
grupo int
OTRA FORMA DE HACER LAS COSAS ES POSIBLE
EMAIL CIFRADO

Servidor de correo

Cuando nos logueamos a un servidor de correo, nuestros datos deben de ir cifrados para que en el caso de tener comprometidas las comunicaciones, no puedan conseguir nuestra contraseña.

Un envío de email se compone, básicamente, de nuestro mensaje y de unas cabeceras que identifican la trazabilidad de las comunicaciones. Nuestro mensaje puede ser leído ya que no viaja cifrado.

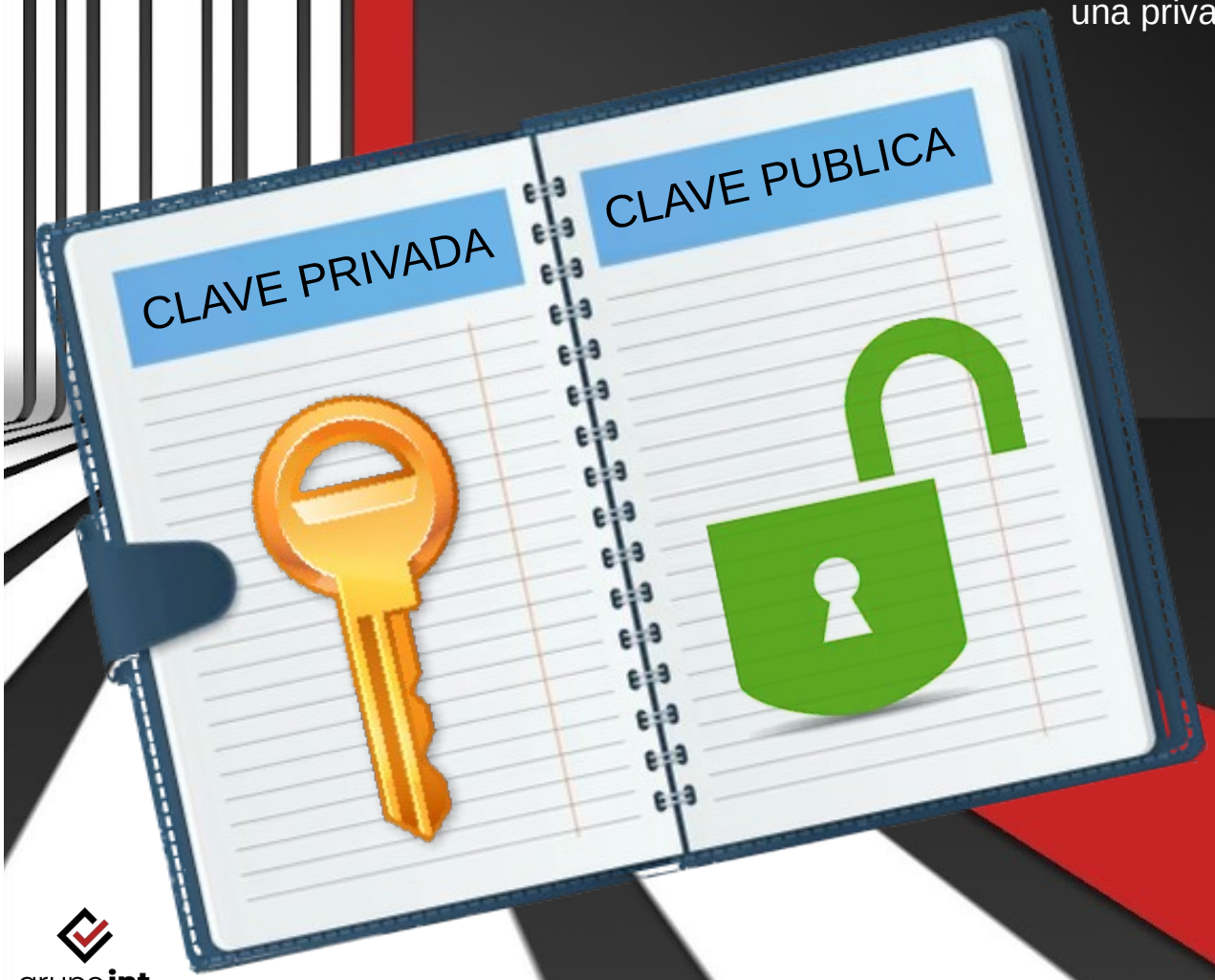
Un delincuente que intercepte nuestros correos, puede modificarlos añadiendo información falsa, por ejemplo, puede cambiar una cuenta bancaria por otra.

Vamos a proteger nuestros correos cifrando los mismos para que resulten ilegibles en caso de que sean interceptados y sólo puedan ser leídos por los destinatarios de los mismos.

Creación de claves

Vamos a usar Thunderbird como cliente de correo y OpenPGP, que ya esta integrado en el mismo, para la creación de claves.

Crearemos para nuestra cuenta de correo dos claves, una privada y otra pública.



Thunderbird

+

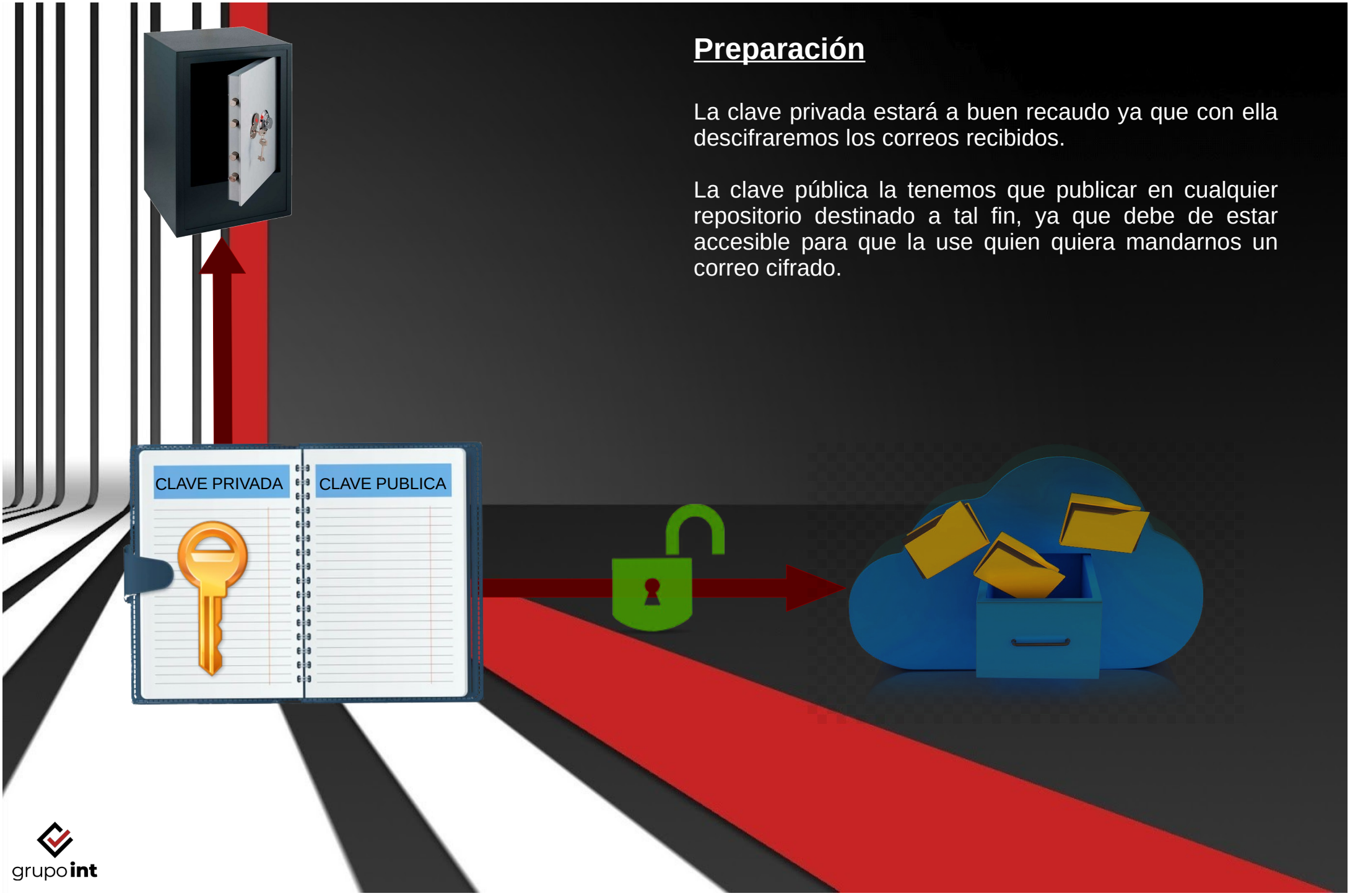
OpenPGP

grupoint

Preparación

La clave privada estará a buen recaudo ya que con ella descifraremos los correos recibidos.

La clave pública la tenemos que publicar en cualquier repositorio destinado a tal fin, ya que debe de estar accesible para que la use quien quiera mandarnos un correo cifrado.



grupoint

Proceso

1. Escribimos un correo a un destinatario
2. Tenemos el cifrado activado, enviamos el correo
3. Antes de enviarse, se busca la clave publica del destinatario
4. Con la clave pública del destinatario, ciframos el correo




5. El correo es enviado al destinatario, cifrado.
6. El destinatario recibe el correo y usa su clave privada para descifrarlo
7. El correo queda descifrado
8. El mensaje puede ser leído por el destinatario




grupoint

Mozilla Thunderbird

POSTFIX

grupo **int**

debian