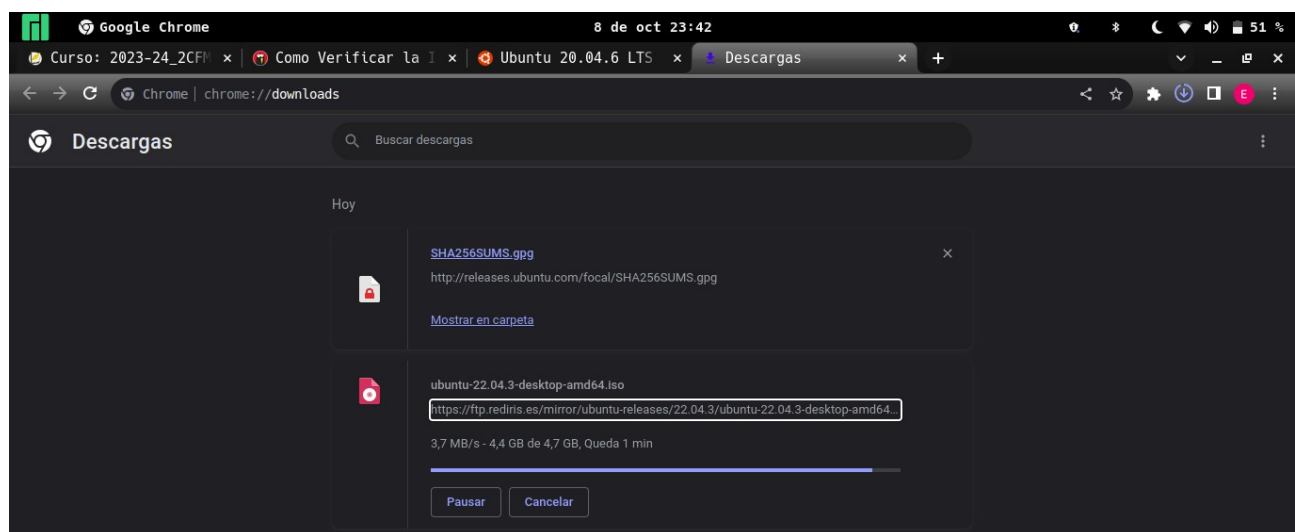
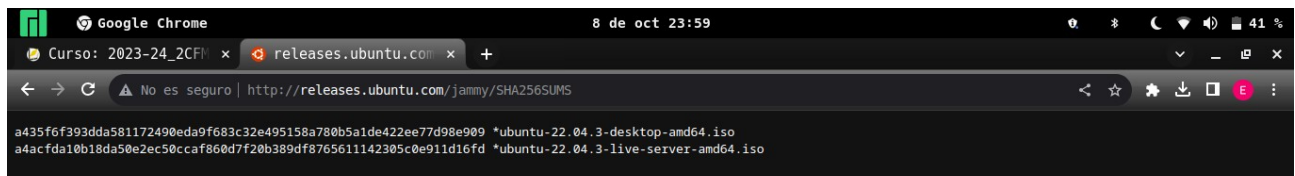


- **NOMBRE:** Enrique Martínez Añón
- **FECHA INICIO:** 8 de octubre 2023
- **FECHA FINAL:** 8 de octubre 2023
- **UNIDAD:** Tema 2 Seguridad Informática
- **CASO PRÁCTICO:** R3T0 - R3PT3 22.  
r
- **ENUNCIADO:** Calcular la función HASH de la iso de Ubuntu Desktop 22.04 LTS  
a
- **VERSIÓN ACTIVIDAD:** A
- **DIFICULTAD:** BAJO
- **TIEMPO ESTIMADO:** 1 hora.
- **TIEMPO REAL:** 40 minutos.
- **CONCLUSIÓN:** Ha sido bastante fácil comprobar gracias a la función hash que la iso es la original y es segura.

## INDICE

Me descargo la imagen iso de Ubuntu 22.04.3 LTS y también su clave SHA256SUM.



Escribo el comando sha256sum sobre la imagen iso y me devuelve la clave que puedo comprobar si es igual que la que me descargué de la página oficial de ubuntu.

```
Terminal
8 de oct 23:52

> sha256sum ubuntu-22.04.3-desktop-amd64.iso
a435f6f393dda581172490eda9f683c32e495158a780b5a1de422ee77d98e909  ubuntu-22.04.3-desktop-amd64.iso
```

## BIBLIOGRAFIA

Esta vez no he seguido todos los pasos que me decía la guía de ayuda de la página oficial de Ubuntu. El comando `# gpg --keyid-format long --verify SHA256SUMS.gpg SHA256SUMS` me devolvía lo siguiente:

```
Terminal
9 de oct 00:32

> gpg --keyid-format long --verify SHA256SUMS.gpg SHA256SUMS
gpg: imposible abrir datos firmados 'SHA256SUMS'
gpg: can't hash datafile: No existe el fichero o el directorio
```

He probado con el siguiente comando y me ha devuelto esto:  
`# gpg --keyid-format long --verify SHA256SUMS.gpg ubuntu-22.04.3-desktop-amd64.iso`

```
Terminal
9 de oct 00:31

> gpg --keyid-format long --verify SHA256SUMS.gpg ubuntu-22.04.3-desktop-amd64.iso
gpg: Firmado el mié 22 mar 2023 15:31:48 CET
gpg: usando RSA clave 843938DF228D22F7B3742BC0D94AA3F0EFE21092
gpg: Imposible comprobar la firma: No hay clave pública
```

Con este comando por lo menos me ha dado una clave y he podido tirar un poco del hilo y he conseguido esto:

```
Terminal
9 de oct 00:36

> gpg --keyid-format long --verify SHA256SUMS.gpg SHA256SUMS
gpg: imposible abrir datos firmados 'SHA256SUMS'
gpg: can't hash datafile: No existe el fichero o el directorio
> gpg --keyid-format long --verify SHA256SUMS.gpg ubuntu-22.04.3-desktop-amd64.iso
gpg: Firmado el mié 22 mar 2023 15:31:48 CET
gpg: usando RSA clave 843938DF228D22F7B3742BC0D94AA3F0EFE21092
gpg: Imposible comprobar la firma: No hay clave pública
> gpg --keyid-format long --keyserver hkp://keyserver.ubuntu.com --recv-keys 0x843938DF228D22F7B3742BC0D94AA3F0EFE21092
gpg: clave D94AA3F0EFE21092: clave pública "Ubuntu CD Image Automatic Signing Key (2012) <cdimage@ubuntu.com>" importada
gpg: Cantidad total procesada: 1
gpg: importadas: 1
> gpg --keyid-format long --verify SHA256SUMS.gpg SHA256SUMS
gpg: imposible abrir datos firmados 'SHA256SUMS'
gpg: can't hash datafile: No existe el fichero o el directorio
> gpg --keyid-format long --list-keys --with-fingerprint 0x843938DF228D22F7B3742BC0D94AA3F0EFE21092
pub  rsa4096/D94AA3F0EFE21092 2012-05-11 [SC]
     Huella de clave = 8439 38DF 228D 22F7 B374 2BC0 D94A A3F0 EFE2 1092
uid   [desconocida] Ubuntu CD Image Automatic Signing Key (2012) <cdimage@ubuntu.com>
```

Así que tengo la clave importada y la huella de la clave.  
Huella de clave = 8439 38DF 228D 22F7 B374 2BC0 D94A A3F0 EFE2 1092  
Pero la forma más fácil de hacerlo para mi ha sido la que he hecho primero.