ACTIVIDAD DE FIRMA PDF

Hecho por: Juan Manuel Restrepo Muñoz

Codigo: 2267209-2724

1. importación de la clave publica:

```
┌──(kali㉿kali)-[~]
└─$ gpg --import clase26-04-25.asc
gpg: key 6F3C993ED29EFF0D: public key "jorge_mesa (privado) <jorge.mesa@correounivalle.edulco>" imported
gpg: Total number processed: 1
gpg:               imported: 1
```

- Lista de claves:

```
┌──(kali㉿kali)-[~]
└─$ gpg --list-keys
/home/kali/.gnupg/pubring.kbx
------------------------------
pub   rsa3072 2025-04-05 [SC] [expires: 2028-04-04]
      8AF99C8D9991CC501FE73667ECF8298F7878D875
uid           [ultimate] juan_restrepo <eljunsyt888@gmail.com>
sub   rsa3072 2025-04-05 [E] [expires: 2028-04-04]

pub   rsa3072 2025-04-05 [SC]
      DBE33AE937CB425AD8B68055D19A7165E9FB3112
uid           [ultimate] juanr (laboratorio) <eljunsyt888@gmail.com>
sub   rsa3072 2025-04-05 [E]

pub   rsa3072 2025-04-05 [SC] [expires: 2028-04-04]
      40794FB39764738782CA841F60D17095A78B8971
uid           [ultimate] valeria <lopezingrid600@gmail.com>
sub   rsa3072 2025-04-05 [E] [expires: 2028-04-04]

pub   rsa3072 2025-04-05 [SC]
      2BE28FF6312FB4FAA1C044D4B6FA63FE9FDD51D4
uid           [ultimate] valeria (practica) <lopezingrid600@gmail.com>
sub   rsa3072 2025-04-05 [E]

pub   rsa3072 2025-04-05 [SC]
      F5DCD4F48CC43FEE1A486E0BB37176F052496D69
uid           [ unknown] cristian (prueba) <crsan256@gmail.com>
sub   rsa3072 2025-04-05 [E]

pub   rsa3072 2025-04-12 [SC]
      9664EC35EF15D360029763160E32258F11B17740
uid           [ultimate] juanR (firma) <eljunsyt888@gmail.com>
sub   rsa3072 2025-04-12 [E]

pub   rsa3072 2025-04-12 [SC]
      E254DAF27951C2DE3204CEE8D187D87E2710A6A0
uid           [ unknown] ingridlopez (firma) <lopezingrid600@gmail.com>
sub   rsa3072 2025-04-12 [E]

pub   rsa3072 2025-04-26 [SC] [expires: 2025-05-03]
      FD79536C274B42BB53B868496F3C993ED29EFF0D
uid           [ unknown] jorge_mesa (privado) <jorge.mesa@correounivalle.edulco>
sub   rsa3072 2025-04-26 [E] [expires: 2025-05-03]
```

2. Verificación del PDF correcto:

```
┌──(kali㉿kali)-[~]
└─$ gpg --verify confidencial.sig "DOCUMENTO CONFIDENCIAL.pdf"
gpg: Signature made Sat 26 Apr 2025 01:17:30 PM EDT
gpg:                using RSA key FD79536C274B42BB53B868496F3C993ED29EFF0D
gpg:                issuer "jorge.mesa@correounivalle.edulco"
gpg: Good signature from "jorge_mesa (privado) <jorge.mesa@correounivalle.edulco>" [unknown]
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: FD79 536C 274B 42BB 53B8  6849 6F3C 993E D29E FF0D
```

3. PDF alterado:

```
┌──(kali㉿kali)-[~]
└─$ gpg --verify confidencial.sig "DOC CONFIDENCIAL.pdf"
gpg: Signature made Sat 26 Apr 2025 01:17:30 PM EDT
gpg:                using RSA key FD79536C274B42BB53B868496F3C993ED29EFF0D
gpg:                issuer "jorge.mesa@correounivalle.edulco"
gpg: BAD signature from "jorge_mesa (privado) <jorge.mesa@correounivalle.edulco>" [unknown]
```

Porque el archivo DOC CONFIDENCIAL.pdf fue alterado tras haber sido firmado, y cualquier modificación en su contenido provoca que la firma digital deje de ser válida respecto al documento original.

4. PDF Firmado:

```
┌──(kali㉿kali)-[~]
└─$ gpg --output mi_firma.sig --detach-sig "diploma.pdf"

┌──(kali㉿kali)-[~]
└─$ ls
clase26-04-25.asc   diploma.pdf                Documents    firma.txt    Jellyfish.jpg   laboratorio.asc      mateo.txt       Music       Pictures        practica1.txt       practicaV   Videos
confidencial.sig    'DOC CONFIDENCIAL.pdf'     Downloads    firmaV.asc   juan.txt        labo.txt             mateo.txt.gpg   notaM.txt   practica        practica1.txt.gpg   Public
Desktop             'DOCUMENTO CONFIDENCIAL.pdf' firmaJ.asc  incluido     juan.txt.gpg    maleducada.txt.gpg   mi_firma.sig    notaV.txt   practica1.asc   practicaM           Templates
```