

AGENCIA PARA LA REINCORPORACIÓN Y NORMALIZACIÓN (ARN)

INSTRUCTIVO DE CIFRADO DE DOCUMENTOS - PGP

BOGOTÁ D.C. JUNIO DE 2021



TABLA DE CONTENIDO

1.	OBJETIVO	3
2.	ALCANCE	3
3.	DEFINICIONES	3
4.	CONSIDERACIONES GENERALES	3
5.	CIFRADO DE DOCUMENTOS	3
6.	INSTALACIÓN DE GPG4WIN	3
7.	CREACIÓN DE UN PAR DE CLAVES UTILIZANDO KLEOPATRA	4
8.	EXPORTAR LA CLAVE COMPARTIDA (CLAVE PÚBLICA)	7
9.	EXPORTAR LA CLAVE SECRETA	9
10.	IMPORTAR UNA CLAVE	10
11.	CIFRAR UN ARCHIVO CON UNA CLAVE PÚBLICA	12
12.	DESCIFRAR UN ARCHIVO CON UNA CLAVE SECRETA	13



1. OBJETIVO

Brindar información y explicar el paso a paso para la instalación de GPG4Win, la generación de claves de OpenGPG y exportación de clave pública.

2. ALCANCE

Este instructivo aplica para los funcionarios de la Entidad, que requieren realizar cifrado de información en el marco de sus funciones.

3. DEFINICIONES

CIFRADO O ENCRIPTACIÓN: Consiste en la acción de transformar la información de archivos en cualquier formato, de tal forma que sea incomprensible o, al menos, difícil de comprender a toda persona que no tenga la clave secreta

CONTRASEÑA: Es una forma de autentificación que utiliza información secreta para controlar el acceso hacia algún recurso o archivo.

FORMATO DE ARCHIVO: Es un estándar que define la forma en que la información se organiza y se codifica en un archivo informático

PGP: Es un programa cuya finalidad es proteger la información distribuida a través de Internet mediante el uso de criptografía de clave pública.

4. CONSIDERACIONES GENERALES

El presente documento tiene una primera versión del 4 de junio de 2020, como un documento complementario. A partir del mes de mayo de 2021 pasa a ser un documento controlado en su primera versión.

5. CIFRADO DE DOCUMENTOS

El presente documento ilustra paso a paso cómo se debe realizar la instalación, configuración, creación de claves y exportación de claves de GPG.

6. INSTALACIÓN DE GPG4WIN

1. Descargar gpg4win desde https://www.gpg4win.de/.

2. Instalar GpgWin incluyendo las siguientes opciones: GnuPG, Kleopatra y GpgEx (requiere reiniciar el sistema una vez finalizada la instalación):



FECHA 2021-06-03 1

VERSIÓN V-

🔒 Instalación de Gpg4win		– 🗆 🗙					
Gpg4win	Selección de componentes Seleccione qué características de Gpg4win desea instalar.						
Marque los componentes q instalar. Presione Siguiente	ue desee instalar y desmarque los co e para continuar.	omponentes que no desee					
Seleccione los componente instalar:	s a GnuPG GPA GPA GpgCL GpgEX Browser integration	Descripción Sitúe el ratón encima de un componente para ver su descripción,					
Espacio requerido: 89.7MB							
Gpg4win-3,1,9							
	< <u>A</u> trás	Siguiente > Cancelar					

Ilustración 1 Instalación de Gpg4Win.

7. CREACIÓN DE UN PAR DE CLAVES UTILIZANDO KLEOPATRA

Iniciar Kleopatra: 1.

⑦ Kleopatra Archivo Ver Certificados Herramienţas P	referencia <u>s</u> V <u>e</u> ntana A <u>v</u> uda		— C	- ×
Firmar/Cifrar Descifrar/verificar Importar	Exportar Certificar Búsqueda en el servidor	. Bloc de notas		
Buscar <alt+q></alt+q>			Todos los certificados	~
Nombre OTI Sede Central	Correo OTISedeCentral@acr.gov.co	ID de los usuarios Válido desde Válido has certificado 16/04/2013	ta ID de la clave BD64 5F18 7EF1 4DDD	

Ilustración 2 Ventana de inicio de Kleopatra.



2. En el menú seleccionar Archivo > Nuevo par de claves:

0	Kleopatra					
Arcl	nivo Ver Co	ertificados	Herramientas	Preferencias	Ventana	Ayuda
	Nuevo par de	claves		Ctrl+N		G
Q	Búsqueda en	el servidor		Ctrl+Shift+I	tificar	Búsqueda en e
eę.	Importar			Ctrl+I		
	Exportar			Ctrl+E		Correo
	Exportar clave	es secretas			ral@ao	r.gov.co
Ģ	Imprimir clav	e secreta				
	Publicar en el	l servidor		Ctrl+Shift+E	E	
iх.	Descifrar/verit	ficar				
	Firmar/Cifrar.					
	Carpeta firma	ar/cifrar				
	Crear archivo	s de suma de	e verificación			
	Verificar archi	ivos de suma	de verificación.			
	Cerrar			Ctrl+W		
	Salir			Ctrl+Q		

Ilustración 3 Nuevo par de claves

3. En elegir formato seleccione Crear un par de claves personales OpenPGP:

	?	\times
Asistente de creación de par de claves		
Elegir formato		
Por favor, elija que tipo quiere usted crear.		
→ <u>Crear un par de claves personales OpenPGP</u> Los pares de claves OpenPGP están certificados por la confirmación de la hue clave pública.	ella digital d	e la
→ Crear <u>u</u> n par de claves personales X.509 y una solicitud de Los pares de claves X.509 se certifican por una autoridad de certificación (CA) generada necesita enviarse a la cA para finalizar la creación.	certificac). La petición	ión n
Next	Car	ncel

Ilustración 4 Crear un par de claves personales OpenPGP

En "Introduzca detalles", escriba el nombre y el correo electrónico. Oprima 4. el botón Next.



		?	×
← Asister	nte de creación de par de claves		
Introd	uzca detalles		
Por favor «Configu	r, introduzca sus detalles personales debajo. Si desea más control sobre los parámetros, p ración avanzada».	oulse	el botón
Nombre:	Pruebas	(0	opcional)
Correo:	prueba@correo.com.co	(0	opcional)
	Pruebas <prueba@correo.com.co></prueba@correo.com.co>		
	Configuración	<u>a</u> van	zada
	Next	Car	nc <u>e</u> l

Ilustración 5 Introducir detalles del par de claves

5. En "Parámetros de revisión" oprima el botón Crear.

		?	\times
 Asistente de creación de par de claves 			
Parámetros de revisión			
Por favor, analice los parámetros de los certificados antes de proceder.			
Nombre: Pruebas Correo: prueba@correo.com.co			
Mostrar todos los detalles			
	<u>C</u> rear	Cance	al

Ilustración 6 Parámetros de revisión del par de claves

6. En "Creando par de claves" suministre una contraseña para el par de claves. Oprima el botón Ok:



Next

Cancel

ves					
🔒 piner	ntry-qt	_		×]
	Por favor introdu: proteger su nuev Frase contraseña Repetir: Calidad:	zca frase cor a clave a: •••••• <u>O</u> K	itraseña p 100%	ara The second s	ırdar
	piner	pinentry-qt Por favor introdu proteger su nuev Frase contraseña Repetir: Calidad:	pinentry-qt Por favor introduzca frase con proteger su nueva clave Frase contraseña: Repetir: Calidad: QK	pinentry-qt Por favor introduzca frase contraseña p proteger su nueva dave Frase contraseña: Repetir: Calidad: 100% QK Cance	pinentry-qt Por favor introduzca frase contraseña para proteger su nueva clave Frase contraseña: Repetir: Calidad: 100% QK Cancelar

Ilustración 7 Crear contraseña para el par de claves

7. En "Par de claves creado con éxito" oprima el botón Finish:

	?	\times
 Asistente de creación de par de claves 		
Par de claves creado con éxito		
Su nuevo par de claves fue creado exitosamente. Encuentre detalles sobre el resultado y algunos seguir sugeridos más abajo.	pasos a	
Par de daves creado satisfactoriamente. Huella digital: 31F18E741F1E8265F3CF611C76BF3DD54EE73421		
Siguientes pasos		
Hacer copia de respaldo de su par de claves		
Enviar clave pública por correo		
Enviar dave pública a un servicio de directorio		
Einish	<u>C</u> ance	el

Ilustración 8 Par de claves creado con éxito.

8. EXPORTAR LA CLAVE COMPARTIDA (CLAVE PÚBLICA)

1. En Kleopatra, seleccione el Certificado que desea exportar:



🙃 Kleopatra	-	\times
<u>A</u> rchivo <u>V</u> er <u>C</u> ertificados Herramientas Preferencias V <u>e</u> ntana A <u>v</u> uda		
Firmar/Cifrar Descifrar/verificar Importar Exportar Certificar Búsqueda en el servidor Bloc de notas		
Buscar <alt+q> Todos los cert</alt+q>	ficados	\sim
Nombre Correo ID de los usuarios Válido desde Válido hasta ID de la cla	ve	
Prueba prueba@correo.com certificado 27/06/2019 76BF 3DD5 4E	7 3421	
OTI Sede Central OTISedeCentral@acr.gov.co certificado 16/04/2013 BD64 5F18 7E	1 4DDD	

Ilustración 9 Seleccionar el certificado en Kleopatra para exportar la clave pública.

Desplegar el menú contextual, haciendo clic con el botón derecho del ratón 2. sobre el nombre del certificado que desea exportar y seleccione la opción Exportar:

큤 Kleopatra						
Archivo Ver Certifi	cados	Herr	amientas	Preferencias	Ventana	Ayuda
Firmar/Cifrar Descifra	LQ ar/veri	ficar	<mark>≣≣</mark> Importar	 Exportar	es Certificar .	Q Búsqueda en e
Buscar <alt+q></alt+q>						
	Nom	ore			(Correo
Prueba OTI Sede Centr	eş T	Certific Certific Cambi Cambi Cambi Agrega Borrar	car cado raíz de cado raíz ne ar la confia ar la fecha ar la frase e ar ID de usu	e confianza o de confianza inza de la certifi de vencimiento de contraseña uario	icación	pw.co
		Exporta	ar			
	ē	Imprin	nir clave se	creta		
		Publica	ar en el sen	vidor		
		Detalle	s			

Ilustración 10 Menú contextual para exportar la clave pública.

Guardar el archivo de la clave pública con el nombre y en la ubicación de su 3. preferencia:



🗇 Exportar certificados		\times
 < · · · · · · · · · · · · · · · · · · ·	Buscar en Descargas	م
Organizar 👻 Nueva carpeta		= - ?
 Acceso rápido Escritorio Descargas Documentos ArpaUWP correos Resources SARA_v2 Carpetas de traba Este equipo 		
> 🔸 Descargas 🗸 <		>
Nombre: 31F18E741F1E8265F3CF611C76BF3DD54EE73421.asc		~
Tipo: Certificados OpenPGP (*.asc *.gpg *.pgp)		~
∧ Ocultar carpetas	<u>G</u> uardar	Cancelar

Ilustración 11 Guardar el archivo de la clave pública

9. EXPORTAR LA CLAVE SECRETA

Nota: La clave secreta debe ser almacenada en un lugar seguro y no debe ser compartida con nadie.

1. En Kleopatra, seleccione el Certificado que desea exportar:

7 Kleopatra					-	\times
<u>Archivo V</u> er <u>C</u> ertificados Herramien <u>t</u> as Pre	eferencia <u>s</u> V <u>e</u> ntana A <u>y</u> uda					
		Ø				
Firmar/Cifrar Descifrar/verificar Importar	Exportar Certificar Búsqueda en el servidor.	Bloc de notas				
Buscar <alt+q></alt+q>					Todos los certificados	\sim
Nombre	Correo	ID de los usuarios	Válido desde	Válido hasta	ID de la clave	
Prueba	prueba@correo.com	certificado	27/06/2019		76BF 3DD5 4EE7 3421	
OTI Sede Central	OTISedeCentral@acr.gov.co	certificado	16/04/2013		BD64 5F18 7EF1 4DDD	

Ilustración 12 Seleccionar el certificado en Kleopatra para exportar la clave privada

2. Desplegar el menú contextual, haciendo clic con el botón derecho del ratón sobre el nombre del certificado que desea exportar y seleccione Exportar claves secretas:

Ŷ			INSTRU	CTIVO	DE CIF	RADO D	Ε	CO	DIGO): 11-1-01	
Agencia para la Reincorporación y la Normalización - ARM	4		DC	CUME	NTOS -	PGP		FECHA 2021-06-	∖ ∙03	VERSIÓN V- 1	-
🔿 Kleopatra Archivo Ver Certifi	icados	Herra	mientas Pr	referencias	Ventana	Ayuda					
Firmar/Cifrar Descifr	ar /verific	ar	<u>∎</u> ⊒ Importar	Exportar	Certificar .	Búsqueda		servidor	Blo	C de notas	
Buscar <alt+q></alt+q>	cados	Cortif									Ī
L+ Todos jos cerun		Cerui	icados importa	ados							
L. Todos jos cerum	Nombr	e	icados importa	ados		Correo			ID de	los usuarios	
Prueba OTL Sede Centr	Nombr	e Certifica	r	ados		Correo			ID de certif	e los usuarios ficado	
Prueba OTI Sede Centr	Nombr	e Certifica Certifica Cambiar	r do raíz de co do raíz no de la confianza	nfianza confianza de la certifi vencimiento	cación	Correo			ID de certif certif	los usuarios ficado ficado	
Prueba OTI Sede Centr	Nombr	e Certifica Certifica Certifica Cambiar Cambiar Cambiar	r do raíz de co do raíz no de la confianza la fecha de v la frase de c ID de usuaric	nfianza confianza de la certifi vencimiento ontraseña 2	cación	Correo		•	ID de certif	los usuarios ficado ficado	
Prueba OTI Sede Centr	Nombr	e Certifica Certifica Certifica Cambiar Cambiar Cambiar Cambiar Agregar	r do raíz de co do raíz no de la confianza la fecha de v la frase de co ID de usuario	nfianza confianza de la certifi vencimiento ontraseña	cación	Correo DV.co			ID de certif certif	los usuarios ficado ficado	
Prueba OTI Sede Centr	Nombr	e Certifica Certifica Certifica Cambiar Cambiar Cambiar Cambiar Cambiar Cambiar Cambiar Cambiar Cambiar Cambiar Cambiar Cambiar Cambiar	r do raíz de co do raíz no de r la confianza r la fecha de v la frase de co ID de usuario	nfianza e confianza de la certifi vencimiento ontraseña	cación	Correo Dv.co			ID de certif certif	i los usuarios ficado ficado	
Prueba OTI Sede Centr	Nombr	e Certifica Certifica Certifica Cambiar Cambiar Cambiar Agregar Sorrar xportar	r do raíz de co do raíz no de la confianza la fecha de v la frase de co ID de usuario	nfianza confianza de la certifi vencimiento ontraseña	cación	Dv.co			ID de certif	los usuarios ficado ficado	
Prueba OTI Sede Centr	Nombr	Certifica Certifica Certifica Cambiar Cambiar Cambiar Agregar Rorrar Xportar Xportar Mprimi	r do raíz de co do raíz no de la confianza la fecha de v r la frase de co ID de usuario claves secret r clave secret	nfianza e confianza de la certifi vencimiento ontraseña a	cación	Dv.co		:	ID de certif	e los usuarios ficado ficado	
Prueba OTI Sede Centr		e Certifica Certifica Certifica Cambiar Cambia	r do raíz de co do raíz no de la confianza la fecha de v la frase de co ID de usuario claves secret r clave secret en el servido	nfianza e confianza de la certifi vencimiento ontraseña o a a	cación	Dv.co		:	ID de certif	e los usuarios ficado ficado	

Ilustración 13 Menú contextual para exportar las claves secretas

3. Guardar el archivo de la clave secreta con el nombre y en la ubicación de su preferencia:

큤 Export Secret Key	×
← → ~ ↑ ↓ > Este equipo > Descargas	> v Ö Buscar en Descargas ク
Organizar 👻 Nueva carpeta	
SARA_v2 ^ Nombre	
Carpetas de traba	ebas.asc
 Este equipo Descargas Quicksand-Regul Escritorio Imágenes Música 	ebas.asc ar
 Objetos 3D Vídeos OS (C:) Nuevo vol (E:) 	
~ <	>
Nombre: clave_secreta_pruebas.asc	~
Tipo: Archivos de clave secreta (*.as	c *.gpg *.pgp) ~
∧ Ocultar carpetas	<u>G</u> uardar Cancelar

Ilustración 14 Guardar el archivo de la clave secreta.

10.IMPORTAR UNA CLAVE.

1. Para importar una clave, inicie Kleopatra y en el menú seleccione Archivo > Importar:



FECHA 2021-06-03

VERSIÓN V-1

Arcl	nivo	Ver	Certificados	Herramientas	Preferencias	Ventana	Ayuda
	Nue	vo par	de claves		Ctrl+N		Q
Q	Búso	queda	en el servidor		Ctrl+Shift+I	tificar	Búsqueda en el ser
eę.	Imp	ortar			Ctrl+1		
	Expo	ortar			Ctrl+E		
	Expo	ortar cl	aves secretas				Correo
ē	Imp	rimir c	lave secreta			ral@a	cr.gov.co
	Pub	licar e	n el servidor		Ctrl+Shift+E		
<u>ix</u>	Dese	cifrar/\	verificar				
	Firm	nar/Cif	rar				
	Carp	oeta fir	mar/cifrar				
	Crea	ar arch	ivos de suma d	e verificación			
	Verif	icar ar	chivos de suma	a de verificación			
	Cerr	ar			Ctrl+W		
-	Salir				Ctrl+Q		

Ilustración 15 Menú para importar una clave en Kleopatra.

Seleccione el archivo a importar y haga clic en el botón Abrir: 2.

7 Seleccione el archivo del certificado		\times
← → ~ ↑ 🕹 > Este equipo > Descargas > 🗸 🗸	Buscar en Descargas	م
Organizar 👻 Nueva carpeta		□ ?
Acceso rápido Escritorio Descargas Documentos ArpaUWP correos SARA_v2 Este equipo Descargas Documentos		No hay ninguna vista previa disponible.
Escritorio 🗸 <	>	
Nombre: clave_publica_pruebas.asc ~	Certificados (*.asc *.cer *.	cert *. ~
	Abrir Car	icelar

Ilustración 16 Seleccionar el archivo de clave para importar.

Al importar el archivo, Kleopatra le preguntará si desea marcar el certificado 3. como válido. Haga clic en el botón No.



11. CIFRAR UN ARCHIVO CON UNA CLAVE PÚBLICA

1. En Kleopatra, en el menú Archivo seleccione la opción Firmar/Cifrar

Archivo R Nue Q Búsc R Impo E Expo C Expo Impo R Publ	Ver Certificados vo par de claves queda en el servidor ortar ortar ortar claves secretas rimir clave secreta	Herramientas	Preferencias Ctrl+N Ctrl+Shift+1 Ctrl+1 Ctrl+E	Ventana Ayuda
Nue Nue Suisc Expo Expo Expo Impi Expo Expo Impi Publ	vo par de claves queda en el servidor ortar ortar ortar claves secretas rimir clave secreta		Ctrl+N Ctrl+Shift+I Ctrl+I Ctrl+E	tificar Búsqueda en e
Q Búsc 国 Impe 国 Expe 回 Expe 日 Impe 国 Publ	queda en el servidor ortar ortar ortar claves secretas rimir clave secreta		Ctrl+Shift+I Ctrl+I Ctrl+E	tificar Búsqueda en e
e Imp e Expo e Expo 合 Imp 器 Publ	ortar ortar claves secretas rimir clave secreta		Ctrl+I Ctrl+E	dos importados
Expo Expo Expo Impo Expo	ortar ortar claves secretas rimir clave secreta		Ctrl+E	los importados
E Expo 合 Impi	rimir claves secretas rimir clave secreta			Correo
母 Impi 酮 Publ	rimir clave secreta			001100
四 Publ				o.com
	licar en el servidor		Ctrl+Shift+E	ral@acr.gov.co
전 Desc	ifrar/verificar			
🖬 Firm	ar/Cifrar			
Carp	eta firmar/cifrar			
Crea	r archivos de suma de	e verificación		
Verif	icar archivos de suma	de verificación.	•	
Cerr	ar		Ctrl+W	
 Salir 			Ctrl+Q	

Ilustración 17 Menú para cifrar un archivo en Kleopatra.

2. Seleccione el archivo para cifrar y oprima el botón Abrir:



Ilustración 18 Abrir archivo para cifrar con Kleopatra.

3. En la ventana Firmar/cifrar archivos solo debe estar seleccionada la opción Cifrar para otros y se debe seleccionar la clave pública con la que se desea cifrar. Hacer clic en el botón Cifrar:



큤 Firmar/cifrar archi	vos - Kleopatra	?	\times
Firmar/cifrar a	archivos nar)		
Eirmar como:	☑ OTI Sede Central <otisedecentral@acr.gov.co> (certifica</otisedecentral@acr.gov.co>	ado, cr	rea 🗸
Cifrar			
Cifrar <u>p</u> ara mí:	▼ OTI Sede Central <otisedecentral@acr.gov.co> (certifica</otisedecentral@acr.gov.co>	ado, cr	rea 🗸
Cifrar para otros:	Prueba <prueba@correo.com> (no certificado, OpenPGP,</prueba@correo.com>	cread	• 💌
	🞗 Por favor, introduzca un nombre o dirección de correo		
Cifrar con contraser	a. Cualquiera con <u>e</u> l que usted comparta la contraseña podrá ve	er los d	atos.
Salida			
Cifrar / Firmar cada	<u>a</u> rchivo por separado.		
E:/Tito Peralt	a Benítez/Downloads/prueba_arn_2019-06-27.txt.gpg		
	Cifrar	Can	:el

Ilustración 19 Seleccionar clave pública para el cifrado

4. Cuando se complete el cifrado, se muestra un mensaje informativo indicando el éxito de la operación:

🗇 Firmar/cifrar archivos - Kleopatra	?	\times
Resultado El estado y progreso de la operación de cifrado se muestra aquí.		
OpenPGP: Todas las operaciones terminadas.		
prueba_arn_2019-06-27.txt → prueba_arn_2019-06-27.txt.gpg: El cifrado tenido éxito. El cifrado tuvo éxito.	o ha	
Einish	Can	cel

Ilustración 20 Mensaje que se muestra cuando se completa el cifrado de un archivo.

12. DESCIFRAR UN ARCHIVO CON UNA CLAVE SECRETA.

Nota: Para descifrar un archivo debe tener importada la clave secreta y conocer la contraseña del certificado. Para más información, consulte la sección Creación de un par de claves utilizando Kleopatra.



1. En Kleopatra, en el menú Archivo seleccione la opción Descifrar/Verificar:

Ø	Kleop	patra				
Arcl	hivo	Ver Certificados	Herramientas	Preferencias V	entana A	yuda
	Nue	vo par de claves		Ctrl+N		Q
Q @	Bús Imp	queda en el servidor ortar		Ctrl+Shift+I Ctrl+I	·tificar	Búsqueda en el servidor
	Expo	ortar		Ctrl+E		
e.	Expo	ortar claves secretas rimir clave secreta			Co	rreo
	Pub	licar en el servidor		Ctrl+Shift+E	ral@acr.g	оv.со
X	Des	cifrar/verificar				
	Firm	nar/Cifrar				
	Carp	peta firmar/cifrar				
	Crea	ar archivos de suma de	e verificación			
	Verif	ficar archivos de suma	de verificación.			
	Cerr	ar		Ctrl+W		
	Salir	r		Ctrl+Q		

Ilustración 21 Menú para descifrar un archivo en Kleopatra.

2. Seleccione el archivo que quiere descifrar y oprima el botón Abrir:



Ilustración 22 Abrir archivo para descifrar en Kleopatra



3. Cuando abra el archivo, le solicita la contraseña de la clave privada:



Ilustración 23 Insertar la contraseña de la clave privada

4. Si ingresó la contraseña correctamente, Kleopatra le informa que el archivo fue descifrado. Oprima el botón Save All para guardar el archivo en la ubicación Carpeta de salida:

7 Descifrar/Verificar archivos - Kleopatra		?	×
Carpeta de salida: E:/Tito Peralta Benítez/Downloads		•8	
Todas las operaciones terminadas.			
		1	00%
prueba_arn_2019-06-27.txt.gpg → prueba_arn_2019-06-27.txt: El cifrado ha tenido éxito.	Mostrar registro de a	suditoría	
Nota: Usted no puede estar seguro de quien ha cifrado este mensaje ya que no está firmado.			
	Save All	Discar	ď

Ilustración 24 Mensaje informando que el archivo fue descifrado correctamente.