# CIFRADO ALMACENAMIENTO

## - Cifrado a nivel de filesystem

### Sistemas de ficheros de propósito general con posibilidades de cifrado:

- NTFS con Encrypting File System (EFS) para Windows
- ZFS desde Pool Version 30
- Ext4, añadido en Linux kernel 4.1 (2015)
- F2FS, añadido en Linux kernel 4.2
- APFS, macOS High Sierra (10.13) y posterior

### Sistemas de ficheros basados en FUSE (File system in USEr space) (fuera del kernel):

- gocryptfs (2021)
- CryFS (2021)
- securefs (2021)
- EncFS (2018)
- Rclone (2021)

### Integrado en el kernel de Linux:

eCryptfs

### Integrado en Windows:

EFS

### Integrado en MAC Os

FileVault

## - Cifrado a nivel de bloque

***Linux***

**Loop-AES** – Cifrado de file system  y swap rápido y transparente para Linux. Funciona con kernels 3.x, 2.6, 2.4, 2.2 y 2.0.

**dm-crypt+LUKS** – dm-crypt es un subsistema de cifrado transparente a partir de Linux kernel v2.6+ y posterior y DragonFly BSD. Puede cifrar discos completos, discos removibles, particiones, volúmenes RAID software, volúmenes lógicos y ficheros.

***Windows:***

**bitlocker** – Cifrado de volúmenes completos incluido a partir de Windows Vista. Si se utiliza el chip TPM la clave se almacena en el mismo por lo que no se pide ninguna contraseña en el arranque . Si por el contrario no se tiene el chip TPM se pedirá la contraseña al iniciar. Además en el primer caso si alguien se hace con el disco y no el ordenador no tendrá la clave de cifrado.

***Ambos:***

**VeraCrypt** – Es un software de cifrado de discos, particiones y contenedores open-source multiplataforma para Windows, MacOS y Linux basado en el descontinuado TrueCrypt.

NOTA: Cuanto más bajo sea el nivel de cifrado, mayor nivel de seguridad.