Informática y Nuevas Tecnologías II

Correo Electrónico (continuación)

Dra. María Paula González
http://cs.uns.edu.ar/~mpg
Depto. de Ciencias e Ingeniería de la Computación
Universidad Nacional del Sur, Bahía Blanca

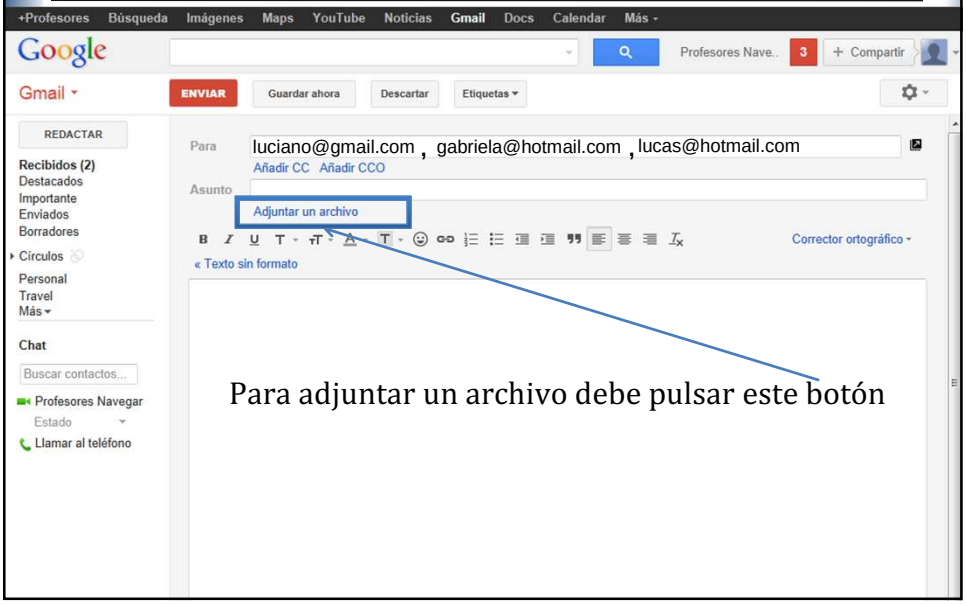
Observacion

El material de esta clase está basado en material desarrollado por el Dr. Luciano H Tamargo para el dictado de materias similares dentro de la curricula del Dpto de Ciencias e Ingeniería de la Computación

Temario

- Funcionamiento del correo electrónico
  - Comparación entre correo web y un cliente de correo
  - Seguridad en el envío de datos a través de Internet.
  - Recomendaciones

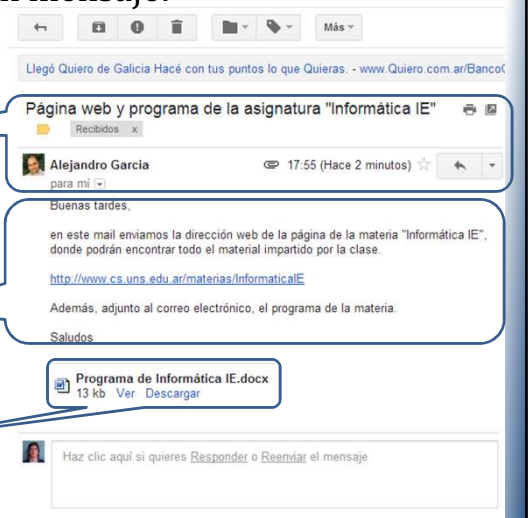
Funcionamiento: Archivos adjuntos



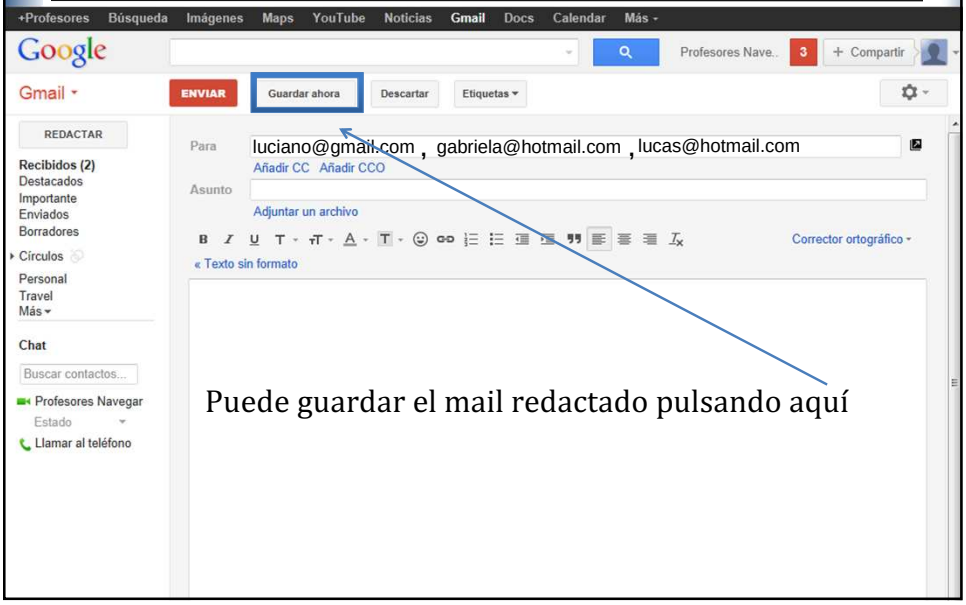
Funcionamiento: Archivos adjuntos

Estructura general de un mensaje:

- Cabeceras
  - Asunto
  - Remitente
  - Destinatario
  - Fecha
- Contenido del mensaje
  - Texto
  - Texto reenviado
  - Enlaces
  - …
- Archivos adjuntos

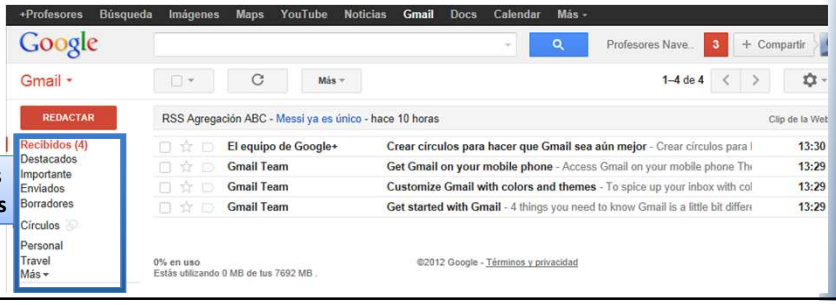


Funcionamiento: Guardar

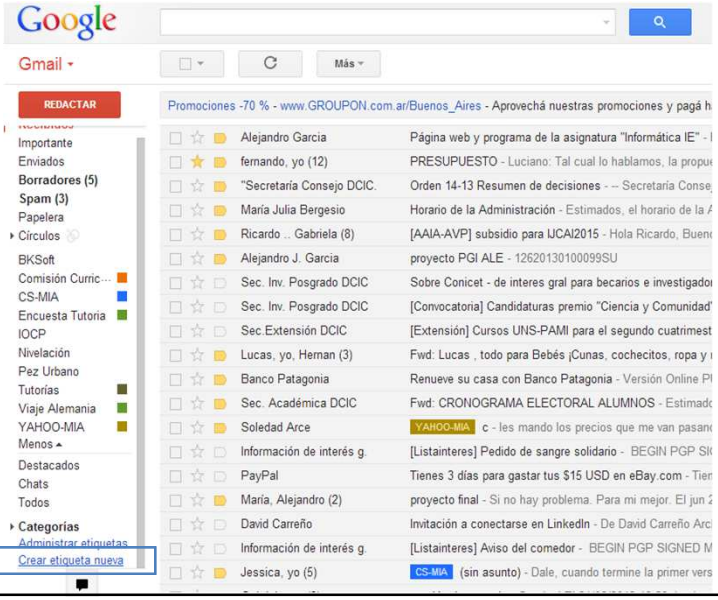


Funcionamiento: Organizar

- Guardar el mensaje en carpetas.
- Organiza la información relativa a los mensajes
  - Trabajo
  - Universidad
  - Familia
  - Amigos



Funcionamiento: Organizar



Funcionamiento: Organizar

Funcionamiento: Organizar Contactos

- Tanto los clientes de correo como los correos web se **permite gestionar una agenda de contactos**, para guardar las direcciones de correos.
- Se pueden añadir/eliminar contactos
  - Datos personales
  - Y, por supuesto… la dirección de correo electrónico
- Al escribir un nuevo correo **no es necesario acordarse de las direcciones** de nuestros contactos.

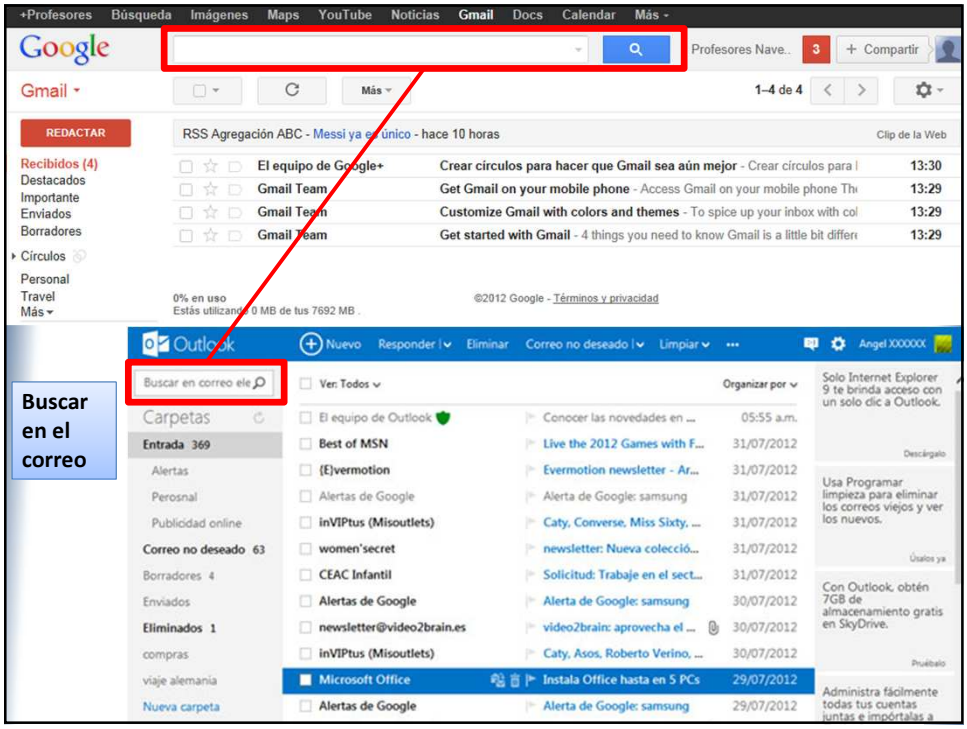
Temario

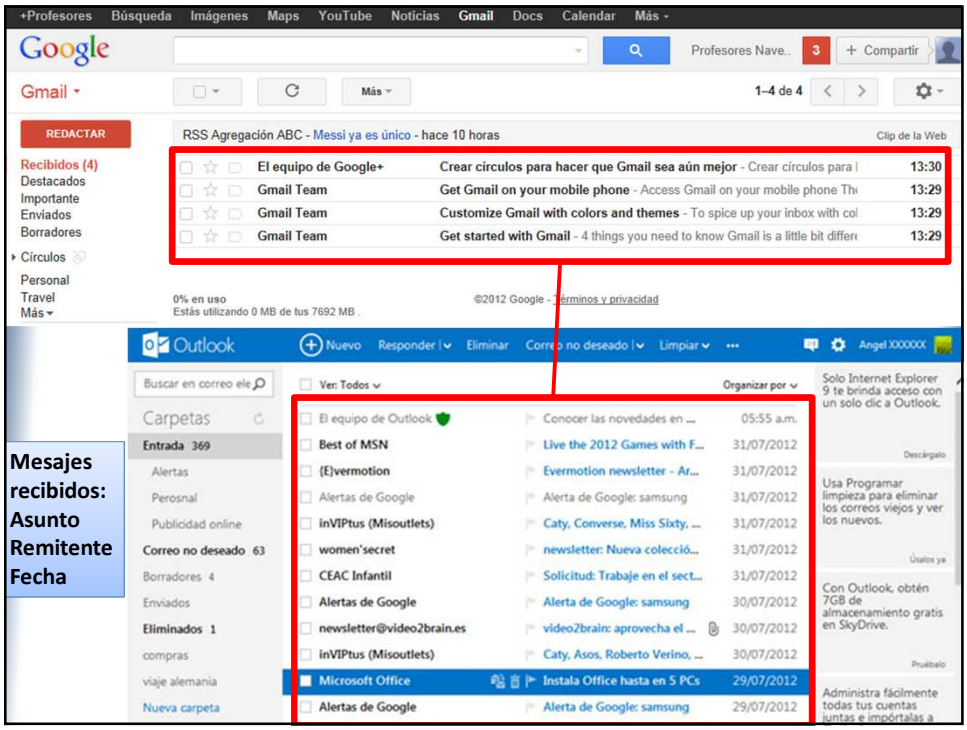
- Funcionamiento del correo electrónico
- Comparación entre correo web y un cliente de correo
- Seguridad en el envío de datos a través de Internet.
- Recomendaciones

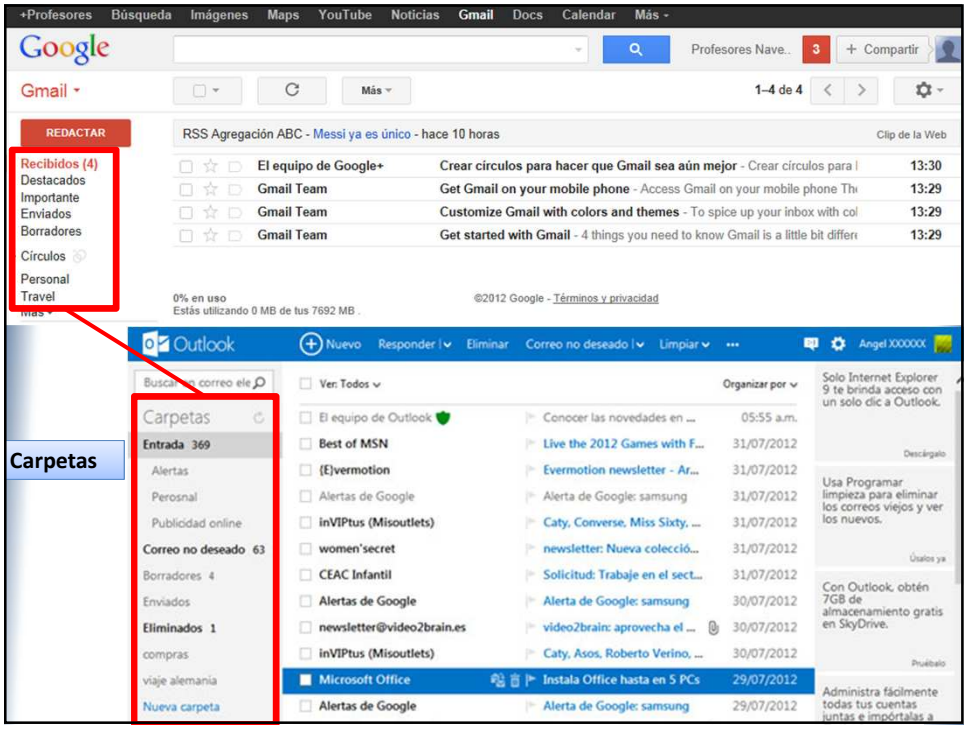
Comparación Correo web/Cliente de correo

Casos de estudio:

- Correo web de **Gmail**
- Cliente de correo **Outlook 2010**


Buscar en el correo


Mesajes recibidos:
Asunto
Remitente
Fecha



Temario

- Funcionamiento del correo electrónico
- Comparación entre correo web y un cliente de correo
- Seguridad en el envío de datos a través de Internet.
- Recomendaciones

Seguridad en el envío de datos a través de Internet

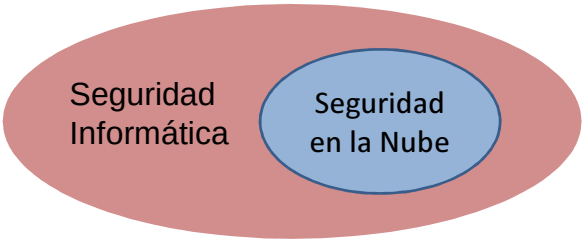
- Algunas Amenazas:
  - **Usuarios:** en algunos casos sus acciones causan problemas de seguridad
  - **Programas maliciosos (malware):** programas destinados a perjudicar o a hacer un uso ilícito de los recursos del sistema. Es instalado (por inatención o maldad) en la computadora, abriendo una puerta a intrusos o bien modificando los datos.
    - Virus informático,
    - Gusano informático
    - Troyano
    - Bomba Lógica
    - Programa Espía o Spyware

Seguridad en el envío de datos a través de Internet

- Seguridad Informática: protege
  - Infraestructura computacional: fallas, robos, incendios, boicot, desastres naturales, fallas en el suministro eléctrico y cualquier otro factor que atente contra la infraestructura informática.
  - Usuarios: debe protegerse el sistema en general para que el uso por parte de ellos no pueda poner en entredicho la seguridad de la información.
  - Información: es el principal activo. Utiliza y reside en la infraestructura computacional y es utilizada por los usuarios.

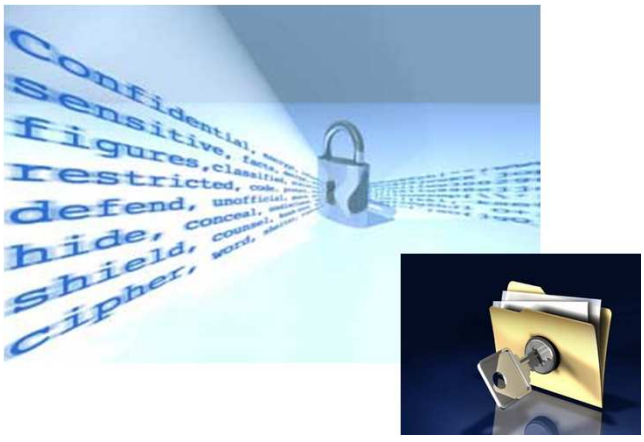
Seguridad en el envío de datos a través de Internet

- Seguridad Informática ≠ Seguridad en la Nube
  - Seguridad en la Nube = Seguridad como servicio: se provee seguridad de manera remota
  - Seguridad Informática: se provee tanto de manera remota como local (software para la seguridad instalado en mi computadora)



Seguridad en el envío de datos a través de Internet

- Seguridad para la información: criptografía de datos

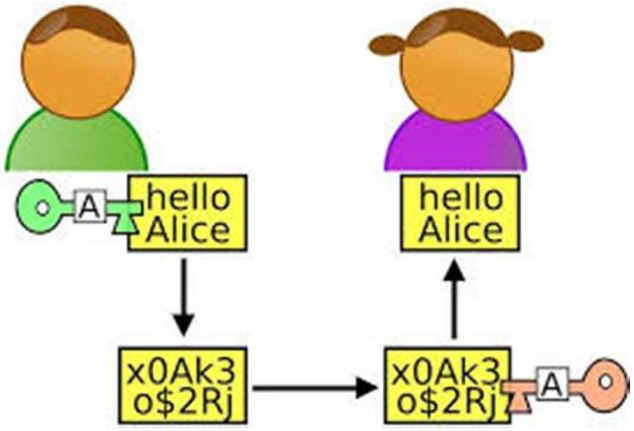


Seguridad en el envío de datos a través de Internet

- Seguridad para la información: criptografía de datos
  - procedimiento que utiliza un algoritmo con dos claves: clave secreta de cifrado y una clave secreta de descifrado
  - Transforma un mensaje sin importar su estructura lingüística o significado para que sea incomprensible o, al menos, difícil de comprender a toda persona que no tenga la clave secreta de descifrado
  - Las claves de cifrado y de descifrado pueden ser iguales (criptografía simétrica) o no (criptografía asimétrica).

Seguridad en el envío de datos a través de Internet

- Seguridad para la información: criptografía de datos



Seguridad en el envío de datos a través de Internet

- Seguridad para la información: criptografía de datos
  - El texto en claro o texto plano (en inglés, plain text) es el mensaje que se cifra.
  - El criptograma o texto cifrado es el mensaje resultante una vez que se ha producido el cifrado, es decir, el mensaje cifrado
  - El algoritmo de cifrado o cifra es el algoritmo que se utiliza para cifrar
  - La clave de cifrado se utiliza en el algoritmo de cifrado.

Seguridad en el envío de datos a través de Internet

- Seguridad para la información: criptografía de datos
- Criptografía simétrica: uso de una sola clave.
- Criptografía de clave pública o Criptografía asimétrica: uso de parejas de claves compuesta por una clave pública, que sirve para cifrar, y por una clave privada, que sirve para descifrar.
- Criptografía con umbral: uso de un umbral de participantes a partir del cual se puede realizar la acción.
- Criptografía basada en identidad: tipo de criptografía asimétrica basada en el uso de identidades.
- Criptografía basada en certificados/ sin certificados
- Criptografía de clave aislada

Seguridad en el envío de datos a través de Internet

- Seguridad para la información: encriptación de correo electrónico
  - La mayor parte de los mensajes de correo electrónico que se transmiten por Internet no incorporan seguridad. La información que contienen es fácilmente accesible a terceros.
  - La criptografía se aplica al correo electrónico.
  - Nos aseguramos que terceras personas (o hackers) no puedan leer su contenido, o bien que tenemos la certeza de que el remitente de éste correo electrónico es realmente quien dice ser.

Seguridad en el envío de datos a través de Internet

- Seguridad para la información: encriptación de correo electrónico
  - Cuando hablamos de cifrar, se supone que quien envía y quien recibe el mensaje comparten una clave para cifrar y descifrar (criptografía simétrica): ambos extremos conocen esa clave (*shared key*), y esa es la que se usa.

El problema de este método es que ambos extremos tienen que "pasarse" la clave en algún momento, con las complicaciones que eso supone (pasar por canales separados y asegurarse de que nadie la sabe).

Seguridad en el envío de datos a través de Internet

- Seguridad para la información: encriptación de correo electrónico

Problema de criptografía simétrica: ambos extremos tienen que "pasarse" la clave en algún momento

Ejemplos: - tecnología wifi

- microchip Clipper lanzado por gobierno de USA para compañías de comunicaciones (lanzado en 93, olvidado en 96)

Solución: cifrado de clave pública (criptografía asimétrica)

Seguridad en el envío de datos a través de Internet

- Seguridad para la información: encriptación de correo electrónico

Cifrado de clave pública: una persona genera dos claves, una privada y una pública.

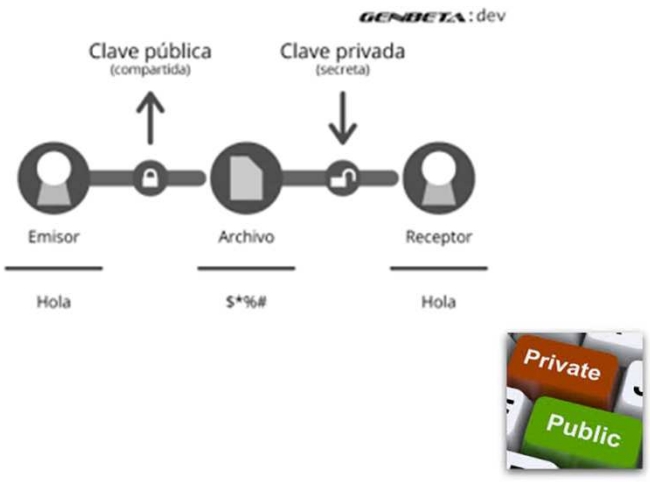
- Clave pública: compartida. Debe ser publicada para que cualquiera pueda usarla para cifrar un mensaje que va a enviarte.
- Clave privada: secreta. Los mensajes sólo puede ser descifrado con la clave privada asociada, que obviamente es la que tiene SOLAMENTE el receptor del correo electrónico.

Seguridad en el envío de datos a través de Internet

- Cifrado de datos en correo electrónico

Seguridad en el envío de datos a través de Internet

- Cifrado de datos en correo electrónico



Seguridad en el envío de datos a través de Internet

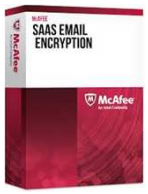
- Cifrado de datos en correo electrónico: protocolo estándar Privacy Guard Protocol o PGP
  - mecanismo de encriptación denominado PGP es una herramienta de cifrado y firmas digitales
  - software libre
  - No tiene una interfaz gráfica, por eso diferentes empresas desarrollan encriptadores para correo electrónico basado en PGP, para que sea posible que los usuarios usen PGP de manera sencilla

Seguridad en el envío de datos a través de Internet

- Cifrado de datos en correo electrónico basado en PGP

Para Thunberbird y Mozilla

Para cliente de correo electrónico



Para computación en la nube

Para cliente de correo electrónico

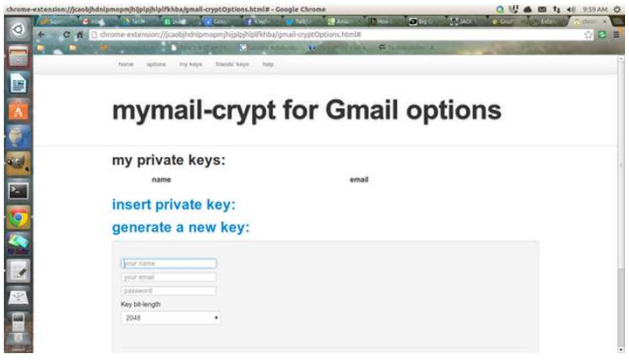
Seguridad en el envío de datos a través de Internet

- Cifrado de datos en correo electrónico basado en PGP

Servicio de la computación en la nube para escribir y encriptar un texto online y despues pegarlo en tu correo electrónico

Seguridad en el envío de datos a través de Internet

- Cifrado de datos en correo electrónico basado en PGP



Extensión específica de Gmail para usar con el navegador Google Crome. Se instala y se utiliza desde la interfaz de Gmail

Seguridad en el envío de datos a través de Internet

- Cifrado de datos en correo electrónico basado en PGP

Mailvelope de la empresa Crome (plug in para varios servicios de correo electrónico)

Seguridad en el envío de datos a través de Internet

- Cifrado de datos basado en PGP para smartphones

Seguridad en el envío de datos a través de Internet

- Cifrado de datos basado en PGP para nuevas tecnologías

Seguridad en el envío de datos a través de Internet

- Cifrado de datos: nuevo estándar Advanced Encryption Standard AES

Seguridad en el envío de datos a través de Internet

- Cifrado de datos: nuevo estándar Advanced Encryption Standard AES

Figure 1

Seguridad en el envío de datos a través de Internet

- Cifrado de datos: nuevo estándar Advanced Encryption Standard AES

Temario

- Funcionamiento del correo electrónico
- Comparación entre correo web y un cliente de correo
- Seguridad en el envío de datos a través de Internet.
- Recomendaciones

Recomendaciones

- **Correo no deseado (SPAM)**: es la recepción de correos no solicitados, normalmente de publicidad engañosa, y en grandes cantidades, promoviendo productos y servicios de calidad sospechosa.
- Si recibimos un mail que contiene algo que desconocemos conviene **consultar su veracidad**.
- **Suplantación de identidad**: correo fraudulento que generalmente intenta conseguir información bancaria.

Recomendaciones

- **Malware informático**: se propaga mediante archivos adjuntos infectando la computadora de quien los abre.
- Si tiene un archivo adjunto, debemos tener cuidado.
- Abrirlo sólo si se está seguro del contenido.

Recomendaciones

- **Cadenas de correo electrónico**: consisten en reenviar un mensaje a mucha gente. La publicación de listas de direcciones de correo contribuye a la propagación a gran escala del correo no deseado y de mensajes con virus, etc.
- Solo si estamos seguros del mensaje lo **reenviaremos**, teniendo cuidado de poner las direcciones de los destinatarios en CCO, borrando del cuerpo del mensaje encabezados previos con direcciones de correo electrónico.

Recomendaciones

- Mensaje sospechoso que ofrece **darse de baja** de futuras recepciones de mensajes o de un boletín.
- No hagan caso. Si hicieran algo de lo citado confirmarían a los remitentes de correo basura que nuestra cuenta de correo electrónico **existe y está activa** y, en adelante, recibiríamos más mensajes no deseados.
- Si nuestro proveedor de correo lo ofrece podemos cliquear en "***Marcar como spam***".

Recomendaciones

- Cifrar, cifrar, cifrar… ¿y si no se puede? También cifrar…

FIN