ANEXO

Manual del Usuario "PGP"

Objetivo

Con PGP se protegerá la privacidad y autenticidad de los archivos enviados utilizando la opción de **Entrega de Información Vía Electrónica** a través de la página WEB de la Comisión Nacional de Seguros y Fianzas (CNSF). Con PGP también se puede firmar digitalmente los archivos, lo cual asegura su autenticidad.

La aplicación PGP tiene como objetivo encriptar cualquier tipo de documentación enviada a través del correo electrónico.

Para efectos del envío de información por parte de las Instituciones o Sociedades a la CNSF a través de Internet, se requiere de esta aplicación, ya que es primordial para las Instituciones y Sociedades el hecho de que su información no sea modificada o editada una vez que ha sido enviada a la CNSF, por lo que requerirán encriptarla con la aplicación PGP utilizando llaves públicas y privadas.

PGP esta basado en una tecnología de encriptación ampliamente aceptada conocida como criptografía de llave pública en donde dos llaves complementarias –un par de llaves – son usadas para mantener la seguridad de las comunicaciones. Para enviar a alguien un archivo privado por correo electrónico se debe tener primero una copia de la llave pública de esa persona para encriptar la información, la cual únicamente será descifrada usando la llave privada correspondiente.

A continuación se describe el funcionamiento de esta aplicación como herramienta de apoyo en el proceso de Entrega de Información Vía Electrónica a través de la página WEB de la CNSF.

I. Como obtener el programa de instalación de PGP de Internet

Como primer paso se debe tener acceso a internet y en el campo de Dirección teclear <u>http://www.download.com</u>, dar Enter y aparecerá la siguiente pantalla:





Dar enter y aparecerá la siguiente pantalla:

and the second se	et desires there Binger	de Fanistic Historia	Espent 1	warden anger	Maddan
In E Hits //download com co	er/3120-20-0 Hinl/7d=PGPSig=d-2001			1	Pr Y
DOWNLO	ID CON	CHEI fech elles Pice pano	amone (Product	strates I Lach to	cess I D pevelos
DOWNLO	AD.COM Search		In Windows	- Gal	
All Downlands Born St	Teare Developer Web Developer	Bastress Personal Terry	William Sar	-	Advanced Sear
Spensor of web results + Bay PGP Personal Se + Actic Saft way to use + Encryption Software CritET + Downloads + Wea	contre 7.03 . 539,95 PGP: Alternative RomwledgeStorm				
and a second second				Found JB Ling	trown to a second
Search results				+ President	up 1 2 Meet
Search results	Alficenses Alfile sizes	Al cotegones	3	Upperate	us 1 <u>2 Newl</u>
Search results Filter by ALCSs Re-cont by Name	All frames All file stress	Al colegones User colleg	Downshouth	Update	us 1 <u>2 Nort</u>

Buscar y seleccionar el programa PGP freeware 7.0.3, dar Enter (Nota: Si se tiene la versión XP de Windows, se recomienda usar la versión 8)

a fueran Ber Desauter Deur	Alani com a Michaelli Internet Exploren Na Edician Ber Forentis Interneteria Angla			
		eda Favoritos Historia	Cores Tara	te tepres Mode
PUP-ICO 0.95 Enclopi pour ICD messages with this privace utility. 05: Windows 85/96/WT/2000 File Size: 15748 License: Free	02/96/2001	833 3 12 volue	14,835	Descinations
PGP SafeBulk 1.0 Send networ enal restragen to large lats of recipients. DS: Windows 25/30/WT File Stars (55/33) License: Free to ty	01/28/2880		2,726	Durnisal.com
PiPt myones 7.6.) pop ProteCula enailhon waathobed viewing 05: Window 95/96/WT/2001 File Size 7.5/HE License: Free	02/20/2001	523 3 231 value	315,481	E Reentaatinee
Her Bot 1,61 peop proc Access radiple a-mail accounts, use comprehensive lifering, potent your letters with another DF and more DS: Windows 55/500.Her/117(200) File Size: 2:37HB Libernet: Files to by, \$25 to buy	08/12/2062		128,139	Deveload zon
Sever Triple Encryption Small Client 2.1	12/13/2000	785 G	21.229	E Download now

Entraremos a la siguiente pantalla en donde daremos inicio al proceso de descarga del software, dando click sobre las palabras "Download Now"



Aparecerán los siguientes mensajes

Descarga de archivos	×
	Ha decidido descargar un archivo de este lugar. PGPFW703.zip de download.nai.com ¿Qué desea hacer con este archivo?
	 Abrir este archivo desde su ubicación actual Guardar este archivo a disco Freguntar siempre antes de abrir este tipo de archivo
	Aceptar Cancelar <u>M</u> ás información

Por default nos indica que se guarde el archivo en disco, no cambiar esta opción y dar click en el botón <u>Aceptar</u>, nos mostrará el siguiente mensaje

4

Guardar como						? ×
Guardar <u>e</u> n:	🔄 Archivos	-	E	<u>*</u>		
0ct_2002						
Nombre del archivo	PGPEW/703 zin			I F	Guarda	
			_		<u>u</u> uaiua	<u> </u>
Guardar como <u>t</u> ipo:	WinZip File		-		Cancela	ar

Aquí indicaremos en qué carpeta de nuestra PC deseamos guardar el programa, posteriormente dar click en el botón Guardar y aparecerá una pantalla indicando el avance de descarga



Al terminar la descarga se cerrará el cuadro de diálogo, siempre y cuando esté activado, en caso

contrario dar click en el botón contrario dar click en el botón que aparecerá en la parte inferior derecha y cerrar la conexión con Internet.

Descarga completa	
Descarga cor	mpleta
Guardado:	
PGPFW703.zip de downle	oad.nai.com
Descargado: 7.	14 MB en 1 min. 33 seg.
Descargaria: D:	\Archivos\PGPFW703.zip
Tasa de transferencia: 78	3.6 KB/Seg
Cerrar el diálogo al ter	minar la descarga.
	Abrir Abrir carpeta Cerrar

II. Cómo instalar la aplicación PGP

Dependiendo del equipo de cómputo y la versión del sistema operativo, el programa lo instalará automáticamente al ejecutar la descompactación del archivo que se bajó de Internet.

La primera vez que se crea una llave privada, el Administrador instala el producto PGP, el cual es de uso libre conforme a lo declarado por Integraciones Administrativas. Siguiendo los pasos de la instalación de PGP, la aplicación le pedirá ingresar una frase secreta o un "passphase" para poder crear una llave privada, el Administrador deberá crear la llave privada SIN ingresar una contraseña (passphase) ni su confirmación.

Procedimiento:

Localizar el archivo descargado PGP que lleva la extensión .exe



Dar doble click sobre el ejecutable ^{TCPGPfreeware 7.0.3.exe} y aparecerá una secuencia de mensajes





Al terminar la secuencia de mensajes aparecerá la pantalla de bienvenida



Dar click en el botón y aparecerá un mensaje de Acuerdo de uso de Licencia

PGPtreeware 7.0.3 - Installer	X
License Agreement	
Please read the following license agreement carefully.	
Press the PAGE DOWN key to see the rest of the agreement.	
Network Associates Fineware End User License Agreement [Non-Commercial Use and Distribution Only]	
NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT ("AGREEMENT"), FOR THE LICENSE OF SPECIFIED SOFTWARE ("SOFTWARE") BY NETWORK ASSOCIATES TECHNOLOGY COMPANY, INC. ("NETWORK ASSOCIATES"), BY CUCKING THE ACCEPT BUITTON OR INSTALLING THE SOFTWARE, YOU JEITHER AN INDIVIDUAL OR A SINGLE ENTITY) CONSENT TO BE BUIND BY AND BECOME A PARTY TO THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, CUCK THE BUTTON THAT	
Do you accept all the terms of the preceding License Agreement? If you choose No, the setup will close. To install PGP, you must accept this agreement.	
Kack Yes No	
ar click en el botón	

7

View the Rea	d Me for PGPheeware	7.0.3		
PGP for Wind	Freeware Version 7.0. lows 95, 98, Millenium	3 ReadMe , NT, and 2000		-
Copyrigh Technoli	t (c) 1990-2001 by Nel ogy, Inc., and its Affilia	tworks Associates ted Companies.		
1 '	unights Neserved.			
Thank you fille contains	ar using Network Asso	ciates' products. This Re exarding PGP. Network	eadMe	
Associates s entire docum	trongly recommends the	hat you read this		
				<u>.</u>
				-

Dar click en el botón

Por default aparecerá marcada la opción de • Yes, I already have keyrings, debemos seleccionar la opción • No, I'm a New User como se muestra en la siguiente pantalla

GPfreeware 7.0.3 - Installer			×
Uzer Type			
Do you already have PGP keyrings yo	ou would like to use?		
Yes, Lakeady have keyrings.			
No, I'm a New User			
	< Back	Next >	Cancel
Next >			

Dar click en el botón para seleccionar el Fólder Destino para la Instalación del Directorio

Setup will ins	tall PGPfreeware 7.0.3	3 in the following fo	lder.		
To install to the select another	nis folder, click NEXT er folder.	. To install to a diffe	erent folder, click	BROWSE and	
Destination	Folder				
C:\\Netw	ork Associates\PGP	for Windows NT		B <u>r</u> owse	

Si deseamos cambiar el Fólder Destino, pulsar el botón , si lo queremos dejar en la ruta marcada por default dar click en el botón wext y aparecerá la ventana de Selección de Componentes

Select Components			
Choose the components Setup will install.			
Select the components you want to install, install.	, and clear the c	omponents you do not	want to
 PGPnet Personal Firewall/IDS/VP1 PGP Plugin for Microsoft Outlook PGP Plugin for Microsoft Outlook E PGP Plugin for Qualcomm Eudora PGP Plugin for ICQ PGP Documentation 	N xpress	This component ind core PGP Key Man files.	ludes the agement
Space Required on C: Space Available on C:	11127 K 669120 K		

Dar click en el botón



y aparecerá la pantalla para comenzar a copiar los archivos

F	PGPfreeware 7.0.3 - Installer
	Start Copying Files
	Review settings before copying files.
	Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files. Current Settings: Date: - 9-10-2002 Product: - 9-GPfreeware 7.0.3 Install Type: - As a New user to PGP, we welcome you and thank you for choosing our product. Operating System:
	- Microsoft Windows NT 4.0 Service Pack 6 Selected Components:
	pgp.com
	< <u>B</u> ack <u>Next></u> Cancel
click e	PGPfreeware 7.0.3 - Installer PO you know what you're missing? PGP Personal Security, the retail version of this product, provides many additional benefits:
	PGPdisk PR PK PK
	Easy-to-use harddisk encryption that protects your data
	Personal Firewall/IDS Industrial strength personal firewall and intrusion detection
	Technical Support
	- Contact our support organization for technical support
	And more
	Read more about it in this product's Read Me file. We invite you to visit your local software retailer or store.mcafee.com and support PGP by purchasing it.
	pgp.com < <u>Back</u> Cancel Cancel
r click e	en el botón Next> y aparecerá la pantalla que indica el avance de instalac

PGP Setup is	performing the request	ed operations.	
Installing: F	GP Key Management	files	
C:\WINNT\S	stem32\PGPsc.dll		
		37%	

Al terminar la instalación se activará y pulsaremos el botón

PGPnet Set Adapter	
Please select the network adapter(s) you want secured/unsecured.	
[1] Intel(R) PRO/100 VM Network Connection	
Select All DK Cancel Help Press OK after making selection.	

<u>N</u>ext >

Dar click en el botón y se activará el botón y aparecerán una serie de mensajes, al terminar éstos aparecerá la siguiente pantalla, la cual nos permitirá crear la llave privada de la Institución o Sociedad, es recomendable que se cree en este momento, sin embargo, en caso de decidir hacerlo después, basta con que cancele el proceso pulsando el botón

<u>Cancelar</u> y posteriormente accese a PGP, como se indica en este manual y realice los pasos que a continuación se indican,



Pulsar el botón

Siguiente >

y aparecerá la siguiente ventana

Asimismo, si usted decidió cancelar la creación de la llave privada al momento mismo de hacer la instalación, cuando decida hacerlo, deberá seguir los pasos que se indican a continuación

Name and Email	Assignment
your correspond	ents know that the public key they are using belongs to you.
Euli name:	
By associating a correspondents	n email address with your key pair, you will enable PGP to assist your in selecting the correct public key when communicating with you.
Email address:	
	< Attás Siguiente > Car
	- Gun Shrows

En el campo ^{run name.} teclearemos el nombre de la compañía

A 4		1 A
N	ame and Emai	II Assignment r must have a name associated with it. The name and email address let
	your correspor	ndents know that the public key they are using belongs to you.
	Full name:	Seguros Génesis
	<u>L</u> air Hamo.	
	By associating correspondent	g an email address with your key pair, you will enable PGP to assist your ts in selecting the correct public key when communicating with you.
	<u>E</u> mail address:	
		< Atrás Siguiente > Cancelar
Emai	Laddress:	Siguiente >
<u>E</u> mai	l address: se	e dejará en blanco y al pulsar el botón
<u>E</u> mai	l address: se	e dejará en blanco y al pulsar el botón
<u>E</u> mai Key G	l address: se	e dejará en blanco y al pulsar el botón Siguiente >
<u>E</u> mai Key G	l address: se	e dejará en blanco y al pulsar el botón Siguiente >
<u>E</u> mai Key G Na	l address: se ieneration Wiz ame and Emai Every key nair	e dejará en blanco y al pulsar el botón Siguiente > zard X il Assignment u must have a name associated with it. The name and email address let
<u>E</u> mai Key G Na	l address: se ieneration Wi: ame and Emai Every key pair your correspor	e dejará en blanco y al pulsar el botón Siguiente > zard il Assignment r must have a name associated with it. The name and email address let ndents know that the public key they are using belongs to you.
<u>E</u> mai Key G Na	l address: Se ieneration Wi: ame and Emai Every key pair your correspor	e dejará en blanco y al pulsar el botón Siguiente > zard il Assignment r must have a name associated with it. The name and email address let ndents know that the public key they are using belongs to you.
<u>E</u> mai Key G Na	l address: Se ieneration Wit ame and Emai Every key pair your correspor Full name:	e dejará en blanco y al pulsar el botón Siguiente > zard il Assignment r must have a name associated with it. The name and email address let ndents know that the public key they are using belongs to you. Seguros Génesis
<u>E</u> mai Key G Na	I address: Se ieneration Wi: ame and Emai Every key pair your correspor Eull name:	e dejará en blanco y al pulsar el botón Siguiente > zard il Assignment r must have a name associated with it. The name and email address let ndents know that the public key they are using belongs to you. Seguros Génesis
<u>E</u> mai Key G Na	I address: Se ieneration Wit ame and Emai Every key pair your correspor Eull name: B. PGP Key	e dejará en blanco y al pulsar el botón Siguiente > zard il Assignment r must have a name associated with it. The name and email address let ndents know that the public key they are using belongs to you. Seguros Génesis Generation
<u>E</u> mai Key G Na	I address: Se ieneration Wit ame and Emai Every key pair your correspor Eull name: B, PGP Key	e dejará en blanco y al pulsar el botón Siguiente > zard il Assignment r must have a name associated with it. The name and email address let ndents know that the public key they are using belongs to you. Seguros Génesis Generation In order to take advantage of PGP's email integration features
Emai Key G Na	address: Se Second Second Sec	e dejará en blanco y al pulsar el botón Siguiente > zard il Assignment r must have a name associated with it. The name and email address let ndents know that the public key they are using belongs to you. Seguros Génesis Generation In order to take advantage of PGP's email integration features (and so others can find your key), it is strongly advised that you
<u>E</u> mai Key G Na	i address: Se Second Second S	e dejará en blanco y al pulsar el botón Siguiente > zard il Assignment r must have a name associated with it. The name and email address let ndents know that the public key they are using belongs to you. Seguros Génesis Generation In order to take advantage of PGP's email integration features (and so others can find your key), it is strongly advised that you enter an email address.
<u>E</u> mai Key G Na	ieneration Wiz ame and Emai Every key pair your correspor Eull name: B PGP Key E	e dejará en blanco y al pulsar el botón Siguiente > zard il Assignment r must have a name associated with it. The name and email address let ndents know that the public key they are using belongs to you. Seguros Génesis Generation In order to take advantage of PGP's email integration features (and so others can find your key), it is strongly advised that you enter an email address.
Emai Key G Na	ieneration Wiz ame and Emai Every key pair your correspor Eull name: B PGP Key E	e dejará en blanco y al pulsar el botón Siguiente > zard × il Assignment r must have a name associated with it. The name and email address let ndents know that the public key they are using belongs to you. Seguros Génesis Generation × In order to take advantage of PGP's email integration features (and so others can find your key), it is strongly advised that you enter an email address. Continue without entering an email address?
Emai Key G Na	address: Se Second Second Sec	e dejará en blanco y al pulsar el botón Siguiente > zard il Assignment r must have a name associated with it. The name and email address let ndents know that the public key they are using belongs to you. Seguros Génesis Generation In order to take advantage of PGP's email integration features (and so others can find your key), it is strongly advised that you enter an email address. Continue without entering an email address?
Emai	address: Se Second Second Sec	e dejará en blanco y al pulsar el botón zard il Assignment r must have a name associated with it. The name and email address let ndents know that the public key they are using belongs to you. Seguros Génesis Generation In order to take advantage of PGP's email integration features (and so others can find your key), it is strongly advised that you enter an email address. Continue without entering an email address? Si No
<u>E</u> mai Key G Na	address: Se Second Second Sec	e dejará en blanco y al pulsar el botón zard Si Assignment r must have a name associated with it. The name and email address let ndents know that the public key they are using belongs to you. Seguros Génesis Generation S In order to take advantage of PGP's email integration features (and so others can find your key), it is strongly advised that you enter an email address. Continue without entering an email address? Si No
<u>E</u> mai Key G Na	address: Se Second Second Sec	e dejará en blanco y al pulsar el botón zard Si Assignment r must have a name associated with it. The name and email address let ndents know that the public key they are using belongs to you. Seguros Génesis Generation S In order to take advantage of PGP's email integration features (and so others can find your key), it is strongly advised that you enter an email address. Continue without entering an email address? Si No
Emai	address: Se Second Second Sec	e dejará en blanco y al pulsar el botón sard Sid Assignment r must have a name associated with it. The name and email address let ndents know that the public key they are using belongs to you. Seguros Génesis Generation In order to take advantage of PGP's email integration features (and so others can find your key), it is strongly advised that you enter an email address. Continue without entering an email address? Si No
Emai	address: se seneration Wiz ame and Emai Every key pair your correspon Eull name: B PGP Key E	e dejará en blanco y al pulsar el botón zard il Assignment r must have a name associated with it. The name and email address let ndents know that the public key they are using belongs to you. Seguros Génesis Generation In order to take advantage of PGP's email integration features (and so others can find your key), it is strongly advised that you enter an email address. Continue without entering an email address? <u>Si</u> No
Emai	address: se seneration Wiz ame and Emai Every key pair your correspon Eull name: B PGP Key E E	e dejará en blanco y al pulsar el botón zard il Assignment must have a name associated with it. The name and email address let ndents know that the public key they are using belongs to you. Seguros Génesis Ceneration In order to take advantage of PGP's email integration features (and so others can find your key), it is strongly advised that you enter an email address? Solution without entering an email address?

de e-mail, pulsar el botón y aparecerá la siguiente pantalla

assphrase Ass Your private ku passokrase se	gnment sy will be protected by a p cost and do not write it do	assphrase. It is	important that y	ou keep this
Your passphra	e should be at least 8 cf	alacters long a	nd should contai	'n
non-alphabeto	characters.			
	-			✓ <u>H</u> ide Typin
Passphrase:	r			-
	Passphrase Quality:			
				_
Confirmation:				
				2
				_

En esta ventana **NO SE DEBE CAPTURAR EL "PASSPHRASE"**, dar click en el botón Siguiente , aparecerá otra pantalla <u>en la que ind</u>ica que es necesario pulsar el "passphrase",

por favor IGNÓRELA y pulse el botón

iener assph	stion Wizard rase Problem
You	passphrase is a potential security hazard because of the following:
≞	It did not meet the suggested length of 8 characters.
	< Attas Siguente> Cance

Aparecerá una ventana indicando el proceso de instalación



Al terminar el proceso aparecerá la siguiente pantalla



Pulsar el botón Finalizar y aparecerá un último mensaje, en el que se encuentra seleccionada por default la opción de reiniciar su PC

Si usted decidió crear su llave privada en un momento diferente al de la instalación, ya no se presentarán las pantallas de Wizard y tampoco le recomendará reiniciar su equipo, ya que esa recomendación sólo la hace después de haber instalado un software nuevo.



III. Cómo accesar a PGP para crear una llave nueva

Para accesar a la aplicación, dar click en el botón regionaria que se encuentra en la barra de tareas, seleccione del primer menú de opciones regionaria, en el segundo menú busque y seleccione regionaria en la barra de tareas, en el segundo menú busque y seleccione regionaria en la barra de tareas, en el segundo menú busque y seleccione regionaria en la barra de tareas, en el segundo menú busque y seleccione regionaria en la barra de tareas, en el segundo menú busque y seleccione regionaria en la barra de tareas, en el segundo menú busque y seleccione regionaria en la barra de tareas, en el segundo menú busque y seleccione regionaria en la barra de tareas, en el segundo menú busque y seleccione regionaria en la barra de tareas, en el segundo menú busque y seleccione regionaria en la barra de tareas, en el segundo menú busque y seleccione regionaria en la barra de tareas, en el segundo menú busque y seleccione regionaria en la barra de tareas, en el segundo menú busque y seleccione regionaria en la barra de tareas, en el segundo menú busque y seleccione regionaria en la barra de tareas, en el segundo menú busque y seleccione regionaria en la barra de tareas, en el segundo menú busque y seleccione regionaria en la barra de tareas, en el segundo menú busque y seleccione regionaria en la barra de tareas, en el segundo menú busque y seleccione regionaria en la barra de tareas, en el segundo menú busque y seleccione regionaria en la barra de tareas, en el segundo menú busque y seleccione regionaria en la barra de tareas, en el segundo menú busque y seleccione regionaria en la barra de tareas, en el segundo menú busque y seleccione regionaria en la barra de tareas, en el segundo menú busque y seleccione regionaria en la barra de tareas, en el segundo menú busque y seleccione regionaria en la barra de tareas, en el segundo menú busque y seleccione regionaria en la barra de tareas, en el segundo menú busque y seleccione regionaria en la barra de tareas, en el segundo menú busque y seleccione regionaria en la barra de ta





Seleccionar el menú Keys y se desplegará un cuadro de opciones

💦 PGPke	ys								_ 🗆 ×
<u>F</u> ile <u>E</u> dit	⊻iew	<u>K</u> eys	<u>S</u> erver	<u>G</u> roup	s <u>H</u> elp				
🤏 🗶 i	4 1	<u>Sig</u> r Set	1 as Defai	ılt Kev	Ctrl+S Ctrl+D				
Keys		Add				alidity	Trust	Size	Description
🕀 🔫 🕀	°GP Sa	Ena	ble					1024	Expired DH/DSS
🕀 🔫 🗄	-GF Sa	 Disa	able					2048/1024	Expired DH/DSS (
🕀 👼 🕂	-GF Sa	Rey	oke			•		1024	Expired DH/DSS p
		Rev	verify Sigr	natures					
		<u>N</u> ev	v Key		Ctrl+N				
		Sha	re S <u>p</u> lit						
		l <u>m</u> p-	ort		Ctrl+M				
		Е <u>ж</u> р	ori		Ctrl+E				
•		Prop	perties		Ctrl+l				Þ

Seleccionar la opción New Key... y aparecerá la siguiente pantalla



Seguir los pasos descritos a partir de la página 12 de este manual.

IV. Envío de la llave pública de la Institución o Sociedad a la CNSF

Accesar a la aplicación PGP y seleccione PGPkeys, al pulsar esta opción aparecerá la siguiente pantalla

age and the second s	Validity	Tout	Size	Desception
🗄 🤫 PGP Security Engolater Centification	0	_	1024	Expired DH/DSS
🗄 🤫 PGP Security Software Release Key 2.	- Q	_	2048/1024	Expired DH/DSS
H PSP Security Software Robace Key 2.	- @		1024	Expired DH/DSS
🗄 🢑 Seguros Génesis	\$	22223	2048/1024	DH/DSS key pair

En esta pantalla aparecerá resaltada en *letras negritas* la llave de su institución o sociedad, la cual tiene que enviar a la CNSF para ser registrada.

Seleccionar la llave de la institución o sociedad y pulsar el botón derecho del mouse para que se despliegue un catálogo de opciones



Seleccionar la opción Export... y aparecerá la siguiente pantalla

			[7]
Guardar gra	Escitorio	· 8 0	
Mi PC			
jombre del archivo	Seguros Génesis.asc		Guardar
Nombre del archivo Guardar como (pox	Seguros Génesis asc ASCII Key File (*.asc)	Ы	<u>G</u> uardar Cancela
Sontre del archivo Guardar como (pox	Seguroz Génesis asc ASCII Key File (*.asc) ey(s)	3	<u>G</u> uardar Cancelar

En esta pantalla se deberá indicar en los campos Guardar en: y Mombre del archivo: el lugar en que se guardará el archivo y con qué nombre.

Es importante aclarar que el campo Guardar como tipo: e Include Private Key(s) no deben ser modificados, es decir se quedarán con los datos que aparecen por default en la pantalla.

Para cerrar esta aplicación pulse el botón

<u>G</u>uardar

Terminado el proceso deberá enviar a la dirección **admin_entrega@cnsf.gob.mx** de e-mail la llave pública de su institución o sociedad.

V. Importar la llave pública de la CNSF

El Administrador de la Comisión Nacional de Seguros y Fianzas enviará al correo electrónico indicado por la Institución o Sociedad la llave pública.

Al recibir el Administrador de la Institución o Sociedad la llave pública de la CNSF deberá importarla para poder realizar la encriptación de sus archivos.

Como primer paso copiar la llave que ha sido enviada por la CNSF en una carpeta de nuestra elección

😅 E-Motorcanhio 💷 💷 🖂
Anchevo Ediction Yos in Eavontos Awada
+ + • 🔤 🕺 🖻 🦄
Anter Anter Cotter Coper Pager
Energian Contestantias
Intercambio
(Chickst and
Child and
PGP Armored File
Modificado: 09/09/2002 12:01 PM
Татраба, 2 КВ
1.71 KB [*] MIPC

Sobre el archivo, dar click con el botón derecho del mouse y aparecerá un cuadro de diálogo en el cual elegiremos la opción PGP que a su vez mostrará otro cuadro de diálogo.

🔁 E:\Intercambio				- D ×
] <u>A</u> rchivo <u>E</u> dición ⊻er <u>I</u> r <u>F</u> avo	ritos Ay <u>u</u> da			
Atrás Adelante Arr	iba Cortar	Cop	iar Pegar	»
Dirección 🗀 E:\Intercambio				•
Intercar	nbio			
	Abrir			
CNSF.asc PGP Armored File	Vi <u>s</u> ta rapida ©Add to Zip			
Modificado:	المَعْقِظِ dd to Cnsf.zip			
09/09/2002 12:01 PM	E <u>n</u> viar a	۲		
Tamaño: 2 KB	P <u>G</u> P		Decrypt & Verify	
	C <u>o</u> rtar		<u>W</u> ipe	
	<u>C</u> opiar	_		
	Crear acceso <u>d</u> irecto			
	Cambjar nombre			
	P <u>r</u> opiedades			_//

Dar click en la opción Decrypt & Verify y aparecerá la siguiente pantalla

Select the key(s) you would like to import to your keyring: Keys Validity Trust Size Comision Nacional de Seguros y Fian 2048/1024 2048/1024 Comision Nacional de Seguros y Fian 2048/1024 Select All Unselect All Import Cancel 	💦 Sele	ct key(s)			?	×
Keys Validity Trust Size Comision Nacional de Seguros y Fian 2048/1024 2048/1024<	Select t	he key(s) you would like to import	to your keyring	g:		
	Keys		Vali	dity Trust	Size	Γ
✓ ▼ Select All Unselect All Import Cancel	÷ 💬	Comision Nacional de Seguros y	Fian 🥥		2048/1024	
✓ ✓ Select All Unselect All Import Cancel						
▲ ▲ Select All Unselect All Import Cancel						
Image: Select All Unselect All Import Cancel						
Image: Select All Unselect All Import Cancel						
Select All Unselect All Import Cancel						
Select All Unselect All Import Cancel						2
		Select All Uns	elect All	Import	Cancel	
				7.04.200	<u>_</u>	-
Import y la llava pública de la CNSE aparacerá deptre de PCKov	ar al batán <u>I</u> n	nport		paracará de	ontro do PCk	Cove

S PGPkeys				
<u>File E</u> dit <u>V</u> iew <u>K</u> eys <u>S</u> erver <u>G</u> roups <u>H</u> el;	D C			
🤏 X 🔏 🌒 🔍 🛫 😓 🖆 I				
Keys	Validity	Trust	Size	Description
🕀 🗁 Comision Nacional de Seguros y Fian			2048/1024	DH/DSS public ke
🔄 🕀 🔫 FGP Security Employee Certification			1024	Expired DH/DSS p
🔄 🗄 🛞 FGP Security Software Release Key 2			2048/1024	Expired DH/DSS p
🔄 🗄 🛞 FGP Security Software Release Key 2			1024	Expired DH/DSS p
🕀 👾 Seguros Génesis	٠	1777.	2048/1024	DH/DSS key pair
				<u> </u>

ΝΟΤΑ

- 🗄 🏆 Este icono aparecerá cuando se trate de una llave privada
- 🗄 👦 Este icono aparecerá cuando se trate de una llave pública

VI. Envío de llave privada de la Institución o Sociedad a otra PC de la misma Institución o Sociedad

Pueden ser diversas personas las que requieran encriptar en su propia máquina con la misma llave privada de la Institución o Sociedad. Para poder cumplir esa funcionalidad, se debe instalar el PGP en dichos equipos e importar la llave pública de la CNSF y la privada de la Institución o Sociedad. Para esto último, primero deberá exportar la llave privada de la Institución o Sociedad, para lo cual deberá seguir las siguientes instrucciones.

Como primer paso es necesario accesar la pantalla de BPGPkeys en la que ya aparece la llave privada.



En esta pantalla aparecerá resaltada en *letras negritas* la llave de su institución o sociedad, selecciónela y pulse el botón derecho del mouse para que se despliegue un catálogo de opciones



Seleccione la opción Export... y aparecerá la siguiente pantalla

xport Key to File			?×
Guardar <u>e</u> n:	Personal	· 🗈 💣	II
Mimúsica Mis imágenes My eBooks Pgp			
Nombre del archivo:	50001.asc		Guardar
Guardar como jipo:	ASCII Key File (".asc)	×	Cancelar
☐ Include Private Kr ✓ Include <u>6</u> 0 Exten	sions		

En esta pantalla se deberá indicar en los campos Guardar en: y Mombre del archivo: el lugar en que se guardará el archivo y con qué nombre.

Es importante aclarar que el campo Guardar como tipo: no debe ser modificado, es decir se quedará con los datos que aparecen por default en la pantalla.

Y ACTIVAR el campo 🗳	[Include <u>P</u> rivate Key(s]	como se muestra en l	la siguiente pantalla
----------------------	---------------------------------	----------------------	-----------------------

Export Key to File				[? ×
Guardar <u>e</u> n:	🔁 Personal	•	e 💣		
☐ Mimúsica ☐ Mis imágenes ☐ My eBooks ☐ Pgp					
<u>N</u> ombre del archivo	: \$0001.asc			<u>G</u> uardar]
Guardar como <u>t</u> ipo:	ASCII Key File (*.asc)		•	Cancelar	1
I✓ Include <u>P</u> rivate I I✓ Include <u>6</u> .0 Exte	Key(s) nsions				_

ya que precisamente, esta alternativa marca la diferencia para que se exporte como llave privada o pública

<u>G</u>uardar

Para cerrar esta aplicación pulse el botón

El archivo que se generó, deberá copiarse en la computadora a la que deseamos importar la llave privada de la Institución o Sociedad.

Una vez que se haya instalado PGP sin haber creado ninguna llave privada, deberá seleccionar desde el explorador de Windows el archivo (dar doble click) en el que exportó la llave privada y aparecerá la siguiente pantalla



Para confirmar como llave privada la que acabamos de importar, deberá ingresar nuevamente a la pantalla de **PGPkeys** dar click con el botón derecho del mouse sobre la llave de nuestra compañía y aparecerá la siguiente pantalla



Pulse la opción Key Properties y aparecerá la siguiente pantalla

General Sublu	eys		
10	DATE: STORE		
Tupe	DH/DSS		
Size	2048/1024		
Created	07/01/2003		
Excises	Never		
Coher	CAST	-	
-+	E. Fachlad		
	Evapled	Change	Eassphrase
Eingesprint			
chatter	hydraulic	shamrock	glossary
dvielling	distortion	skydive	hazardous
seabild	dinosaur	jawbone chipel	pedigree
			Hegadecimal
Trust Model			
Invalid .	Valid	Untrusted	Trusted
🗌 🗌 Implicit 1	rust	-	-
		Ce	nar Ay

En esta pantalla seleccionaremos la opción 🗖 Implicit Trust

General Subkr	94		171
jD: Lype: Size: Dreated Expire: Cipber:	0xEF25307C DH/DSS 2048/1024 07/01/2003 Never CAST F2_End/ed	Change	Passphrase
Eingesprint chatter stohet dwelling seabird uncut	hydraulic Waterloo distortion dinosaur conformist	shamrock. soybean skydive jawbone chizel	glossary uniavel hazardous pedigree informant Hexadecimal
Trust Model Invalid	Valid	Detroited -	Trusted
		Cer	nar Ayuda

Para terminar pulse el botón y aparecerá la siguiente pantalla

Fig PGPkeys File Edit View Keys Server Scourse Hele				-O×
	, 			
<u>_~</u>				
Keys	Validity	Trust	Size	Description
🕀 🕞 FGP Security Employee Certification			1024	Expired DH/DSS p
🔄 🕀 📆 FGP Security Software Release Key 2			2048/1024	Expired DH/DSS p
🔄 🕀 📆 FGP Security Software Release Key 2			1024	Expired DH/DSS p
😑 🧙 S0001	9	87777	2048/1024	DH/DSS key pair
📥 🚾 S0001	0			User ID
S0001				DSS exportable sig
1 key(s) selected				

NOTA:

Validity
•

Esta columna aparecerá con círculos grises antes de reconocer la llave privada



Esta columna aparecerá con círculos grises y verdes después de reconocer la llave privada

VII. Encriptación de archivos

Para encriptar sus archivos y poder realizar el Envío de Entrega de Información Vía Electrónica por Internet a la CNSF, primero debe realizar la generación de el (los) archivo(s) (SIIF, VAR, OPERACIONES RELEVANTES, ETC.) y copiarlos en una carpeta que pueda localizar con facilidad.



Seleccione uno a uno los archivos dando click con el botón derecho del mouse donde aparecerá un cuadro de diálogo en el cual seleccionaremos la opción PGP apareciendo un segundo cuadro de diálogo en el que seleccionará, la opción Encrypt & Sign como se muestra a continuación



Aparecerá la siguiente pantalla

式 PGPshell - Key Selection Dialog			?×
Drag users from this list to the Recipients list	Validity	Size	
📧 Comision Nacional de Seguros y Fianzas		2048/1024]
Desisionts	A ZEREDA.	Cier	
Hecipients	validity	2048/1024	
	**	2040/1024	
	1		
E Iext Output			eip
🔲 🔟 ipe Original			
Conventional Encryption			

De la sección Drag users from this list to the Recipients list donde aparece la llave de la Comisión, seleccionarla con el botón derecho del mouse y arrastrarla hasta la sección Recipients

🕵 PGPshell - Key Selection Dialog					? ×
Drag users from this list to the Recipients list	V	/alidity	Siz	e	
Recipients		/alidity	Siz	e	
Comision Nacional de Seguros y Fianzas Seguros Génesis		 	2048/102	24 24	
		-	. 1		
🗖 Iext Output	<u>0</u> K	<u>C</u> ar	ncel	<u>H</u> el	p
Wipe Original Conventional Encruption					
el botón <u>QK</u> y aparecerá el siguiente me	iensaje				
PGPshell - Enter Passphrase			3	2 X X	
Signing key : Seguros Génesis (DSS/1024)				•	
The currently selected key has no passphrase.					
	<u>0</u> K		<u>C</u> ancel		
04					

Pulsar el botón y aparecerá nuestro archivo encriptado y firmado con la llave privada de la Institución o Sociedad.

	-	Leur							
E: VArch	IVOS .2	21012111							
Archivo	<u>E</u> dició	in <u>V</u> er	<u>Ir E</u> a	avoritos	Ay <u>u</u> da				
-	-	\rightarrow	~	t	L X	L.	1	a	>>
Atrás		Adelante		Arriba	Corta	ır Cop	iar	Pegar	
<u>Dirección</u>	🚞 E:\	Archivos .z	ip\SIIF						-
C1004 WinZip Modific 07/03/3 Tamañ	83101 File ado: 2002 4 o: 2 KI	Siif 025.zip :47 PM 3	വ പ്രാം എന്ന എന്ന എന്ന പ്രാം പ് പ്രാം പ്രാം പ്രാം പ്രാം പ്രാം പ്രാം പ്രാം പ്രാം പ്രാം പ്രാം പ്രാം പ്രാം പ്രാം പ്രാം പ്രാം പ്രാം പ്രാം പ്രാം പ്രാം പ് പ് പ് പ പ് പ് പ പ് പ പ് പ പ പ് പ	0048310 0483101 0048310 0048310 0048310 0048310	102S.zip 102S.zip 102S.zip 102S.zip 102S.zip.pg;				
1 objetos sel	ecciona	idos			1.56 KB	🛄 Mi PC			

La etiqueta del archivo encriptado debe ser el nombre del archivo original y el programa de encriptación agregará la extensión PGP Ejemplo:

Deberá seguir los pasos anteriormente descritos para cada uno de los archivos que desee encriptar, o bien, seleccionar un bloque y encriptarlos siguiendo los mismos pasos antes descritos.

Después de encriptar y firmar electrónicamente los archivos, deberá enviarlos a la CNSF a través de la página WEB, para esto refiérase al **Manual del Usuario para la Entrega de Información Vía Electrónica**.