PROYECTO DE GRADO

PGP

EDGAR ORLANDO BORRERO VILLAMIL

JAIME ANDRES REYES AVILA

Curso Preparatorio de Grado presentado a

Al programa de Electrónica Y Telecomunicaciones

Como requisito parcial para optar al titulo de

TECNÓLOGO EN ELECTRÓNICA Y TELECOMUNICACIONES

Ing. Duilio A. Buelvas P.

ASESOR

CORPORACIÓN UNIVERSITARIA UNITEC

FACULTAD DE ELECTRÓNICA Y TELECOMUNICACIONES

BOGOTÁ, D.C.

26 de julio de 2007

TABLA DE CONTENIDO

PLANTEAMIENTO DEL PROBLEMA

JUSTIFICACIÓN

INTRODUCCIÓN

OBJETIVOS

**I. PREÁMBULO ( INTRODUCCIÓN A LA SEGURIDAD EN MEDIOS DE COMUNICACIÓN )**

1. ¿Qué es seguridad?
1.1. ¿Qué queremos proteger?
1.2. ¿De qué nos queremos proteger?
1.3. ¿Cómo nos podemos proteger?
1.4. Vulnerabilidad

**II. NATURALEZA DEL PROYECTO**

2. PGP ( Pretty Good Privacy)
2.1. Introducción
2.2. Servicios
2.3. Enviando y recibiendo mensajes PGP
2.4. Ejemplo de uso de PGP en la práctica

**III. ESTUDIO DE LOS SISTEMAS CRIPTOGRÁFICOS**

3. Introducción
3.1. Cifrado simétrico (o de clave secreta SKC)
3.2. Aplicaciones
3.3. Algoritmos
3.4. Cifrado asimétrico (o de clave pública PKC)
3.5. Algoritmos
3.6. Comparación entre los sistemas criptográficos

**IV. NIVEL DE APLICACIÓN**

4. Aplicación de correo electrónico seguro: PGP
4.1. Segmentación y reensamblado
4.2. Envió y recepción de correo electrónico privado

CONCLUSIONES

GLOSARIO

ANEXO

BIBLIOGRAFIA

# PLANTEAMIENTO DEL PROBLEMA

No hay nada más fácil que leer los correos de otras personas, ya que viajan desnudos por la red. Un correo electrónico normal es como una tarjeta postal sin sobre, que puede ser leida por personas mal intencionadas como son: empleados, ex-empleados, curiosos, piratas, terroristas, intrusos etc. Causando daños personales como suplantación, modificación y duplicación; no olvidemos que el activo mas importante de una empresa es su información Por consiguiente, la mejor manera de preservar la intimidad en los mensajes de correo electrónico es recurrir a la criptografía. Por medio de potentes técnicas criptográficas, el contenido del mensaje puede ser enviado cifrado, permitiendo asi que sólo el verdadero destinatario del correo sea capaz de leerlo. Lo mejor es instalar un programa de cifrado de correo. Indiscutiblemente, la mejor opción es PGP. Con este mecanismo se garantiza la confidencialidad del correo. La integridad, que garantiza que el contenido del mensaje no ha sido alterado por el camino; la autenticación, que asegura la identidad del remitente del correo, de manera que podemos estar seguros de que fue escrito por quien lo envió y no ha sido falsificado.

# JUSTIFICACIÓN

La causa que nos llevo a realizar este proyecto fue la de implementar una técnica basada en la seguridad de la información; debido a que hoy en dia hay programas capaces de capturar información con el único fin de perjudicar la integridad de la información.

Es por eso que la finalidad de nuestro proyecto es la brindarle al lector un amplio informe de cómo puede de alguna forma blindar el contenido de un mensaje electrónico.

# INTRODUCCIÓN

PGP es un programa que nos ayuda a proteger nuestros datos, especialmente orientado a incrementar la seguridad de nuestros mensajes electrónicos. PGP es gratuito y podrás generar tus propias llaves sin depender de ninguna empresa o agencia.

Cada usuario tiene dos claves personales "su pareja de llaves" que podrán emplearse con el PGP para encriptar información. Cualquier documento puede ser encriptado utilizando una de las llaves, y ese documento quedará cifrado en forma totalmente incomprensible. El cifrado resultante de emplear una u otra llave es distinto, y por eso estos métodos criptográficos son conocidos como sistemas (de clave doble asimétrica). Solo hay una forma de descifrar el documento y eso se hace utilizando necesariamente la otra llave de la misma persona.

Con PGP no se necesitan canales seguro para intercambiar las llaves entre los usuarios, lo cual hace más fácil su utilización; esto es porque PGP esta basado en una tecnologia llamada criptografía de llave pública.

## OBJETIVOS

- Garantizar la integridad de la información
- Entender los principios básicos de seguridad
- Analizar sus ventajas y desventajas respecto a los diferentes cifrados
- Realizar prácticas o procedimientos para los usuarios con el fin de mostrarles las ventajas que se tienen al aplicarlo

# I. PREÁMBULO (INTRODUCCIÓN A LA SEGURIDAD EN MEDIOS DE COMUNICACIÓN)

## 1. ¿QUÉ ES SEGURIDAD?

- La seguridad absoluta es indemostrable. Se habla de fiabilidad.
- Mantener un sistema seguro consiste en garantizar (CIA: Confidentiality, Integrity, Availability):
  - Confidencialidad: Sólo pueden acceder a los recursos de un sistema los agentes autorizados.
  - Integridad: Los recursos del sistema sólo pueden ser modificados por los agentes autorizados.
  - Disponibilidad: Los recursos del sistema tienen que estar a disposición de los agentes autorizados (contrario: denegación de servicio).

Para determinar si un agente está o no está autorizado para llevar a cabo determinadas tareas dentro del sistema, se necesitan, además otros servicios de seguridad:

- Autenticación: Identificación de los agentes y demostración de que un agente es "quien dice ser".
- Control de acceso: Especifica qué acciones pueden llevar a cabo los agentes del sistema.
- No repudio: El emisor de un mensaje no puede negar que lo ha enviado, y el receptor de un mensaje no puede negar que lo ha recibido.
- Auditoria: Registrar y analizar las acciones desarrolladas por los distintos agentes del sistema.

### 1.1. ¿QUÉ QUEREMOS PROTEGER?

LOS RECURSOS DEL SISTEMA

- Hardware
- Software
- Datos

TIPOS DE ATAQUE A LOS RECURSOS:

- Interrupción: el recurso queda inutilizable o no disponible
- Interceptación: captura de un recurso o acceso al mismo
- Modificación o destrucción: Interceptación y manipulación del recurso
- Fabricación: generación de recursos similares a los atacados

## 1.2. ¿DE QUÉ NOS QUEREMOS PROTEGER?

De todos aquellos agentes que puedan atacar a nuestros recursos

• Personas: empleados, ex-empleados, curiosos, piratas, terroristas, intrusos.
• Amenazas lógicas: software defectuoso, herramientas de seguridad, puertas traseras, bombas lógicas, canales ocultos, virus, gusanos, caballos de Troya.
• Catástrofes naturales.

## 1.3. ¿CÓMO NOS PODEMOS PROTEGER?

• Análisis de amenazas.
• Evaluación de (posibles) pérdidas y su probabilidad.
• Definición de una política de seguridad.
• Implementación de la política: mecanismos de seguridad
  – De prevención: durante el funcionamiento normal del sistema
  – De detección: mientras se produce un intento de ataque
  – De recuperación: tras un ataque, para retornar a un funcionamiento correcto: análisis forense

## 1.4. VULNERABILIDAD

• La vulnerabilidad de una organización depende de:

  – El grado de publicidad de la organización
  – El coste de los ataques
  – La exposición de la organización a los ataques externos
  – La exposición de la organización ante ataques internos, o ante la facilitación de servicios (involuntaria o consciente) desde el interior

En definitiva, depende de la:

• Motivación: ¿Qué ventaja o provecho se puede sacar por obtener o destruir información?
• Confianza: ¿En qué medida se puede contar con los usuarios?

II. NATURALEZA DEL PROYECTO
2. PGP (Pretty Good Privacy)

PGP (Pretty Good Privacy ó Encriptación bastante buena) es un sistema de encriptación por llave pública escrito por Philip Zimmermann, y sirve para que nadie salvo uno mismo y el destinatario o destinatarios a los que vaya dirigido el mensaje puedan leerlo al ir los mensajes codificados, también puede usarse para comprobar la autenticidad del mensaje asegurándonos que lo ha escrito el remitente en realidad, realmente es muy bueno y es prácticamente indescifrable, esto mismo le ha llevado al autor del mismo Philip Zimmermann a tener bastantes quebraderos de cabeza con la ley en Estados Unidos, afortunadamente su caso ya se ha cerrado.

**2.1. Introducción**

PGP ha sido y es un hito a tener en cuenta dentro de Internet, desde su introducción en 1991, debido a su imparable crecimiento, debido a:

1. El paquete PGP es de dominio público (existe una versión comercial distribuida por Pretty Good Privacy, Inc.).
2. PGP es asequible para una gran variedad de plataformas (DOS/Windows, UNIX, Mac, VMS) e independiente del S.O (SISTEMA OPERATIVO).
3. Esta basado en algoritmos extremadamente seguros como: RSA para cifrado de claves de sesión, IDEA para el cifrado del mensaje y MD5 para la generación de firmas digitales.
4. El paquete incluye código fuente y documentación.
5. No ha sido desarrollado ni es controlado por ninguna organización gubernamental.

**2.2. Servicios**

PGP ofrece tres tipos de servicio:

1. **Confidencialidad:** Permite a un usuario, mediante cifrado, garantizar que solamente el destinatario podrá leer el mensaje.
2. **Autentificación**: Permite a un usuario firmar un documento antes de enviarlo, lo cual permite:
    - Tener certeza de que el documento no ha sido modificado puesto que ha sido firmado. Si se alterara el mensaje la firma no seria válida.
    - Verifica que el mensaje ha sido firmado por una determinada persona.
3. **Integridad**: La firma antes mencionada tiene la particularidad de que depende no sólo de la identidad del remitente sino también del contenido del mensaje, por lo que si este es alterado, la firma ya no es válida.

### 2.3. Enviando y recibiendo mensajes PGP.

El envio de mensajes consiste básicamente de 4 pasos:

1. **Firma digital.**

   Este primer paso es opcional. Partiendo de un texto normal lo primero que hace PGP es la creación de una "firma digital", la cual garantiza tanto la integridad del mensaje como la autenticidad de su origen, como se ha explicado.

2. **Compresión.**

   Este paso es automáticamente ejecutado por PGP a no ser que el usuario no desee hacerlo. Se obtiene una reducción notable del tamaño del mensaje, sobre todo si es texto. PGP usa ZIP para la compresión. Por defecto, sólo las partes cifradas son comprimidas.

3. **Cifrado del mensaje.**

   Este paso también es opcional. PGP utiliza el algoritmo IDEA para cifrar, combinado con RSA. Se genera una clave de sesión. Mediante el algoritmo IDEA y esta clave de sesión, se cifra el mensaje. La clave se cifra a su vez mediante el algoritmo RSA y la clave pública del receptor. El motivo de no usar RSA para todo el mensaje es que no sería eficiente, especialmente si tiene varios receptores (habría que incluir un mensaje cifrado completo por receptor, mientras que con el sistema elegido sólo hay que incluir un cifrado de la clave de sesión por receptor).

4. **Codificación.**

   Firma, compresión y cifrado no generan un fichero de texto sino binarios. Como la aplicación principal de PGP es el correo, que requiere caracteres ASCII, PGP puede codificar el documento resultante mediante el algoritmo BASE64 automáticamente.

Para la **recepción** de mensajes PGP simplemente se invierten todos los pasos del proceso de envio:

1. Paso de ASCII a binario, si el mensaje fue codificado.
2. Si el mensaje está cifrado PGP recupera la clave de sesión, la cual fue cifrada usando RSA con la clave pública del receptor. Por lo tanto el receptor usará su clave privada para obtener la clave de sesión. Con la clave de sesión PGP descifra el mensaje usando el algoritmo de descifrado IDEA.
3. Descompresión del mensaje, si estaba comprimido.

4. Si el mensaje fue firmado PGP verifica la firma, la cual fue cifrada con la clave privada del emisor del mensaje por lo que PGP usara la clave pública de este usuario. Se extrae el "hash" del mensaje y PGP lo compara con el que ha calculado; si los dos encajan la firma es verificada.

**2.4. Ejemplo de uso de PGP en la práctica.**

PGP mantiene para cada usuario dos ficheros, pubring.pgp (con todas las claves públicas que este usuario conoce) y secring.pgp (con su clave privada). El procedimiento para la generación de las claves se ejecuta una vez por usuario.

Los siguientes ejemplos asumen un entorno UNIX. Las versiones disponibles para Windows o Macintosh incluyen interfaces de usuario para realizar las mismas funciones.

- ***Generación de claves.***

  Ejecutar "pgp -kg". Se nos pedirá una identificación (normalmente es nombre mas dirección de email), y un password. Generara un par de claves, asociadas a esa identificación y protegidas con el password.

- ***Recepción de un mensaje.***

  Ejecutar "pgp fichero". Automáticamente se ejecutaran los siguientes pasos:

  - Si contiene claves públicas son incluidas en pubring.pgp.
  - Si contiene firmas digitales son comprobadas, indicando si son válidas o no, y de quién son (siempre que conozca sus claves públicas correspondientes).
  - Si contiene algún texto cifrado lo descifra (siempre que conozca sus claves públicas correspondientes).

- ***Emisión de un mensaje.***

  Ejecutar alguna de las tres opciones siguientes (se necesita el password utilizado durante la generación de las claves)

  - Cifrado: **"pgp -e fichero"**
  - Firmado: **"pgp -s fichero"**
  - Ambas cosas: **"pgp -es fichero"**

Si se requiere cifrado se nos preguntará el destinatario, y se requerirá tener ya su clave pública.

## III. ESTUDIO DE LOS SISTEMAS CRIPTOGRAFICOS

### 3. Introducción

Un mensaje puede cifrarse mediante la aplicación de una regla que transforme el texto en claro del mensaje a un texto cifrado. Para esto el receptor debe conocer la regla inversa para transformar el texto cifrado en el texto original.

La mayoría de los sistemas criptográficos se basan en dos técnicas:

- Sustitución
- Transposición

**Cifrado por Sustitución**

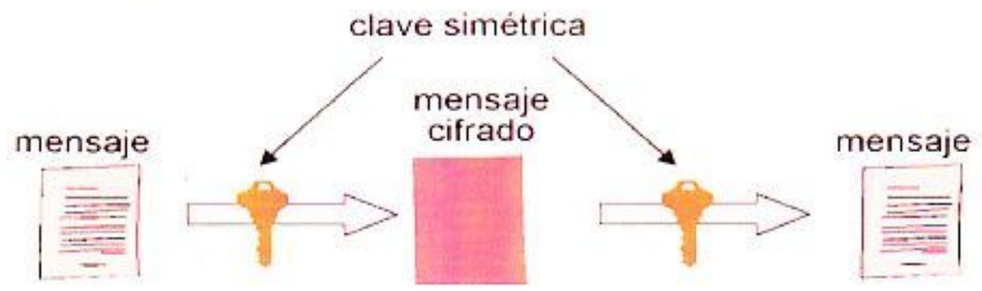
El cifrado por sustitución esta basado en el principio de reemplazar cada letra del mensaje original por otra.

**Cifrado por Transposición**

Se basa en cambiar el orden de los caracteres en el mensaje.

### 3.1. CIFRADO SIMÉTRICO (O DE CLAVE SECRETA SKC)

Un sistema de cifrado simétrico es un tipo de cifrado que usa una misma clave para cifrar y para descifrar. Las dos partes que se comunican mediante el cifrado simétrico deben de estar de acuerdo en la clave a usar de antemano. Una vez de acuerdo, el remitente cifra un mensaje usando la clave, lo envía al destinatario, y éste lo descifra usando la misma clave.



3.2. APLICACIONES

- Transmisión segura en canales no seguros
- Almacenamiento seguro en medios no seguros
- Autenticación

3.3. ALGORITMOS

- DES: DATA ENCRYPTION STANDARD
  Claves de 64 (56) bits para cifrar bloques de 64 bits

- IDEA: INTERNATIONAL DATA ENCRYPTION ALGORITHM
  Claves de 128 bits para cifrar bloques de 64 bits

- AES: ADVANCED ENCRYPTION STANDARD
  Claves de tamaño variable (128...256) y bloques de tamaño variable (128...256).

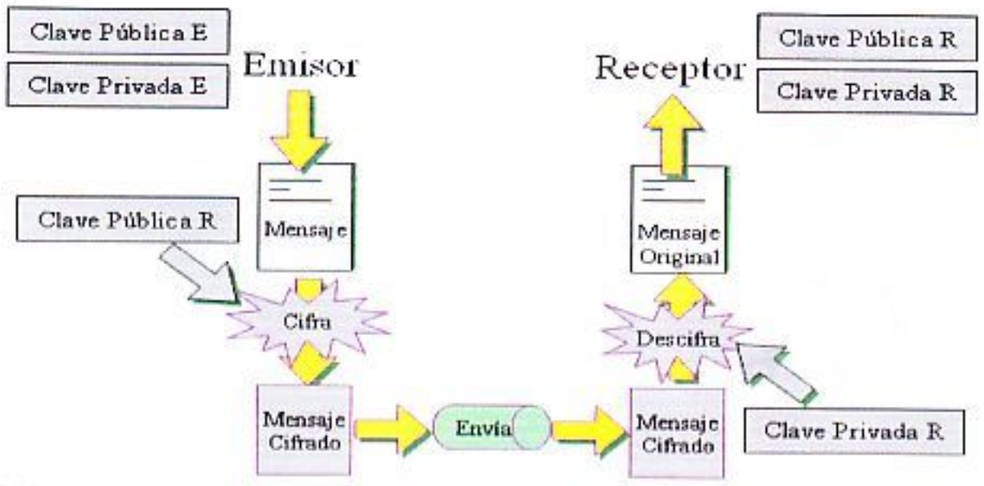
3.4. CIFRADO ASIMÉTRICO (O DE CLAVE PÚBLICA PKC)

Los sistemas de cifrado de clave pública surgieron debido al problema del intercambio de claves. Un sistema de cifrado de clave pública usa dos claves para el envio de mensajes; las dos claves pertenecen a la misma persona a la que se ha enviado el mensaje. Una clave es pública y se puede entregar a cualquier persona. La otra clave es privada y el propietario debe guardarla para que nadie tenga acceso a ella. El remitente usa la clave pública del destinatario para cifrar el mensaje, y una vez cifrado, solo la clave privada del destinatario podrá descifrar este mensaje.
Los sistemas de clave pública se basan principalmente en que todos conocen las claves públicas de los entes con los cuales se van a comunicar. Estas llaves pueden ser obtenidas de un directorio público o del ente con el cual se va ha establecer la comunicación.

El cifrado asimétrico o de clave pública hace uso de:

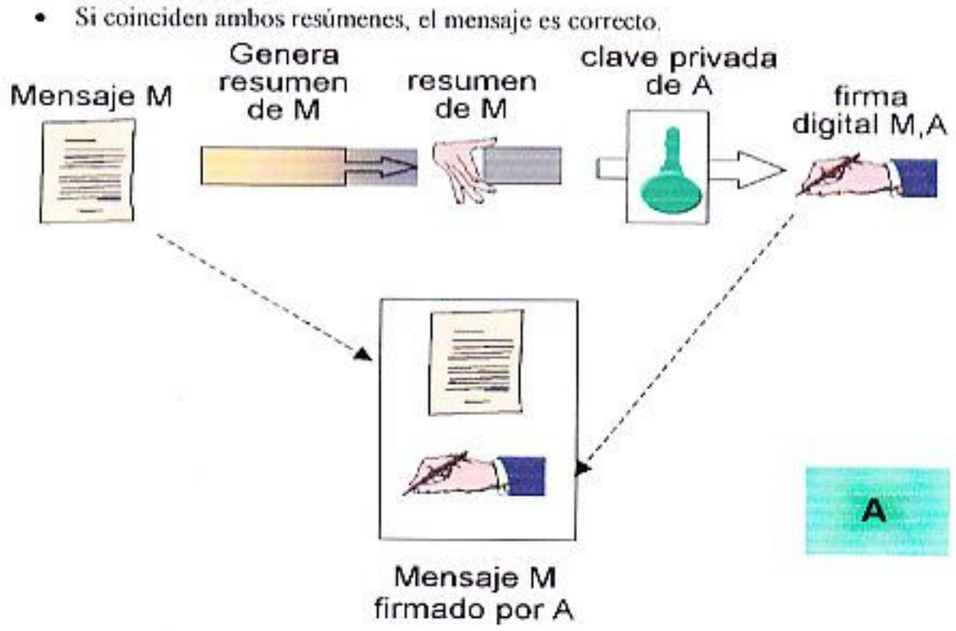
1. CIFRAR

- El emisor usa la clave pública del receptor para cifrar el documento.
- El receptor usa su clave secreta para descifrar el documento.




2. FIRMAR

- Se genera un resumen del mensaje.
- El resumen es cifrado con la clave privada del emisor.
- El resumen se adjunta con el mensaje en texto en claro.
- El receptor hace el resumen del mensaje recibido y descifra el mensaje con la clave pública del emisor.
- Si coinciden ambos resúmenes, el mensaje es correcto.



## 3.5. ALGORITMOS

- RSA (Rivest, Shamir and Adleman)
  Claves de tamaño variable. La más común es 1024 bits
  Bloques de tamaño variable, menos que el tamaño de la clave

- DIFFIE-HELLMAN
  No soporta cifrado ni firmas digitales. Se utiliza para acordar claves de sesión (generar un secreto compartido).
  Basado en el cálculo de logaritmos discretos.

## 3.6. COMPARACIÓN ENTRE LOS SISTEMAS CRIPTOGRAFICOS

| CIFRADO SIMÈTRICO | CIFRADO ASIMÈTRICO |
|---|---|
| VENTAJAS<br><br>• Seguro si la clave es escogida de forma aleatoria y es suficientemente grande.<br>• Simple de implementar y computacionalmente eficiente.<br><br>DESVENTAJAS<br><br>• La necesidad de utilizar nuevas claves para cada mensaje.<br>• No sirve para firmar<br>• Tiene graves problemas con la distribución de las claves.<br><br>PROBLEMAS DEL CIFRADO SIMÉTRICO<br><br>• Hay que mantener las claves en secreto<br><br>• Punto débil → Intercambio de claves | VENTAJAS<br><br>• La mayor ventaja de la criptografía asimétrica es que se puede cifrar con una clave y descifrar con la otra.<br><br>DESVENTAJAS<br><br>• Para una misma longitud de clave y mensaje se necesita mayor tiempo de proceso.<br>• Las claves deben ser de mayor tamaño que las simétricas.<br>• El mensaje cifrado ocupa más espacio que el original.<br><br>PROBLEMAS DEL CIFRADO ASIMÉTRICO<br><br>• Algoritmo computacionalmente costoso. Son muchos más lentos que los algoritmos simétricos.<br>• No tenemos garantías de que la clave pública sea de quien dice ser.<br>Solución → Un 3º certifica la clave pública.<br>• Las claves tienen que ser de mayor tamaño.<br>• El mensaje cifrado ocupa más espacio que el mensaje original.<br>Solución → Los usamos solo cuando es Necesario.<br>Ej. Intercambio de claves simétricas. |

## IV. NIVEL DE APLICACIÓN
## 4. APLICACIÓN DE CORREO ELECTRÓNICO SEGURO: PGP

PGP proporciona un servicio de confidencialidad y de autentificación que se puede usar para correo electrónico y aplicaciones de almacenamiento de ficheros.

### 4.1. SEGMENTACIÓN Y REENSAMBLADO

- Las herramientas de correo electrónico se limitan con frecuencia a una longitud máxima.
- Cualquier mensaje mayor debe subdividirse en segmentos.
- PGP subdivide automáticamente los mensajes demasiado largos.
- En el extremo receptor PGP retira todas las cabeceras del correo electrónico y reensambla el bloque.

### 4.2. ENVIO Y RECEPCIÓN DE CORREO ELECTRÓNICO PRIVADO

Cifrado y firma de mensajes de correo electrónico

La manera más rápida y fácil de cifrar y firmar mensajes de correo electrónico es con una Aplicación soportada por los complementos PGP [plug-ins]. Aunque el procedimiento varía ligeramente entre las diferentes aplicaciones de correo electrónico, usted realiza los procesos de cifrado y firma haciendo clic sobre los botones apropiados en la barra de herramientas de la aplicación. Además, si está usando una aplicación que soporta o que no requiere la norma PGP/MIME, puede cifrar y firmar sus mensajes de correo electrónico así como archivos adjuntos cuando envía o recibe su correo electrónico.
Si usted está usando una aplicación de correo electrónico que no es soportada por los complementos PGP, puede cifrar y firmar sus mensajes de correo electrónico por medio del portapapeles de Windows seleccionando la opción apropiada luego de hacer clic sobre el icono del candado y la llave ubicado en la barra de tareas del sistema. Para incluir archivos adjuntos, previamente debe cifrarlos desde el Explorador de Windows.

# CONCLUSIONES

- El sistema PGP nos colabora en la protección de la información, ya que se considera en las empresas un 80% de importancia.
- El sistema PGP nos ha garantizado la confidencialidad del mensaje y que podemos confiar en plena seguridad de nuestra información.
- El sistema PGP nos proporciona una propia identidad sin que se pueda adulterar la información tanto del emisor como del receptor.
- El sistema PGP ha demostrado que es una herramienta eficaz y accesible para aquellos usuarios que conocen y han manejado PGP.
- El sistema PGP obtiene diversos tipos de encriptamiento para tener mayor nivel de seguridad.
- El sistema PGP mejora la publicación de los documentos más confidenciales sin que se pierda su integridad.
- El sistema PGP podemos integrar a un grupo de contactos VIP con que queremos establecer una asociación privada.
- Escoger el algoritmo que se adapte a nuestras necesidades (simétrico, asimétrico).

# BIBLIOGRAFIA


Handbook of applied cryptography: http://www.cacr.math.uwaterloo.ca/hac/

[PDFs], Disponibles en Internet en las direcciones:

Manual PGP Desktop User's Guide, del software PGP Desktop 9

Http://www.pgpi.org/,

Http://es.wikipedia.org/wiki/Pretty_good_privacy

Http://www.caravantes.com/pgp/pgp.htm

PGP: Disponible en Internet en la dirección:

Http://www.pgp.com/products/universal_server/index.html