1. OBJETIVO

Proteger la confidencialidad, autenticidad o integridad de la información de IGS a través de medios criptográficos

2. ALCANCE

Este procedimiento aplica desde la solicitud de uso de llaves criptográficas hasta la eliminación de la misma por diferentes motivos.

3. REPONSABLE

- La solicitud de acceso o actualización al sistema o claves de cifrado se debe efectuar de manera formal al departamento de seguridad informática. Aquellas personas autorizadas deberán velar por la conservación de la disponibilidad, integridad y confidencialidad de las claves criptográficas, así como de la información a la cual se le haya aplicado algún proceso de cifrado.
- De igual modo, la información cifrada o descifrada deberá ser tratada conforme a su nivel de clasificación y su eliminación deberá realizarse a través de borrado seguro.
- Los responsables del sistema de cifrado y de las claves criptográficas serán los encargados de establecer los controles para asegurar el sistema y las claves, así como gestionar el acceso sólo a los funcionarios, contratistas y terceros autorizados.

- Las actividades relacionadas con la administración y eliminación de las claves criptográficas deberán ser registradas por la persona encargada. Las claves serán deshabilitadas cuando estas tengan riesgo de divulgación o cuando los funcionarios, contratistas y terceros autorizados culminen la relación laboral o contractual con la Entidad

- Los funcionarios, contratistas y terceros tendrán la responsabilidad de reportar, mediante las fallas reales o potenciales y los posibles riesgos del sistema de cifrado o firma digital de datos.

4. DEFINICIONES

El departamento de Seguridad Informática, es la encargada de definir los mecanismos de cifrado de información más apropiados frente a las necesidades de la organización. Con base en el análisis de riesgos y considerando los criterios de confidencialidad, integridad, autenticidad y no repudio en las comunicaciones o en el tratamiento de la información, se adoptan los controles de cifrado y firma digital de datos que reduzcan los riesgos de seguridad de la información. El uso de herramientas de cifrado será autorizado conforme a los roles o responsabilidades de los funcionarios y contratistas de la organización.

Para establecer el sistema de cifrado, se tienen en cuenta la normatividad vigente frente a la protección de los datos, estándares aplicables y la tecnología existente. Los diferentes departamentos de IGS, son las encargadas de realizar la respectiva adquisición, creación, activación, distribución de dispositivos de control criptográfico para sus respectivas dependencias. Las diferentes dependencias deben adoptar las medidas de seguridad recomendadas por el departamento de Seguridad Informática

5. DESARROLLO

Generar Claves

Para poder cifrar asimétricamente primero tenemos que crear la pareja de claves (pública y privada) con el comando gpg --gen-key.

```
usuario@

gpg (GnuPG) 1.4.11; Copyright (C) 2010 Free Software Foundation, Inc.

This is free software: you are free to change and redistribute it.

There is NO WARRANTY, to the extent permitted by law.

Por favor seleccione tipo de clave deseado:

   (1) RSA y RSA (predeterminado)

   (2) DSA y Elgamal

   (3) DSA (sólo firmar)

   (4) RSA (sólo firmar)

¿Su selección?:
```

GPG nos permite elegir el tipo de clave que queremos usar, hay opciones que solo permiten firmar y otras que permiten firmar y cifrar, en este caso usaremos DSA y Elgamal.

```
las claves DSA pueden tener entre 1024 y 3072 bits de longitud.

¿De qué tamaño quiere la clave?
```

Nos piden el tamaño de la clave que puede variar entre 1024 bits y 3072, esto es de libre elección, yo tomaré el término medio que es el que propone por defecto (2048).

A partir de aquí todo es más trivial, nos pide la fecha en la que expirará la clave, la información del emisor de la clave (nombre, mail y algunos datos extra que queramos dar) y por último nos pedirá la contraseña que salvaguarda la clave privada.

Tras generar las claves podemos verlas con el comando gpg -k que nos muestra nuestro anillo de claves, lo importante de este paso es que veremos la identificación de cada una, que es necesaria para poderlas exportar y enviar.

```
usuario@IGS:~/gpg$ gpg -k

/home/.gnupg/pubring.gpg

------------------------------

pub   2048D/1838464

uid                  Usuario IGS <info@igs.com>

sub   2048g/
```

Exportar y enviar la clave privada

El objetivo de esta pareja de claves es **que cualquiera nos pueda mandar un archivo cifrado** que solo veremos nosotros y esto se hace difundiendo la clave pública que acabamos de crear (la pública, **nunca** la privada), para exportarla en un archivo usaremos el comando gpg -output [archivo destino] --export [ID de a clave pública] (la clave pública generada antes tiene la ID).

```
usuario@:~/gpg$ gpg --output CPub.gpg --export

usuario@I:~/gpg$ ls

CPub.gpg
```

Este archivo ahora se puede difundir por el medio que queramos, tenemos que tener en cuenta que el único problema de seguridad que habría en difundir la clave es que alguien se hiciese pasar por otro al mandarnos un mensaje, algo que pasaría igual si no estuviese cifrado, por eso el que nos envíe algo lo debería de firmar (si fuese pertinente).

Podéis descargar esta clave pública, que ahora veremos como importar y sirve para mandarme un archivo cifrado o para comprobar que un archivo.

```
usuario@:~/gpg$ gpg --send-keys pgp.mit.edu

gpg: enviando
```

A partir de este momento la clave estará accesible desde este servidor específico.

Importar la clave desde el archivo o servidor de claves

Para poder usar la clave pública para cifrar o comprobar la identidad del remitente tenemos que importar previamente la clave, desde un archivo debemos de usar el comando gpg --import [Archivo de la clave pública] (el que hemos descargado anteriormente).

Descrifrar un archivo con clave privada.

Y ahora es el momento de descifrar con nuestra clave privada el documento tras recibirlo, con el comando gpg -d [Archivo] e introduciendo la contraseña que creamos para salvaguardar la clave privada.

```
usuario@I:~/gpg$ gpg -d documento.txt.gpg

Neinfo@igs.com>»

Igs Dev
```

Y el resultado nos lo muestra a continuación (Igs Dev), aunque si queremos especificar la salida debemos de usar el parámetro -o [Archivo de salida].

Firmar archivos

```
usuario@IGSSERVER1:~/gpg$ echo "Igs Dev" > firmar.txt
```

Y ahora para asegurarse la confidencialidad del documento (ahora que esta firmado por nosotros) deberíamos de cifrarlo con la clave pública del destinatario.

Verificar y descifrar un archivo firmado

Cualquiera con la clave pública asociada a la que ha firmado el documento puede leerlo, de la misma forma que desciframos un archivo (gpg -d [Archivo]) o verificándolo únicamente con el comando gpg --verify

6 ANEXOS

Sin anexos

7 CONTROL DE CAMBIOS

Revisión	Ítem Modificado	Objeto de la Modificación
Rev. 00	Creación del Documento	
Rev. 01	Pie de pagina con “uso de la compañía”	Etiquetado del documento de acuerdo a la clasificación en nivel de acceso de la información.

Brian Cortes	**Brian Cortes**	**Russell Aparicio**
Elaboró/Controló	**Revisó**	**Aprobó**