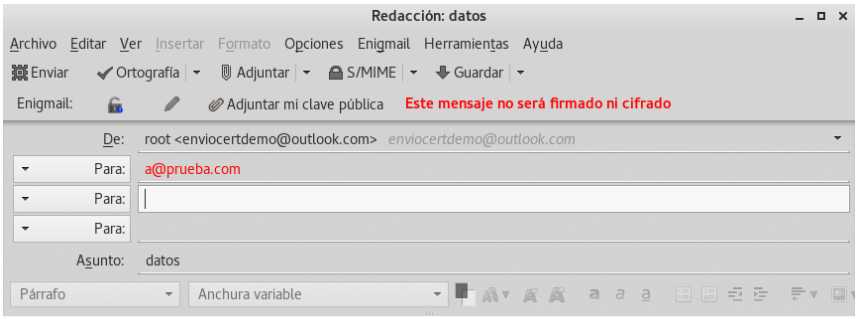

Figura 124.- Envío de correo cifrado a destinatario del que no se tiene la clave pública

200. Puede darse el caso que se quiera enviar un mensaje cifrado a varios destinatarios a la vez. En el supuesto que se tengan importadas las claves públicas de todos los destinatarios, en la ventana de redacción del correo Enigmail indicará, como se ha visto anteriormente, que el mensaje se enviará cifrado.

201. Por otro lado, en el caso que no se disponga de la clave pública de alguno de los destinatarios del correo electrónico, Enigmail nos alertará de este hecho mostrando una ventana emergente en la que solicita la selección de la clave pública a utilizar para poder enviar el mensaje cifrado a este destinatario.

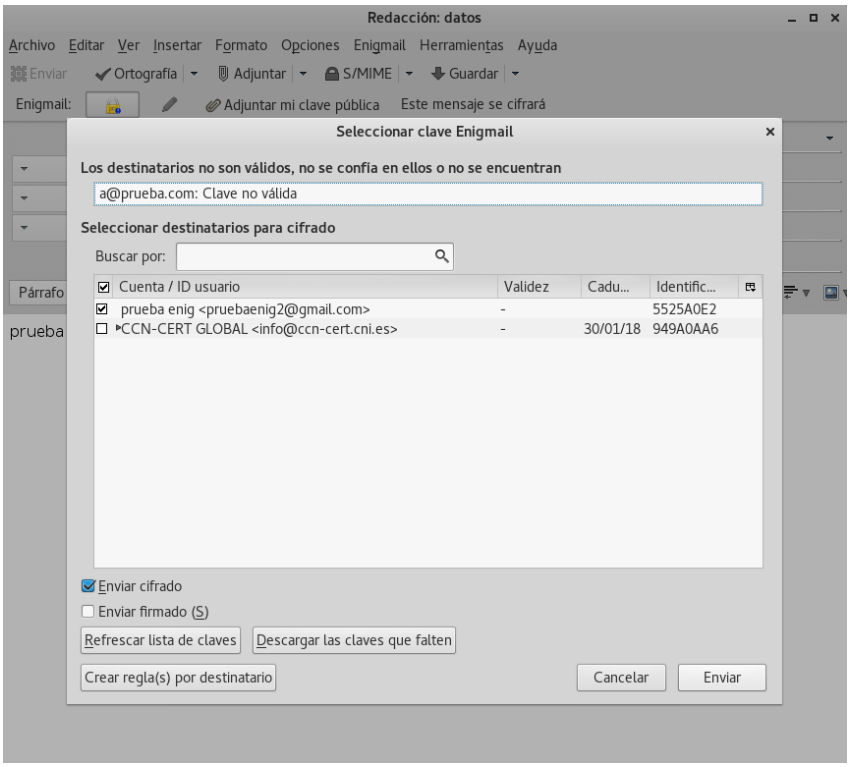

Figura 125.- Ventana emergente tras intento de envío de correo cifrado a destinatario sin clave pública

202. Si aún así, se selecciona la opción **Enviar** el cliente de correo pedirá confirmación para enviar el mensaje cifrado a todos los destinatarios. Pulsando en **Continuar** el mensaje se enviará pero cifrado únicamente con las claves públicas disponibles, por lo que el destinatario del que no se tenía la clave pública recibirá el mensaje pero no será capaz de descifrarlo y, por lo tanto, no podrá ver su contenido.

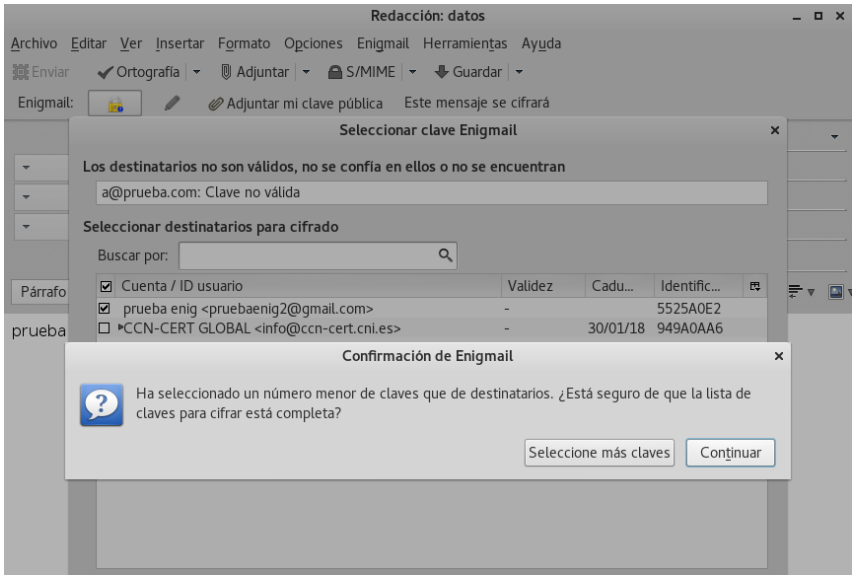

Figura 126.- Confirmación de envío de correo cifrado sin tener las claves públicas de todos los destinatarios

6.1.3. RECEPCIÓN DE CORREO

203. Cuando se reciba un correo electrónico cifrado se hará uso de las opciones que ofrece el complemento Enigmail para descifrar un correo electrónico.

204. Seleccione en la bandeja de entrada el correo electrónico cifrado que se haya recibido y pulse sobre la opción **Reparar mensaje**.

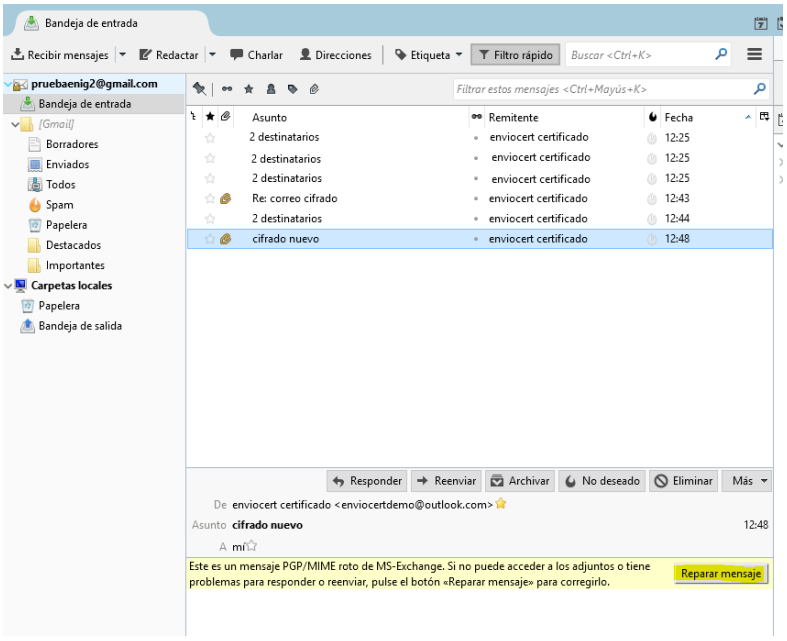

Figura 127.- Recepción de un correo electrónico cifrado

205. Introduzca la contraseña de descifrado de su clave privada para descifrar el mensaje.

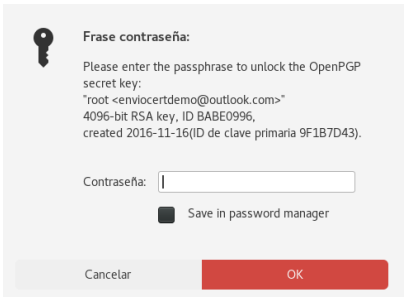

Figura 128.- Solicitud de contraseña de descifrado

206. Si el remitente del mensaje hubiera adjuntado su clave pública al correo electrónico recibido será posible importarla al almacén de claves, en el supuesto que no se tuviera esta clave pública, pulsando sobre **Importar clave**.

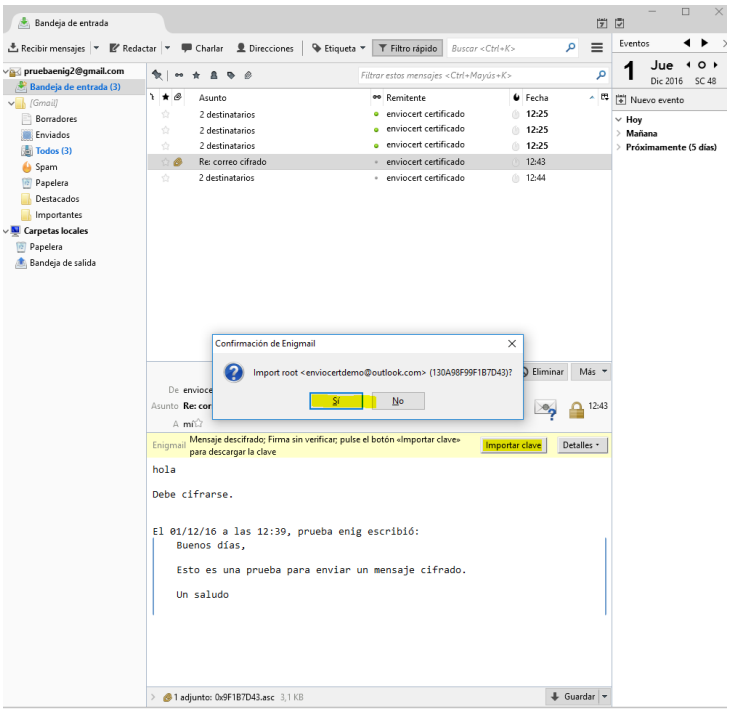

Figura 129.- Importar clave pública desde correo recibido

207. Si la clave se ha importado correctamente obtendrá el siguiente mensaje.

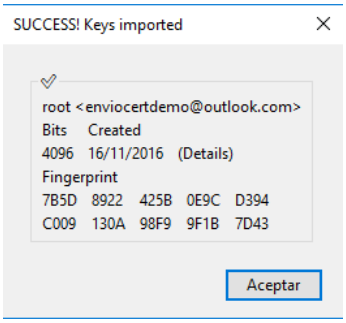

Figura 130.- Clave importada correctamente

6.2. COMPLEMENTO KLEOPATRA PARA MICROSOFT OUTLOOK

208. Kleopatra es un complemento para Microsoft Outlook que permite proteger la privacidad de los correos enviándolos de manera cifrada. Este complemento se basa en criptografía asimétrica, por lo que cada usuario debe generarse su par de claves personales (clave pública y clave privada).

6.2.1. INSTALACIÓN DE KLEOPATRA

209. Es posible instalar el complemento Kleopatra para Microsoft Windows desde el instalador de GnuPG para Microsoft Windows, tal y como puede verse en el apartado 2.1 de esta guía.

210. Para importar claves en Outlook acceda a la pestaña **GpgOL** y seleccione **Start certificate manager**.

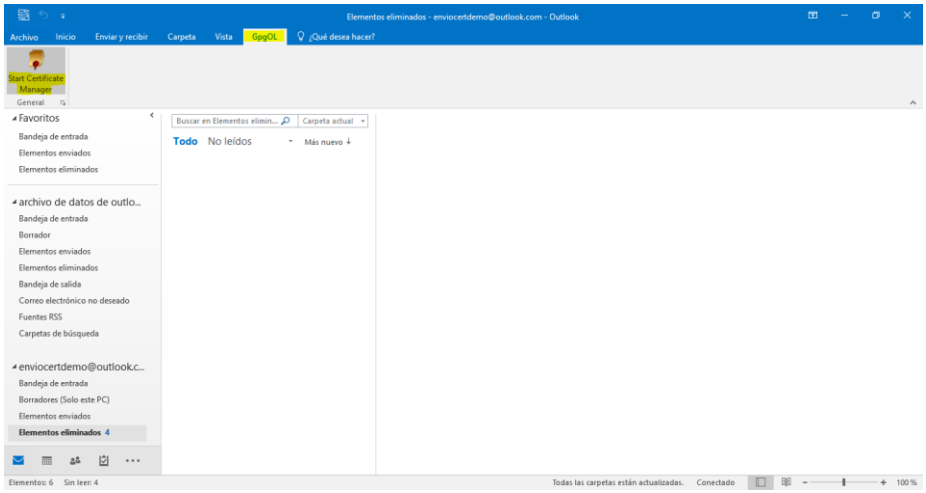

Figura 131.- Importar claves

211. Seleccione la opción **Import Certificates**.

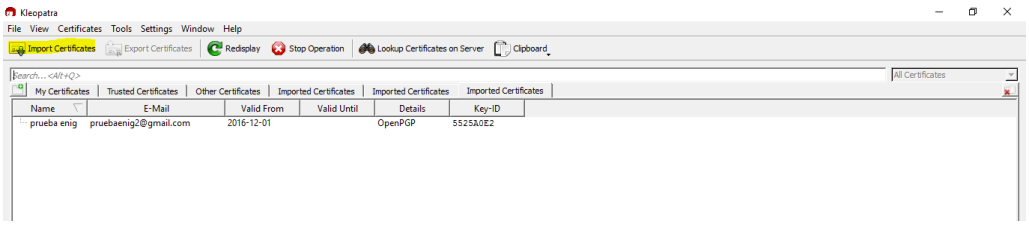

Figura 132.- Importar claves

212. Seleccione la clave que se desee importar y pulse **Abrir**.

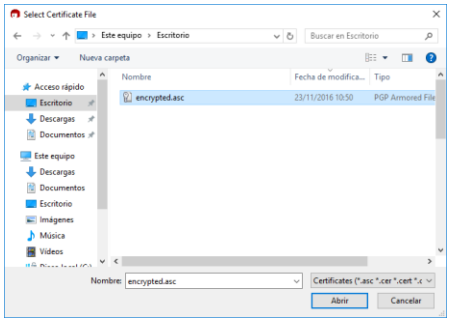

Figura 133.- Importar claves

6.2.2. ENVÍO DE CORREO

213. Para el envío de un correo electrónico cifrado se hará uso de las opciones que ofrece el complemento Kleopatra a la hora de redactar un correo electrónico. Las opciones de cifrado de los correos electrónicos incluirán también la posibilidad de cifrar cualquier documento que se adjunte al mensaje.

214. Inicie la redacción de un mensaje nuevo y escriba en el **Para** la dirección de correo del destinatario al que quiera enviar el mensaje cifrado.

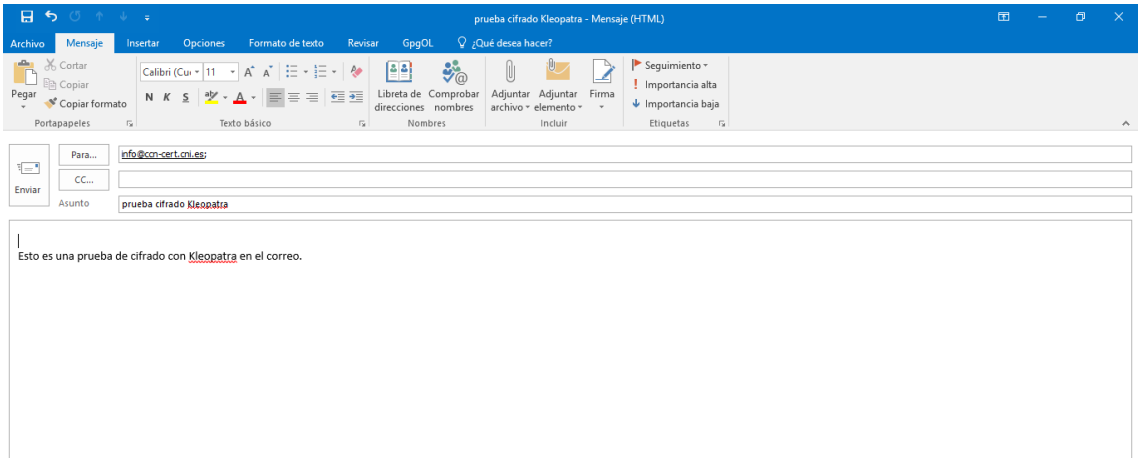

Figura 134.- Redacción de un correo nuevo

215. Seleccione la pestaña **GpgOL** y pulse el botón **Encrypt**.

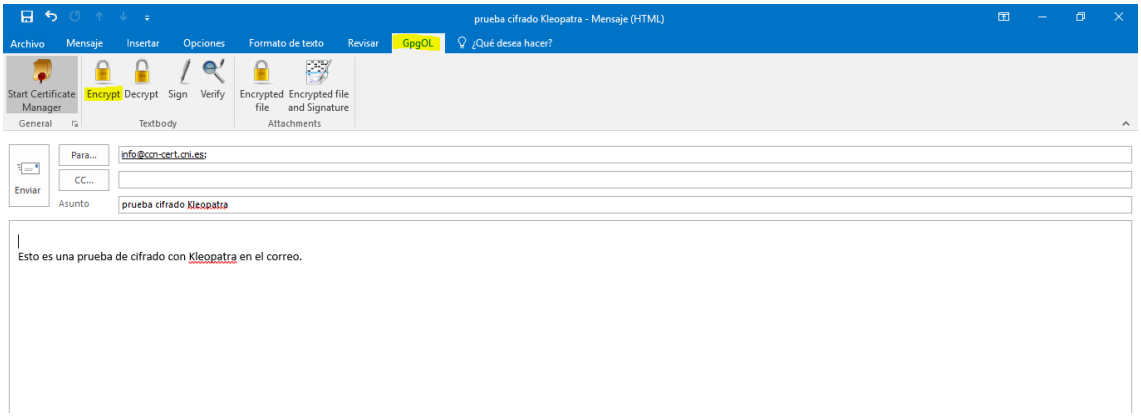

Figura 135.- Redacción de un correo nuevo cifrado

216. Seleccione la clave con la que se quiere cifrar el correo y pulse **OK**.

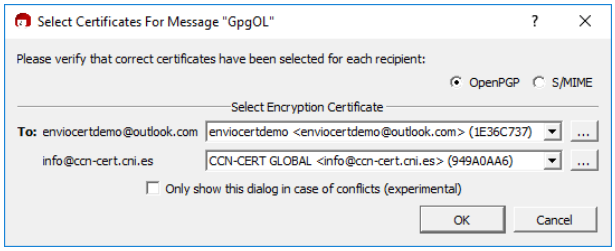

Figura 136.- Selección de la clave de cifrado

217. A continuación aparecerá el correo electrónico con el texto cifrado.

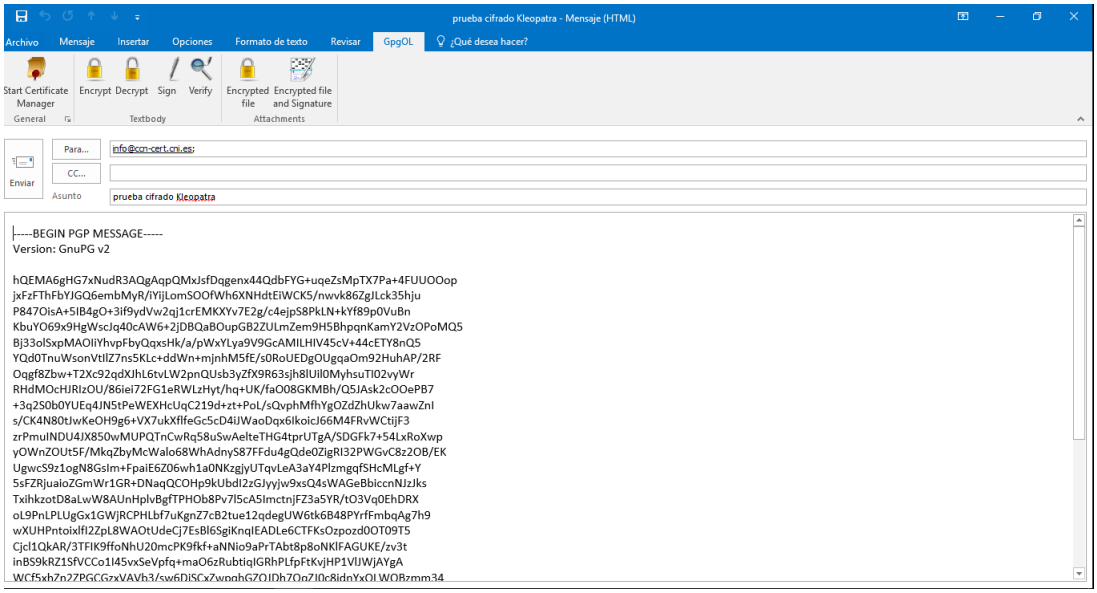

Figura 137.- Texto del correo electrónico cifrado

218. Para adjuntar al correo un archivo cifrado seleccione la pestaña **GpgOL**, pulse el botón **Encrypted file** y seleccione el archivo.

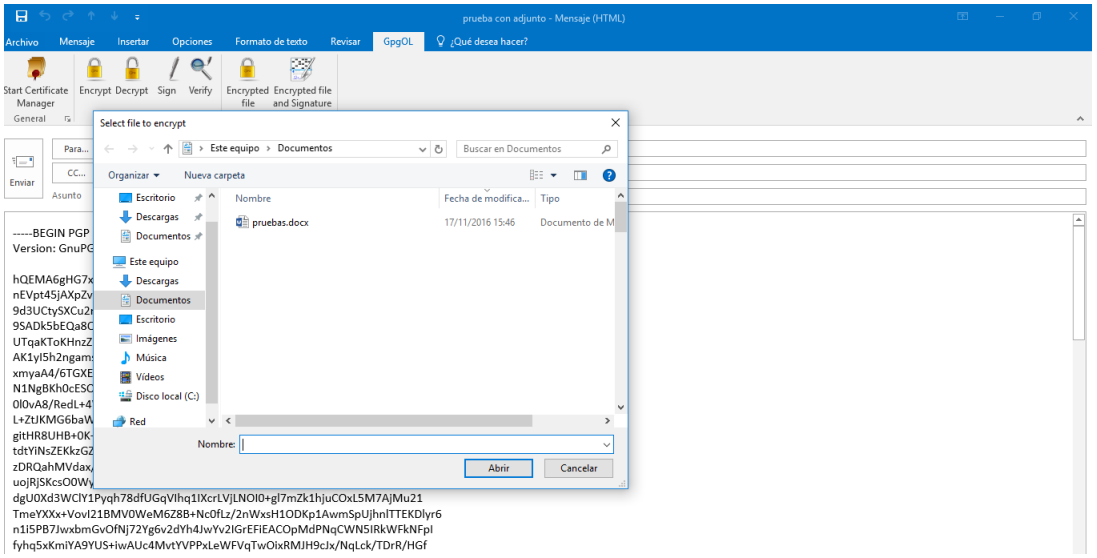

Figura 138.- Selección de un fichero para enviar cifrado adjunto al correo

219. Seleccione la clave con la que se quiere cifrar el fichero adjunto y pulse **OK**.

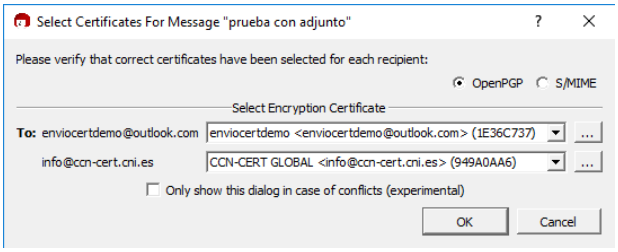

Figura 139.- Selección de la clave de cifrado

220. A continuación aparecerá adjunto al correo electrónico el archivo cifrado.

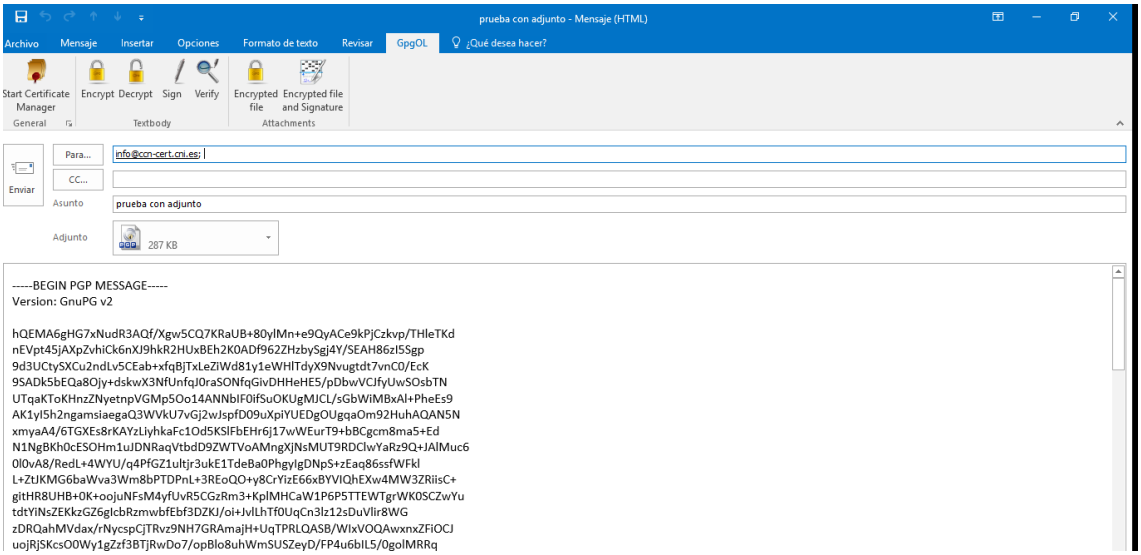

Figura 140.- Correo electrónico cifrado con fichero adjunto cifrado

221. Desde Microsoft Outlook utilizando el complemento Kleopatra, no se permite el envío de un correo electrónico cifrado a diferentes usuarios si no se tiene la clave pública de alguno de ellos.

222. Si se intenta el envío de un correo electrónico cifrado a diferentes usuarios sin tener la clave pública de alguno de los destinatarios, se muestra el listado de destinatarios y sus claves públicas, pero no se activa el botón de **OK** al faltar la clave pública de uno ellos, no pudiéndose realizar le envío del correo electrónico.

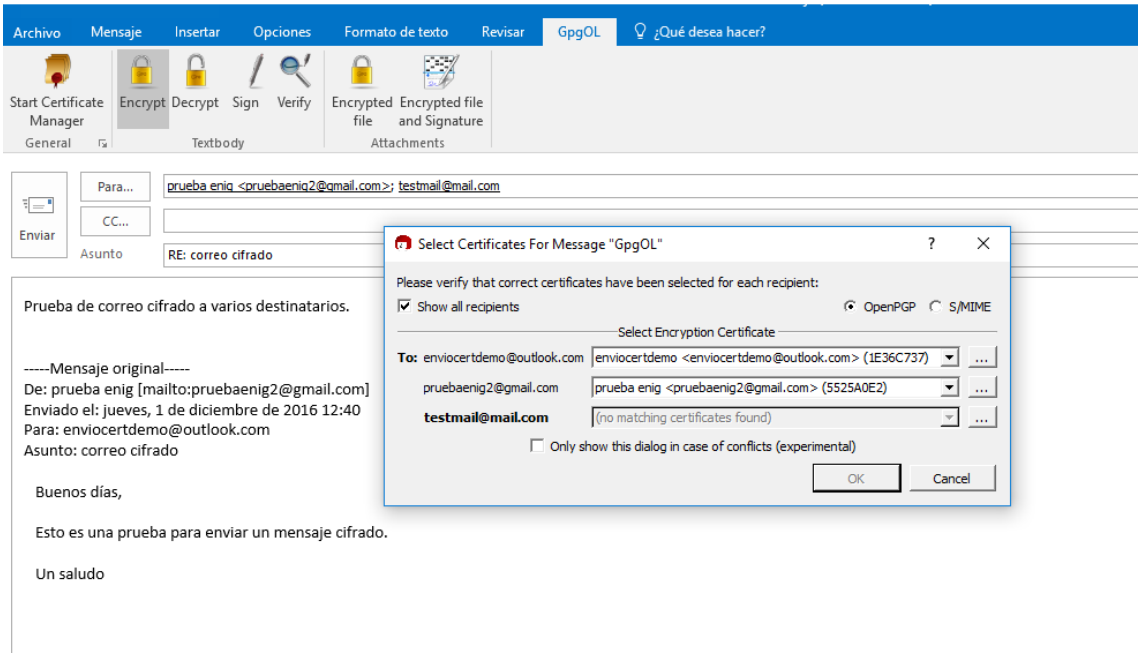

Figura 141.- Correo electrónico cifrado con fichero adjunto cifrado

6.2.3. RECEPCIÓN DE CORREO

223. Cuando se reciba un correo electrónico cifrado se hará uso de las opciones que ofrece el complemento Kleopatra para descifrar un correo electrónico.

224. Seleccione en la bandeja de entrada el correo electrónico cifrado que se haya recibido y ábralo en una ventana para desplegar todas las opciones y herramientas de Outlook para el mensaje.

225. Seleccione la pestaña **GpgOL** y pulse el botón **Decrypt**.

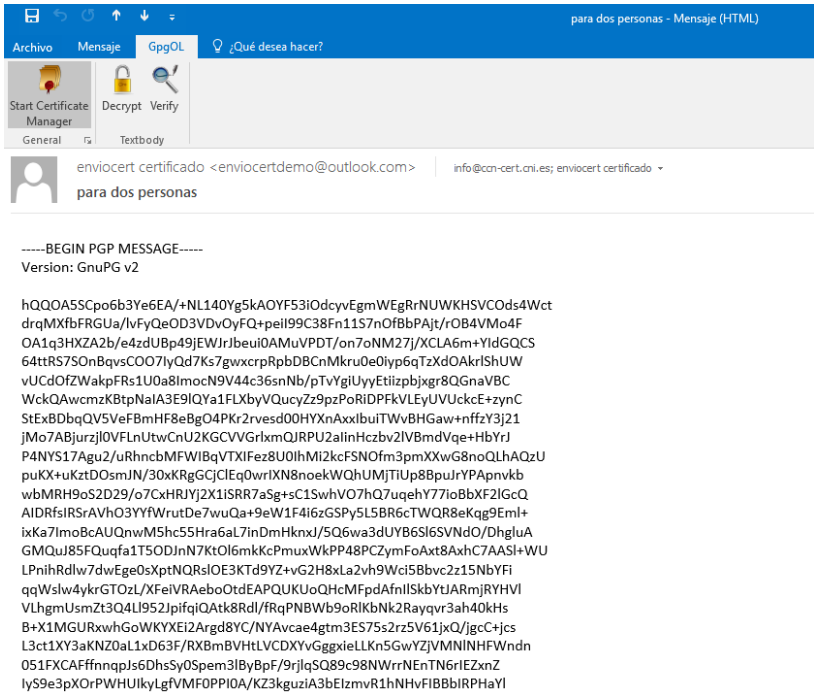

Figura 142.- Recepción de un correo electrónico cifrado

226. Introduzca la contraseña de descifrado de su clave privada para descifrar el mensaje.

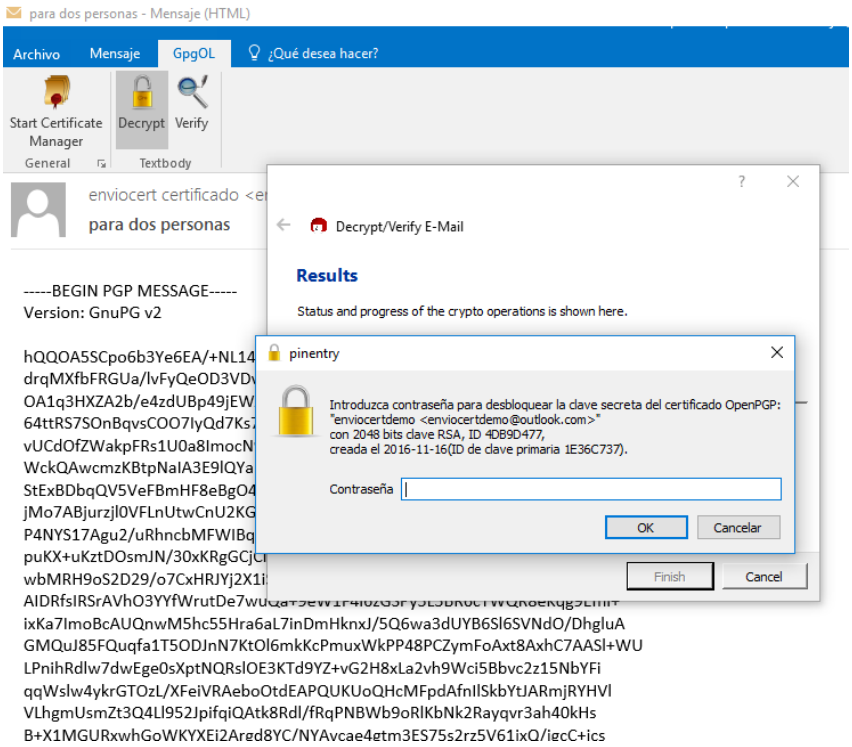

Figura 143.- Solicitud de contraseña de descifrado

227. Si la contraseña introducida es correcta recibirá un mensaje de confirmación indicándole que el mensaje se ha descifrado correctamente.

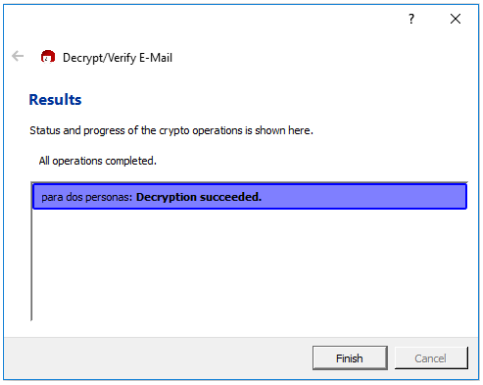

Figura 144.- Descifrado de mensaje correcto