



3 Xestión da información

Sumario












3	Xestión da información.....	1
3.1	Convencións empregadas.....	5
3.2	Introdución.....	6
3.3	Estrutura lóxica dun disco duro: Particións e sistemas de arquivos.....	6
3.3.1	Ferramentas para crear particións.....	6
3.3.1.1	Ferramentas internas dos Sistemas Operativos para crear particións.....	6
3.3.1.2	Ferramentas externas dos Sistemas Operativos.....	6
3.3.1.3	Por que se adoitan utilizar estas ferramentas externas?.....	6
3.3.2	Administrador de discos de Windows.....	7
3.3.3	GParted (Gnome Partition Edit, Editor de particións Gnome).....	10
3.3.4	Particións: BIOS-MBR.....	11
3.3.5	Particións: UEFI-GPT.....	12
3.3.6	Sistemas de arquivos. Formato de particións.....	15
3.4	Configuración de xestores de arranque.....	19
3.4.1	Estudo do arranque de Windows 10.....	19
3.4.2	Configuración do xestor de arranque bcd (Boot Configuration Data).....	23
3.5	Terminal de comandos de Windows.....	25
3.5.1	Comandos básicos.....	25
3.5.2	Comandos para directorios e ficheiros.....	29
3.5.2.1	Estrutura na unidade C.....	29
3.5.2.2	Roteiros absolutos e relativos.....	29
3.5.2.3	Comandos para directorios.....	31
3.5.2.4	Comandos para ficheiros.....	32
3.5.3	Direccionamiento e tubaxes.....	34
3.5.3.1	Operadores de direccionamiento de saída.....	34
3.6	Terminal de comandos de GNU-Linux.....	38
3.6.1	Interfaces de texto: terminais ou consolas de texto.....	38
3.6.1.1	Sintaxe dos comandos.....	38
3.6.1.2	Primeiros comandos.....	39
3.6.1.3	Usuarios de Linux. Traballar como administrador. Cambios de usuario..	39
3.6.1.4	Cambiar a outro usuario. Comando o seu.....	40
3.6.1.5	Lenda para os exemplos que se mostre.....	41
3.6.1.6	Varios comandos sinxelos.....	42
3.6.1.7	Inicio de sesión do usuario en Linux. Directorio /home.....	42
3.6.1.8	Significado dos parámetros do Prompt ou Shell do sistema.....	42
3.6.2	Comandos de directorios.....	43
3.6.3	Comandos de ficheiros.....	46
3.6.3.1	Editor de texto plano.....	46
3.6.3.2	Visualización de ficheiro en terminal.....	47
3.7	Almacenamento redundante e distribuído.....	48
3.7.1	RAID por Hardware.....	49
3.7.2	RAID por Software.....	50
3.7.3	RAID Híbrido ou FakeRAID.....	50
3.8	Tipos de RAID.....	51
3.8.1	RAID 0.....	51
3.8.2	RAID 1.....	51
3.8.3	RAID 5.....	52
3.8.4	RAID 6.....	53

3.8.5 RAID aniñados.....	53
3.8.5.1 RAID 0 + 1.....	54
3.8.5.2 RAID 1 + 0.....	54
3.8.6 RAID en Windows.....	55
3.8.7 RAID en Linux.....	56
3.8.8 Cálculo de paridade.....	56
3.9 Almacenamento remoto e extraíble.....	58
3.9.1 NAS.....	58
3.9.2 SAN.....	58
3.9.3 Cloud Storage.....	59
3.10 Copias de seguridade.....	61
3.10.1 Introducción.....	61
3.10.2 Definición de copia de seguridade.....	61
3.10.3 Almacenamento das copias de seguridade.....	62
3.10.4 Boas prácticas.....	63
3.10.5 Política de copias de seguridade.....	64
3.10.6 Tipos de copias de seguridade.....	65
3.10.6.1 Copia completa.....	65
3.10.7 Copia diferencial.....	66
3.10.8 Copia incremental.....	66
3.11 Aplicación práctica das copias de seguridade.....	67
3.11.1 Copias de seguridade con ferramentas do sistema.....	67
3.11.1.1 Windows.....	67
3.11.1.2 Linux.....	68
3.11.2 Copias de seguridade con aplicacións específicas.....	70
3.11.2.1 Windows.....	70
3.11.2.2 Linux.....	71
3.11.3 Copia de seguridade do rexistro de Windows.....	71
3.12 Imaxes de respaldo e restauración.....	71
3.12.1 Introducción.....	71
3.12.2 Imaxes de respaldo.....	71
3.12.2.1 Sistemas Live.....	73
3.12.3 Puntos de restauración en Windows.....	74
3.12.4 Recuperación de datos.....	74

Material docente elaborado a partir da base dos materiais formativos de FP En liña
propiedade do Ministerio de Educación e Formación Profesional.

[Aviso Legal](#)

3.1 Convencións empregadas

	Esta icona fai referencia a notas de introdución
	Esta icona indica aclaración
	Esta icona fai referencia a arquivos de configuración, de rexistro...
	Esta icona indica casos de uso
	Esta icona fai referencia a avisos o advertencias
	Esta icona indica incidentes
	Esta icona fai referencia a sección que inclúen instrucións paso a paso
	Esta icona fai referencia a sección que inclúen capturas de pantalla
	Esta icona fai referencia a actividades
	Esta icona fai referencia a documento esencial (licenza: http://www.ohmyicons.com)
	Referencia a ligazón recomendada (licenza: http://iconleak.com)

3.2 Introducción

Neste epígrafe imos estudar a estrutura lóxica do disco, para iso falaremos de particións, MBR, GPT, mínima unidade lóxica... Finalmente, os distintos sistemas de arquivos coas súas características principais.

3.3 Estrutura lóxica dun disco duro: Particións e sistemas de arquivos

Como sabemos, o disco duro é unha unidade física. Dentro do disco duro, creamos particións, estas particións son unidades lóxicas pois non é unha división física, senón unha división creada por software, que se pode desfacer e realizar noutro sitio.

3.3.1 Ferramentas para crear particións

3.3.1.1 *Ferramentas internas dos Sistemas Operativos para crear particións*

Cando falamos de ferramentas internas, falamos dos programas que incorporan o propio sistema operativo.

Nos sistemas Microsoft antigos desde MS-Dos ata Windows 98 utilizouse fdisk.

Nos sistemas Microsoft, desde Windows XP utilízase diskpart en contorna comando, xunto con ferramenta gráfica Administrador de discos. O Administrador de discos ábrese co menú contextual en Equipo e Administrar.

Nos sistemas Unix-Linux utilízase fdisk.

3.3.1.2 *Ferramentas externas dos Sistemas Operativos*

As externas, son as que non pertencen ao kernel do sistema operativo. As máis coñecidas son:

Gparted, software libre, normalmente incluído nas distribucións de Linux. Páxina do programa.

Easeus Partition Master: software propietario con versión freeware para casa. Páxina do programa.

3.3.1.3 *Por que se adoitan utilizar estas ferramentas externas?*

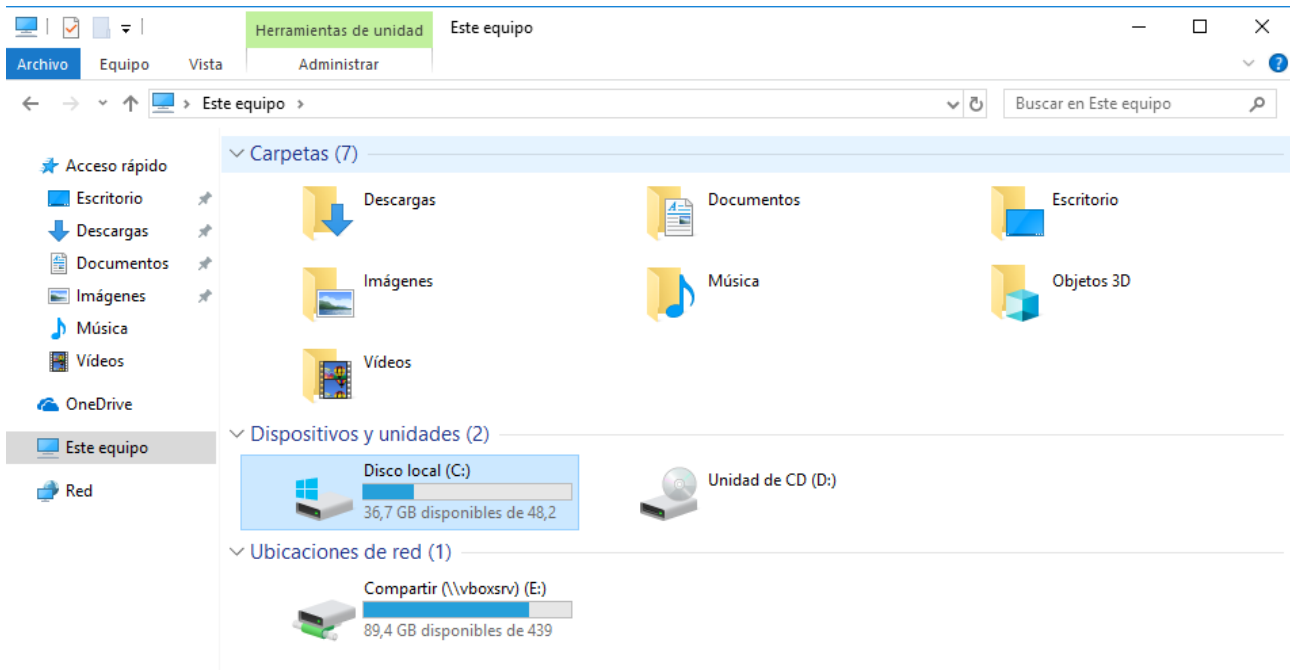
- Permiten crear tanto particións Windows como Linux.
- Permiten redimensionar (cambiar o tamaño) dunha partición.
- Permiten mover particións de sitio, sempre que estea libre no medio.

As ferramentas propias non permiten estas opcións, ou as permiten de forma moi limitada.

3.3.2 Administrador de discos de Windows

A continuación, preséntase 1 captura de Equipo da máquina "Windows10Sistemas".

Ilustración de Equipo.



Miguel Ángel García Lara ([CC BY-NC-SA](#))

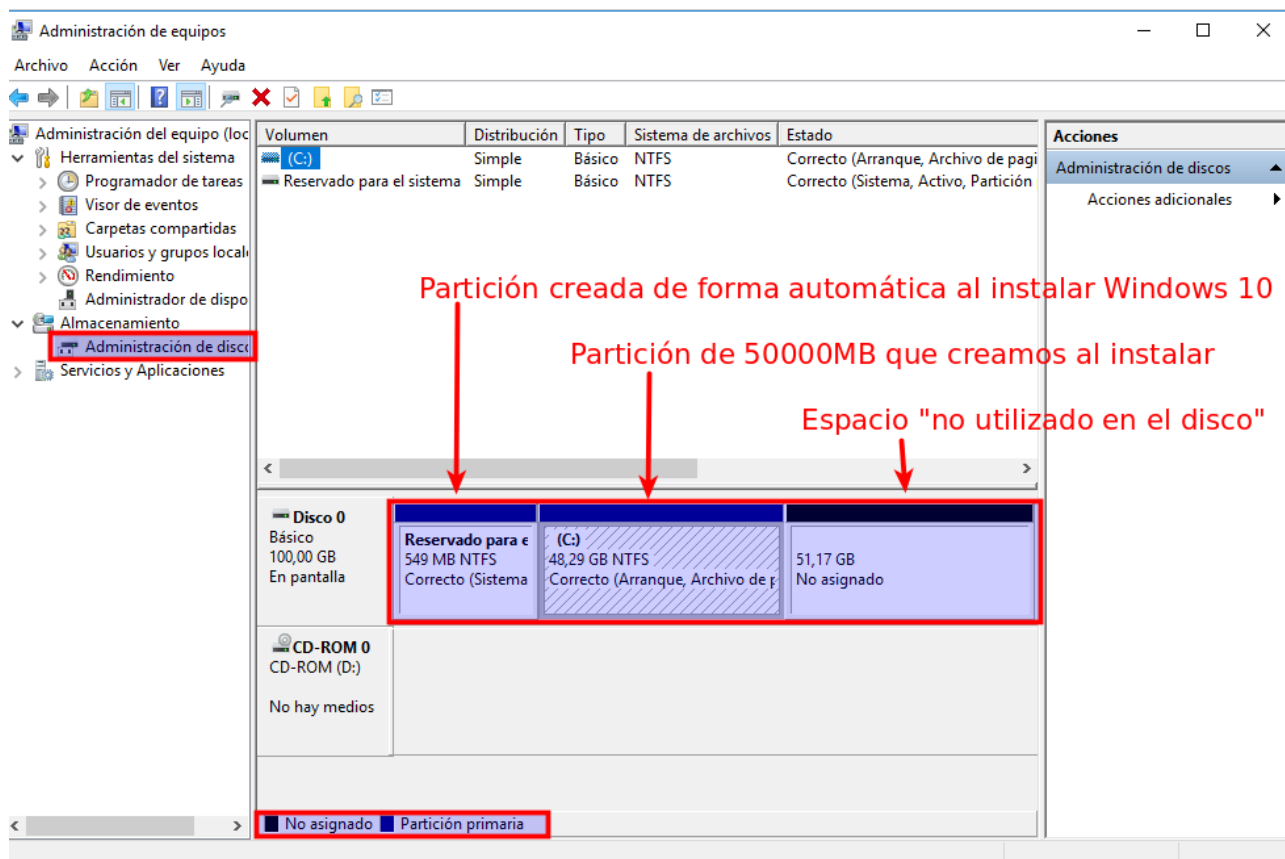
Observa que só se ve unha única partición de 48GB. Lembra que a instalación a fixemos nun disco de 100GB, onde creamos unha partición de 50000MB = $(50000/1024)$ GB = 48,8GB

A maioría dos usuarios pensan que en Equipo, vese todo o disco duro. Iso non é así, en equipo ven exclusivamente as particións creadas e montadas. De feito, lembra que o sistema creou automaticamente unha partición de 500MB, que non se ve nin sequera en Equipo.

Tamén aclarar, que debemos dicir, que “temos libres 36GB na partición C”, non que “temos 36 GB libres” no disco duro.

Aquí móstrase a captura do Administrador de discos da mesma máquina Windows10Sistemas:

Ilustración de Administrador de discos.

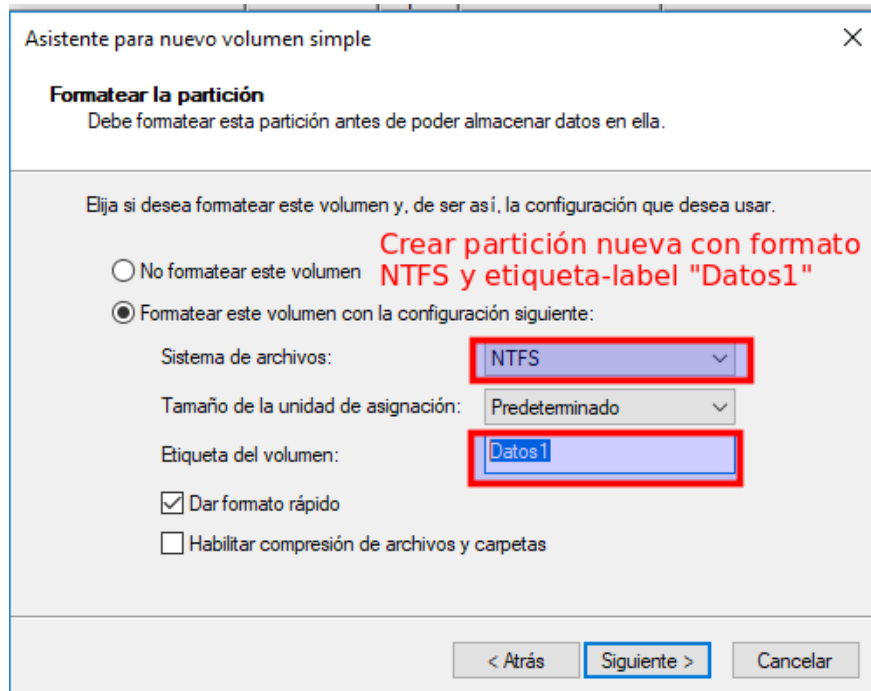


Miguel Ángel García Lara ([CC BY-NC-SA](#))

Como se ve nesta captura, o disco ten 2 particións primarias e un espazo libre de 51GB. Iremos crear unha partición de datos, de 20GB. Para iso, en espazo non asignado, pulsar menú contextual e seleccionar “Novo volume simple”. Seguir os pasos do asistente: tamaño 20000MB, letra por defecto, sistema NTFS e etiqueta “Datos1”. Pulsar seguinte para finalizar a creación da partición nova.

Observación: Sempre que creamos particións, por comodidade, para non estar cunha calculadora, utilizaremos o redondeo de 1GB coma se fosen 1000MB. De aí, que as particións case sempre terán algún gigabyte menos.

Ilustración de Partición nova.



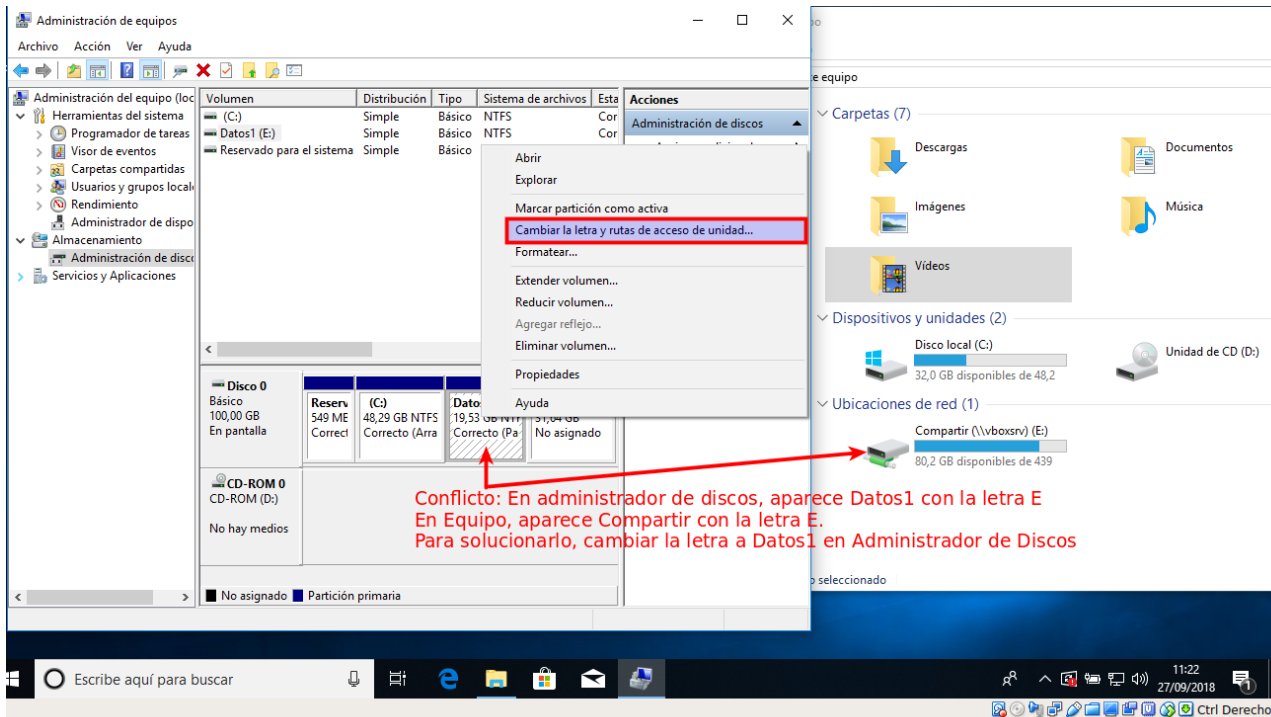
Miguel Ángel García Lara ([CC BY-NC-SA](#))

Unha vez creada a partición, a partición xa é visible en Equipo.

Atención: Neste caso houbo un pequeno conflito non habitual, pero Windows puxo á partición nova a letra E e resulta que en Equipo, aparece que a letra E é o recurso “Compartir”, é dicir, o cartafol compartido que tiñamos na máquina anfitrión. Por tanto, non temos acceso á nova partición.

Como resolvemos este conflito?

Ilustración de Cambiar letra de unidad.



Miguel Ángel García Lara ([CC BY-NC-SA](#))

Pulsamos o menú contextual, na partición creada no administrador de discos, e seleccionamos “Cambiar letra de unidad”.

Seleccionamos a letra F, e Cambiar. Unha vez aceptado o cambio, xa vemos a partición nova F en Equipo. Xa podes escribir nela o que queiras.

A este concepto, chámasele, que “montamos a partición Datos 1 na unidade F:”

3.3.3 GParted (Gnome Partition Edit, Editor de particións Gnome)

O programa gparted, adoita vir incluído en moitas distribucións Linux, pero non é unha ferramenta interna, senón software adicional.

Podemos arrincar calquera computador, teña Windows ou Linux instalado, co CD de Ubuntu (ou ben, co pendrive creado na tarefa da unidade 2). Unha vez arrincado, iniciamos o programa gparted.

Na imaxe vese unha captura de gparted dunha máquina virtual con 1 disco duro que ten 3 particións.

Ilustración Gparted.

Partición	Sistema de archivos	Etiqueta	Tamaño	Usado	Libre	Opciones
/dev/sda1	ntfs	Reservado para el sistema	549.00 MiB	396.48 MiB	152.52 MiB	boot
/dev/sda2	ntfs		48.29 GiB	17.19 GiB	31.11 GiB	
/dev/sda3	ntfs		29.30 GiB	14.67 GiB	14.63 GiB	
sin asignar	sin asignar		21.88 GiB	—	—	

En este disco duro hay 3 particiones primarias, y espacio libre.

Podemos iniciar cualquier PC con el CD de Ubuntu,
y crear, eliminar particiones con GParted

0 operaciones pendientes

Miguel Ángel García Lara (CC BY-NC-SA)

3.3.4 Partición: BIOS-MBR.

O esquema tradicional de arranque desde os primeiros PC no ano 1981 baseouse na BIOS do equipo e o sector MBR no disco duro.

Hai uns anos, hai outro tipo de particionamento chamado GPT, pero que necesita que a BIOS do equipo sexa BIOS-UEFI

Tipos de particións en MBR (Master Boot Record – Rexistro de arranque principal)

Como dicíamos o particionamento foi MBR desde os primeiros PC e discos duros.

Cando creamos particións nun disco duro con MBR, temos que decidir que tipo de partición queremos crear. Vexamos os tipos de particións que hai:

- **Partición primaria:** Por construción, só pode haber 4 particións primarias nun disco duro MBR. Poden conter datos ou un Sistema Operativo (partición de Sistema)
- **Partición estendida:** O límite de 4 particións é moi pequeno, como saltarlló? Créase unha partición estendida, onde dentro créanse outras particións. No límite de 4 particións primarias, está incluída a partición estendida. É dicir, un disco pode

conter 4 primarias ou 3 primarias e 1 estendida, pero non 4 primarias e 1 estendida.

- **Particións lóxicas:** A partición estendida divídese en particións lóxicas.
- O número de particións lóxicas que se pode crear é distinto segundo o sistema operativo, en Windows son 23. Non se pode instalar un sistema operativo nunha partición lóxica.
- **Partición activa ou arrincable:** A que arrinca. Só hai unha no disco duro. A partición activa ten que ser obrigatoriamente una das particións primarias (non pode ser activa nin a partición estendida, nin as particións lóxicas)

Sector MBR

O sector MBR é o sector de arranque do disco duro. É o primeiro sector do disco duro, ocupando como todos os sectores, 512 bytes.

Os programas para crear particións (fdisk, diskpart, gparted) crean este sector da mesma forma.

O MBR contén nos 512 bytes a información seguinte:

- Sector de inicio e sector final de cada partición primaria.
- Cal é o sistema de ficheiros de cada partición (FAT 16, FAT 32, NTFS, ext2, ext3, ext4,,...)
- A información de cal é a partición "activa"

Ao iniciar o PC, lese a BIOS, comproba o hardware do equipo e inicia o programa POST (programa da BIOS), busca o disco duro ou dispositivo configurado como arranque na BIOS. Ao chegar ao disco duro, vai ao sector MBR, como sector de arranque do disco. Neste sector, le cal é a partición activa, e finalmente vai á partición activa para arrincar o sistema operativo instalado na activa.

Observacións:

Cando creamos unha partición, o único que facemos é escribir no MBR os datos da partición.

Se eliminamos todas as particións nun disco, aínda que estea cheo de datos, tárdase 1 segundo, pois o único que fai o computador é escribir no MBR, é dicir nesas 512 bytes, e dicir que non hai particións. O resto do disco non o borra, aínda que pareza que está baleiro (de aí, que se oia tantas veces nas noticias que se recuperou a información de discos duros)

3.3.5 Particións: UEFI-GPT.

Que é UEFI

UEFI empezouse a incorporar nos PC, ao mesmo tempo que se introduciu Windows 8

Poderíase dicir, que para o usuario UEFI é unha BIOS gráfica, pois mentres que a BIOS é contorna texto e hai que utilizar teclado. UEFI admite imaxes e utilizar o rato.

Cambia o sistema de arranque BIOS-MBR, pois pode arrincar máis sistemas operativos de forma máis rápida e segura.

Que é GPT (Táboa de particións GUID)

GPT é un esquema novo para particionar un disco duro, máis eficiente que MBR.

As vantaxes de GPT sobre MBR son:

- Só hai particións primarias (non hai estendida nin lóxicas), pois nun disco particionado con GPT, pódense crear ata 128 particións primarias. (de feito, adóitase omitir a palabra primaria, pois non hai outro tipo de particións en GPT)
- Cada partición pode ter como tamaño máximo 256TB, con todo nun disco MBR, o tamaño máximo de cada partición é 2 TB.

GPT xa existe hai anos, pero empeza a ter sentido con UEFI. Pois as súas vantaxes non son compatibles cunha BIOS normal.

Regras UEFI-GPT

- Se poñemos un disco duro novo nun PC, antes de crear particións, hai que iniciar o disco e informar que tipo queremos. Na imaxe posterior, vese como ao iniciar un disco no Administrador de discos de Windows, debemos dicirlle se é MBR ou GPT.
- GPT non se admite en dispositivos extraíbles
- Só se poden instalar sistemas operativos de 64 bits.
- Un sistema operativo nun disco GPT, só pode traballar con UEFI, iso significa, que non podemos arrincar un PC cun disco baseado en GPT e instalado Windows 10, se ese PC traballa con BIOS.
- De aí, que pasará un tempo, ata que todos os discos duros estean particionados con esquema GPT, por compatibilidade con sistemas antigos.
- Na configuración de UEFI, hai unha opción para dicir que queremos traballar en modo compatibilidade BIOS-MBR, para iso, configuramos modo Legacy.
- Mentres que MBR ocupa 1 sector ao comezo do disco, GPT ocupa 34 sectores (LBA0 a LBA33)
- En discos MBR, só pódense crear discos básicos. En discos GPT, pódense crear discos dinámicos, que consisten en crear unha partición, utilizando máis dun disco, ou usando espazos non contiguos do disco.

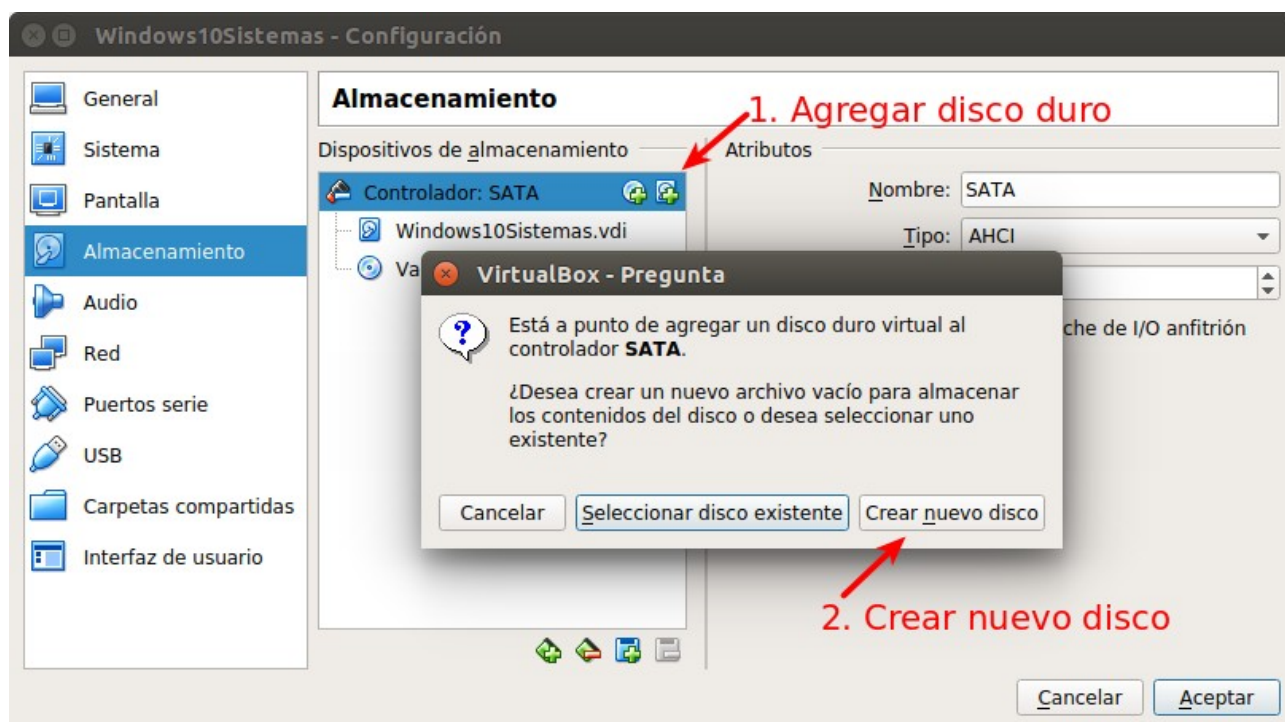
Exemplo:

Engadir un segundo disco novo de 10GB á máquina Windows10Sistemas. Co administrador de discos, iniciar o disco como MBR e crear 2 particións novas, unha de 3GB con formato NTFS e outra de 2GB con formato FAT32.

Pasos:

1. Engadir o segundo disco á máquina. Para iso, coa máquina apagada, ir a configuración de VirtualBox e almacenamento, e engadir disco duro, tal como móstrase na figura.

Ilustración de Engadir disco duro en VirtualBox.



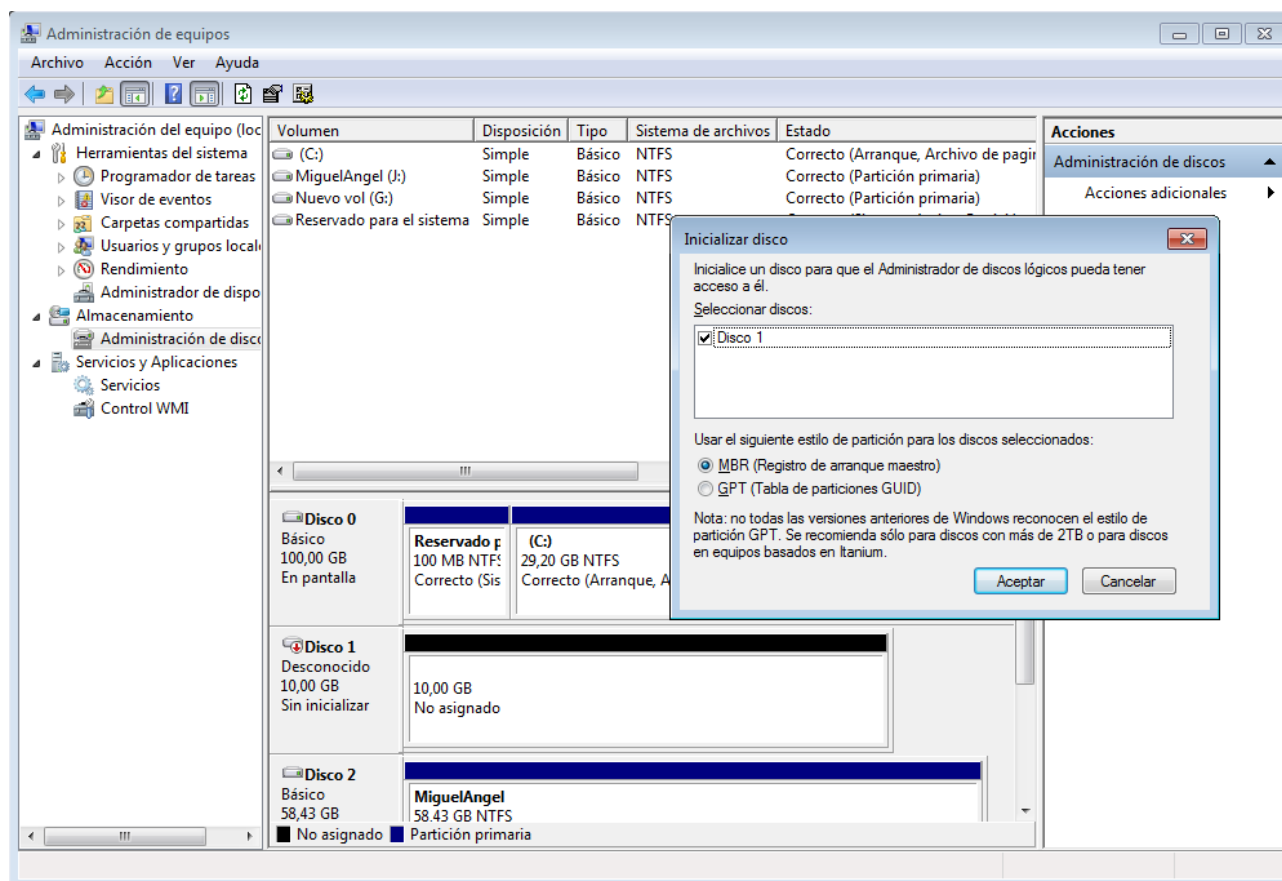
Miguel Ángel García Lara (CC BY-NC-SA)

Unha vez pulsado "Crear novo disco" seleccionar extensión .vdi, tamaño dinámico, 10GB e poñer como nomee "SegundoDisco"

2. Iniciamos Windows e o administrador de discos. Iniciamos o disco duro, para iso, menú contextual no nome do disco.

Aparece a imaxe seguinte, onde seleccionamos MBR.

Ilustración Iniciar disco duro en Windows.



Miguel Ángel García Lara (CC BY-NC-SA)

3. Pulsar menú contextual no disco duro para crear particións. Tal como fíxose no apartado 1 deste libro.

3.3.6 Sistemas de arquivos. Formato de particións

Nese apartado, referímonos a se unha partición ten formato FAT 32, NTFS. A isto chámase “Sistema de arquivos” ou “Tipo de formato”. Que non hai que confundir con “Tipo de partición” que sería se é unha partición primaria, lóxica...

Cando creamos unha partición, hai que formatala para podela utilizar. O formatar a partición, consiste en deixar unha táboa ao principio, para saber buscar os arquivos posteriormente.

Mínima unidade lóxica: a agrupación industrial ou unidade de asignación.

Lembrar que a mínima unidade física é o sector con 512 bytes.

A mínima unidade lóxica ten que ser igual ou máis grande que a mínima unidade física. Pois un software non poderá facer máis pequena o que é máis pequeno fisicamente.

A agrupación industrial ou unidade de asignación: é un conxunto contiguo de sectores (sectores seguidos) que compoñen a unidade lóxica máis pequena de almacenamento dun disco.

Os arquivos almacénanse nun ou máis agrupacións industriais, dependendo do seu tamaño; con todo, unha agrupación industrial non pode almacenar información de 2 arquivos distintos, se un arquivo ten un tamaño inferior a unha agrupación industrial, o espazo restante pérdese. De aí, que a agrupación industrial é a mínima unidade lóxica.

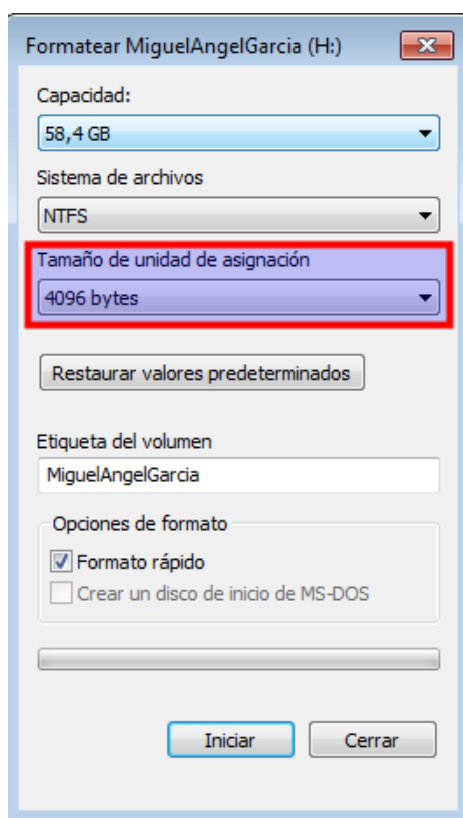
O tamaño dos agrupación industrial pode ser 1, 2, 4, 8, 16,...sectores (é dicir, potencia de 2); que se traduce en tamaños de 512 bytes, 1KB, 2KB, 4KB, 8KB,...

Exemplo: Abre en Windows o bloc de notas, e escribe “ola mundo”, como ten 10 letras en código ASCII estendido, ocupa 10 bytes (por iso é polo que moitas veces identifícase byte con carácter). Pulsa en menú contextual no nome do arquivo, e observa como di que ten 10 bytes, pero que en disco, ocupa moito máis. Case seguro que ocupa 4KB = 4096 bytes. É dicir, están a desaproveitarse 4086 bytes. (Hai 4086 bytes de fragmentación)

Estes 4KB, (ou o que vexas no teu caso), é o tamaño da unidade de asignación.

Cando formatamos unha partición, podemos decidir o tamaño da unidade de asignación. Aínda que normalmente non o tocamos.

Ilustración de Formato. Unidade de asignación.



Miguel Ángel García Lara (CC BY-NC-SA)

Pero entón, a pregunta sería, porque non crear a unidade de asignación con 1 só sector, 512 bytes, pois así, no exemplo anterior só perderíanse 502 bytes.

A resposta consiste na velocidade, pois se a unidade de asignación é moi pequena,

un arquivo está partido en máis unidades de asignación que se a unidade de asignación é grande. Pero ademais, estas unidades non teñen por que estar contiguas, o que significa, que para ler o arquivo habería que ir a moitos sitios distintos, perdendo moito tempo, en mover os cabezais a distintas partes.

De aí, que o tamaño ideal da unidade de asignación, é unha decisión de compromiso entre velocidade e fragmentación. Por tanto:

- Unha agrupación industrial pequena ten como vantaxe menor fragmentación e como desvantaxe, menor velocidade
- Unha agrupación industrial grande ten como vantaxe maior velocidade e como desvantaxe, maior fragmentación.

Na actualidade, ao formatar NTFS, o tamaño da agrupación industrial por defecto adoita ser 4KB. O tamaño da agrupación industrial depende do tamaño da partición e sistema de ficheiros que se utilice. [Ver seguinte ligazón de Microsoft](#).

Sistemas de arquivos (de Microsoft)

Os máis coñecidos son **FAT 16**, **FAT32** e **NTFS** en Windows e as distintas versións de ext2, **ext3** e **ext4** en Linux. Pero hai máis, por exemplo, HFS, reiserf, FreeBSD, MacOS, novell, iso9660, exFAT.

Cando formatamos unha partición, debemos seleccionar que sistema de arquivos ou ficheiros queremos utilizar.

O primeiro sistema de arquivos de Microsoft utilizado en MS-DOUS fué FAT 16, tamén coñecido simplemente por FAT. Fat significa File Allocate Table (Táboa de localización de ficheiros).

Ao formatar unha partición, escríbese unha táboa ao principio con tantas filas, como número de agrupación industrial que ten a partición. Nesa táboa, informárase que hai gardado en cada agrupación industrial. Esta táboa é o que se coñece como a táboa FAT.

A seguinte táboa mostra diferéncias-limitacións dos distintos sistemas de arquivos de Microsoft (en negrita as máis importantes):

Ilustración de Táboa sistema arquivos.

	Máximo tamaño fichero	Máximo tamaño partición	Límite Nombre Archivo
FAT 16	2 GB	2 GB	8 para el nombre y 3 para la extensión
FAT 32	4 GB	2 Terabytes	256 caracteres
exFat	2 Terabytes	2 Terabytes	
NTFS	256 Terabytes	256 Terabytes (*)	256 caracteres

(*) Este límite solo tiene sentido en discos con GPT, pues recordar que en MBR el máximo tamaño de una partición es 2 Terabytes.

Miguel Ángel García Lara ([CC BY-NC-SA](#))

Recomendacións sobre sistema de arquivos a utilizar:

- **Formato FAT16**

É o primeiro sistema de arquivos de Microsoft, coñecido tamén simplemente por FAT. Non se utiliza na actualidade, salvo para medios de almacenamento moi pequenos, antigos pendrives de menos de 2 GB.

- **Formato FAT 32**

É moi utilizado nos medios extraíbles: discos duros externos, tarxetas de memoria e pendrives. É o sistema máis compatible entre distintos sistemas operativos: Windows, Linux, Mac VOS e tamén con distintos aparellos: consolas, televisións. O seu límite máis importante, é o tamaño máximo dun ficheiro de 4 GB.

- **Formato exFAT**

O formato exFAT significa FAT 32 estendida. É un sistema de arquivos creado por Microsoft, para medios extraíbles. Pois ten como mellora sobre FAT32, o que se admiten arquivos maiores a 4GB. Utilízase principalmente para dispositivos externos.

- **Formato NTFS**

O formato utilizado hoxe día en practicamente todas as particións de discos duros de Windows.

NTFS, ten sobre FAT32, as principais vantaxes seguintes:

Mayor seguridade: Permisos nos arquivos distintos para cada usuario.

Esta é a diferenza máis importante, entre NTFS e FAT 32. Se unha partición é NTFS, pódense poñer permisos a cada arquivo segundo os usuarios. Con todo, se a partición é FAT 32, calquera usuario que teña acceso á partición, ten acceso a calquera ficheiro.

Máximo de ficheiro e partición moi superiores.

Mayor fiabilidade: unha partición NTFS, ten mecanismos para que en caso de erro, recupérense os arquivos noutra agrupación industrial, marcando esa agrupación industrial como inservible.



Que misión cumpre o MBR dun disco duro durante o arranque do computador?

- a) Contén a lista dos dispositivos nos que a BIOS busca sistemas operativos instalados.
- b) Cargar directamente o sistema operativo que se instalou no disco duro.
- c) Localizar a súa partición activa e dirixirse ao seu primeiro sector para facer que se execute o código alí almacenado.
- d) Define as características dos discos duros que poden ter sistemas operativos instalados e listos para o arranque.

3.4 Configuración de xestores de arranque

No epígrafe B falamos do arranque do PC co programa POST, que verifica que o hardware instalado funciona ben, dando paso a buscar a BIOS o dispositivo de arranque. Unha vez seleccionado o dispositivo de arranque, chégase ao sector MBR do disco duro, para ler cal é a partición activa. Desa forma, vaise á partición activa e le o primeiro sector desa partición, nese sector, ao instalar o sistema operativo haberá escrito o código necesario para continuar o arranque do equipo.

Nos novos equipos baseados en UEFI e con particionado GPT, modificouse o proceso de arranque, de forma que cando se acende o equipo a CPU executa o firmware inicial da máquina, cuxa misión é configurar e inicializar os dispositivos, para a continuación, ceder o control aos "servizos de arranque de UEFI" para que localicen no disco duro de inicio un xestor de arranque ou un cargador de sistema, que carguen o sistema operativo en memoria e finalmente transfíranlle o control.

3.4.1 Estudo do arranque de Windows 10

Microsoft efectuó algúns cambios no proceso de inicio desde o sistema operativo Windows 7, de forma que ao instalar créase unha partición de forma automática. Esta partición chámase “Reservado para o sistema”. Inicialmente, tiña un tamaño de 100MB en Windows 7, sendo de 550MB en Windows 10. Esta partición permite algunhas utilidades de recuperación e de seguridade como Bitlocker.

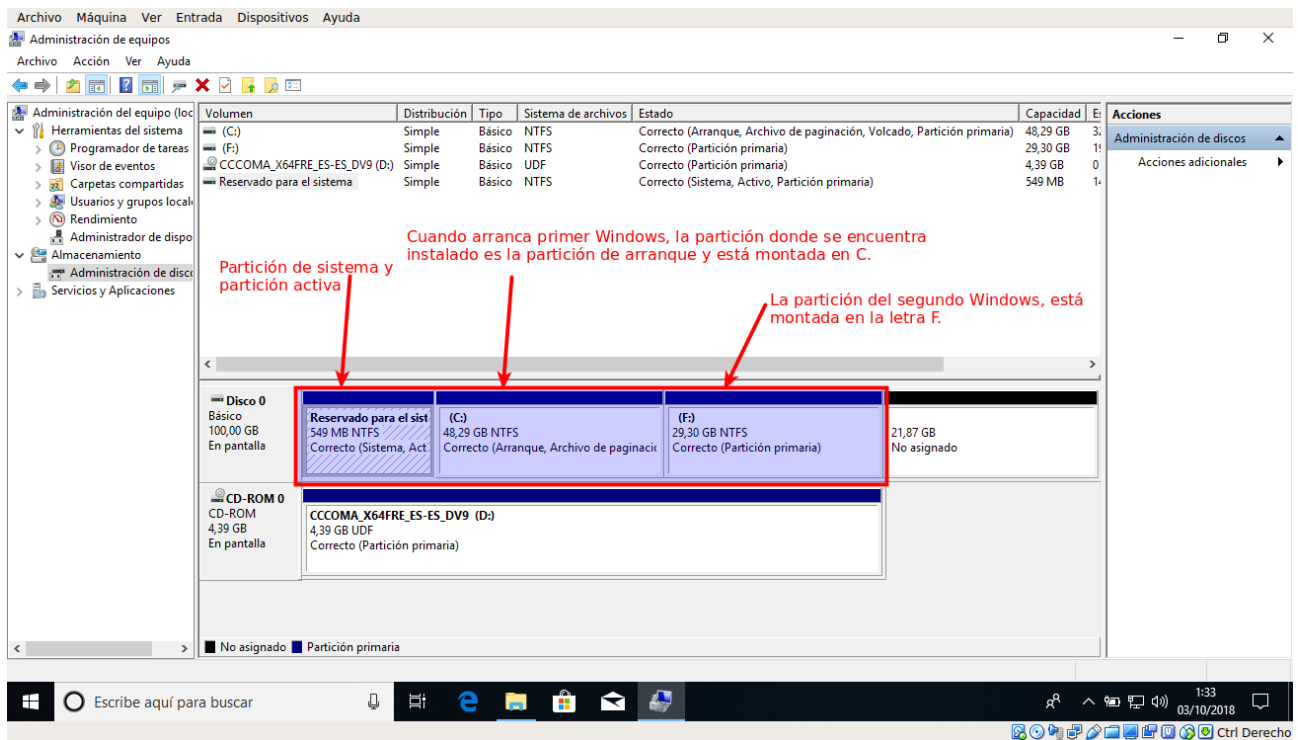
Esta partición, é a partición activa e chámasele partición de sistema, dentro pon unha serie de arquivos relacionados co hardware propio da máquina e o cartafol cos ficheiros coa configuración que o xestor de arranque de Windows necesita para iniciar o sistema operativo Windows, permitindo así a configuración de arranque dual.

Windows protexe a esta partición de forma especial. Non lle asigna letra de unidade, para o usuario é coma se non existise, pois como vimos non aparece no “Explorador de Windows”, aínda que si será recoñecida en “Administración de discos”.

Soamente pode existir unha partición de sistema por equipo, aínda mesmo habendo varias instalacións de Windows nel. Isto é así porque unha vez creada a partición de sistema, as seguintes instalacións, recoñécena e actualizan o contido dos ficheiros para incluírse como novas opcións no menú de arranque dos sistemas operativos.

Para entendela mellor, a continuación móstranse 2 capturas, a primeira delas co primeiro Windows iniciado:

Ilustración de Iniciado primeiro Windows.

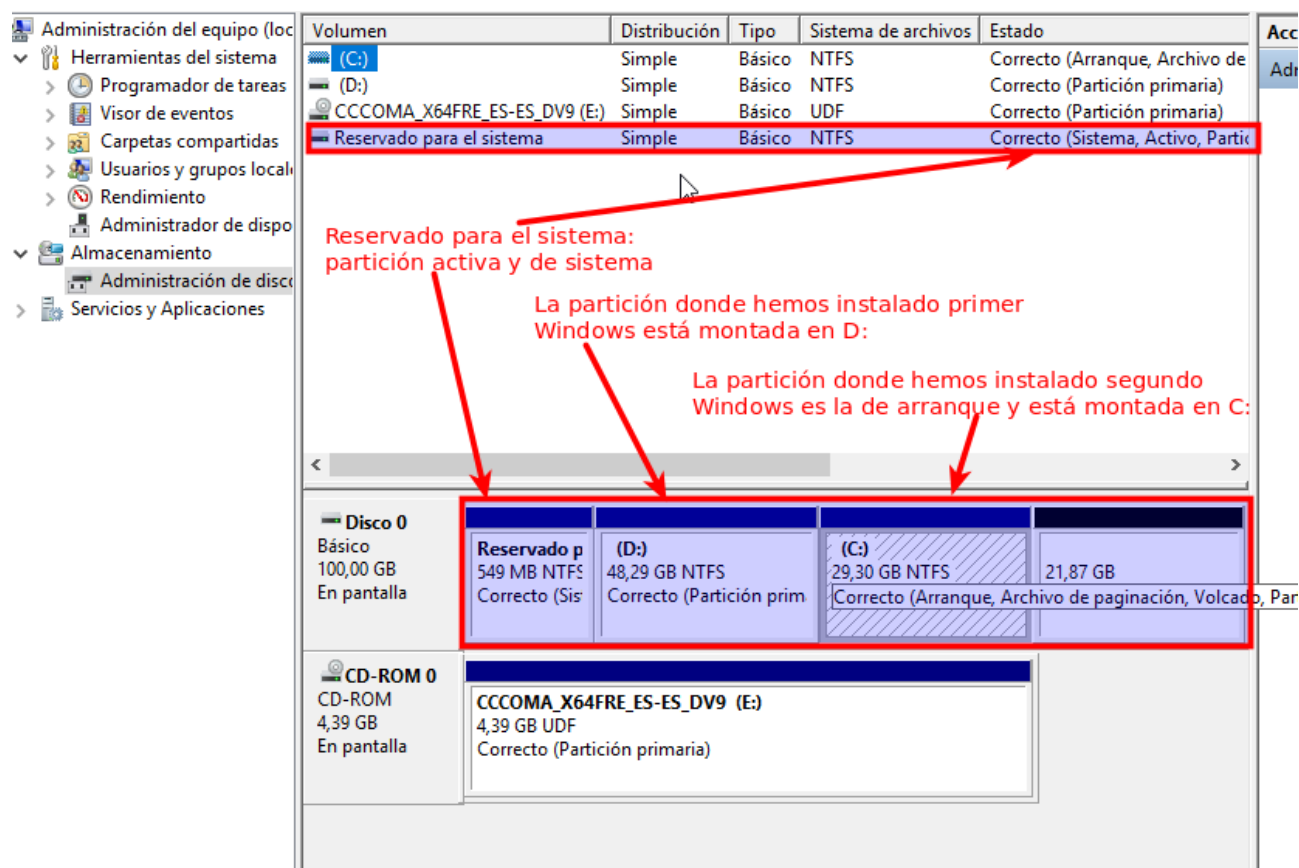


Miguel Ángel García Lara

Nesta imaxe, a partición “Reservado para o sistema” é tanto a partición activa como a partición de sistema, é dicir onde están os arquivos para cargar o sistema operativo. Con todo, a partición de arranque, é a partición onde instalamos o primeiro Windows de 50GB. A partición onde instalamos o segundo Windows, está montada na letra F, e neste caso, simplemente é unha partición de Datos.

Vexamos a captura, cando reiniciamos o equipo, co segundo Windows.

Ilustración Iniciado segundo Windows.



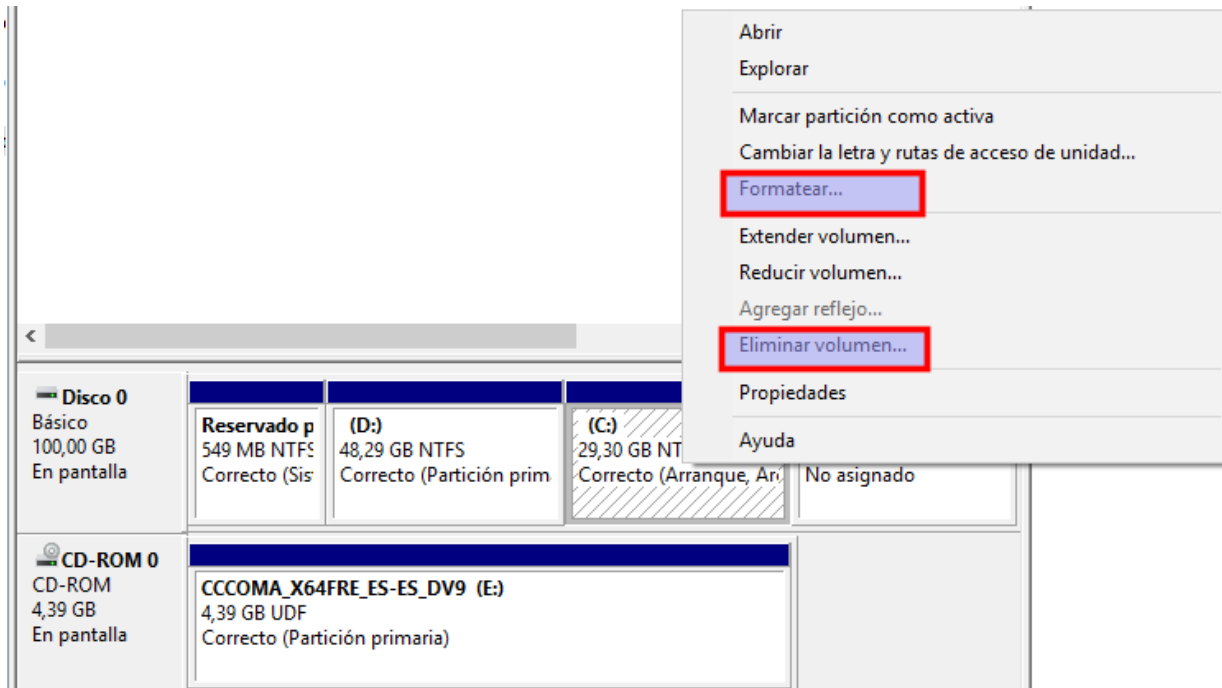
Miguel Ángel García Lara (CC BY-NC-SA)

A partición “Reservado para o sistema” segue sendo a partición activa e de sistema. Agora a partición de arranque, é onde instalamos o segundo Windows de 30GB, que corresponde coa letra C. A partición do primeiro Windows, está montada na letra D, como partición de Datos.

Por que dicimos que esta partición é de Datos?, ao non ser nin de sistema, nin de arranque, simplemente ten datos. De feito, poderíamos formatala ou eliminala. Con todo a partición C non se deixa eliminar, pois é o sistema que temos arrincado.

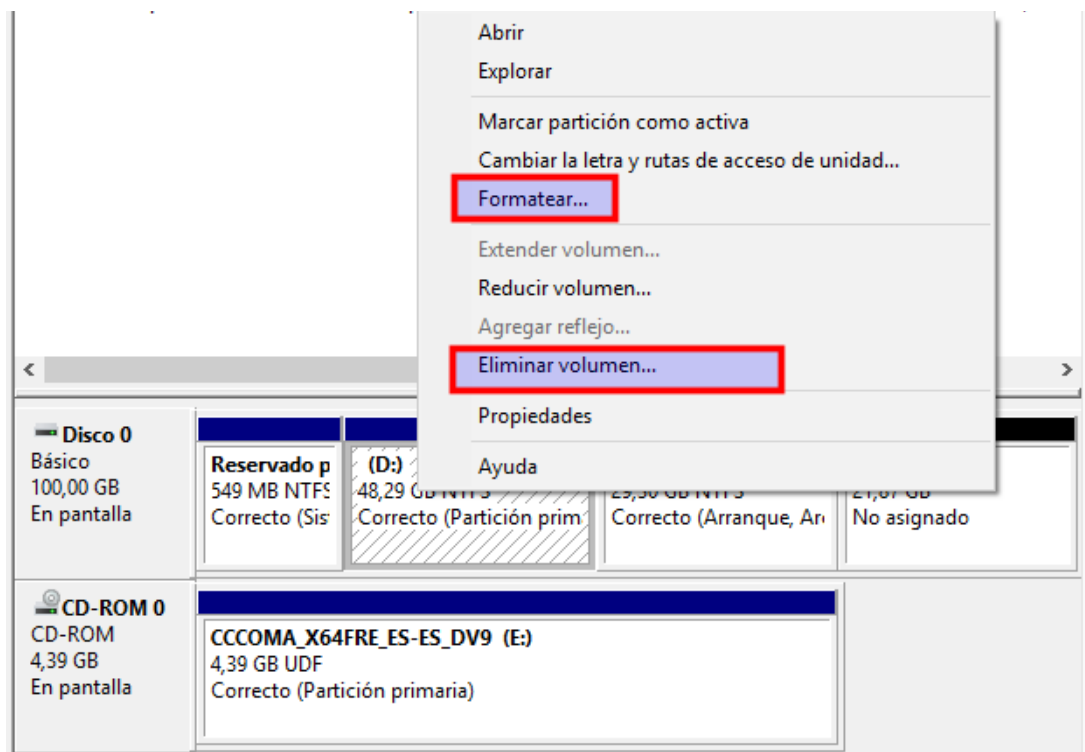
Móstranse capturas de como na partición C, non están habilitados formatar e eliminar, e con todo na partición D, se están habilitadas ambas as opcións.

Ilustración Deshabilitado formatar C:



Miguel Ángel García Lara (CC BY-NC-SA)

Ilustración Habilitado formatar D:



Miguel Ángel García Lara (CC BY-NC-SA)

3.4.2 Configuración do xestor de arranque bcd (Boot Configuration Data)

A forma de iniciar Windows, cambiou desde Windows Vista.

Unha vez, que se le o sector MBR, e diríxese á partición activa, o primeiro arquivo que se executa na partición de sistema é o bootmgr. Este arquivo encárgase de ler o ficheiro bcd.log que é o propio xestor de arranque, onde se atopan as entradas dos sistemas operativos a arrincar. Se en bcd.log hai máis dunha entrada, mostra o xestor en pantalla, para que o usuario decida o sistema operativo a iniciar. Se bcd.log só ten unha entrada, non se mostra o xestor en pantalla e segue o inicio co ficheiro winload.exe

Habemos visto que ao instalar o segundo Windows, o propio xestor de arranque deixa cambiar a opción por defecto do sistema operativo a iniciar, como o tempo que se deixa ao usuario para seleccionar sistema.

Pero Windows incorpora un programa moito máis completo para editar o arquivo bcd.log. Este programa chámase bcdedit.

Programa bcdedit

O programa bcdedit inclúe opcións que permiten eliminar, editar ou agregar entradas ao menú de arranque. Mesmo se pode configurar para conseguir que arrinquen sistemas operativos tipo GNU/Linux que usan métodos de inicio diferentes.

Tamén nos pode interesar cambiar a descrición. Por exemplo, supoñamos que o motivo polo que queremos ter 2 Windows 10 nunha aula, sexa porque hai quenda de mañá e quenda de tarde, e queremos que os alumnos utilicen Windows distintos. Nese caso, a descrición por defecto, “volume 3” e “volume 2” é pouco clara. Interesaranos cambiar a descrición, e poñer, por exemplo: “Quenda de mañá” e “Quenda de tarde”.

O programa bcdedit execútase en modo comando e como administrador. Para iso, escribir cmd e en menú contextual, seleccionar “executar como administrador”

Para ver información sobre as opcións admitidas por bcdedit, executamos: bcdedit.exe /?

Outros xestores de arranque

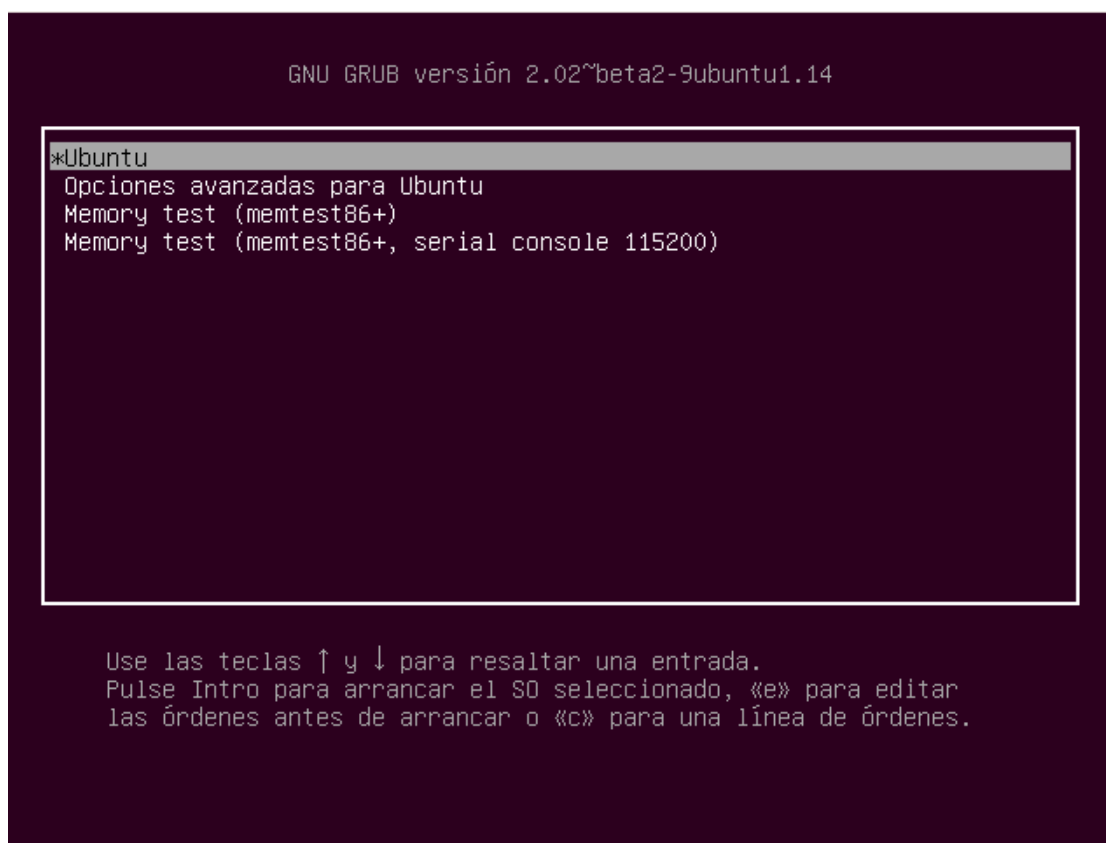
Tamén hai algunha utilidade gráfica coas posibilidades de engadir particións a bcd.log. Un programa para este fin é easybcd. Esta ferramenta non é de Microsoft. A utilidade easybcd é gratuíta.

Outros sistemas operativos teñen os seus propios sistemas de arranque.

GNU-Linux utiliza como xestor de arranque o xestor grub. Este xestor si recoñece as particións de Windows sen configuración adicional, por ese motivo, se nun computador, instalamos tanto Windows como Linux, instalamos Windows primeiro, pois ao instalar Linux, Linux escribirá o xestor grub, coas entradas tanto de Windows como Linux.

Na imaxe, móstrase o aspecto do xestor grub nun PC con Linux.

Ilustración Xestor grub de GNU-Linux.



Miguel Ángel García Lara (CC BY-NC-SA)

Observacións importantes:

- Débense instalar os sistemas operativos Microsoft por orde de antigüidade, primeiro o máis antigo e despois o máis recente. De non facelo así, non funcionará o arranque dual; aínda que se instalen de forma independente en particións distintas. O motivo, é que habemos visto que ao realizar a segunda instalación, se sobrescriben arquivos na partición “Reservado para o sistema”. Se por exemplo, instalamos primeiro Windows 10, e logo Windows 7. ficheiros de Windows 7 sobrescriben os de Windows 10. Ao ser máis antigos os de Windows 7, non poden iniciar Windows 10.
- Por defecto, o xestor de arranque de Windows só recoñece sistemas Microsoft, por tanto se queremos ter instalado no mesmo equipos Windows e GNU-Linux, debemos instalar primeiro Windows. Pois o xestor de arranque de Linux, xestor “grub” si que recoñece Windows, dando a posibilidade de iniciar Windows ou Linux.
- Estas recomendacións, fará que funcione todo ben á primeira. Senón, hai solucións, pero dedicaremos bastante tempo a resolvelas. Teremos que reinstalar grub ou bcd.log, e mesmo escribir novos ficheiros de sistema.



Indica as certas sobre particionamento GPT

- a) Só pódense instalar sistemas operativos de 64 bits nun disco duro con GPT
- b) O tamaño máximo dunha partición GPT son 2 Terabytes
- c) Pódese instalar un sistema operativo nun disco con particionamento GPT en todos os equipos
- d) Un disco GPT NON pode ter 128 particións primarias

3.5 Terminal de comandos de Windows

Moitas veces creamos cartafol, movemos, copiamos, eliminamos arquivos e cartafol, renomeamos...

Todas estas opcións, realizámoas de forma gráfica en Windows co programa "Explorador de Windows". Pero tamén as podemos realizar con interface de texto na terminal de Windows.

3.5.1 Comandos básicos

Para abrir a terminal, hai 2 formas: En "Sistema de Windows" abrir "Símbolo de sistema" ou executar "cmd". En bastantes casos, necesitaremos ser administrador. Para iso, pulsar en menú contextual de "Símbolo de sistema" e pulsar "Executar como administrador".

Directorios (Cartafol en Windows)

Un directorio ou cartafol, non é máis que unha zona reservada para almacenar ficheiros. Dentro de cada partición, atópase o directorio raíz recoñecido por unha letra. Por exemplo C:\

Este directorio conterá arquivos e outros subdirectorios, onde cada subdirectorio, á súa vez, poderá conter arquivos e subdirectorios.

Unidades de disco e árbores de directorios

Hai que diferenciar a unidade física ou real, así habemos visto que un disco duro (unidade física) pode conter 3 particións (unidades lóxicas), chamadas c: d: e:

Nunha árbore de directorios, hai unha raíz (a unidade c) coas súas ramas (directorios e subdirectorios) e follas (ficheiros)

Cada unidade representa unha única árbore, de forma que en Windows hai tantas árbores como unidades lóxicas.

Roteiro dun arquivo

O arquivo axuda.hlp dentro do directorio Windows en C, denótase co seu roteiro completo da forma:

C:\Windows\axuda.hlp

O prompt do sistema

Cando se abre a terminal, aparece o prompt do sistema. No prompt aparece o roteiro na que nos atopamos:

C:\Windows\system32>

O prompt espera a que se introduza unha orde e púlsese intro para que se execute. Cando finaliza a execución, devólvese o prompt. Mentres que non se devolva o prompt a termínaa, é que non terminou a execución do comando.

Sintaxe dos comandos

As ordes estarán formadas por:

1.- Nome do comando.

2.- Parámetros. O roteiro onde se executa o comando. Hai comandos, que non é necesaria o roteiro. Por iso dise que os parámetros son opcionais.

3.- Opcións ou modificadores. Tamén opcionais, indícanos como queremos que se execute a orde.

Exemplo: C:\> DIR C:\DOUS\ /p

O comando dir (comando que lista os arquivos) contidos no directorio dous do disco duro C (parámetros), e farao pantalla a pantalla (opción p).

Execución de ficheiros

Os ficheiros executables son os que teñen a extensión exe, com ou bat. Un ficheiro execútase co seu roteiro e nome. Non é necesario ningún comando.

Exemplos:

C:\> C:\windows\system32\calc.exe Abre a calculadora de Windows

C:\> "C:\Program Files\Microsoft Office\Office14\winword.exe" Abre Word

Observar, que cando un roteiro ten espazos, ponse entre comiñas. (En segundo exemplo)

Maiúsculas e acentos

En Windows non se diferencian maiúsculas e minúsculas. É dicir, no mesmo directorio non poden existir practica1.docx e Practica1.docx

Pero se se poden utilizar acentos, de forma que se poden existir á vez práctica1.doc e practica1.doc

Axuda de comandos

O comando help mostra na terminal todos os comandos que se poden executar.

Para solicitar a axuda dun comando, hai 2 posibilidades: Utilizar /? e help.

Por exemplo, a axuda do comando dir obtémola de 2 formas:

dir /?

help dir

Na axuda, móstranse os distintos modificadores que se poden utilizar. Normalmente a opción help adoita mostrar unha axuda máis completa que /

Exemplo. Se solicitamos a axuda do comando ATTRIB, devólvese a información seguinte:

C:\Users>attrib /?

Mostra ou cambia os atributos dun arquivo.

ATTRIB [+R | -R] [+A | -A] [+S | -S] [+H | -H] [+I | -I][unidade:][roteiro][nombreDeArchivo]
[/S [/D] [/L]

Interpretación da axuda: Símbolos “[“ e “]”

Os corchetes [], significan que o roteiro ou os modificadores son opcionais. Por exemplo, pódese executar:

ATTRIB +A +S C:\cartafol\arquivo Cambia os atributos A e S ao arquivo

ATTRIB /S→ Mostra os atributos no directorio actual con información das súas subdirectorios.

O símbolo | representa unha “ou”, é dicir unha opción. Por exemplo,

Son válidos:

ATTRIB +R +S

ATTRIB +R -H

Pero non é válido:

ATTRIB +R -R

Primeiros comandos

BOTO Mensaxe

Repite en pantalla a mensaxe

CLS

Serve para limpar a pantalla (CLS= Clear screen)

VER

Serve para ver a versión de Windows que estamos a utilizar

DÁCHE [dd-mm-aa | T]

Sen modificadores, mostra a data actual e pregunta a nova

DÁCHE dd-mm-aa modifica a data directamente

DÁCHE /T mostra a data e devolve o prompt directamente

TIME [hh:mm | T]

Igual que DÁCHE, pero para a hora.

LABEL [unidade:]

Permite crear a etiqueta a unha partición. É interesante que as particións teñan etiqueta, pois axuda a recoñecelas. Por exemplo, un pendrive perdido que teña como etiqueta o nome do dono, facilita a devolución.

MORE

Utilízase cando o resultado dunha orde non vaia a coller na pantalla.

Exemplo: Mostrar a axuda do comando prompt

Executar o comando prompt /?

Ao executar prompt /? mostra a axuda completa, e devolve o prompt. Temos que subir e baixar a barra de desprazamento para ler a axuda.

Executar agora prompt /? | more

Aquí o signo | ten un significado distinto ao de modificador opcional. Aquí funciona como tubaxe. O resultado de prompt / ? no canto de sacalo na pantalla, metémolo nunha tubaxe e filtrámolo con more (aos poucos)

Móstranos só a primeira pantalla. Para que nos mostre as seguintes pantallas, pulsamos Intro.

Comandos para particións

FORMAT [Unidade:] [/FS:sistArch]

Exemplo: formatar a partición D con sistema de ficheiros NTFS: C:\> format d: /fs:ntfs

DEFRAG unidade:

O desfragmentador de Windows, o que fai, é reorganizar os arquivos en clusters contiguos, de forma que se gañe velocidade por poder facer a lectura de forma contigua. Nos pendrive e discos SSD, pola súa optimización en lectura aleatoria, non é necesario desfragmentar a unidade.

Exemplo: Desfragmentar a partición montada na letra D: C:\> defrag D:

CHKDSK [Unidade:] [/F]

Chkdsk significa Check Disk (Comprobar disco)

Dá unha información completa do disco duro en canto a número de unidades de asignacións libres, ocupadas e defectuosas. Busca erros. Por defecto, o seu modo é lectura, é dicir busca erros pero non os corrixe.

/F → Se atopa erros repáraos. Garda os arquivos con erros nun cartafol chamado found000. É curioso, que este cartafol non é fácil ver o seu contido en Windows, e con Linux si.

É un comando moi importante, para tentar reparar particións. Se un equipo apágase mal, ao iniciar o PC execútase de forma automática. Así mesmo, en dispositivos extraíbles, cando os extraemos mal, soluciónanos bastantes erros.

Exemplo: Buscar erros e reparar na unidade E. Executar: **chkdsk /F e:**

3.5.2 Comandos para directorios e ficheiros

3.5.2.1 Estrutura na unidade C

Unha vez instalado Windows, hai 3 cartafoles principais no raíz de C. Estes cartafoles representan:

- Windows: Nela están todos os arquivos da instalación de Windows, con todos os executables de Windows.
- Program Files; (Arquivos de programa): Cartafol onde se instalan por defecto os programas de usuario.
- Users: cartafoles de todos os usuarios. Para cada usuario, créase un cartafol co seu nome dentro. De forma que o roteiro do cartafol de Juan en C:\Users\Juan

Á vez, en cada directorio dun usuario créanse varios subdirectorios: Desktop (Escritorio), Documents (Documentos), Downloads (Descargas), pictures (Imaxes), Music (Música)...

3.5.2.2 Roteiros absolutos e relativos

Directorio actual e directorio pai

En calquera directorio, sempre hai 2 directorios anotados por . e ..

“.” representa ao directorio actual

“..” representa sempre ao directorio pai

Traxectoria ou roteiro absoluta dun arquivo

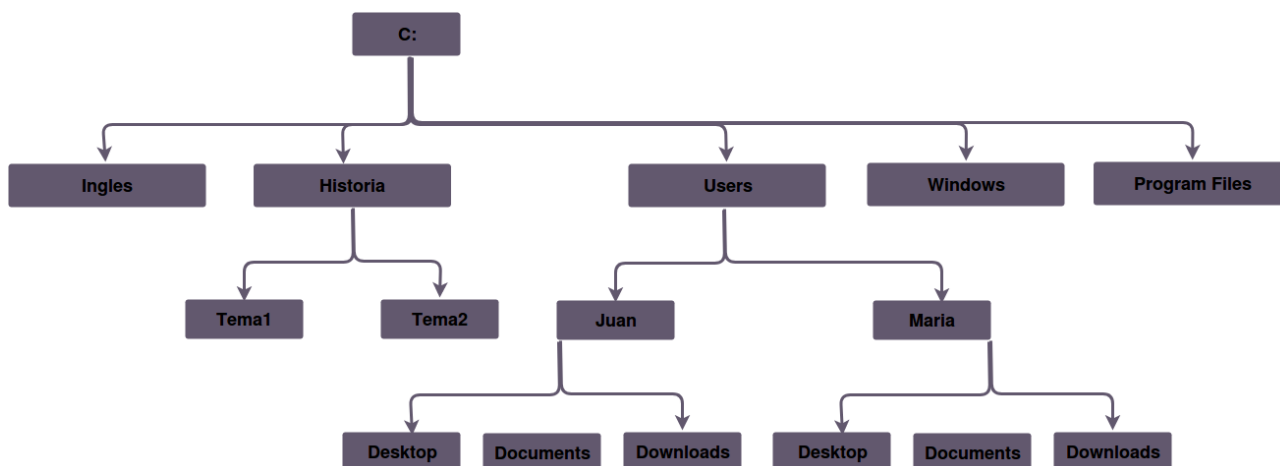
Traxectoria absoluta: é a que sempre empeza desde a raíz. De aí, que se chame absoluta, dará o mesmo onde esteamos, que sempre se escribirá igual.

Traxectoria ou roteiro relativa dun arquivo

Traxectoria relativa: é a que empeza a partir do lugar onde estamos situados. Escribirase de forma distinta, segundo onde esteamos.

Para ver algúns exemplos, inclúese unha imaxe onde se mostran os 3 cartafoles principais que colgan de C con 2 usuarios, Juan e María. Tamén se crearon en C, 2 cartafoles chamados Liguas e Historia.

Ilustración Estrutura de arquivos en C.



Miguel Ángel García Lara ([CC BY-NC-SA](#))

Exemplos:

1. Supoñamos que estamos no directorio Tema2, e queremos saber o que hai no directorio Linguas. Utilizando o comando dir, devolve o que hai nun directorio.

Se utilizamos roteiro absoluto: C:\Historia\Tema2> dir c:\Linguas

Se utilizamos roteiro relativo: C:\Historia\Tema2> dir ../../Linguas

(Temos que subir 2 veces para chegar ao directorio común que é a raíz C)

2. Supoñamos que seguimos querendo saber o que hai no directorio Linguas, pero que agora estamos no directorio Windows.

Se utilizamos roteiro absoluto: C:\Windows> dir c:\Linguas

Se utilizamos roteiro relativo: C:\Windows> dir ../Linguas

(Temos que subir 1 vez para chegar ao directorio común que é a raíz C)

3. Supoñamos que estamos no Escritorio de Juan e queremos ver que hai en Documentos de Maria.

Se utilizamos roteiro absoluto: C:\Users\Juan\Desktop> dir c:\Users\Maria\Documents

Se utilizamos roteiro relativo: C:\Users\Juan\Desktop> dir ../../Maria/Documents

(Temos que subir 2 veces para chegar ao directorio común que é Users)

4. Supoñamos que estamos no Escritorio de Juan e queremos ver que hai en Tema2 de Historia.

Se utilizamos roteiro absoluto: C:\Users\Juan\Desktop> dir c:\Historia\Tema2

Se utilizamos roteiro relativo: C:\Users\Juan\Desktop> dir ../../..Historia/Tema2

(Temos que subir 3 veces para chegar ao directorio común que é a raíz C)

3.5.2.3 *Comandos para directorios*

CD [nome do directorio]

Serve para cambiar de directorio activo. Cd significa “change directory.

2 opcións que se utilizan moito son:

cd .. Cambia ao seu directorio pai.

cd \ Cambia ao directorio raíz

DIR [unidade:] [/s] [/p]

Visualiza os directorios e ficheiros que contén o directorio solicitado.

Mostra un só nivel de profundidade no sistema de ficheiros.

O modificador /s serve para visualizar tamén a información dos subdirectorios.

O modificador /p realiza unha pausa cada vez que se enche a pantalla.

Hai moitos máis modificadores neste comando. Lembrar utilizar a axuda para ver todas as opcións.

MKDIR nome do directorio

O comando mkdir serve para crear un directorio novo. Pódese utilizar mkdir ou md. O seu nome vén de “make directory”

RMDIR nome do directorio [/s] [/q]

O comando rmdir sive para borrar un directorio. Pódese utilizar rmdir ou rm. O seu nome vén de remove directory.

Por defecto, o directorio ten que estar baleiro.

A opción /s serve para borrar o directorio aínda que non estea baleiro, con todos os seus subdirectorios.

A opción /q serve para borrar de forma silenciosa, é dicir, sen pedir confirmación en cada arquivo.

XCOPY [/E] orixe destino

Serve para copiar un directorio con todos os seus ficheiros.

A opción /E copia todos os subdirectorios, incluso os baleiros. É dicir, realiza unha copia idéntica dun directorio.

Exemplo completo:

C:\Windows\system32> dir ..\setup Se lista o directorio setup que está dentro de Windows, con roteiro relativo

C:\Windows\system32> cd ..\..\Users Cambia ao directorio Users con roteiro relativo

C:\Users> mkdir C:\Users\Garcia\cartafol Crea cartafol no directorio do usuario Garcia con roteiro absoluto

C:\Users> rmdir /S /Q Garcia\cartafol Elimina o cartafol creado antes con roteiro relativo

C:\Users> dir C:\Users\Garcia\Desktop Se lista o escritorio do usuario Garcia con roteiro absoluto

C:\Users> xcopy /e Garcia C:\copiaAlumno Crea unha copia idéntica do directorio do usuario Garcia gardándoa no raíz de C. Utilizouse roteiro relativo na orixe e roteiro absoluta no destino.

3.5.2.4 Comandos para ficheiros

COPY orixe destino

Serve para copiar ficheiros. Non copian subdirectorios, polo que utilizaremos copy cando copiemos só ficheiros e xcopy cando copiemos directorios.

DO[roteiro] [/S]

Serve para borrar ficheiros. Vén de DELETE.

O modificador /S serve para borrar os ficheiros dos subdirectorios. En ningún caso do borra cartafoles.

Utilizaremos do cando borremos só ficheiros e rd cando borremos subdirectorios.

Exemplo:

C:\> DO /s c:\users\Garcia*.docx Borra todos os ficheiros de word que hai dentro do directorio do usuario Garcia, incluso subdirectorios. Utilizouse roteiro absoluto.

REN [camiño]nombreAntiguo nombreNuevo

Serve para renombrar un ficheiro pero no mesmo directorio. Polo que en destino, só ponse o nombreNuevo (sen roteiro)

Exemplo: C:\> REN C:\users\Garcia\Jose.txt Jaime.txt Cambia o nome do arquivo Jose.txt a Jaime.txt no directorio do usuario Garcia.

MOVE camiño_orixe camiño_destino

Serve para mover o ficheiro dun directorio a outro, mesmo podemos cambiar o nome. (Equivale gráficamente no explorador para cortar e pegar, e renombrar)

TYPE ficheiro

Mostra en pantalla o contido dun ficheiro de texto plano, sen abrir o bloc de notas ou notepad.

Os arquivos de texto plano, son os que teñen a extensión txt e chámanse planos, porque non admiten formato (non admiten distintos tipos de letra, nin negrita, tamaños de papel...)

Como crear un ficheiro de texto en terminal?

Utilízase que a terminal é coma se fose o arquivo con

Executamos copy con nombreFichero despois escribimos texto, e cando acabemos, pulsamos "Ctrl+Z" e enter.

Exemplo completo

C:\Windows\system32> cd ..\..\Users\Garcia\cartafo1 Cámbiase a cartafo1 do usuario Garcia con roteiro relativo (cartafo1 creouse en anterior exemplo)

C:\Users\Garcia\cartafo1> copy con arquivo1.txt

este é o contido de arquivo1.txt "Ctrl+Z" e "Intro" Créase arquivo1.txt con ese contido

C:\Users\Garcia\cartafo1> cd .. Cámbiase ao directorio pai, é dicir ao directorio do usuario Garcia

C:\Users\Garcia> type cartafo1\arquivo1.txt Mostra por pantalla o contido de arquivo1.txt con roteiro relativo

C:\Users\Garcia> copy cartafo1\arquivo1.txt cartafo1\arquivo2.dat Créase unha copia de arquivo1.txt, co nome arquivo2.dat na mesma cartafo1, utilizando roteiro relativo en orixe e en destino.

C:\Users\Garcia> ren cartafo1\arquivo2.dat arquivo2.txt Se renombra arquivo2.dat a arquivo2.txt, fixarse que só se utilizou roteiro na orixe.

C:\Users\Garcia> move apuntamentos.docx cartafo1\apuntes.docx Móvese o arquivo apuntes.docx (supúxose que existía o arquivo apuntes.docx) de cartafo1 do usuario ao directorio "cartafo1"

C:\Users\Garcia> dir cartafo1 Ao executar dir, debe devolver 3 arquivos listados, 2 arquivos .txt e 1 arquivo .dat

C:\Users\Garcia> do C:\users\Garcia\cartafo1*.txt Bórrase todos os arquivos txt de cartafo1 con roteiro absoluto

ATRIBUTOS DE ARQUIVOS. Comando attrib

ATTRIB [/S] [camiño e nome] [+R | - R] [+H | - H] [+S | - S] [+A | - A]

Serve para ver ou modificar os atributos dun ficheiro ou directorio

Se executamos attrib sen opcións, móstranos todos os atributos que teñen os arquivos do directorio.

A opción /S serve para mostrar tamén os atributos de todos os arquivos, incluídos dos subdirectorios.

Os signos + son para poñer ese novo atributo.

Os signos – son para quitálos.

Cales son os atributos e o seu significado?

R (Read=lectura) Son arquivos que se abren de só lectura, sen poderse modificar.

H (hidden=oculto) Son os arquivos ocultos

S (system=sistema) Son os arquivos de sistema.

A (arquivos) Arquivos de lectura e escritura, os normais.

Por defecto, en explorador de Windows, os arquivos ocultos e arquivos de sistema non ven. Para velos, hai que ir segundo Windows a Organizar/Opcións, Ferramentas/Opcións ou Ver/Opcións.

Calquera arquivo de lectura ou oculto ou de sistema, non se pode borrar. Para borrarlo hai que quitarlle ese atributo.

Exemplo de utilización de attrib:

C:\> attrib Mostra todos os arquivos cos seus atributos en C

A SH C:\pagefile.sys

A SH C:\swapfile.sys

C:\> attrib /S Mostra todos os arquivos da árbore C cos seus atributos (árbore significa que inclúe a información de todos os subdirectorios, é dicir de todas as ramas da árbore). A listaxe é moi longo, para terminar o proceso antes de tempo, pulsar Ctrl + C

C:\> attrib /S | more Igual, pero parando páxina a páxina. Para seguir pulsar intro ou espaciador. Terminar o proceso cando se queira con Ctrl+C

C:\> attrib +R proba.txt Pon ao arquivo proba.txt o atributo de lectura. Se se abre e edita co bloc de notas, non se poden gardar os cambios.

C:\> do proba.txt Non nos deixa borrar. Di acceso denegado

C:\> attrib +H proba.txt Ao poñelo oculto, cando listemos con dir, non se ve o arquivo

C:\> attrib -R +H +S proba.txt Quítaselle o atributo de lectura. Poñémoslle oculto e sistema. Con dir non se verá, pero o arquivo pódese modificar. Iso si, non se poderá borrar.

3.5.3 Direccionamiento e tubaxes

3.5.3.1 Operadores de direccionamiento de saída

Operador de saída >

Por defecto, a saída estándar dos comandos é a mesma terminal. Co operador > direccionamos a saída a outro sitio. Desta forma, podemos gardar nun arquivo o resultado dun comando. Se o arquivo xa existía, se sobrescribe.

Exemplos

C:\> dir /S C:\users > arquivo.txt Garda en C:\arquivo.txt a listaxe de arquivos e subdirectorios de todos os usuarios

C:\> dáche /t > windows\arquivo.txt Garda a data de hoxe en C:\windows\arquivo.txt

C:\> boto ola > arquivo.txt Garda en C:\arquivo.txt a palabra ola

C:\> dir /S > C:\users\Garcia\listadoC.txt Con este comando sinxelo, vese a potencia da terminal. Gardamos unha listaxe completa de todo a árbore C no arquivo listado.txt. Faltaría que aparecesen os arquivos ocultos e de sistemas, pero para iso hai opcións en dir

C:\> type arquivo.txt > arquivo2.txt Garda en arquivo2.txt o contido de arquivo.txt

Operador de saída >>

O operador >> tamén direcciona a saída do mesmo xeito que o operador >

A diferenza, é que ao direccionar a un arquivo, a nova información engádese ao contido que xa tiña o arquivo

Exemplo

Gardar nun arquivo novo, a data, hora e unha listaxe completa de todos os directorios e ficheiros que hai na unidade C: (Aquí, cun exemplo sinxelo, móstrase a potencia da terminal)

Para este exemplo, hai que executar 3 comandos. No primeiro, utilízase >, para sobrescribir o ficheiro Listado.txt se existía e nos seguintes >> para engadir, sen borrar o anterior. Inclúese un boto para que o arquivo quede máis organizado.

C:\> dáche /T > Listado.txt

C:\> estafe /T >> Listado.txt

C:\> boto Listaxe completa de arquivos e directorios >> Listado.txt

C:\> dir /S >> Listado.txt

Unha vez executadas estas 4 liñas, Listaxe.txt pódese abrir co bloc de notas, e verase a listaxe completa da árbore C.

Tubaxes e filtros; more, sort e find

CONCEPTO; A información de saída por defecto dun comando é a pantalla. Esta información, no canto de sacala na pantalla, introdúcese nunha tubaxe e fíltrase con outro comando para realizar outra operación: ordenar, buscar...

O operador utilizado para encadear ordénelas é | (Teclas AltGr+1)

Nas tubaxes adóitanse utilizar os comandos ou filtros: more, sort e find

MORE

A información de saída dun comando, filtrámola pantalla a pantalla, grazas a MORE.

Exemplos:

C:\> type Listado.txt | more Visualiza o contido de Listaxe.txt creado no exemplo de direccionamiento, pantalla a pantalla.

C:\> attrib /s | more Mostra todos os arquivos cos seus atributos da árbore C, pero pantalla a pantalla

SORT [/R] [/+número]

Serve para ordenar un conxunto de filas. A ordenación por defecto é ascendente e co primeiro carácter de cada fila. Ten dous modificadores:

A opción /R serve para facer a ordenación con orde inversa (R de reverse)

A opción /+n serve para dicir que columna queremos ordenar

Exemplos:

C:\> dir C:\sistemas | sort Lista o contido dun directorio, ordenado polo primeiro carácter

C:\> sort config.sys Mostra en pantalla o arquivo config.sys ordenado por primeiro carácter

C:\> type config.sys | sort /+2 Mostra en pantalla o arquivo config.sys ordenadas as liñas por 2º carácter.

C:\> type ficheiro1.txt /R /+20 | sort > ficheiro2.txt Ordena o arquivo 1 por orde descendente por columna 20 e gárdao en ficheiro2.txt

FIND [/V] [/C] [/N] [/I] “CADEA” [ficheiro]

Serve para buscar unha cadea de texto. Devolve as liñas que contén a cadea de texto buscada

Exemplo:

Os 2 comandos seguintes son equivalentes, e devolve en pantalla as liñas do arquivo listado.txt que teñan a cadea de texto “folla”

C:\> type C:\listaxe.txt | find “folla”

C:\> find “folla” listado.txt

Outro exemplo:

C:\> dir/s | find "practica.docx" Devolve tantas liñas como número de arquivos que se chamen exactamente practica.docx

Opcións-modificadores do FIND

/v Mostra as liñas que non teñen a cadea indicada

/c Mostra o número de liñas que contén a cadea indicada (Coidado: non aparecen as liñas)

/n Mostra as liñas nas que aparece a cadea de texto e o número de liña na que se atopa

/i Non fará distinción á hora de buscar entre minúsculas e maiúsculas

Exemplo 1: Cantos arquivos hai en C co nome de practica.docx? Devolver só número

C:\> dir/s | find "practica.docx" /c → Devolve tantas liñas como número de arquivos que se chamen exactamente practica.docx

Exemplo 2: Devolver os arquivos que teñen os 3 atributos SHR en C

Explicación: Se executamos attrib, vemos que os arquivos que teñen os 3 atributos, aparece a cadea "SHR". Se buscamos con esa cadea, devólvenos/pode devolver algún arquivo cuxo nomee teña as 3 letras. Por iso ao buscar, puxen un espazo entre as letras e as comiñas.

C:\> attrib/s | find " SHR " Devolve todas as liñas que teñan a cadea " SHR "

Ficheiros por lotes ou batch. Extensión bat

Concepto

Un ficheiro por lotes, é un arquivo de texto plano, (código ASCII estendido), que contén varias ordes. Así, cando executemos devandito ficheiro, execútase unha tarefa tras outra sen a intervención do usuario. En Windows, teñen a extensión .bat

Exemplo

Crear un ficheiro por lotes chamado lote.bat, que cando se execute, obteña o ficheiro lote.txt coa data, a hora e listaxe de todos os arquivos e directorios da unidade C.

C:\>copy con lote.bat (Escribimos na terminal as 4 liñas seguintes, para gardalas en lote.bat)

@boto off

Dáche /T > lote.txt

Time /T >> lote.txt

Dir /S C:\ >> lote.txt

Para terminar, Ctrl+Z e Intro.

A liña @boto off é para desactivar o boto. Para que non moleste ao executar o ficheiro na terminal.

Execución: 2 formas:

En liña de comandos: escribimos o nome do arquivo: C:\> lote.bat

En contorna gráfica: dobre clic no nome do ficheiro

Programación dos ficheiros por lotes. Script de Powershell

Os ficheiros bat, tamén se lles chama programas bat, pois á parte de todos os comandos de Windows, admiten instrucións específicas que dan moitas posibilidades aos ficheiros por lotes.

Powershell é unha nova consola para a execución de scripts moito máis potente que cmd. Powershell non vén instalado por defecto nas versións Home, pero pódese instalar.

3.6 Terminal de comandos de GNU-Linux

3.6.1 Interfaces de texto: terminais ou consolas de texto

Desde a interface gráfica iniciada, pódese iniciar a aplicación terminal, para iso pulsamos en Actividade e escribimos terminal.

Ademais, na maioría das versións de Linux, á parte da sesión gráfica, iníciáanse varias terminais de texto. Estas sesións gráficas ou terminais de texto, chamadas tty1, tty2, ..., tty6 móstranse en pantalla, pulsado as teclas “Ctrl+Alt+F1”,..., “Ctrl+Alt+F6”

Cada terminal pode estar iniciada por distintos usuarios.

En Ubuntu 18.04 tty1 e tty2 son sesións gráficas (por defecto iníciase a terminal gráfica tty2). Desde tty3 ata tty6 son terminais de texto.

Coa sesión gráfica iniciada, podemos cambiar a tty3 con Ctrl+Alt+F3 e iniciar sesión con outro usuario, e volver á gráfica pulsando Ctrl+Alt+F2.

Noutros Linux, as terminais cambian, mesmo nas versións anteriores de Ubuntu, tty1 a tty6 representan terminais de texto, mentres as gráficas son tty7 e tty8.

Lembrar que ao utilizar VirtualBox, a combianción “Ctrl + Alt” substitúese pola tecla anfitrión de VirtualBox “Ctrl dereita” (das 2 teclas de control que hai no teclado, a que hai á dereita). De forma, que para iniciar sesión en tty1 nunha máquina virtual utilízase “Ctrl dereita + F1”

3.6.1.1 *Sintaxe dos comandos*

A sintaxe xeral dos comandos é:

comando [opcións][parámetros]

Exemplo de comando:

Se queremos coñecer o que hai no directorio home de alumno, con información longa e mostrando arquivos ocultos, executaremos o comando seguinte (as 2 formas son válidas):

```
ls -l -a /home/alumno
```

```
ls -a /home/alumno
```

- **Comando:**

ls é o comando que mostra o que ten un directorio (posteriormente vemos o comando de forma máis detallada)

Os comandos sempre se escriben en minúsculas, como se comentou antes.

- **Opcións do comando:**

A opción l serve para que a información de cada arquivo e directorio sexa longa ou estendida.

A opción para serve para mostrar os arquivos ocultos.

Cada opción escríbese cun guion diante, ou cun único guion, neste caso as opcións non se separan con espazo, sendo equivalentes: -l -a e -a

- **Parámetros:**

Onde imos realizar a acción, neste caso no directorio home de alumno:
/home/alumno

3.6.1.2 *Primeiros comandos*

Comezamos cuns primeiros comandos fáciles de utilizar, antes de entrar aos comandos de ficheiros e directorios.

passwd usuario

Comando para cambiar o contrasinal do usuario.

O sistema pide o contrasinal antigo e despois hai que introducir o novo contrasinal 2 veces.

exit

Comando para saír da sesión.

Exemplos:

Se temos unha terminal aberta na sesión gráfica, exit pecha a terminal.

Se estamos na terminal de texto tty1, e escribimos exit, o sistema finaliza a sesión e volve mostrar a petición de login para iniciar unha nova sesión.

man e help

A axuda dun comando pódese solicitar de 2 formas distintas, por exemplo, para pedir a axuda do comando passwd, pódese executar das 2 formas seguintes:

1. passwd --help (atención, antes de help, hai un dobre guión)

2. man passwd

O comando help ofrece a axuda de forma resumida, mentres que man ofrece a axuda completa do manual de Linux. Para desprazarnos pola axuda podemos utilizar ademais dos cursores, as teclas RePg e AvPg. Para saír de novo ao prompt ou Shell do sistema púlsase a tecla q (q vén de quit).

3.6.1.3 *Usuarios de Linux. Traballar como administrador. Cambios de usuario.*

Traballar como administrador

Cando se instalou Linux, creamos un usuario “o teu_nome”. Este usuario, ten poderes para converterse en superusuario ou root.

Calquera usuario posterior que se cre, non terá eses poderes, salvo que se configuren.

De momento, é importante ter claro que ese primeiro usuario creado “o teu_nome” e “root” son 2 usuarios distintos. Isto non é así en Windows, o usuario que se creou ao instalar Windows era administrador, aínda que debido ao UAC Control de usuarios, pídasele identificación.

Ademais, no noso Ubuntu, creamos un terceiro usuario "alumno", creado en anterior libro e que non ten poderes para ser root.

súo comando_a_executar

Se queremos executar un só comando como root (superusuario ou administrador) utilizamos súo.

A terminal pediranos o contrasinal do noso usuario, e executará o comando coa identidade de root e os seus permisos.

súo o seu

Se queremos realizar varias comandos como root, é máis cómodo cambiarnos temporalmente a root, para iso execútase súo o seu. Nos seguintes comandos seguimos sendo root ata que salgamos co comando exit.

É moi importante ser root só cando sexa necesario. Para entendelo, os arquivos teñen un propietario, que é quen o cree. Se son o usuario miguel e creo un arquivo, terei permisos para cambialo. Pero se creo o arquivo sendo root, o usuario miguel non terá permisos para cambiar o ficheiro.

3.6.1.4 *Cambiar a outro usuario. Comando o seu*

Pódese cambiar a calquera usuario na terminal, utilizando:

o seu nome_usuario

Ao introducir o anterior comando, solicítase o password do usuario, e cámbiase a sesión da terminal a ese usuario.

o seu root

Da mesma forma, a súa root serve para cambiar a sesión a root.

Por defecto, esta opción non funciona nas distribucións Ubuntu, pois o usuario root vén deshabilitado porque non ten contrasinal. Por iso, por defecto para ser root hai que utilizar obrigatoriamente súo. Con todo, noutras distribucións Linux, vén deshabilitado súo, polo que hai que utilizar a súa.

Para que o usuario root, poida ter sesión propia en Ubuntu, só hai que poñer contrasinal a root con:

súo passwd root

3.6.1.5 *Lenda para os exemplos que se mostre*

Exemplo:

```
miguel@sistemasubuntu:$ cat /etc/shadow
```

```
cat: /etc/shadow: Permiso denegado
```

#Como usuario miguel téntase mostrar o arquivo /etc/shadow en pantalla. O sistema devolve permiso denegado

```
miguel@sistemasubuntu:$ súo cat /etc/shadow
```

```
[súo] contrasinal para miguel:
```

```
root:!:17848:0:99999:7:::
```

.....

#Execútase o mesmo comando pero con súo, de forma que o sistema solicita o password de miguel, (usuario que pode converterse en root). Móstrase a información do ficheiro en pantalla (este ficheiro ten os contrasinais encriptadas dos usuarios)

```
miguel@sistemasubuntu:$ súo o seu
```

#Con súo o seu, cámbiase a root, de forma que cando devolve o prompt ou Shell, aparece a primeira palabra root (que significa que está conectado o usuario root).

```
root@sistemasubuntu:/home/miguel# cat /etc/shadow
```

```
root:!:17848:0:99999:7:::
```

.....

#Como xa somos root, podemos mostrar o arquivo sen utilizar súo

```
root@sistemasubuntu:/home/miguel# mkdir cartafol1
```

#Creamos cartafol1 en directorio actual

```
root@sistemasubuntu:/home/miguel# exit
```

```
exit
```

#Saímos de root, e volvemos ao usuario miguel con exit (fixarse en shell)

```
miguel@sistemasubuntu:$ mkdir cartafol2
```

#Creamos cartafol2 en directorio actual

```
miguel@sistemasubuntu:$ ls -l
```

```
total 52
```

```
drwxr-xr-x 2 root root 4096 nov 22 12:24 cartafol1
```

drwxr-xr-x 2 miguel miguel 4096 nov 22 12:24 cartafol2

.....

#Listamos o noso directorio actual, ao listar vese cartafol1 e cartafol2, pero ven os seus propietarios, onde o propietario de cartafol1 é root, e o propietario de cartafol2 é miguel

3.6.1.6 *Varios comandos sinxelos*

poweroff

Apagar o equipo. Na maioría das distribucións, hai que ser root.

reboot

Reiniciar o equipo.

who

Devolve todos os usuarios conectados ao equipo, ben en distintas terminais, ben desde a rede.

boto

Igual que en Windows, boto mensaxe devolve en pantalla a mensaxe.

pwd

Devolve o directorio actual no que nos atopamos.

clear

Limpa a pantalla (equivalente ao cls de Windows)

3.6.1.7 *Inicio de sesión do usuario en Linux. Directorio /home*

Cando un usuario inicia sesión nunha consola de Linux, accede por defecto ao seu directorio \$HOME. No directorio \$HOME dun usuario, só ten acceso a escribir ese usuario e os administradores. Por defecto, en Ubuntu, se se permite a lectura dos arquivos doutros usuarios.

Se o usuario chámase alumno, o seu directorio \$HOME é /home/alumno

Cando un usuario atópase no seu \$HOME, na maioría das shell aparece o símbolo en lugar de /home/usuario

3.6.1.8 *Significado dos parámetros do Prompt ou Shell do sistema*

root@localhost:/etc#

1 2 3 4

1. Estamos conectados co usuario root.

2. O nome do computador é localhost

3. O directorio actual é /etc. Se aparece significa que estamos no directorio HOME do usuario.

4. Identificaa # que o usuario conectado é un administrador. Cando o usuario conectado non é administrador, visualízase \$.

Exemplo:

```
miguel@sistemasubuntu:/Documentos$ pwd
```

```
/home/miguel/Documentos
```

#O comando pwd devolve o roteiro actual completo, como estamos en /Documentos e representa \$HOME, o roteiro completo en /home/miguel/Documentos

```
miguel@sistemasubuntu:/Documentos$ o seu alumno
```

```
alumno@sistemasubuntu:/home/miguel/Documentos$
```

#Ao cambiar ao usuario alumno, vese os cambios nos parámetros 1 (usuario) e 3 (directorio actual)

3.6.2 Comandos de directorios

Neste epígrafe estúdanse os comandos para crear e eliminar directorios. No seguinte os de ficheiros, ao final inclúese un exemplo coa execución de varios comandos.

Antes de comezar, vexamos algunhas analogías e diferenzas entre Linux e Windows:

- A utilización de roteiros absolutos e relativos, é igual en Linux que en Windows.
- Linux utiliza tamén os comodines *, ? co mesmo significado que Windows.
- En Linux, un arquivo ou directorio oculto é simplemente o que o seu nome empeza polo carácter punto “.”
- En Linux, un arquivo executable non se distingue pola súa extensión, senón polos seus permisos, onde se poderá configurar lectura, escritura e execución.

pwd

Mostra o directorio actual co seu roteiro absoluto

cd

Cambiar de directorio (change directory)

Exemplos:

cd .. Este comando cambia ao directorio pai

cd / Este comando cambia ao directorio raíz

Estamos no directorio /home/usuario2 e queremos cambiar ao directorio home do usuario1. Como se faría con roteiro absoluto e con roteiro relativo?

usuario2@SistemasUbuntu:\$ cd /home/usuario1 Usando roteiro absoluto

usuario2@SistemasUbuntu:\$ cd ../usuario1 Usando roteiro relativo

mkdir

Crear novos directorios

rmdir

rm -rf

O comando rmdir borra un directorio, pero ten que estar baleiro.

Para borrar un directorio con todo a súa árbore de ficheiros e subdirectorios temos que utilizar rm -rf

En realidade, rm é o comando para borrar ficheiros, pero para borrar unha árbore de directorios, hai que utilizar este comando, con estas opcións, pois con rmdir non é posible.

tree

Mostra a información xerárquica dun directorio, cos seus ficheiros e subdirectorios.

ls

O comando ls lista (list) os arquivos dun directorio

Sintaxe do comando: ls [-laRtr] [roteiro]

Este comando ten moitas opcións, as máis importantes son:

-l A opción l, mostra información longa (long) ou detallada de cada arquivo (propietario, data, permisos)

-a opción a, serve para que ao listar inclúa os arquivos ocultos. En Linux, un arquivo ou directorio oculto, é cando o seu nome empeza polo carácter punto. Por exemplo, se listamos ls -a no noso \$HOME, vemos que hai unha chea de arquivos que empezan por . como: .bashrc, .cache, .profile

-R A opción R mostra a información dos subdirectorios, é dicir da árbore enteira (R de recursive)

-t A opción t mostra os arquivos ordenados por data (t de estafe)

-r A opción r, mostra a orde inversa. Por defecto ao listar aparecen os arquivos ordenados por nome da á a z. Coa opción r, faríano da z á a (r de reverse). Fixarse, que aínda que dixemos que os comandos sempre se usan en minúsculas, as súas opcións si que as hai en maiúsculas e minúsculas con significados distintos.

Exemplos:

- Obter todos os arquivos e directorios do sistema, incluíndo ocultos con información detallada: ls -lareira /

- Mostrar contido do directorio /var/log en formato longo e mostrando arquivos ocultos: `ls -la /var/log`

Significado da información que devolve a opción `-l` (información longa ou detallada)

`drwxr-xr-x 2 alumno alumno 4096 2012-04-15 23:43 Descargas`

1 2 3 4 5 6 7 8

1. Se o primeiro carácter é unha “d”, é un directorio. (no exemplo é o directorio descargas) Se non é “d” é un ficheiro. No caso de ficheiro pode aparecer::

Un guion “-“ que son os arquivos normais ou regulares

Unha “b” que significa arquivo de bloque, úsase nos dispositivos, por exemplo os discos duros, onde as transferencias de información realízanse en bloques (ou anacos)

Unha “c” que significa arquivo de carácter, úsase nos dispositivos de carácter a carácter, por exemplo as terminais `tty1`, `tty2`,...

Unha “l” é unha ligazón simbólica ou branda, igual que os accesos directos de Windows.

2. Os outros 9 caracteres son os permisos de ficheiro. De momento, se aparece a x nesas permisos, significa que o arquivo é executable (eXecute).

3. O seguinte campo, significa que ten 2 ligazóns duras. En Linux hai 2 tipos de ligazóns: duros e brandos.

4. O usuario propietario do ficheiro é alumno.

5. O grupo propietario do ficheiro é alumno.

6. Tamaño do ficheiro, en bytes.

7. Data e Hora: Indica a data e a hora de creación ou modificación do ficheiro.

8. Nome do ficheiro ou directorio.

Observación: Parece repetitivo dicir que o propietario é alumno, e o grupo propietario é alumno. Pero non é así, en Linux todo usuario pertence a un grupo principal, que por defecto, chámase igual que o. Cando se creou o usuario alumno se realizaron 3 cousas:

1. Creouse o grupo alumno.

2. Creouse o usuario alumno.

3. Introduciuse ao usuario alumno dentro do grupo alumno.

A partir de aí, todos os ficheiros que cre alumno, pertencen ao usuario alumno e ao grupo alumno.

Na seguinte unidade crearanse grupos con distintos nomes que os usuarios.

3.6.3 Comandos de ficheiros

3.6.3.1 Editor de texto plano

Se estamos en gráfico, Ubuntu incorpora o editor de texto plano gedit (equivalente ao bloc de notas ou notepad de windows)

En terminal, hai moitos, os máis coñecidos son: nano, vi, emacs.

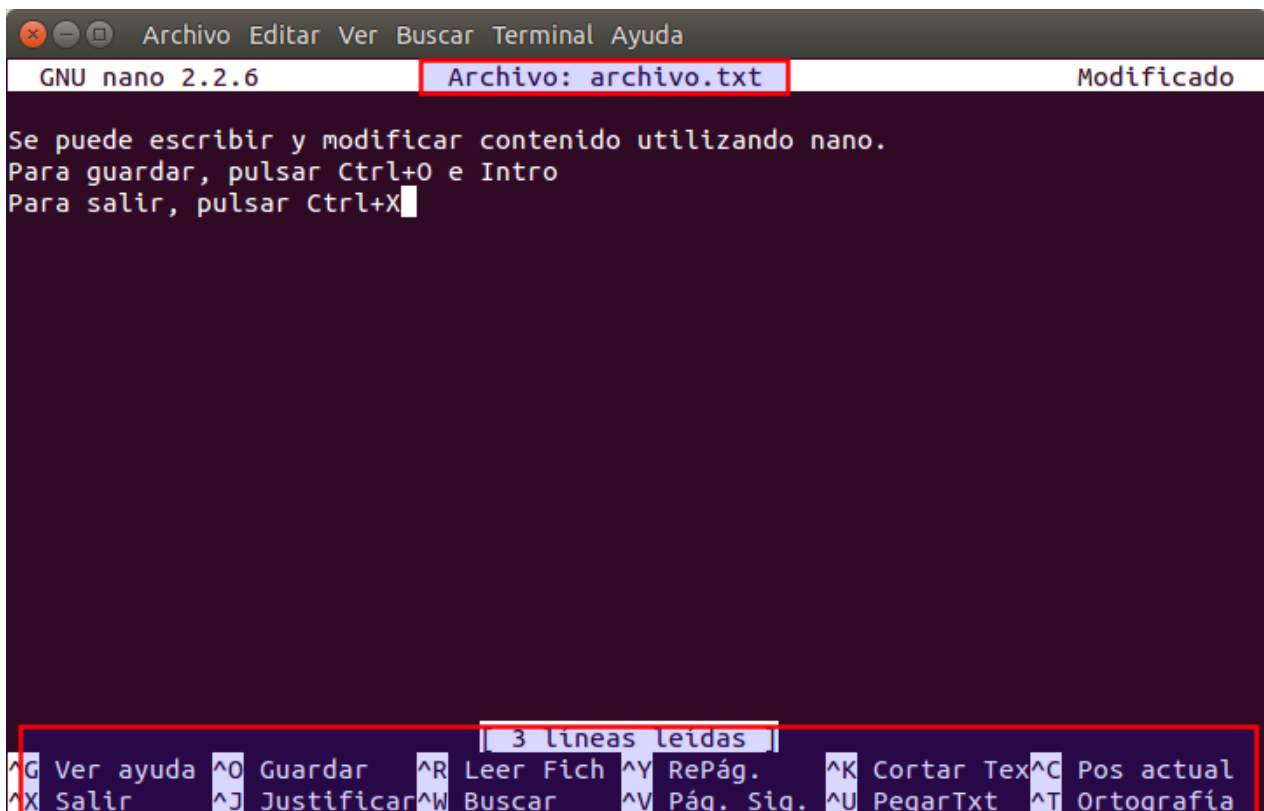
En Ubuntu están instalados **nano** e **vi**. En contorna comando, desde o primeiro UNIX utilizouse o editor vi, moi completo pero que se utiliza só con comandos. No noso caso, imos utilizar o editor nano, con menos opcións que o vi, pero fácil de utilizar.

Exemplo: nano arquivo.txt abre o editor nano. Se existía arquivo.txt, mostra o seu contido en pantalla. Se non existía, mostra baleiro o contido. En calquera caso, podemos engadir ou modificar o contido que queiramos.

Para saír e gardar hai que utilizar as combinacións de tecla que aparecen na mesma xanela do editor na zona de abaixo.

Móstrase captura do editor nano (executouse nano arquivo.txt).

Ilustración de Editor nano.



Miguel Ángel García Lara (CC BY-NC-SA)

touch

Crea un ficheiro baleiro, se xa existía, actualiza a súa hora de modificación.

Por exemplo, touch arquivo.txt crea arquivo.txt sen contido no interior.

3.6.3.2 Visualización de ficheiro en terminal

Os comandos `cat`, `less` e `more` serven para visualizar arquivos de texto en pantalla (equivalen ao comando `type` en Windows)

As diferenzas entre eles, é que `cat` mostra o contido enteiro, devolvendo o Shell do sistema. Con todo, `less` e `more`, mostran o contido do ficheiro, pódese subir e baixar cos cursores, e para saír débese pulsar `q` (quit)

O comando `head` mostra as 10 primeiras liñas dun ficheiro.

O comando `tail` mostra as 10 últimas liñas dun ficheiro.

Comando `type`

Realiza unha acción totalmente distinta que en Windows. En Linux, mostra onde se atopa o executable dun comando.

Exemplo:

Onde se atopa o ficheiro executable do comando `touch`?

```
alumno@sistemasubuntu:$ type touch
```

```
touch is /usr/bin/touch O arquivo touch atópase en /usr/bin/touch
```

Comando `cp`

Sintaxe: `cp [-R] orixe destino`

O comando `cp` copia arquivos ou directorios, pódense copiar con outro nome.

-R A opción “R” copia recursivamente, toda a estrutura de subdirectorios e ficheiros. Copia a árbore enteira.

Exemplos:

- Estando en `$HOME` de alumno, copiar o arquivo “arquivo.txt” no `$HOME` de miguel co nome `copia.txt`.

Utilizando roteiro relativo:

```
alumno@sistemasubuntu:$ cp arquivo.txt ../miguel/copia.txt
```

Utilizando roteiro absoluto:

```
alumno@sistemasubuntu:$ cp /home/alumno/arquivo.txt /home/miguel/copia.txt
```

- Copiar todos os arquivos `.txt` do directorio home de usuario 1 ao subdirectorio `datos` coa extensión `.dat`

```
cp /home/usuario1/*.txt /home/usuario1/datos/*.dat
```

- Copiar toda a estrutura do directorio home de usuario1 ao directorio home de usuario 2 (con roteiro absoluto)

```
cp -R /home/usuario1 /home/usuario2
```

Comando mv

Sintaxe: mv orixe destino

O comando mv move arquivos ou directorios, pódese cambiar o nome á vez.

Tamén serve para renommer ficheiros ou directorios.

Comando rm

Sintaxe: rm [-irf] ficheiro

O comando rm borra ficheiros (remove)

-i A opción i pide confirmación antes de borrar cada arquivo.

-r A opción r borra recursivamente, polo que borra directorios enteiros.

-f A opción f forza o borrado dos arquivos, sen preguntar

Para borrar un directorio cunha soa orde, e sen ter que confirmar cada borrado, execútase
rm -rf

Exemplo:

Borrar o directorio hoxe situado dentro do directorio home de alumno con roteiro absoluto:

```
alumno@sistemasubuntu:$ rm -rf /home/alumno/hoxe
```

Direccionamientos ">", ">>", "2>", "2>>"

Os operadores de direccionamiento > e >> utilízanse da mesma forma que en Windows. A saída esperada na terminal; se redirecciona a un arquivo.

O operador > sobrescribe o arquivo e o operador >> engade ao que xa tivese.

Cando se executa un comando, devólvense 2 saídas distintas en terminal: a esperada ou estándar (buffer stdout) e os erros (buffer stderr). Mentres que os operadores > e >> redireccionan a saída estándar, os operadores 2> e 2>> redireccionan o buffer de erros.

3.7 Almacenamento redundante e distribuído



O almacenamento redundante consiste en que os datos almacenados nalgún dispositivo atópanse replicar noutro. Así podemos ter a garantía de que aínda que perdamos, corrómpanse ou se volvan inaccesibles os datos dun dos dispositivos, sempre teremos máis copias dos mesmos datos para acceder a eles. O importante na redundancia dos datos é que os discos nos que se atopa a información replicar atópanse sincronizados de forma que ambos teñan a mesma información.

Os sistemas de almacenamento distribuído baséanse en separar a información dun arquivo en distintos dispositivos. Deste xeito cando se quere ler un arquivo o tempo empregado para recuperar o arquivo é menor dado que todas as partes chegan a partir de

ler diferentes anacos do arquivo nos distintos dispositivos á vez. En termos xerais, o que se pretende co uso do almacenamento redundante e distribuído é:

- Aumentar a tolerancia a fallos: consiste na tolerancia que ten o sistema para poder seguir operando no caso de que ocorra algún fallo nalgún dos discos que forman o conxunto de discos, de forma que haxa capacidade para restablecer o sistema cos discos que quedan en estado correcto.
- Ter redundancia de datos: consiste en que a información se atopa duplicada, de maneira que sempre se teñen dúas copias da mesma información para ter dispoñible unha copia dos datos no caso de que ocorra algún problema coa outra copia. □ Aumentar a capacidade de almacenamento: algúns dos niveis de RAID permiten aumentar o espazo máximo do que dispoñemos para o almacenamento da información.
- Mellorar o rendemento en lecturas e escrituras: mellórase a velocidade de escritura e lectura da información nos discos.

É habitual utilizar o termo de RAID para referirse ao almacenamento redundante e distribuído. O acrónimo RAID ven do inglés *Redundant Array of Independent Disks*, que no noso idioma ven sendo conxunto redundante de discos independentes. Este termo fai referencia a un sistema de almacenamento de datos que usa múltiples unidades de almacenamento de datos, como discos duros, entre os cales se distribúen ou replicar os datos.

Dependendo da configuración que se utilice no RAID, as vantaxes que se acaban de listar poden estar dispoñibles en maior ou menor medida, ou mesmo non existir algunha delas. No nivel máis simple, un RAID combina varios discos duros nunha soa unidade lóxica. Isto é completamente transparente para o sistema operativo que so ve un disco.

O RAID pode construírse de dúas formas, por software ou por hardware.

3.7.1 RAID por Hardware

Neste tipo de RAID requírese polo menos unha controladora RAID específica para xestionar a administración dos discos. Estas controladoras teñen os seus propios procesadores e memoria, co cal descarga de traballo á CPU do sistema. O problema deste RAID é que, ademais de que é máis caro, engade un punto máis de fallo posible no sistema, xa que ademais de fallar os discos tamén pode fallar a controladora. Pero ten outras vantaxes:

- Máis rápido xa que é a controladora a que atende e fai as operacións nos discos en lugar de facelo o sistema operativo.
- Sinxelo de configurar, xa que a configuración faise a través da consola de configuración RAID da controladora.
- Rápida recuperación ante un fallo de disco, xa que en caso de ocorra un erro nun disco, o único que se precisa facer é extraer o disco e inserir un novo. A controladora encárgase do proceso de réplica.



Consultar StoreData RAID 2246:

www.smdata.com/process.php/?file=downloads/SDRAID2246A-12R-4.pdf

3.7.2 RAID por Software

Neste caso é o sistema operativo o que crea, equitación e xestiona o RAID sobre os discos do conxunto.

Este tipo de RAID permite gran flexibilidade e permite non só construír RAID de discos completos, senón tamén de particións e agrupar nun mesmo RAID discos conectados en varias controladoras.

A desvantaxe é que é máis lento que o RAID por hardware xa que vai consumir máis recursos do procesador para manter o RAID.

3.7.3 RAID Híbrido ou FakeRAID.

Este RAID está baseado en software e hardware específico, mediante controladoras RAID hardware e cun sistema que incorpora unha aplicación de baixo nivel que permite aos usuarios construír RAID controlado pola BIOS. Consiste na agrupación simulada de discos para que o Sistema Operativo cando arrinca pense que se trata de tal agrupación de discos. Esta idea imita ao funcionamento dos RAID por hardware pero con recursos máis limitados, co que os resultados tamén estarán máis limitados.

A vantaxe é que o Sistema Operativo ve montado o RAID no mesmo momento de arrincar, pero isto non evita que os recursos que o xestionan sexan a propia CPU e RAM do sistema.

A continuación veranse distintos tipo de RAID que se poden implementar, pero é importante ter en conta que todas esas implementacións poden soportar un ou varios discos extra, que son unidades de disco que están preinstaladas e listas para empezar a usalas cando ocorra algún fallo dun disco do RAID. Estes discos chámanse comunmente co termo inglés *hot spare*. Esta solución permite que se reduza o tempo de reconstrución do RAID cando ocorra o fallo.



Figura 1: Servidor RAID

3.8 Tipos de RAID

Entre os tipos de RAID máis importantes atopámonos co RAID 0, RAID 1 e RAID 5 que se comentarán nos seguintes apartados.

3.8.1 RAID 0

Un RAID 0, tamén chamado (*data striping* en inglés) conxunto dividido ou volume dividido, distribúe os datos equitativamente entre dous ou máis discos sen información de paridade que proporcione redundancia.

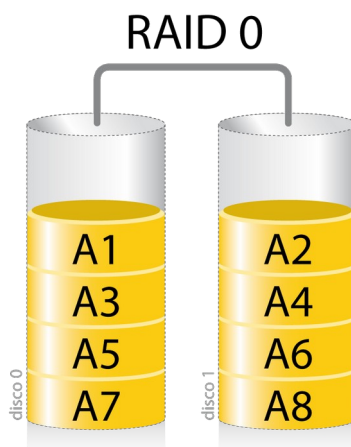


Figura 2: Raid 0

Utilízase normalmente para incrementar o rendemento, aínda que tamén pode utilizarse como forma de crear un pequeno número de grandes discos virtuais a partir dun gran número de pequenos discos físicos.

Pode ser creado con discos de diferentes tamaños, pero o espazo de almacenamento engadido ao conxunto estará limitado polo tamaño do disco máis pequeno. Por exemplo, ter dous discos, un de 20GB e outro de 15GB, o tamaño do conxunto será de 30GB, xa que cada disco achega o espazo do disco máis pequeno, é dicir, 15GB.

Unha boa implementación de RAID 0 dividirá as operacións de lectura e escritura en bloques de igual tamaño, polo que distribuirá a información equitativamente entre os dous discos.

3.8.2 RAID 1

Un RAID 1 (*Data mirroring*) crea unha copia exacta, chamada espello, dun conxunto de datos en dous ou máis discos. O conxunto só pode ser tan grande como o é o máis pequeno dos seus discos.

Un RAID 1 clásico consiste en dous discos en espello, o que incrementa exponencialmente a fiabilidade respecto a un só disco, xa que para que o conxunto falle é necesario que fallen todos os seus discos.

O RAID 1 resulta útil cando o rendemento en lectura é máis importante que a capacidade, isto débese a que este tipo de RAID pode estar a ler simultaneamente dous datos

diferentes en dous discos diferentes, polo que o rendemento duplícase. O tempo medio de lectura, por tanto, redúcese xa que os sectores para buscar poden dividirse entre os discos, baixando o tempo de busca.

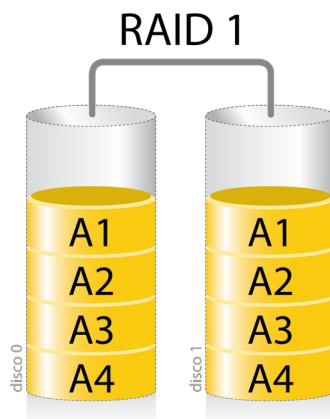


Figura 3: RAID 1

Ao escribir o conxunto compórtase como un só disco, dado que os datos debe ser escritos en todos os discos do RAID 1. Por esta razón, o rendemento en escritura non mellora.

O RAID 1 ten moitas vantaxes de administración. Por exemplo, nalgúns contornos 24/7, é posible dividir o espello para marcar un dos discos como inactivo, facer unha copia de seguridade da información que contén o devandito disco e logo reconstruír o espello de novo.

3.8.3 RAID 5

Un RAID 5, tamén denominado distribuído con paridade, é unha división de datos a nivel de bloques distribuindo a información de paridade entre todos os discos membros do conxunto. Necesita como mínimo de 3 discos para poder ser implementado.

Os discos atópanse divididos en bloques, e aos bloques dos discos do mesmo nivel denomínase banda (ou no seu termo en inglés stripe). Cada vez que se escribe un bloque de datos nun RAID 5, xérase un bloque de paridade dentro da mesma banda. Se un dos bloques, ou algunha porción dun bloque, é escrito, o bloque de paridade da mesma banda é recalculado e volto escribir. O disco utilizado polo bloque de paridade está graduado dunha banda á seguinte, de aí o termo de bloques de paridade distribuídos. As escrituras nun RAID 5 son custosas en termos de operacións de disco e tráfico entre os discos e a controladora.

Os bloques de paridade non son lidos nas operacións de lectura de datos, xa que isto sería unha sobrecarga innecesaria e diminuíría o rendemento. Aínda así, os bloques de paridade léense cando a lectura dun sector de datos provoca un erro de CRC. Neste caso, para ocultar e solucionar o erro, o sector na mesma posición relativa dentro de cada un dos bloques de datos restantes na división e dentro do bloque de paridade na división utilízanse para reconstruír o sector erróneo.

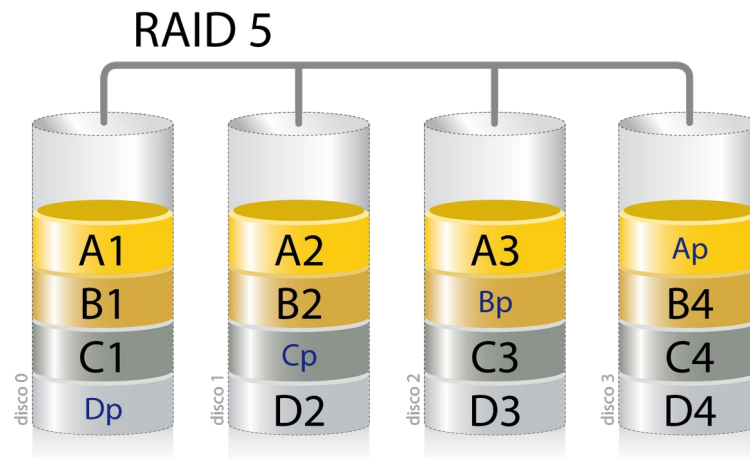


Figura 4: RAID 5

Da mesma forma, fállase un disco do conxunto, os bloques de paridade dos restantes discos son combinados matematicamente cos bloques de datos dos restantes discos para reconstruír os datos do disco que fallou. Canda falla un disco, as lecturas e escrituras continúan normalmente no conxunto de discos, aínda que con algunha degradación de rendemento. O fallo nun segundo disco provoca a perda completa dos datos.

3.8.4 RAID 6

Un RAID 6 amplía o nivel RAID 5 engadindo outro bloque de paridade, polo que divide os datos a nivel de bloques e distribúe os dous bloques de paridade entre todos os membros do conxunto. O RAID 6 non era un dos niveis RAID orixinais.

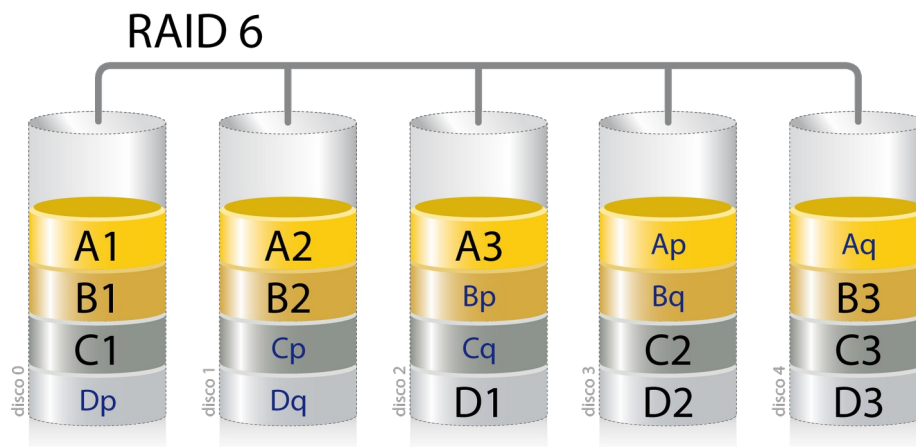


Figura 5: RAID 6

3.8.5 RAID anidados

Hai controladoras que permiten anidar niveles de RAID, é dicir, que un RAID poida usarse como elemento básico doutro en lugar de discos físicos.

Os RAIDs anidados indícanse normalmente unindo nun só número os correspondentes aos niveis de RAID empregados, engadindo ás veces un + entre eles. Por exemplo, o RAID 10, ou RAID 1+0, consiste conceptualmente en múltiples conxuntos de nivel 1 almacenados en discos físicos cun nivel 0 arriba, agrupando os anteriores niveis 1.

Ao aníñar niveis RAID, adóitase combinar un nivel RAID que proporcione redundancia cun RAID 0 que aumenta o rendemento.

3.8.5.1 RAID 0+1

Un RAID 01 é un espello de divisións. É un RAID usado para replicar e compartir datos entre varios discos. Coma se ve na seguinte imaxe, primeiro créanse dous conxuntos RAID 0 (dividindo os datos en discos) e logo, sobre os anteriores, créase un conxunto RAID 1 (realizando un espello dos anteriores).

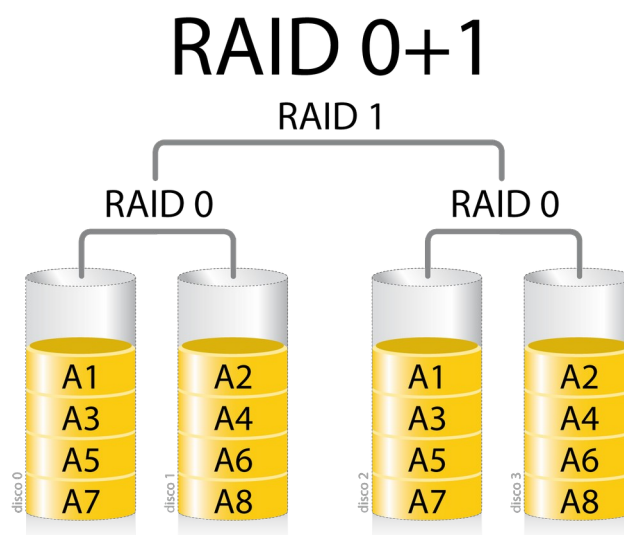


Figura 6: RAID 0+1

A vantaxe dun RAID 0 + 1 é que cando falla un disco duro, os datos perdidos poden ser copiados do outro conxunto de nivel 0 para reconstruír o conxunto global. Pero para engadir un disco duro adicional nunha división, é obrigatorio engadir outro ao da outra división para equilibrar o tamaño do conxunto.

Este RAID non é tan forte como o que se vai a ver a continuación, o RAID 1+0, non podendo tolerar dous fallos simultáneos de discos salvo que sexan na mesma división. É dicir, cando un disco falta, a outra división convértese nun punto de fallo único. Ademais, cando se substitúe o disco que fallou, necesítase que todos os discos do conxunto participen na reconstrución dos datos

3.8.5.2 RAID 1+0

Un RAID 1+0 é parecido ao RAID 0+1 coa excepción de que os niveis RAID que o forman invértense. Este RAID é unha división de espellos.

En cada división RAID 1 poden fallar todos os discos excepto un sen que se perdan datos. Aínda que, se os discos que fallaron non se substitúen, o restante pasa a ser un punto único de fallo para todo o conxunto. Se ese disco falla entón perderanse todos os datos do conxunto completo.

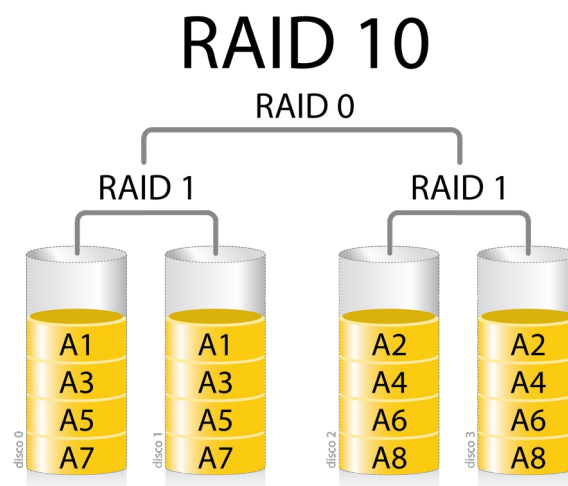


Figura 7: RAID 10

O RAID 10 é a miúdo a mellor elección para bases de datos de altas prestacións, posto que a ausencia de cálculos de paridade proporciona maior velocidade de escritura.

3.8.6 RAID en Windows

Windows distingue os seguintes tipos de volumes:

- **Distribuído:** é a unión dunha ou máis áreas de espazo dispoñible que se poden dividir en particións e unidades lóxicas. Este tipo de volume pódese utilizar cando se necesite un volume con espazo maior ao dun único disco. O espazo que dedicou pódese ampliar pero non diminuír. Neste caso é necesario eliminar o volume completamente, e como consecuencia, os datos tamén serían eliminados, e volvelo a crear co espazo necesario. Este volume ben representado por unha letra de unidade.
- **Seccionado:** correspóndese cun RAID 0, co cal cada un dos discos que forman o volume divídense en bandas. Todos os discos están divididos no mesmo número de bandas do mesmo tamaño. Os datos que se van gardando vanse almacenando de forma distribuída en cada unha das bandas dos discos, cando a primeira banda de todos os discos está ocupada séguese gardando a información na segunda banda, e así sucesivamente. Deste xeito, elimínase parte do tempo que o cabezal tarda en buscar os sectores e pistas onde se atopa o arquivo. A escritura é máis rápida xa que os datos cópanse simultaneamente entre os diferentes discos.
- **Reflectido:** correspóndese cun RAID 1, co que son dúas particións que se configuran para que ambas sexan idénticas entre si. Desta forma os datos aparecerán reflectidos en cada unha das particións.
- **Volume RAID 5:** correspóndese cun RAID 5 e é similar ao volume seccionados despois de que os discos divídense en bandas. A diferenza é que para cada banda uno dos discos almacena información de paridade en función dos datos almacenados nos outros discos na mesma banda. Isto permite recuperar información cando falla a banda dun disco, xa que entre as outras bandas máis a

de paridade pódese reconstruír o anaco que falta. Outra diferenza co anterior, é que se perde espazo de almacenamento, debido a que en total, un dos discos pérdese de almacenamento pois almacena a información de paridade.

3.8.7 RAID en Linux

Os conceptos do RAID en Linux son os que se viron en apartados anteriores cando se explicou os niveis de RAID existentes.

3.8.8 Cálculo de paridade

A paridade é un método que utilizan moitos niveis de RAID. Comunmente emprégase en tecnoloxías da información para proporcionar tolerancia a erros nun conxunto de datos.

A maioría dos RAID utilizan a operación lóxica XOR para definir como se crean e como se usa a paridade no RAID. Emprégase tanto para a protección dos datos, como para recuperar datos que se perderon. A operación OR exclusivo, XOR, no álgebra de Boole, significa ou un ou o outro, pero non ambos. Na seguinte táboa pode verse a táboa de verdade para esta operación:

Valor A	Valor B	XOR
0	0	0
0	1	1
1	0	1
1	1	0

Supoñamos agora que temos un RAID composto por 6 discos: 4 para datos, 1 para paridade e un de reposto (o *hot spare*):

Discos	Datos	Utilidade
Disco 1:		(datos)
Disco 2:		(datos)
Disco 3:		(datos)
Disco 4:		(datos)
Disco 5:		(reposto)
Disco 6:		(paridade)

Cada disco vai ter unicamente un byte para gardar, así que imos supoñer que se escriben os seguintes datos nos discos:

Discos	Datos	Utilidade
Disco 1:	00101010	(datos)
Disco 2:	10001110	(datos)

Disco 3:	11110111	(datos)
Disco 4:	10110101	(datos)
Disco 5:		(reposto)
Disco 6:		(paridade)

Cada vez que se escriben datos nos discos, débese calcular o valor da paridade para que o RAID sexa capaz de recuperar os datos en caso de fallo dun dos disco. Para o cálculo da paridade emprégase un XOR bit a bit para cada un dos datos dos discos. Calcúlase da seguinte forma:

$$00101010 \text{ XOR } 10001110 \text{ XOR } 11110111 \text{ XOR } 10110101 = 11100110$$

Os datos de paridade 11100110 escríbense ao disco destinado a gardar os datos de paridade:

Discos	Datos	Utilidade
Disco 1:	00101010	(datos)
Disco 2:	10001110	(datos)
Disco 3:	11110111	(datos)
Disco 4:	10110101	(datos)
Disco 5:		(reposto)
Disco 6:	11100110	(paridade)

Supoñer agora que o disco 3 falta, xa non podemos acceder aos seus datos. Para restaurar os datos que contiña o devandito disco, empregamos a mesma operación XOR que antes, pero esta vez utilizando os datos dos discos duros que quedan e os datos de paridade do Disco 6:

$$00101010 \text{ XOR } 10001110 \text{ XOR } 11100110 \text{ XOR } 10110101 = 11110111$$

Podemos comprobar que os datos que se obteñen son os que tiñamos inicialmente no Disco 3. Os datos recuperados escríbense no disco de reposto, o cal actuará desde ese intre como membro do RAID permitindo que todo o grupo funcione con normalidade.

Discos	Datos	Utilidade
Disco 1:	00101010	(datos)
Disco 2:	10001110	(datos)
Disco 3:	FALLO	(datos)
Disco 4:	10110101	(datos)
Disco 5:	11110111	(reposto)
Disco 6:	11100110	(paridade)

O mesmo principio básico aplícase coa paridade en grupos RAID sen importar a capacidade nin o número de discos. Mentres haxa discos suficientes para permitir a

operación XOR, a paridade pode ser utilizada para recuperar os datos cando haxa un fallo nun só disco. Como se pode comprobar con estas operacións, como mínimo deben existir tres discos para utilizar a paridade, porque a operación XOR require dúas operandos e un lugar onde gardar o resultado.

3.9 Almacenamento remoto e extraíble

Con almacenamento remoto, referímonos ao dispositivo de almacenamento de información que non se atopa na máquina local. Con almacenamento extraíble, referímonos ao dispositivo de almacenamento de información que se pode conectar e desconectar en quente, é dicir, sen ter que apagar o sistema.

3.9.1 NAS

O acrónimo NAS ven do termo en inglés *Network Attached Storage*, que é o nome dado á tecnoloxía de almacenamento na que se empregan dispositivos de almacenamento específicos que comparten a súa capacidade de almacenamento cos clientes que acceden a eles a través dunha rede, normalmente facendo uso do protocolo TCP/IP.

Este sistema baséase en que os clientes solicitan arquivos completos ao servidor de almacenamento, unha vez que os obteñen manéxanos localmente. É por iso que están orientados a información almacenada en arquivos de pequeno tamaño pero en gran cantidade.

Moitos dos sistemas NAS contan cun ou máis dispositivos de almacenamento para incrementar a súa capacidade local. Ademais, frecuentemente, estes dispositivos están dispostos en RAID ou contedores de almacenamento redundante, o que permite aumentar a súa capacidade, eficiencia ou tolerancia ante fallos.

Os dispositivos NAS non requiren pantalla, nin rato ou teclado, senón que para controlalos utilízase unha interface Web, na que se pode seleccionar o dispositivo NAS que se vai a xestionar.

O sistema NAS proporciona escalabilidade, xa que en caso de necesitarse máis capacidade de almacenamento poden engadirse máis dispositivos NAS adicionais. O inconveniente é que isto aumenta a complexidade de xestión do conxunto, xa que cada un dos dispositivos opera de forma independente ao resto dos dispositivos.

O prezo das aplicacións NAS baixou durante os últimos anos, ofrecendo redes de almacenamento flexibles para o consumidor doméstico con menos custos do habitual. Existen distribucións de software libre orientadas a servizos NAS por exemplo FreeNAS.

3.9.2 SAN

Unha rede SAN, ou tamén coñecida como rede con área de almacenamento (do inglés *Storage Area Network*), é unha rede dedicada que proporciona acceso a almacenamento de datos a nivel de bloque. Nun SAN os discos están nun “armario”, onde leva a cabo a configuración RAID. O “armario” dispón de cachéas/cachés de alto rendemento para

reducir os tempos de operación. Os servidores conéctanse ao “armario” mediante conmutadores de fibra óptica (por iso falamos de network).

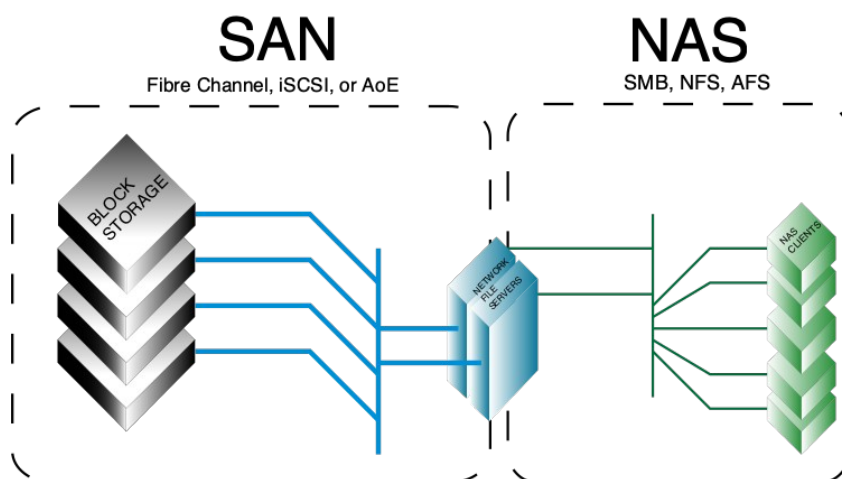


Figura 8: SAN vs NAS

O almacenamento de datos centralizado reduce a administración necesaria e proporciona un tipo de almacenamento de alto rendemento e flexible, que está relacionado directamente co tipo de rede que utiliza, xa que no caso dunha rede de fibra o ancho de banda é maior.

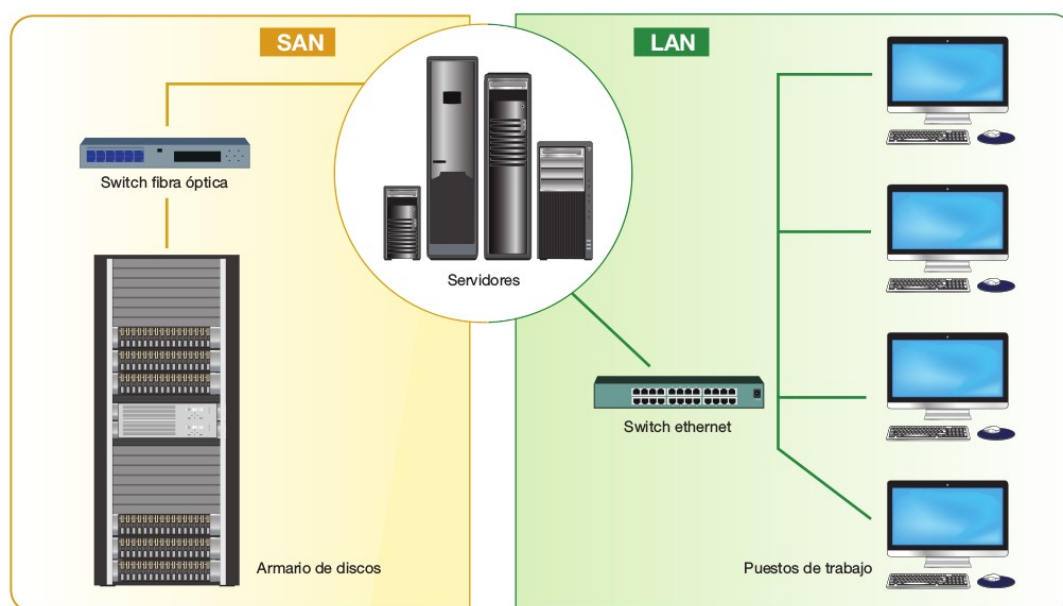


Figura 9: SAN vs LAN

3.9.3 Cloud Storage

Na planificación do almacenamento dunha organización tamén se debe pensar nos servizos que ofrece a computación na nube (Cloud computing), xa que entre estes servizos de computación a través de Internet ofrécese o de almacenamento de información. Desta forma, os clientes poden acceder á información en calquera momento mediante unha conexión a Internet desde calquera dispositivo fixo ou móbil situado en calquera lugar.

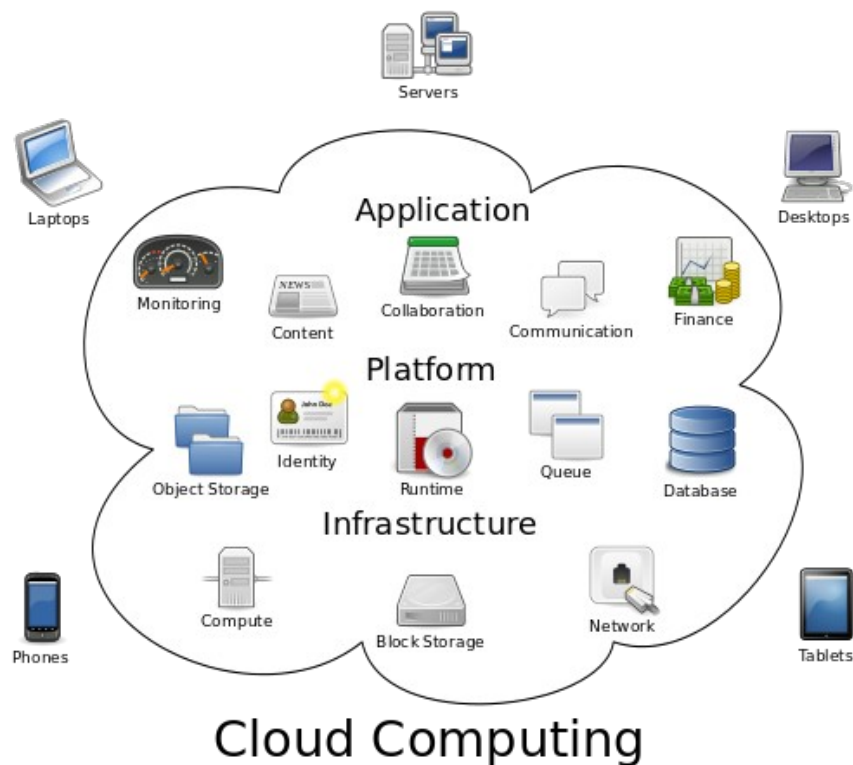


Figura 10: Paradigma Cloud

Entre outras, as vantaxes que proporciona este tipo de computación son as seguintes:

- Prestación de servizos a nivel mundial.
- Simplicidade e moito menor investimento inicial.
- Implantación máis rápida e con menos riscos, xa que as aplicacións adoitan estar dispoñibles en cuestión de horas ou días, en lugar de semanas ou meses. □ Actualizacións automáticas, co cal o usuario non se ve obrigado a dedicar tempo e recursos para volver personalizar e integrar a aplicación.

Pero tamén ofrece desvantaxes, como son, entre outras, as seguintes:

- Dependencia do provedor de servizos ao centralizar as aplicacións e o almacenamento de datos.
- A dispoñibilidade está suxeita á dispoñibilidade de acceso a Internet.
- Os datos sensibles non residen nas instalacións das organizacións, o que pode xerar un contexto de alta vulnerabilidade para a subtracción ou roubo de información.
- Seguridade da información, xa que debe recorrer diferentes nodos para chegar ao seu destino, sendo cada un deles un foco de inseguridade.

O almacenamento na nube, o como se coñece en inglés Cloud Storage, é un máis dos servizos que ofrece a computación na nube. Trátase, por tanto, dun modelo de almacenamento baseado en redes, onde os datos están aloxados en espazos de almacenamento virtualizados.

Os servizos de almacenamento na nube poden ser accedidos por diferentes medios, por exemplo a través dunha interface web.

A grande vantaxe do almacenamento na nube é a gran tolerancia a fallos que proporciona porque implementa redundancia e distribución de datos que posibilita a perpetuidade ou recuperación da información.

Hai distintos exemplos de almacenamento na nube (iCloud, Drive, Dropbox, OneDrive, etc...). Por exemplo, o iCloud de Apple Inc. que foi lanzado o 12 de outubro de 2011, permite aos usuarios almacenar datos en servidores remotos, tales como arquivos de música, vídeos, fotos, aplicacións, documentos, ligazóns favoritas do navegador, recordatorios, notas ou contactos. Cada conta ten 5 GB de almacenamento gratuíto.

3.10 Copias de seguridade

3.10.1 Introducción

En apartados anteriores viuse como nos sistemas RAID, algúns dos seus niveis, proporcionan redundancia de datos para poder ter acceso á información aínda que esta pérdase, corrompa ou se volva inaccesible nalgún dos dispositivos que conforman o RAID. Tamén se viu que se podía almacenar remotamente a información, de forma que se temos algún problema co equipo local, isto non afecta á información que está noutro dispositivo remoto, de forma que seguirá dispoñible.

Pero isto non é suficiente para manter a información segura e asegurarnos de que sempre estará dispoñible polo menos unha copia dos datos independentemente do que ocorra no sistema informático.

De todas as maneiras é necesario realizar copias de seguridade periódicas da información do noso sistema informático. Nesta unidade veremos tanto estratexias para realizar copias de seguridade dos datos como copias de seguridade do sistema operativo.

3.10.2 Definición de copia de seguridade

As copias de seguridade, copias de respaldo ou backups (polo seu nome en inglés) son unha medida preventiva na seguridade informática que consisten en copias dos datos orixinais, ou mesmo programas, co obxectivo de dispoñer dunha maneira de recuperalos en caso de perda sexa calquera a circunstancia que provoque que xa non teñamos accesible a información. As copias de seguridade garanten dúas características da información, vistas na primeira unidade:

- **Integridade:** refírese á calidade da información, xa que esta debe ser precisa e completa e non sufrir ningunha manipulación ou alteración respecto á orixinal sen a debida autorización.
- **Dispoñibilidade:** a información debe estar accesible en todo momento para calquera usuario que teña permisos para poder acceder a ela

3.10.3 Almacenamento das copias de seguridade

Recoméndase que as copias de seguridade realícense en dispositivos de almacenamento externos polos seguintes motivos:

- Poida que o sistema operativo non arranque e non sexamos capaces de acceder á información, e aínda que podamos o tempo necesario pode ser moi alto debido á súa complexidade.
- Borrado accidental dos datos.
- O disco duro deixa de estar accesible.
- O equipo informático estrágase.
- Virus que borra a información
- Roubo do equipo informático
- Desastres na contorna como: incendio, inundación, problemas eléctricos ou calquera outra catástrofe, que nos mellores dos casos deixa temporalmente non dispoñible e accesible a información, e nos peores dos casos resulta nunha perda total da información.

Os soportes de almacenamento externo onde se poden gardar as copias de seguridade son moi variados, pódese consultar a unidade de almacenamento de información onde se definen distintos dispositivos para almacenar información. Cada un destes soportes ten as súas vantaxes e desvantaxes que hai que ter en conta á hora de elixilos como soporte para gardar a copia de seguridade.

Hai uns anos a estratexia máis empregada para almacenar as copias de seguridade eran as cintas magnéticas, con todo estas están a ser desprazadas polos discos como soporte de destino dos backups. Os motivos principais deste fenómeno, entre outros son:

- Abaratamento dos discos.
- Mellora da fiabilidade.

Os discos duros de estado sólido ou SSD (*Solid-state drive*) son unha boa proposta para almacenar copias de seguridade pois usan memoria non volátil (como a memoria flash) para o almacenamento en lugar de pratos giratorios magnéticos dos discos duros convencionais. Desta forma, as unidades de estado sólido son menos sensibles a golpes, son practicamente inaudibles e teñen un menor tempo de acceso e de latencia (ao ser memorias de acceso aleatorio o tempo de busca de datos é sempre o mesmo). Outra característica é que consomen menos que un disco duro convencional.

As cintas, doutra banda, ofrecen unha serie de vantaxes que as fan un soporte de almacenamento a ter en conta:

- Son moi fiables.
- Facilmente transportables.
- Escaso custo para o seu almacenamento remoto de grandes volumes de datos.
- Sistema ecolóxico, debido a que durante o almacenamento non emprega corrente eléctrica. A robótica e as unidades de biblioteca consomen enerxía pero habitualmente menos que unha matriz de discos de capacidade similar.

3.10.4 Boas prácticas

Ala hora de realizar as copias de seguridade hai que ter en conta unha serie de aspectos para previr problemas relacionados coas copias de seguridade, xa que non só é importante seguir unha boa estratexia para realizar as copias de seguridade, senón que tamén hai que gardalas correctamente, elixir unha localización idónea e conservalas correctamente.

A continuación cítanse unha serie de boas prácticas que se deberían seguir cando se realice unha copia de seguridade:

- O dispositivo no que se garde a copia de seguridade non debe ser o mesmo que contén os datos sobre os que se realiza a copia, pois se se dana o dispositivo perderanse tanto os datos orixinais como a copia.
- Os dispositivos que conteñen as copias de seguridade non se deberían gardar na mesma sala ou mesmo no mesmo edificio que onde estea o sistema que contén os datos orixinais. A razón é que se hai algunha situación que provoque algún tipo de dano na área ou recinto e que afecte a que se perdan os datos orixinais, entón tamén se perderían as copias. Por exemplo, se un incendio destrúe a localización onde están os equipos e por tanto os datos, se as copias están no mesmo espazo físico, tamén se perderán.
- As copias de seguridade deberán etiquetarse seguindo unha estratexia que permita identificalas dunha maneira rápida, para poder dispoñer dela no menor tempo posible no momento de tela que usar para recuperar a información que contén. A etiquetaxe non debería conter información demasiado exhaustiva de forma que se algún atacante pretende subtraela poda identificar rapidamente o seu contido. Unha política correcta poderá ser utilizar códigos impresos en cada etiqueta, de forma que o seu significado sexa coñecido polos usuarios que teñen acceso a cópialas pero non por un potencial atacante.
- Con certa frecuencia debería verificarse o estado correcto das copias de seguridade, por se no momento de facer uso delas nos de a un erro inesperado. Como restaurar unha copia completa pode resultar ser demasiado traballo poderían recuperarse varios arquivos aleatorios da copia, asumindo que lla recuperación funciona, entón toda a copia é correcta.

- Os dispositivos de almacenamento non deberían reutilizarse por tempo indefinido, xa que co tempo poden dar erros, co que convén substituílos para evitar calquera problema.
- Un bo costume é realizar as copias de seguridade en momentos nos que o sistema non está a traballar a pleno rendemento. Debería buscarse o momento no que o sistema está menos saturado, e no que haxa a menor posibilidade de poder afectar os usuarios. Dependendo do sistema, en horas da noite e mesmo en fins de semana sería o mellor momento para realizar as copias.

3.10.5 Política de copias de seguridade

Para estar preparados ante calquera desastre que elimine a información do sistema, debemos planificar unha política de realización de copias de seguridade periódicas. Esta planificación idónea das copias de seguridade que se realizan, forma parte do plan de continxencia dunha empresa, xa que a perda de datos pode poñer en perigo a continuidade do negocio.

Algúns dos requisitos que debe cumprir a planificación de copias de seguridade son:

- Identificar os datos que requiren ser preservados. Son aqueles cuxa perda afectaría á continuidade do negocio. Débense indicar os discos, directorios, arquivos, etc., que se deben copiar.
- Establecer a frecuencia coa que se van a realizar os procesos de copia, así como o tipo de copia. Esta frecuencia inflúe na cantidade de información que se pode perder con respecto á fonte orixinal. Este parámetro é de suma importancia e require dunha análise exhaustiva. Por exemplo, se se realiza unha copia cada noite e o soporte estrágase ás 12 h toda a información xerada desde a noite anterior ata as 12 h non se atopará na copia de seguridade.
- Establecer o esquema de rotación: a rotación refírese á forma na que se almacenan e resgardan as copias de seguridade. Un esquema de rotación indica cantas cintas (ou outro tipo de soporte de almacenamento) utilízanse para realizar a copia de seguridade.
- Dispoñer o almacén físico para as copias. Este almacén determínase en función da seguridade que require a información entre almacéns no mesmo edificio ou remotos en edificios externos. Por exemplo, se se produce un incendio no edificio da empresa, a información almacenada nun edificio externo segue estando dispoñible.
- Buscar unha probabilidade de erro mínima, asegurándose que os datos son copiados integramente do orixinal e nuns soportes fiables e en bo estado. Non se deben utilizar soportes que estean preto de cumprir a súa vida útil para evitar que fallen cando se vaia a recuperar a información que conteñen.
- Controlar os soportes que conteñen as copias, gardándoos nun lugar seguro e restrinxindo o seu acceso só ás persoas autorizadas.

- Planificar a restauración das copias:
 - Formando aos técnicos encargados de realizalas.
 - Dispoñendo de soportes para restaurar a copia, diferentes dos de produción.
 - Establecendo os medios para dispoñer da dicha copia no menor tempo posible.
- Probar o sistema de forma exhaustiva para comprobar a súa correcta planificación e a eficacia dos medios dispostos.
- Definir a vixencia das copias, establecendo un período no que a devandita copia deixa de ter validez e pode substituírse por unha copia máis actualizada da información.
- Controlar a obsolescencia dos dispositivos de almacenamento. Para o caso daquelas copias que almacenan información histórica da organización, por exemplo proxectos xa pechados, débese ter en conta o tipo de dispositivo no que se realizou a copia, para evitar que no momento que se requira a restauración da devandita información non existan xa lectores acomodados para o devandito dispositivo.

Cando se descarten os soportes de almacenamento, porque chegasen ao límite de vida útil fixado na política de copias de seguridade, é importante realizar un proceso de borrado seguro ou destrución para asegurar que a información que contén non poderá ser recuperada posteriormente.

- Especificar os sistemas de copias de seguridade sobre todo cando se deben realizar copias de seguridade en sistemas que non é posible detelos para realizar a copia en frío, polo que se debe indicar que estratexia se vai a utilizar para realizar a copia en quente.



Consultar copias de seguridade e esquemas de rotación:

<https://searchdatacenter.techtarget.com/es/consello/Como-optimizar-a-sua-estratexia-de-rotacion-de-cintas-de-respaldo>

3.10.6 Tipos de copias de seguridade

Hai tres tipos de copias de seguridade: completa, diferencial e incremental.

3.10.6.1 *Copia completa*

Neste tipo de copia créase unha copia de todos os arquivos e directorios seleccionados. A primeira vez que se realiza unha copia sobre a información adoita ser deste tipo. Como estas copias ocupan unha gran cantidade de espazo de almacenamento, non é práctico utilizar sempre este tipo de copias, senón que se deben alternar cos dous tipos seguintes.

- Vantaxes:
 - A recuperación total ou parcial dunha copia completa é fácil de realizar.

- Desvantaxes:
 - Este tipo de copia, dependendo do tamaño dos arquivos, pode consumir moito tempo e espazo.
 - O tempo de busca e recuperación tamén pode ser alto.

3.10.7 Copia diferencial

A copia de seguridade diferencial conterá todos os arquivos que se crearon ou modificaron desde a última copia completa. Para restaurar os datos necesítase a última copia completa e a última copia diferencial.

- Vantaxes:
 - Este tipo de copia require menos tempo e menos espazo para o seu almacenamento que a copia completa.
- Desvantaxes:
 - É máis lenta que as copias incrementais, e non ten un uso tan eficiente do espazo, xa que todos os arquivos engadidos ou modificados despois da copia completa serán duplicados en cada copia diferencial.
 - A restauración é máis lenta e un pouco máis complexa que nas copias completas, pero máis sinxela que nas copias incrementais.

3.10.8 Copia incremental

Neste caso só xérase unha copia dos datos que foron creados ou modificados desde a última copia, sexa do tipo que sexa. Para restaurar os datos, necesítase a última copia completa e todas as copias incrementais realizadas desde entón.

- Vantaxes:
 - É o tipo de copia máis rápida.
 - Fai un uso eficiente do espazo de almacenamento xa que os ficheiros non están duplicados.
 - Necesítase menos espazo de almacenamento comparado coas copias completas e diferenciais.
- Desvantaxes:
 - As restauracións son máis lentas que nas copias completas e diferenciais.

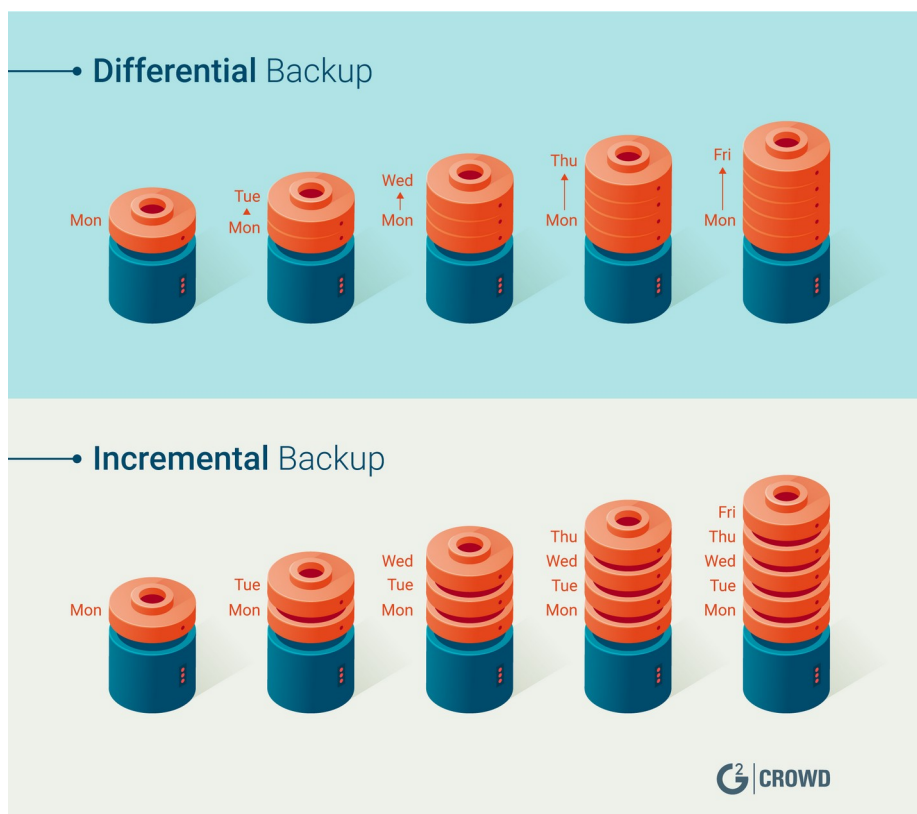


Figura 11: Backup diferencial vs incremental

3.11 Aplicación práctica das copias de seguridade

Existen multitude de ferramentas que nos permiten realizar copias de seguridade dos datos nos sistemas operativos. Hai ferramentas que son propias do sistema e outras de terceiros que permiten realizar distintos tipos de copias de seguridade.

3.11.1 Copias de seguridade con ferramentas do sistema

Tanto o sistema operativo Windows como Linux, teñen ferramentas propias que permiten realizar copias de seguridade.

3.11.1.1 Windows

Neste sistema operativo proporciona dous métodos para realizar e restaurar copias de seguridade dos volumes existentes localmente:

- Liña de ordes coa utilidade wadmin: permite ademais configurar ou modificar unha programación de copia de seguridade diaria.
- Ferramenta gráfica Copias de seguridade de Windows: permite programar a realización das copias para que se realicen nun determinado momento, por exemplo, semanalmente.

3.11.1.2 Linux

As distribucións Linux ofrecen unha serie de comandos básicos que son estándares e están presentes en todas as distribucións o que supón unha gran vantaxe xa que é posible realizar as copias de seguridade en calquera distribución así como restauralas en caso de necesidade. Isto non ocorre do mesmo xeito coas ferramentas propias que proporcionan moitas distribucións, xa que se se realizan as copias con estas ferramentas necesitaranse as mesmas ferramentas para restaurar as copias. Isto significa que llo computador onde realizamos as copias falta, debemos de dispoñer doutro computador coa mesma distribución para poder acceder as copias de seguridade e poder traballar con elas para posibles restauracións. Entre os comandos básicos está o programa tar: o seu nome provén de Tape ARquiver (arquivador en cinta) xa que foi deseñado para almacenar arquivos en cintas magnéticas.

Este programa é usado para almacenar arquivos ou directorios nun só arquivo. Tar é unha orde que pode ser executada desde un terminal e o seu formato comunmente é:

```
tar <opcións> <arquivoSaída> <arquivo1> <arquivo2> ... <arquivoN>
```

onde:

- <arquivoSaída> é o arquivo resultado
- <arquivo1><arquivo2>...<arquivoN> son os diferentes arquivos que serán empaketados no <arquivoSaída>

Unha vez realizado o empaquetado de arquivos, o arquivo empaquetado con extensión .tar que se tratará como unha copia de seguridade, deberá almacenarse noutra localización, co cal sería conveniente almacenar o arquivo noutro dispositivo de almacenamento, ou mesmo nun dispositivo de almacenamento remoto. Deberían aplicarse as boas prácticas das copias de seguridade comentadas nun apartado anterior a leste arquivo empaquetado. Linux proporciona tamén unha forma para a automatización de tarefas usando crontab ou o programador de tarefas, que é unha interface gráfica para crontab. Para utilizar crontab débese coñecer a diferenza del con cron. Cron é un servizo, un proceso que se executa en segundo plano, sen interactuar co usuario, que é usado para programar tarefas que serán executadas nun tempo específico. Por outra banda, crontab é un arquivo de texto e cada usuario posúe o seu. Neste arquivo o usuario pode especificar o momento en que se executará unha determinada tarefa. É así como no interior do arquivo crontab atópase unha lista de comandos e os seus respectivos tempos de execución. Ambos os factores son controlados polo servizo cron e son levados a cabo en segundo plano polo sistema. Como usuario pódese usar cron de dúas formas: editando o arquivo crontab ou mediante o programador de tarefas.

A estrutura dunha entrada no arquivo crontab é a seguinte:

```
[m] [h] [dom] [mon] [dow] [command]
```

Na seguinte táboa vemos o que significa cada parámetro:

- m: minute (0-50)

- h: hour (0-23)
- dom: day of month (1-31)
- mon: month (1-12)
- dow: day of week (1-7)
- command: comando a executar

Na seguinte liña podemos ver un exemplo onde se desexa executar un script chamado `copia_completa.sh` o primeiro día de cada mes, ás 9 da tarde:

```
* 21 1 * * /home/proba/copia_completa.sh
```

Outra ferramenta de interese que proporciona Linux é `rsync`, que ven instalada por defecto en Ubuntu. Esta ferramenta é moi potente e permite sincronizar cartafolios de forma incremental e permite traballar tamén con datos comprimidos e cifrados. Mediante unha técnica de delta decoding, permite sincronizar arquivos e directorios entre dúas máquinas dunha rede ou entre dúas localizacións nunha mesma máquina, minimizando o volume de datos transferidos.

A invocación máis sinxela da aplicación a través da liña de ordes é cando se usa de forma local:

```
rsync [OPCIONES] ... ORIXE [ORIXE]...DESTINO
```

Para o acceso remoto temos dúas opcións:

- Cando se realiza a sincronización desde unha orixe local a un destino remoto
 - `rsync [OPCIONES] ... ORIXE [ORIXE]...[USUARIO@]HOST:DESTINO`
- Cando se realiza a sincronización desde unha orixe remota a un destino local
 - `rsync [OPCIONES] ... [USUARIO@]HOST:ORIXE [DESTINO]`

Onde:

- ORIXE: é o arquivo ou directorio (ou unha listaxe de múltiples arquivos e directorios) dos que realizar a copia.
- DESTINO: é o arquivo ou directorio onde se realizará a copia.
- OPCIONES: opcións para indicar como se realizará a sincronización

Como para usar `rsync` simplemente temos que executar un comando, podemos utilizar `cron` ou a aplicación Tarefas planificadas para programar a sincronización. Tamén se pode crear un script que conteña o comando para realizar a sincronización, e logo executalo de forma automática como se fixo en tarefas anteriores.



Consultar `rsync`:

<https://en.wikipedia.org/wiki/Rsync>

3.11.2 Copias de seguridade con aplicacións específicas

Existen multitude de ferramentas, moitas delas gratuítas, que permiten facer copias de seguridade en Windows ou en Linux. Algunhas delas mesmo son multiplataforma, de forma que se poden empregar ben en Linux ou en Windows. Ao ser máis específicas que as ferramentas incluídas nos sistemas operativos, fan que teñan opcións moi interesantes á hora de realizar copias de seguridade, como son que poden elixirse distintos algoritmos de cifrado ou que permiten compresión.

3.11.2.1 Windows

Cobian Backup é unha das ferramentas gratuítas para sistemas operativos Windows. Este programa é multitarefa, co que se poden crear copias de seguridade de forma local, nunha rede local ou mesmo en/desde un servidor FTP.

As características que achega esta aplicación son as seguintes:

- Consome poucos recursos e pode estar a funcionar en segundo plano.
- Permite programar tarefas para realizarse no instante, de forma diaria, semanal, mensual, anual ou nun tempo especificado.
- Permite realizar calquera dos tres tipos de copias de seguridade: completa, incremental ou diferencial.
- Soporta compresión ZIP ou 7Zip.
- Ofrece a opción de protexer todas as funcións do programa por contrasinal.
- Existe a opción de cifrar os seus arquivos usando 4 métodos diferentes de cifrado forte.
- Pode definir eventos disparados antes ou despois da copia, por exemplo provocar o peche dun determinado programa que utilice un arquivo que se vai a copiar e facer que unha vez inicializada a copia volva iniciar



Consultar ConbianSoft:

<https://www.cobiansoft.com>

Outra aplicación da que podemos facer uso en Windows para facer copias de seguridade e restauracións é Areca. A principal vantaxe desta aplicación é que é unha solución Open source e pode ser executada tanto en Windows como en Linux. Así, todas as características e a tarefa realizada con este software poden aplicarse tanto a un sistema operativo Linux como a un Windows. A ferramenta ademais, pode utilizarse coa interface gráfica ou a través da liña de ordes.



Consultar Areca Backup:

<http://www.areca-backup.org>

3.11.2.2 Linux

En Linux tamén se poden instalar ferramentas específicas como en Windows, para poder realizar copias de seguridade. Por exemplo a aplicación Areca Backup pode tamén instalarse en Linux, co cal o modo de traballo e as características van ser idénticas.



Consultar aplicacións de copia de seguridade:

<https://help.ubuntu.com/community/BackupYourSystem>

3.11.3 Copia de seguridade do rexistro de Windows

O rexistro de Windows é unha base de datos xerárquica que almacena os axustes de configuración e opcións nos sistemas operativos Microsoft Windows. Contén a configuración dos compoñentes de baixo nivel do sistema operativo, así como das aplicacións que hai funcionando na plataforma.

Por tanto, o rexistro contén información que Windows utiliza como referencia continuamente, por exemplo os perfís dos usuarios, as aplicacións instaladas no equipo e os tipos de documentos que cada aplicación pode crear, as configuracións das follas de propiedades para os cartafolios e as iconas de aplicacións, os elementos de hardware que hai no sistema e os portos que se están utilizando.

Así, é conveniente facer unha copia de seguridade do rexistro, xa que un cambio erróneo no rexistro pode orixinar que o equipo deixe de funcionar.

3.12 Imaxes de respaldo e restauración

3.12.1 Introducción

En apartados anteriores vimos como se podían facer copias de seguridade dos datos e como realizar a súa restauración. Agora veremos como facer copias de seguridade do sistema, que aínda que non é tan importante como a copia de seguridade dos datos, si que será útil á hora de restaurar o sistema operativo no caso de que este falle, xa que nos aforra moito tempo. Veremos tamén en que consiste a conxelación dun sistema, que é outra estratexia que se pode levar a cabo para ter que recuperar un sistema operativo en caso de fallo ou erro. Outro aspecto que se tratará neste tema é como realizar a recuperación de datos que foron borrados do sistema

3.12.2 Imaxes de respaldo

Unha imaxe do sistema é unha copia exacta do estado completo do sistema nalgún modo non volátil, por exemplo un arquivo. Pode considerarse que é unha copia de seguridade do sistema. A leste proceso tamén se lle denomina clonación.

Unha imaxe de respaldo proporciona un método para volver instalar todo o sistema operativo, todos os programas, toda a estrutura e contido do disco ou partición do que se fixo a imaxe, e deixalo no mesmo estado que estaba xusto antes de que ocorrese o fallo

que provocou ter que restaurar unha imaxe, dunha maneira sinxela, cómodo e sobre todo permitindo que todo o proceso realícese en moi pouco tempo.

Poderíase pensar que para manter unha copia de seguridade dos datos poderíase facer unha imaxe do sistema, e desta forma poder ter a seguridade de poder recuperar tanto os datos como os programas e o sistema en xeral. Así, poderíamos aforrar traballo e tempo porque non nos necesitaría facer dous procesos diferentes, é dicir, por unha banda realizar a copia de seguridade só dos datos, e doutra banda clonar todo o sistema. Pero este pensamento non é correcto, xa que realizar unha imaxe do sistema pode levar moito tempo, así como tamén a súa restauración. Por exemplo, se chan necesitamos restaurar un directorio teríamos que restaurar todo o sistema, co que se provoca, por unha banda, que o sistema estea non dispoñible durante todo o tempo que tarda a restauración da imaxe e, doutra banda, estamos a investir un tempo demasiado excesivo, xa que a restauración da imaxe leva un tempo moito maior que o tempo que pode levar restaurar un directorio a través da copia de seguridade dos datos. Por iso, considérase máis apropiado facer unha copia de seguridade dos datos por unha banda e do sistema polo outro.

Outra características das imaxes de respaldo é que permite un despregamento rápido de sistemas de clons. Hai empresas que necesitan instalar ou restaurar computadores de forma masiva, isto implica que en cada un deles hai que instalar o sistema operativo e os programas, o cal implica moito tempo e esforzo, ademais de engadir outro aspecto, como é a posibilidade de erros humanos. Así, pódese preparar unha imaxe de disco, incluíndo o SO, software común e datos necesarios, e clonar con ela rapidamente o contorna software. Este método aforra tempo e esforzo, permitindo así poder enfocarse nas distincións únicas que deben levar cada sistema, no caso de que sexa necesario. A clonación pode realizarse das seguintes formas:

- De disco a disco: neste caso cópiase o contido de todo o disco noutro disco, que ben pode ser interno ou externo.
- De partición a partición: cópiase toda a partición noutra partición, que pode estar no mesmo disco ou noutro disco.
- A un arquivo de imaxe: neste caso pódese copiar todo o disco ou partición e esta copia almacenarse como un arquivo de imaxe, o cal podemos almacenar onde queiramos.

Existen varias ferramentas que permiten realizar a clonación dun sistema, a continuación indicamos algunhas delas:

- De pago: Acronis True Image, Norton Ghost, R-Drive Image, Paragon Backup & Recovery.
- Licenza GPL: Clonezilla, Paragon Backup & Recovery Free, DriveImage XML (Private Edition Free)

Existen outras moitas máis ferramentas para facer unha copia de seguridade do disco que contén o sistema operativo. Na actividade anterior viuse a utilidade propia de Windows

para realizar copias de seguridade, entre as opcións que presenta pódese crear unha copia e restaurar o volume que contén.



Consultar aplicacións de clonado de discos:

https://en.wikipedia.org/wiki/Comparison_of_disk_cloning_software

3.12.2.1 *Sistemas Live*

Unha opción interesante para crear imaxes de disco pode ser usar un sistema Ao vivo. Este sistema estará instalado nun CD ou, máis habitualmente na actualidade, unha memoria USB.

Consiste nunha instalación completa executable nun computador que a miúdo inclúe un sistema operativo. O sistema Live execútase na memoria do equipo, en lugar de cargarse desde un disco duro, por tanto o equipo debe ter suficiente RAM para almacenar eses arquivos e manter a operación normal. Para o seu funcionamento, non inflúe o sistema operativo que estea instalado na máquina anfitrión.

Estes sistemas Ao vivo permiten executar un programa, ou sistema operativo, sen telo que instalar nin facer cambios na configuración da máquina. Normalmente veñen acompañadas dun conxunto de aplicacións e mesmo poden incluír algunha ferramenta que permita instalalos no disco duro.

A miúdo, a execución dun sistema Ao vivo, non altera ningún sistema operativo ou arquivos xa instalados no almacenamento secundario da máquina, como pode ser en discos duros, pero moitos sistemas Ao vivo inclúen mecanismos software e utilidades para modificar datos almacenados no computador anfitrión, incluíndo a instalación dun sistema operativo. Isto é importante para aspectos de xestión de sistemas Ao vivo, xa que pode ser útil para eliminar malware, para crear imaxes de disco e para recuperación de sistemas. A menos que este tipo de software sexa utilizado, ao finalizar a sesión co sistema Ao vivo, o computador permanece como estaba anteriormente.

Para usar un sistema Ao vivo, o primeiro paso é obter un deles. Isto pode ser sinxelo pois moitos se distribúen libremente mediante unha imaxe ESO que pode descargarse da internet e gravarse nun disco, CD, DVD ou memoria flash. A continuación é necesario configurar o equipo anfitrión de forma que arranque desde a unidade lectora, así cando se reinicie o computador co disco na lectora o sistema Ao vivo executarase automaticamente.

Hai moitos sistemas Ao vivo para usar, no noso caso utilizaremos Clonezilla Ao vivo e Hiren's BootCD para crear imaxes do sistema.



Consultar sistemas ao vivo:

<https://clonezilla.org>

<https://www.hiren.info/pages/bootcd>

Como a execución dun sistema Ao vivo non depende do sistema operativo que estea instalado na máquina anfitrión, as tarefas que se van a levar a cabo poderían realizarse indistintamente sobre un sistema operativo Windows ou Linux.

3.12.3 Puntos de restauración en Windows

Os puntos de restauración de Windows son unha copia exacta do sistema operativo. Basicamente inclúe a súa configuración e o estado das preferencias dos programas, librerías e demais arquivos de Windows. A súa utilidade, como o seu nome indica, é poder restaurar o estado de Windows no caso de que ocorra un contratempo, como que o computador se infecte por un virus ou se eliminen certos arquivos imprescindibles para o bo funcionamento do sistema. É importante ter en conta que os puntos de restauración están enfocados ao sistema operativo Windows, non aos arquivos persoais, polo que se queremos protexer os documentos, imaxes ou vídeos, deberemos usar unha ferramenta para xerar copias de seguridade.

Por defecto, Windows crea puntos de restauración automaticamente cada sete días se non se creou ningún outro punto de restauración durante o últimos sete días ou cando detecta o comezo da realización de cambios no equipo. Aínda así, tamén se poden crear manualmente puntos de restauración, en especial antes de realizar unha tarefa ou acción que poida resultar potencialmente daniña para Windows, como instalar un programa ou desinstalar certo compoñente do sistema.

A protección do sistema atópase activa automaticamente para a unidade na que está instalado Windows e só pódese activar para as unidades formatadas co sistema de arquivos NTFS.

3.12.4 Recuperación de datos

Hai ocasións nas que a pesar de realizar copias de seguridade periódicas dos datos e imaxes de respaldo do sistema, podémonos atopar nunha situación de perda de datos. Isto pode darse por unha gran variedade de circunstancias como a acción dun virus, un borrado accidental, etc. Se non dispoñemos dunha copia destes datos perdidos hai dúas alternativas para tentar a recuperación dos datos:

- Levar o disco á empresa especializada en recuperación de datos, o que aínda que pode ser moi efectivo tamén ten un alto custo.
- Utilizar aplicacións de recuperación de datos. Esta solución aínda que pode non ser moi efectiva é bastante económica.

Cando se borra un arquivo, o que se fai realmente é marcalo como espazo non reutilizable, polo que é relativamente sinxelo recuperalo, a condición de que o espazo que ocupaba non fose escrito de novo. Isto fai que canto menos tempo pase desde o incidente que orixinou o borrado de datos e o intento de recuperación dos mesmos, máis posibilidades hai de poder conseguir a recuperación.

Hai numerosas aplicacións que nos permiten tentar a recuperación de arquivos, e como sempre unhas son gratuítas e outras de pago: Recuva, R-Linux, GetDataBack, Pandora Recovery, etc