Universidad de los Andes

Infraestructura Computacional

Sistema de Archivos

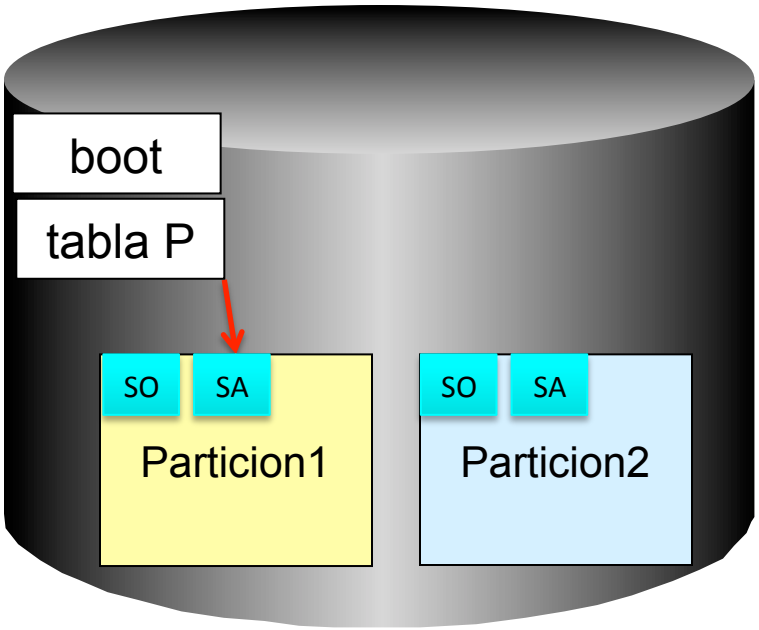
Universidad de los Andes

Sistema de Archivos

- Uno de los elementos más visibles del sistema operativo
- Elementos
  - Almacenamiento secundario
  - Administración del espacio
  - Representación para el usuario
  - Protección de archivos

Universidad de los Andes

Organización del Disco



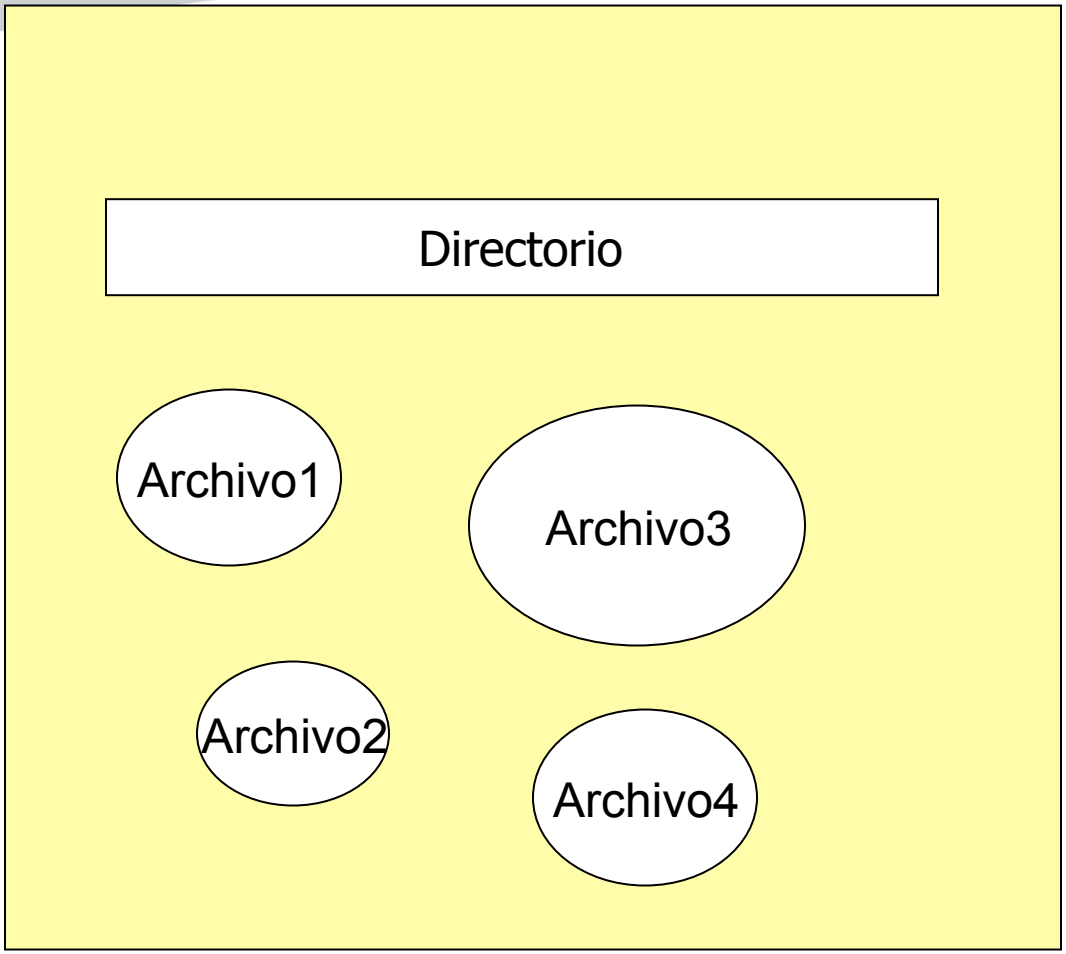
Universidad de los Andes

Organización del Disco

- La zona de boot sirve para la iniciación del sistema
- Hay una tabla que define la partición que se va a usar
- En cada partición hay un sistema de archivos

Universidad de los Andes

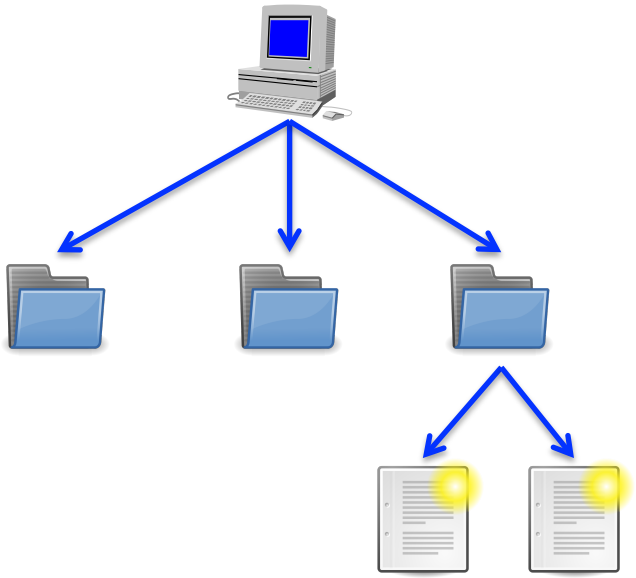
Sistema de Archivos



Universidad de los Andes

Directorios

- Aunque hay varias formas posibles de organizar el directorio, la más usual es en forma jerárquica



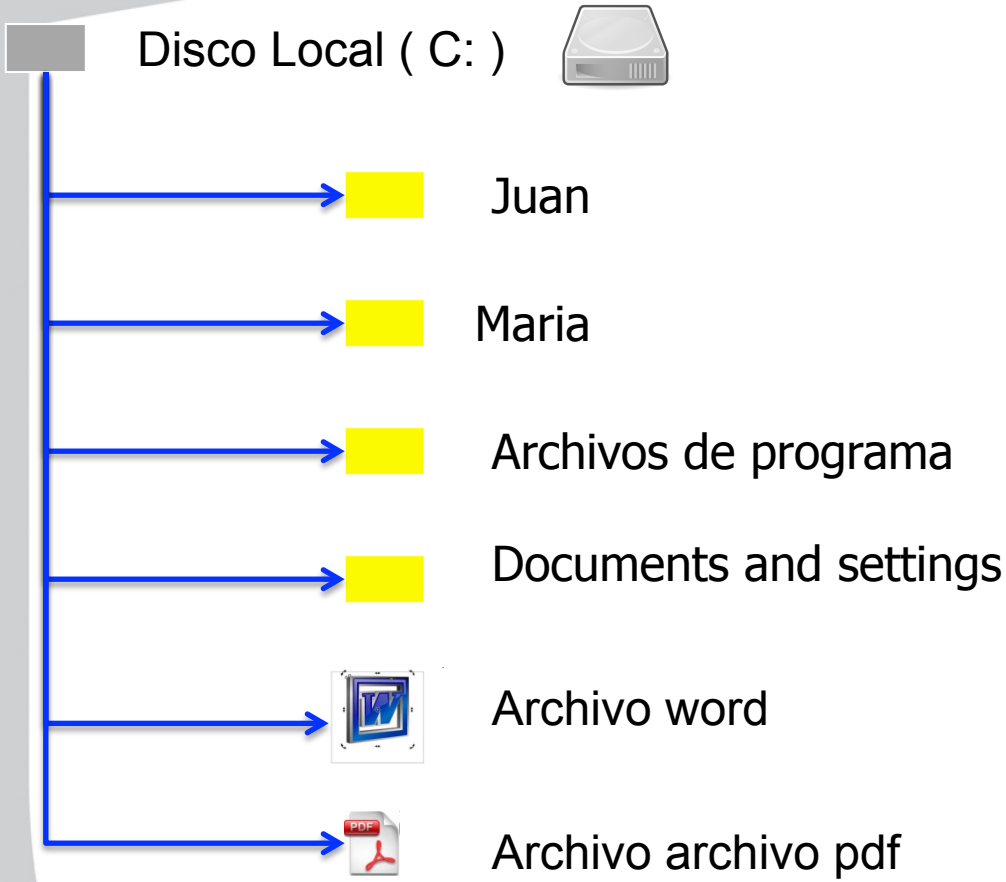
Organización en Windows

Mi PC

- Documentos de PPerez 
- Mis carpetas para compartir 
- Documentos compartidos 
- Unidad DVD –RW (E:) 
- Unidad CD –RW (D:) 
- Disco Local (C:) 

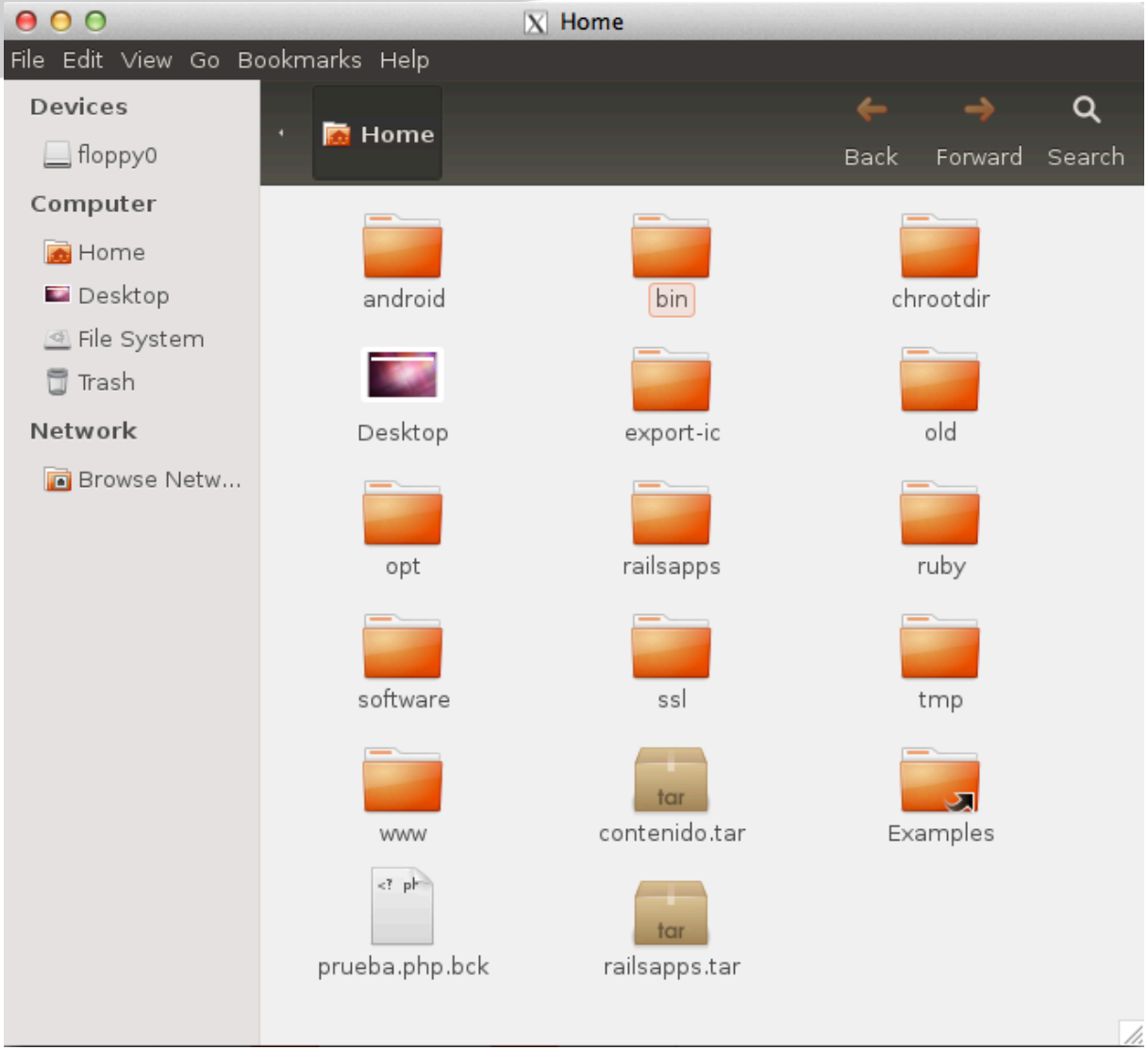
Organización en Windows

Contenido de una unidad Lógica



Universidad de los Andes

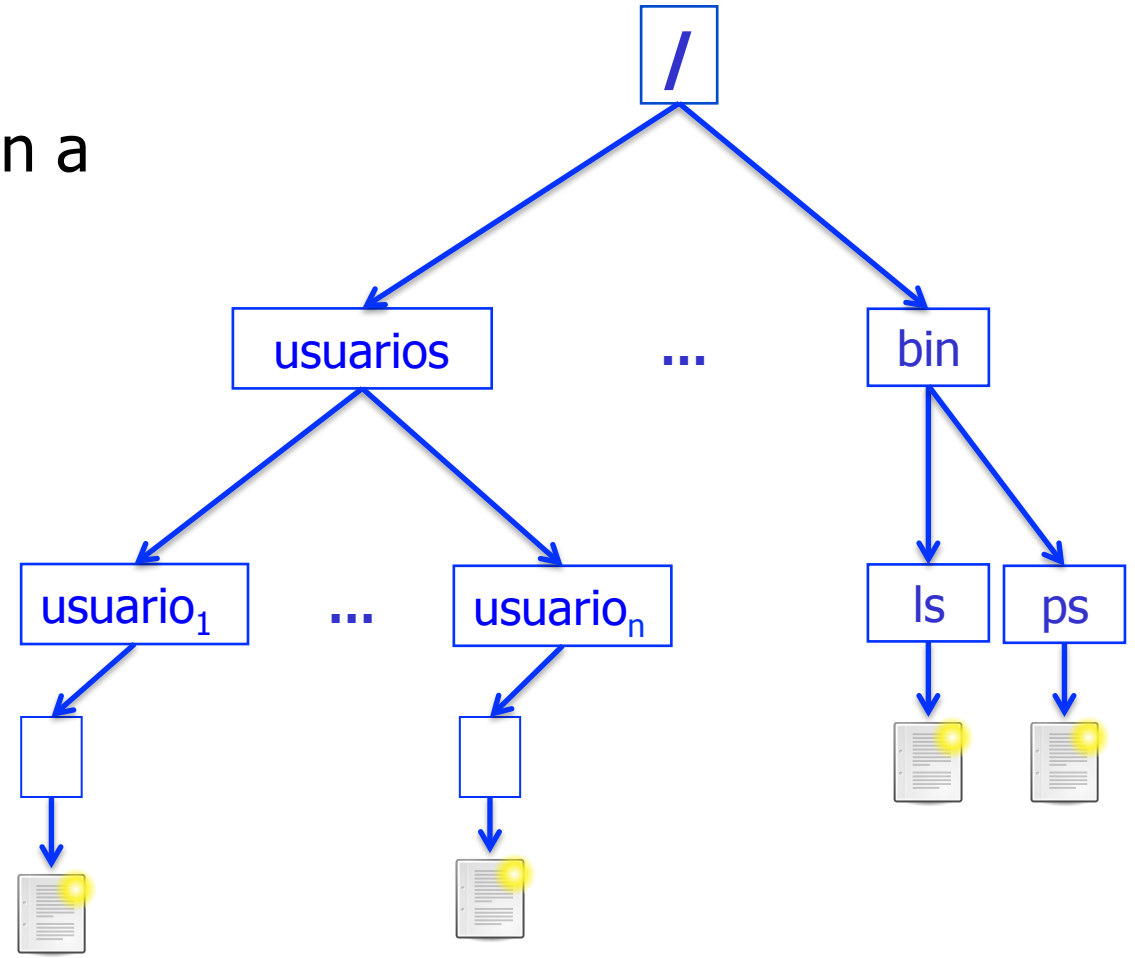
Organización en Unix/Linux



Universidad de los Andes

Directorios

- En el directorio hay subdirectorios o carpetas que ayudan a organizar la información



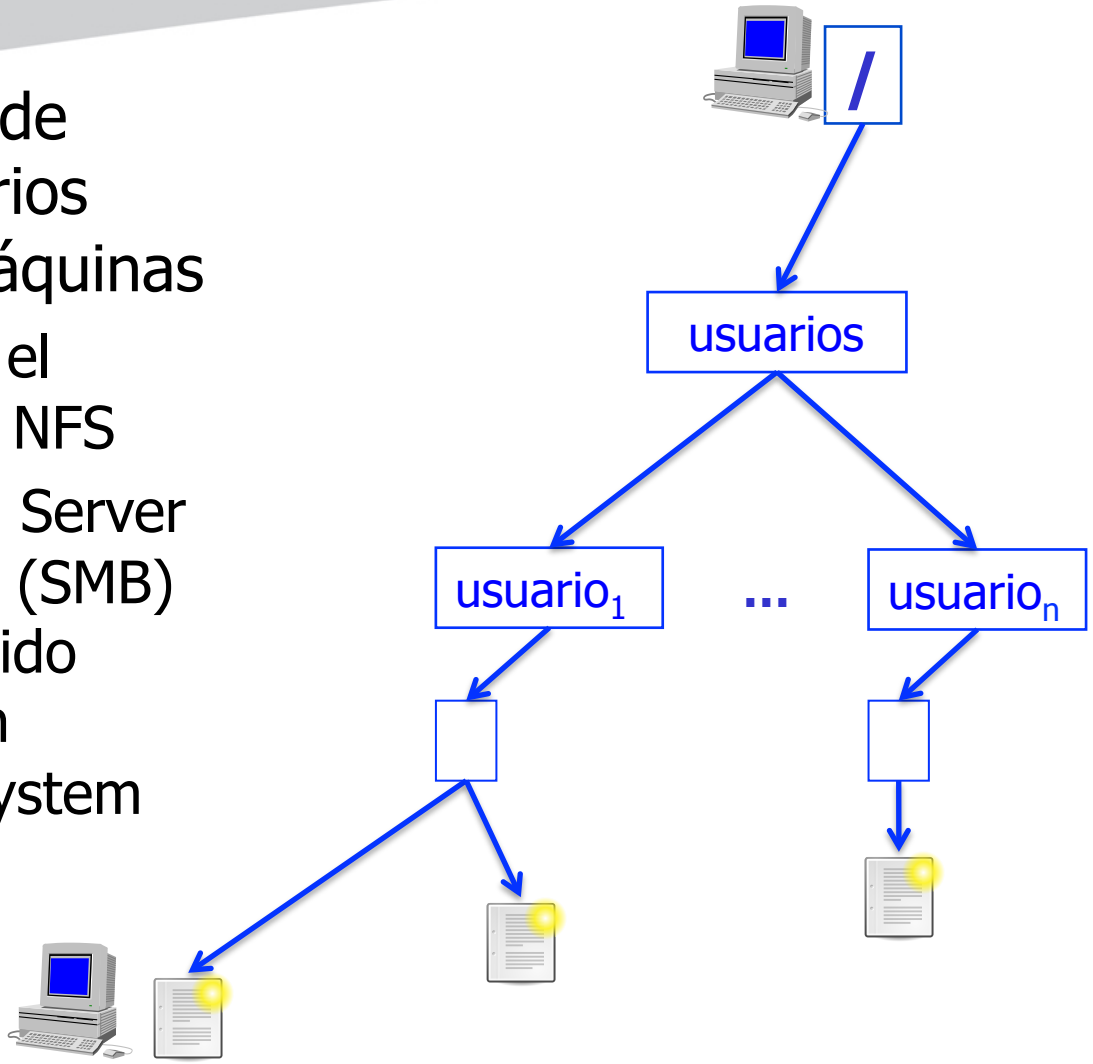
Universidad de los Andes

Descriptores

- Una ventaja del sistema FAT es que los subdirectorios son archivos
  - por consiguiente no tienen limitación en su tamaño
  - una tabla está limitada por el espacio asignado

Directorios

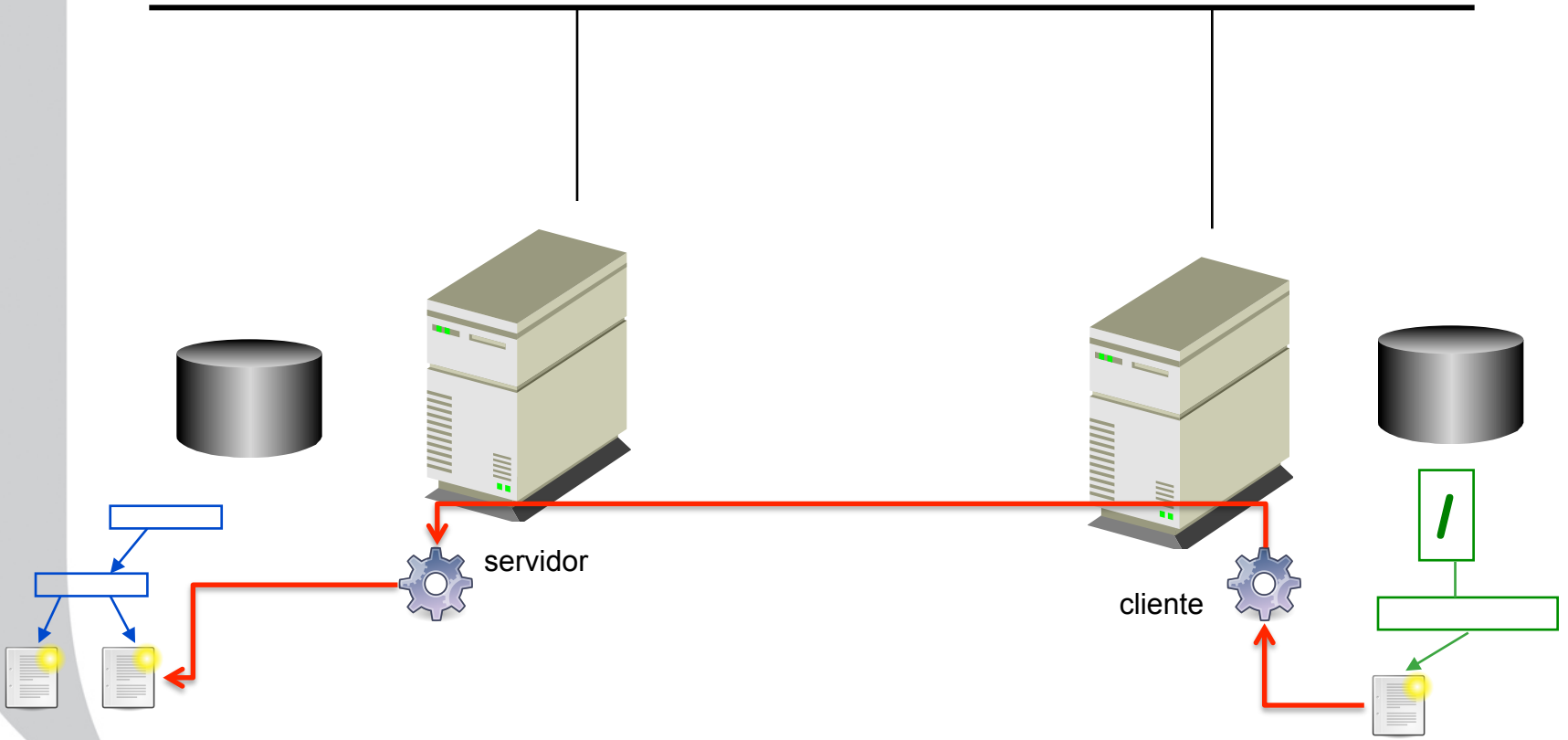
- El directorio puede extenderse a varios dispositivos y máquinas
  - En Unix existe el mecanismo de NFS
  - En Windows el Server Message Block (SMB) también conocido como Common Internet File System (CIFS)



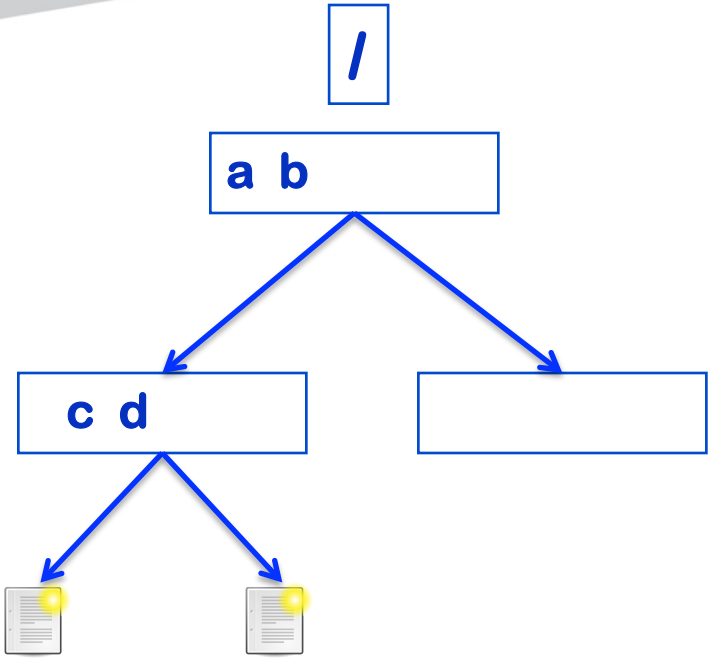
Universidad de los Andes

Directorios

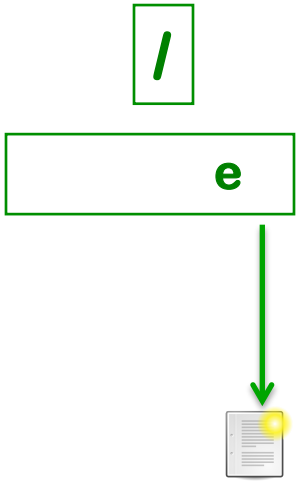
Funcionamiento de NFS



Directorios

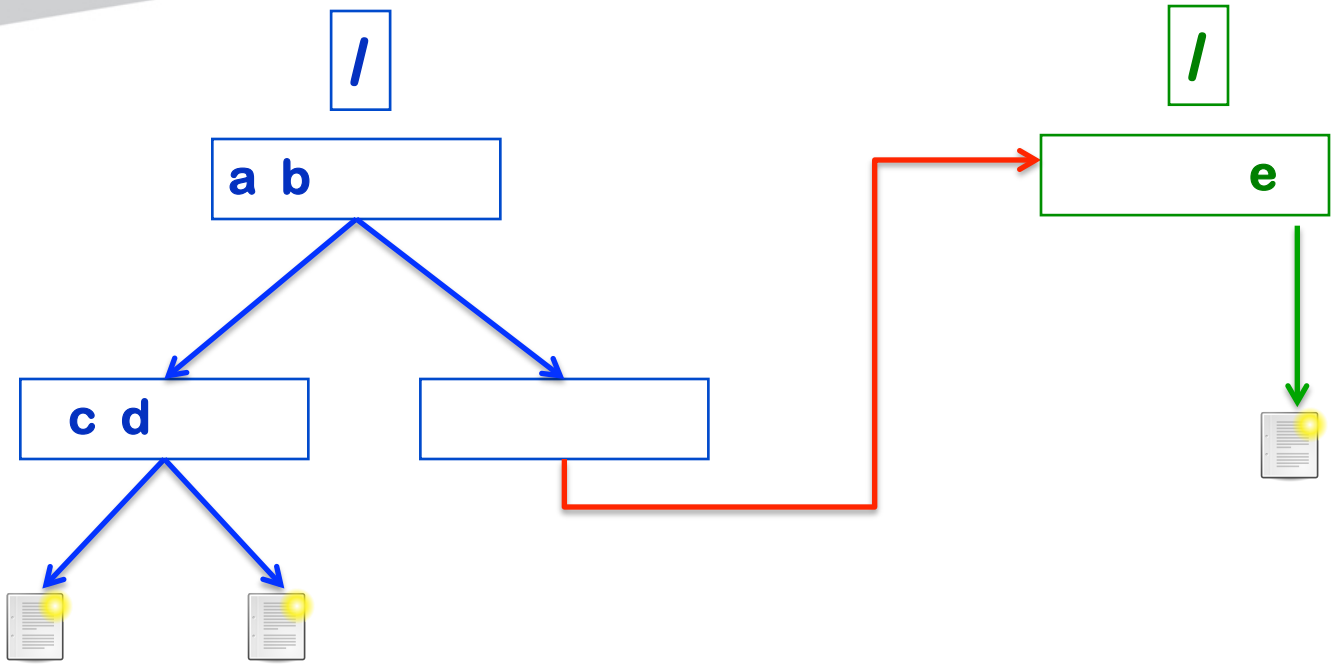


/ a / c
/ a / d
/ b



/ e

Directorios



/ a / c
/ a / d
/ b

/ b / e

/ e

Directorios

Mi PC

Documentos de PPerez

Mis carpetas para compartir

Carpeta remota

Documentos compartidos

Unidad DVD –RW (E:)

Disco Local (C:)

Universidad de los Andes

Directorios

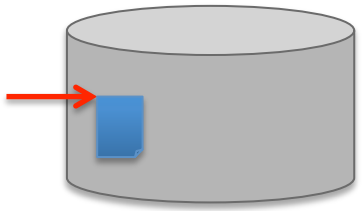
Mi PC

- Documentos de Maria
- Mis carpetas para compartir
- Documentos compartidos
- Unidad DVD –RW (E:)
- Disco Local (C:)
- Disco Local (D:)

Universidad de los Andes

Descriptores

- Un descriptor de archivo es una estructura de datos que contiene la información necesaria para manipular (leer de/escribir a) un archivo
  - Es un apuntador a un archivo



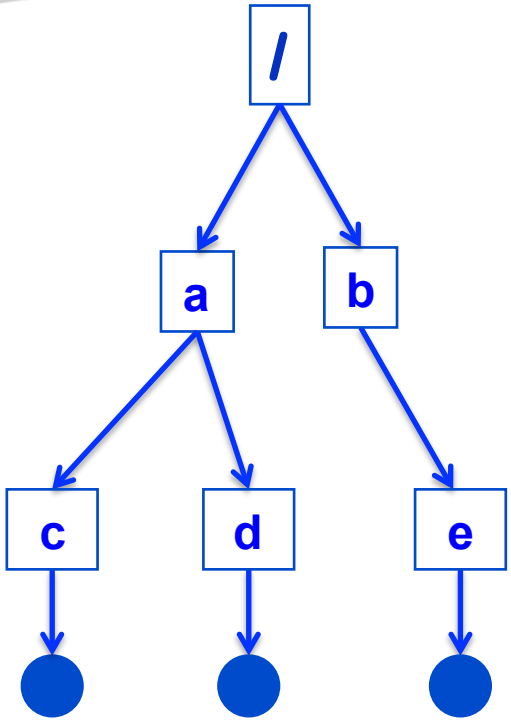
Universidad de los Andes

Descriptores

- Cada sistema tiene su forma de organizar un directorio
- Por ejemplo en el sistema de arhivos FAT los descriptores se encuentran en los subdirectorios

Universidad de los Andes

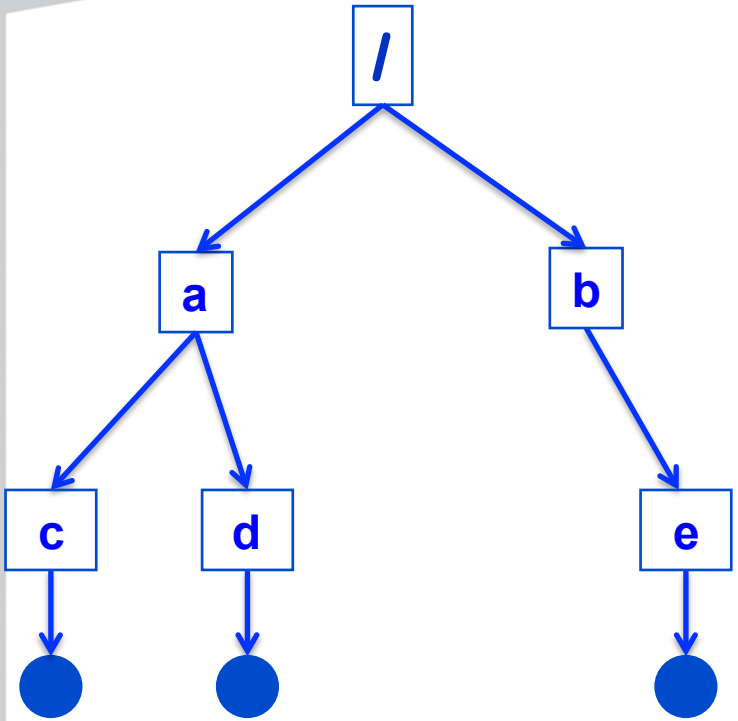
Descriptores

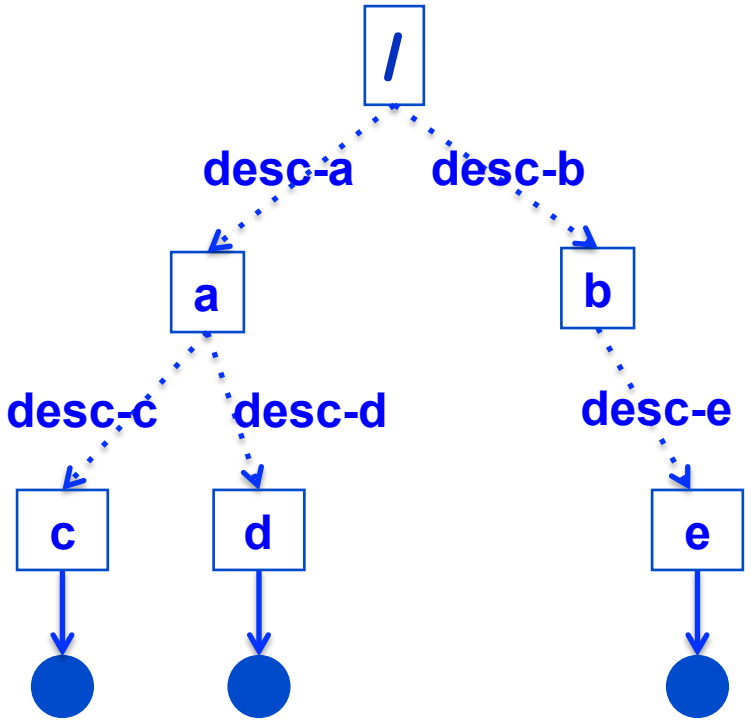


Representación Lógica

Universidad de los Andes

Descriptores





En algunos sistemas los descriptores están en los subdirectorios

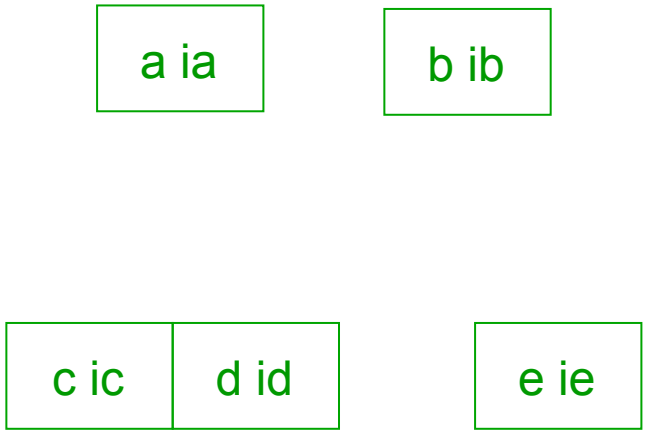
Universidad de los Andes

Descriptores

- En el sistema de arhivos de Unix los descriptores (nodos i) se encuentran en una tabla especial llamada tabla-i

Universidad de los Andes

Descriptores



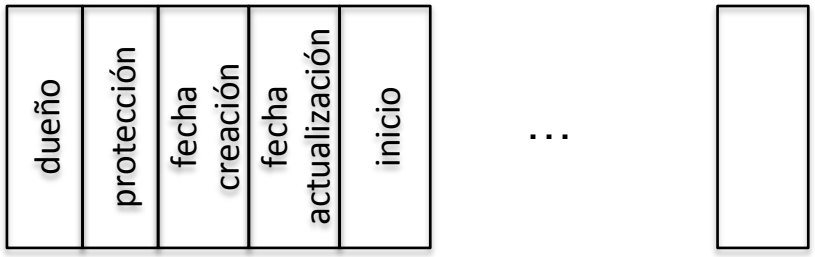
ia	a
ib	b
ic	c
id	d
ie	e

Tabla de i-nodos

Universidad de los Andes

Descriptores

- En el directorio, la información de cada archivo está representada con descriptores



Universidad de los Andes

Descriptores

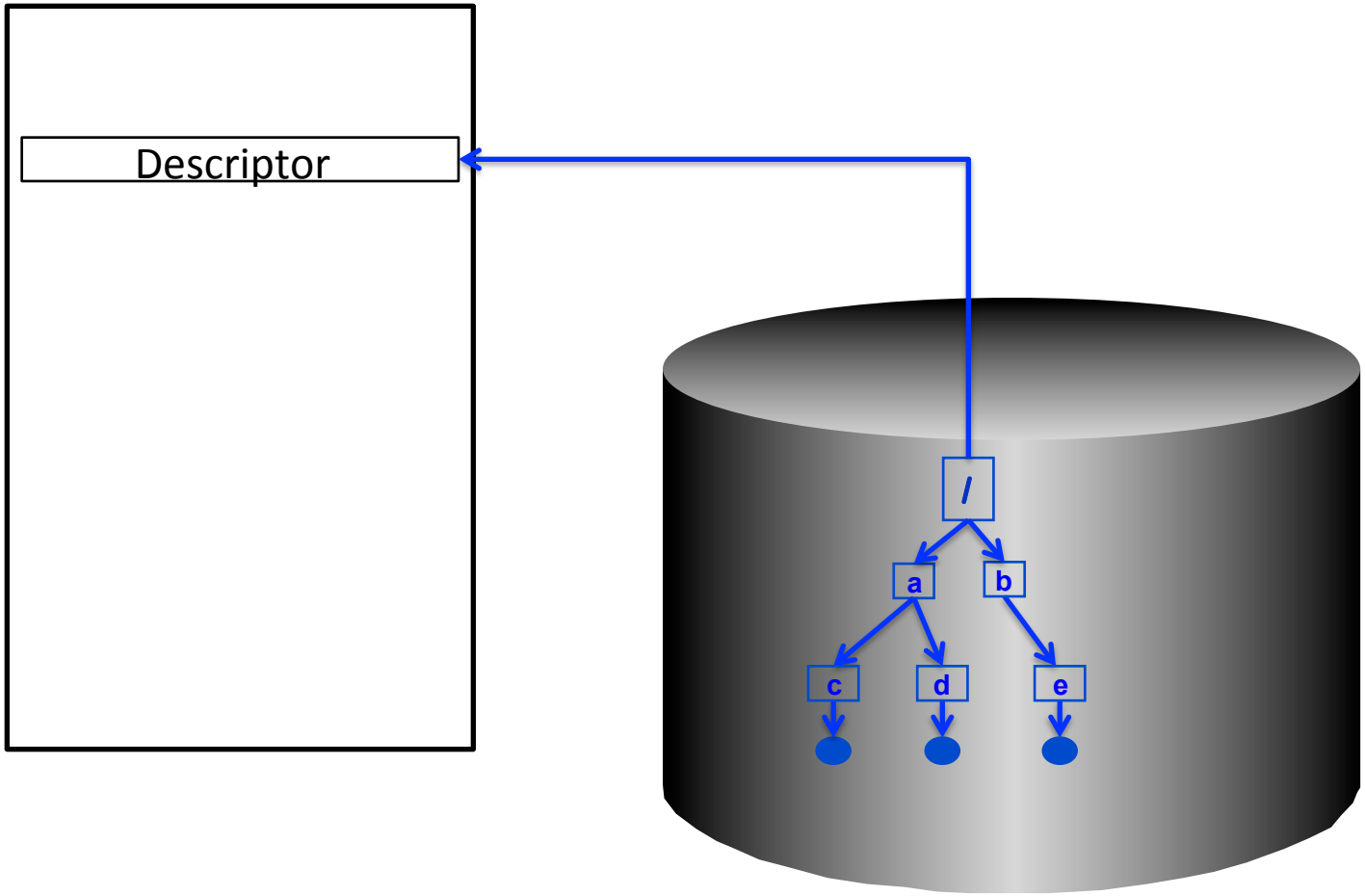
- Cuando se abre un archivo

```
des = open ( a1,…)
```

Lo que se hace es buscar su descriptor y llevarlo a memoria

Universidad de los Andes

Descriptores



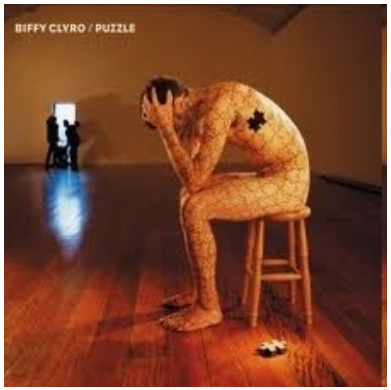
Universidad de los Andes

Descriptores

- De esa forma son mucho más eficientes las operaciones sobre el archivo
- ¿Por qué?

Universidad de los Andes

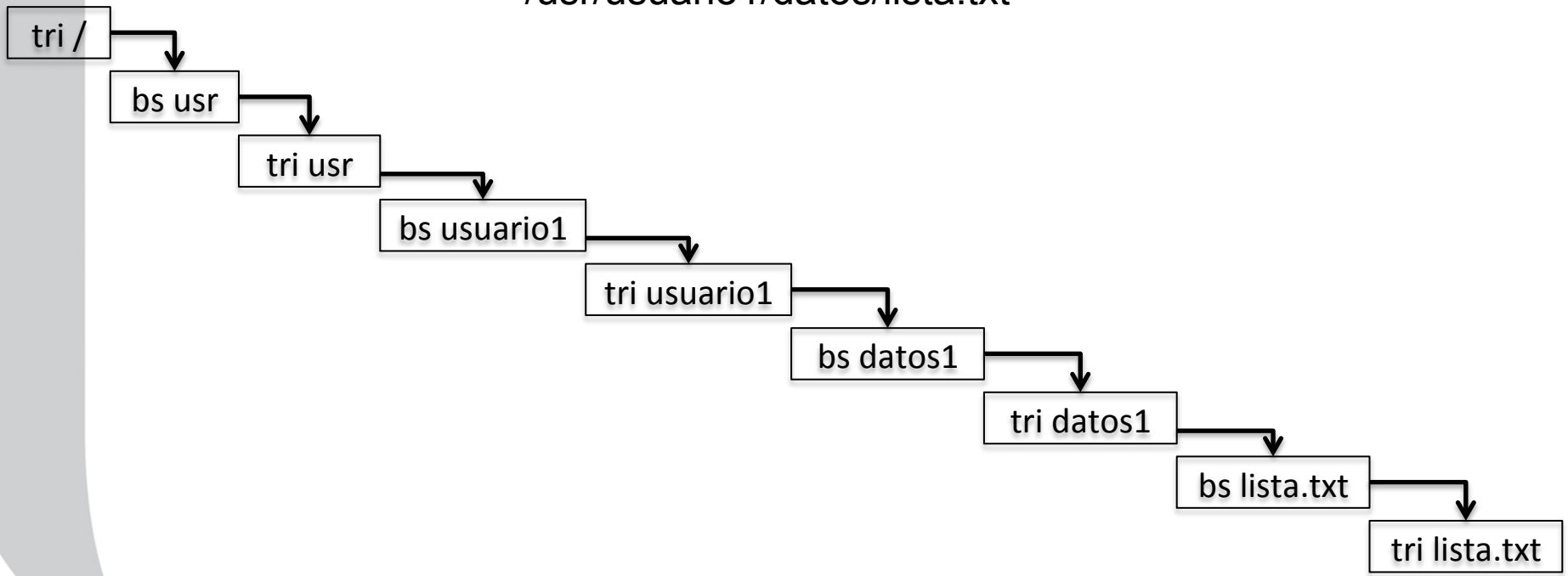
Hacer el algoritmo de lo que debe hacerse para abrir un archivo (en Unix).



Universidad de los Andes

Hacer el algoritmo de lo que debe hacerse para abrir un archivo (en Unix).

/usr/usuario1/datos/lista.txt



Universidad de los Andes

Hacer el algoritmo de lo que debe hacerse para abrir un archivo (en Unix).

¿Qué ocurre si se trabaja con NFS?

Universidad de los Andes

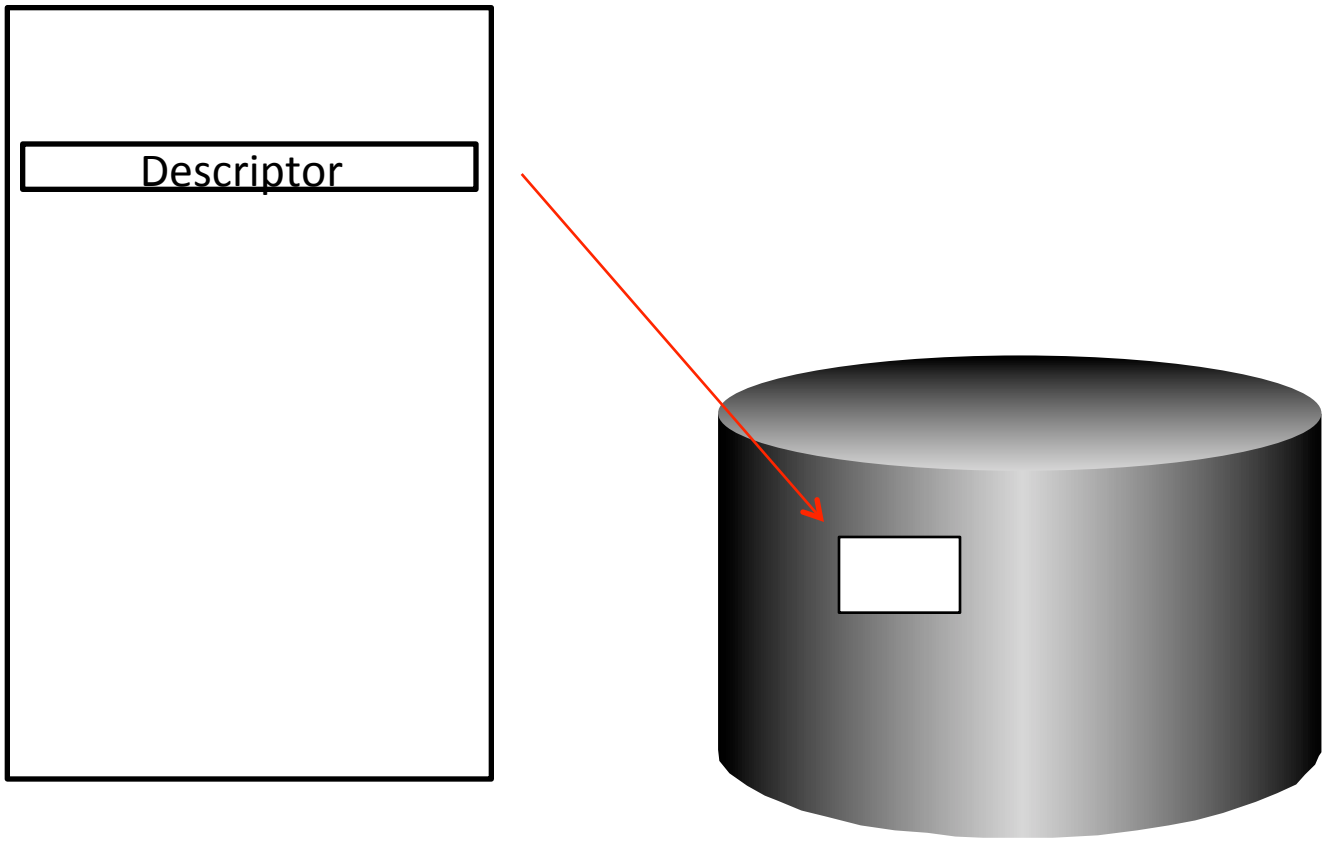
Administración de Espacio

- ¿Cómo asignar espacio a un archivo?
  - Un archivo tiene tamaño variable

Universidad de los Andes

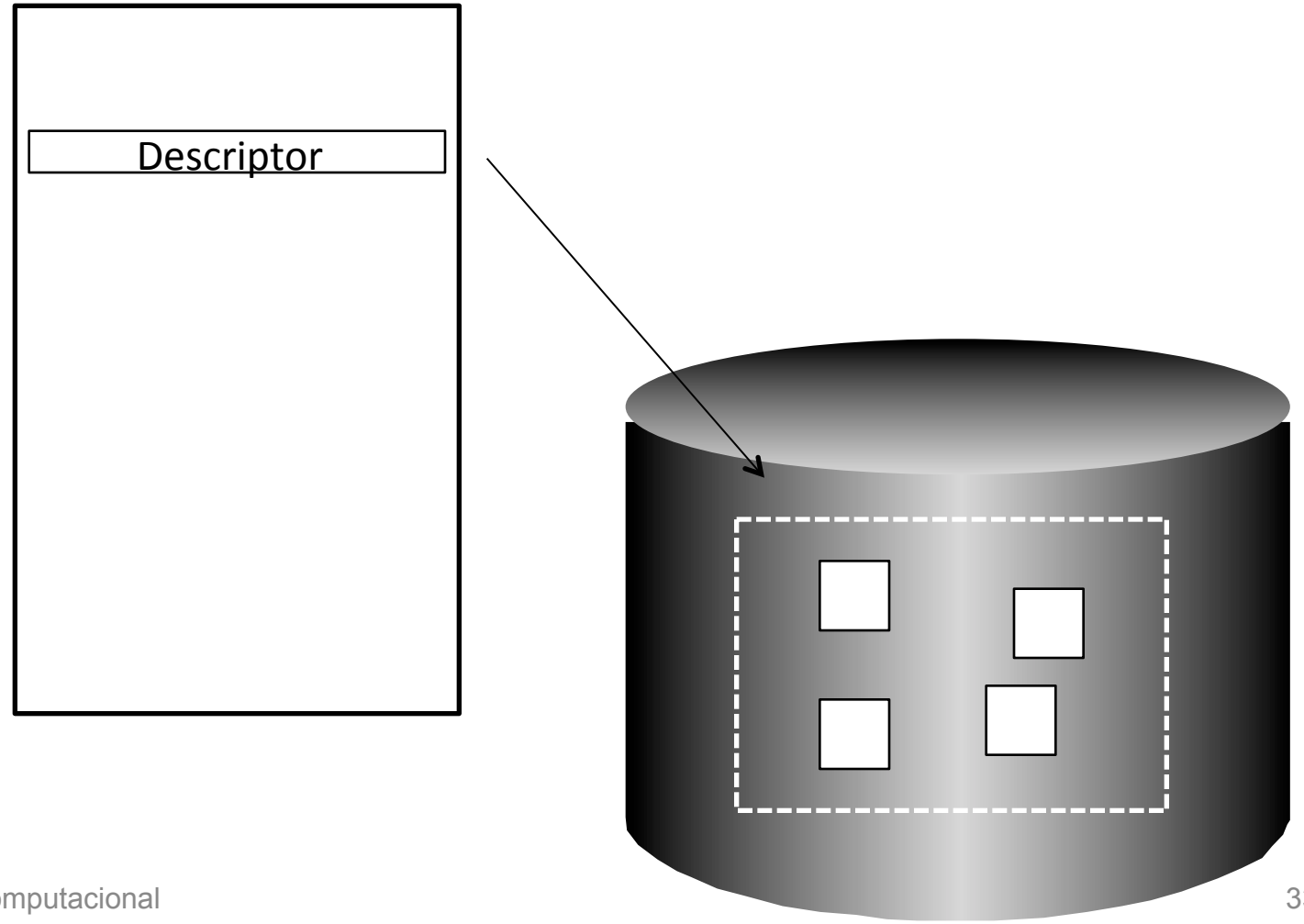
Administración de Espacio

- ¿Cómo asignar espacio a un archivo?
  - Un archivo tiene tamaño variable



Universidad de los Andes

Administración de Espacio



Universidad de los Andes

Administración de Espacio

- ¿Cuál esquema de asignación es mejor ?
  - Un bloque grande
  - Varios bloques pequeños

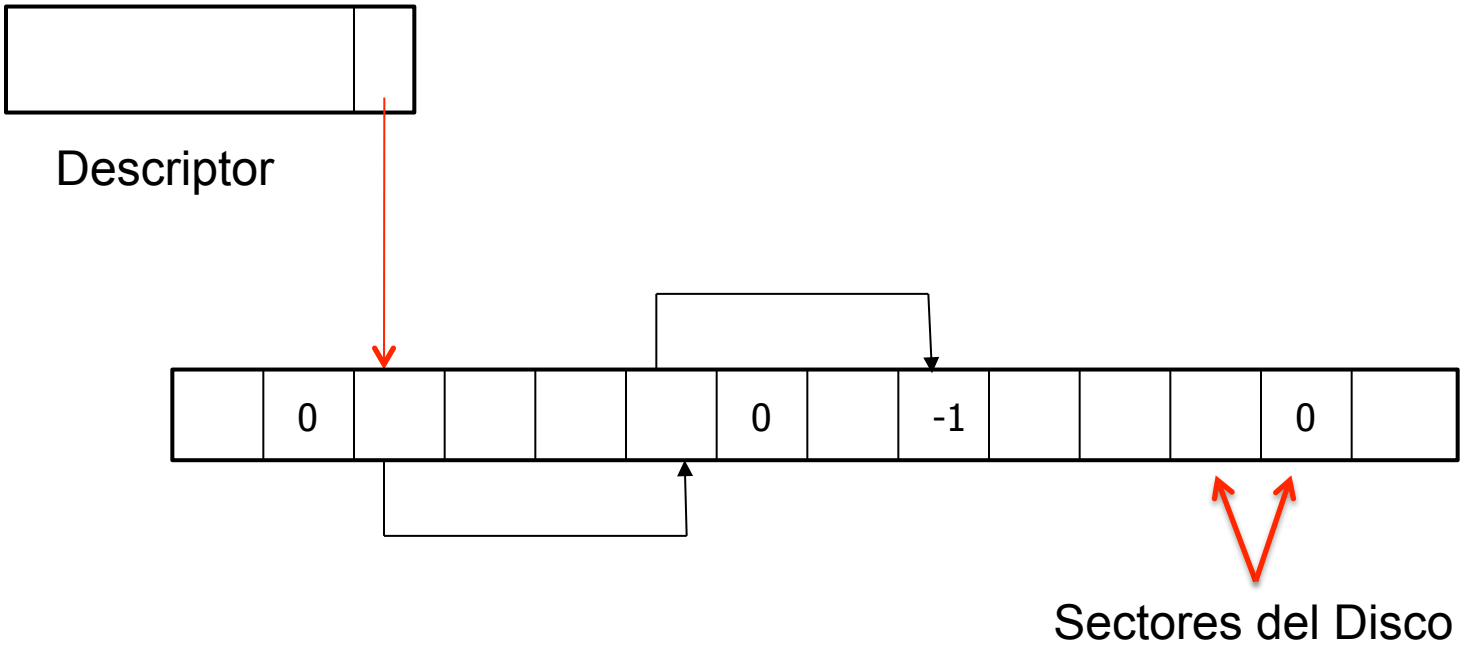
Universidad de los Andes

Administración de Espacio

- Cómo representar el espacio asignado a un archivo cuando hay varios bloques?

Administración de Espacio

- File Allocation Table



Universidad de los Andes

Administración de Espacio

- ¿Qué tan confiable es el sistema FAT ?
- ¿Por qué no se recomienda usar el sistema FAT ?
  - ¿Qué pasa si se daña la tabla?

Universidad de los Andes

Administración de Espacio

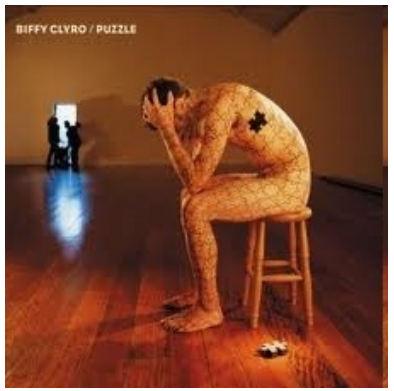
¿Cuánto espacio ocuparía la FAT en un disco de 32 GB?

¿Cuál es el tamaño máximo de espacio que puede ser manejado por una tabla FAT?

¿Cuál es el tamaño del archivo más pequeño?

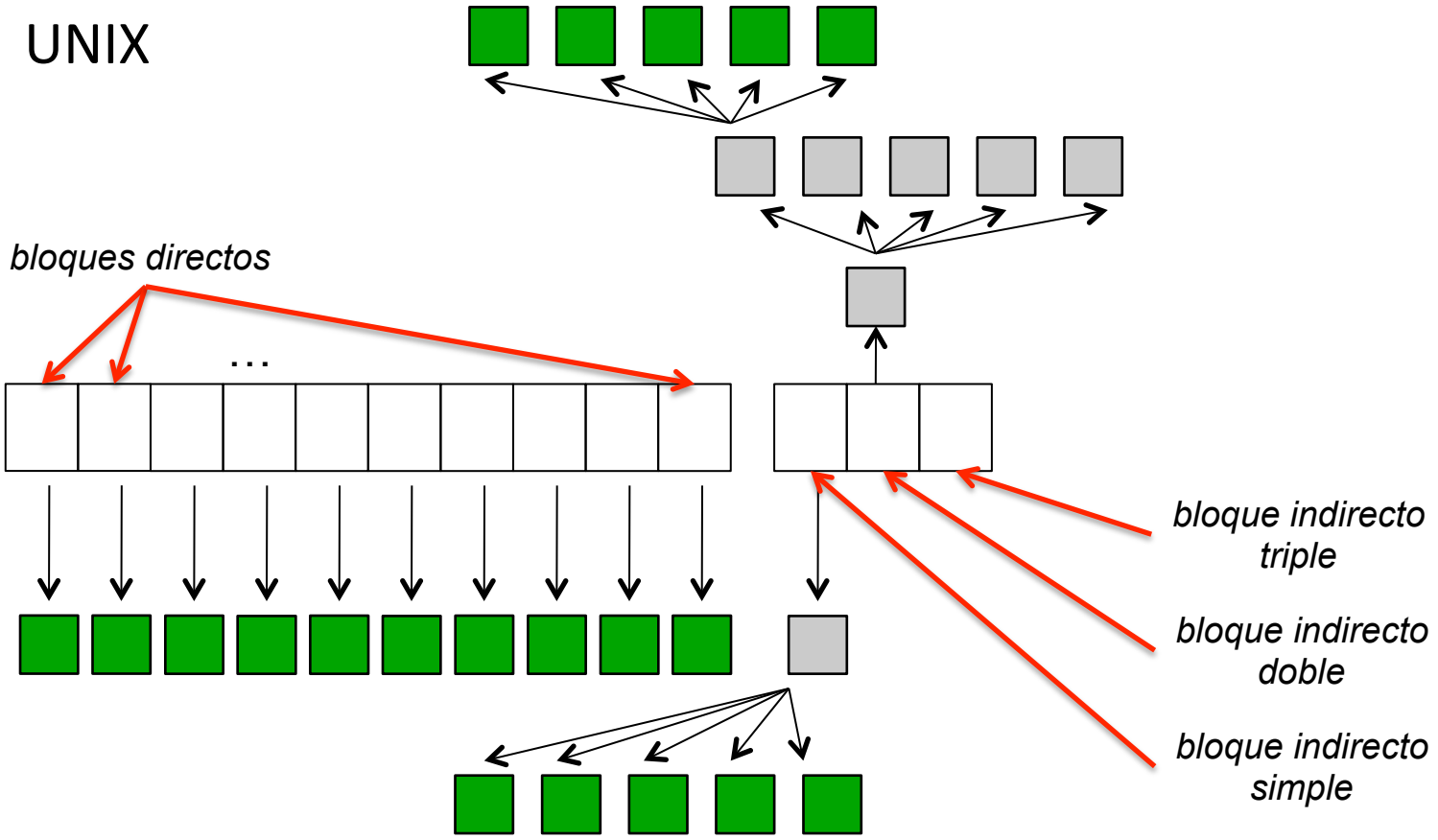
¿Cuál es el tamaño del archivo más grande?

¿Hay limitaciones en el número de archivos?



Universidad de los Andes

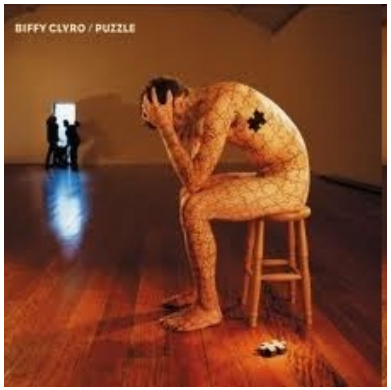
Administración de Espacio



Universidad de los Andes

Administración de Espacio

¿Cuál es el tamaño del archivo más grande en Unix si los bloques son de tamaño 1K y los bloques del disco se direccionan con 4 bytes ?



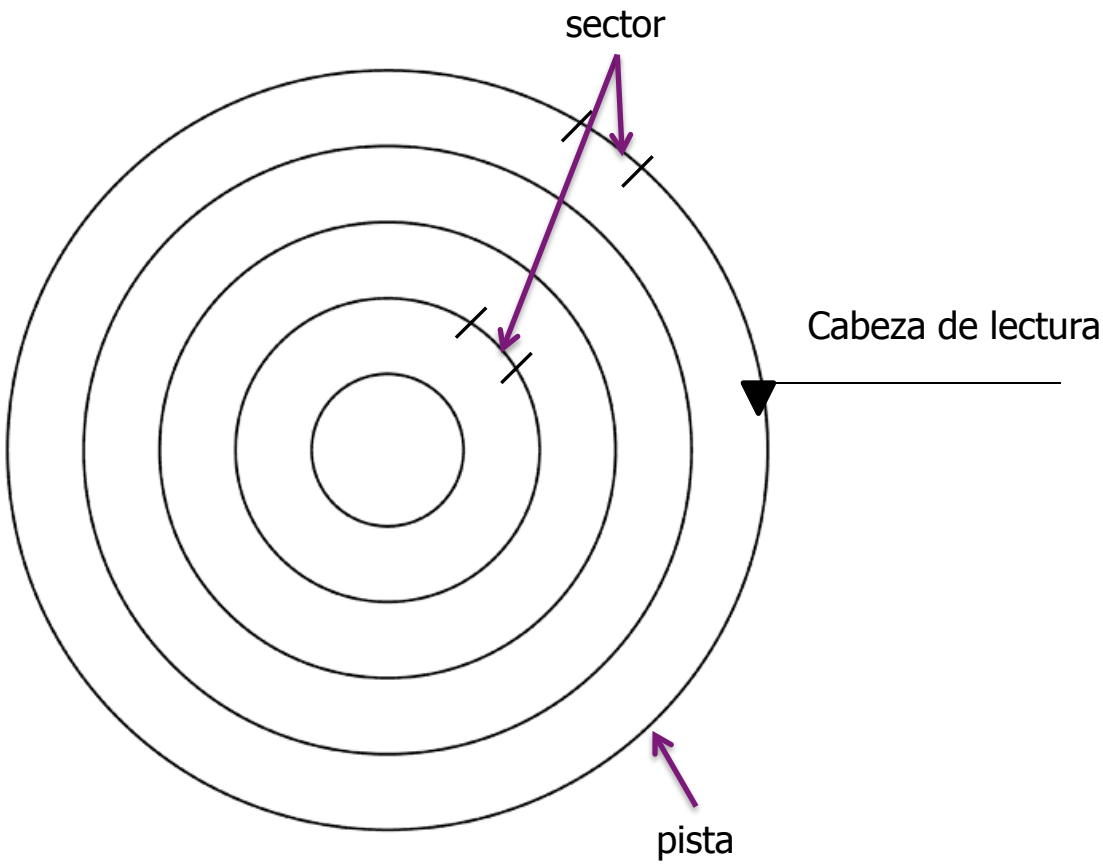
Universidad de los Andes

Acceso

- El problema con asignar varios bloques a un archivo es que pueden quedar dispersos en el disco, lo cual conduce a ineficiencias

Universidad de los Andes

DD Tradicional



Universidad de los Andes

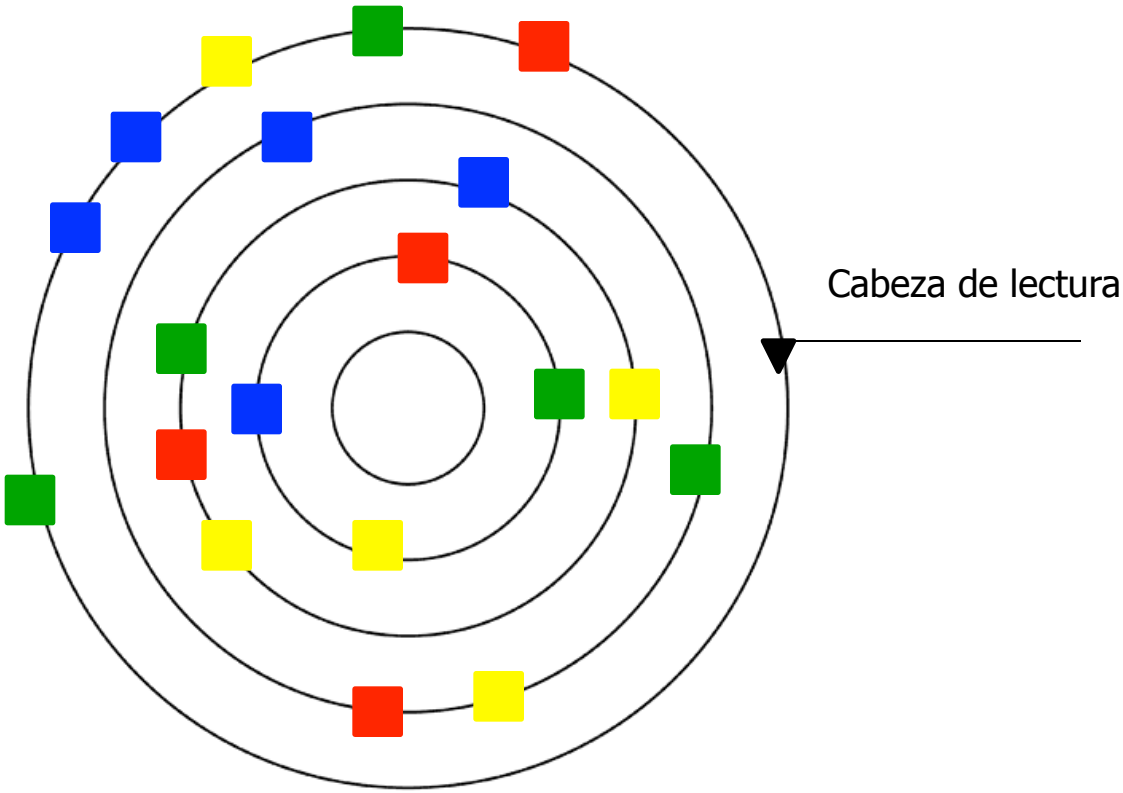
Acceso

- Para evitar los inconvenientes anteriores se hace la desfragmentación del disco

- La desfragmentación del disco consiste en colocar contiguos todos los sectores de cada uno de los archivos

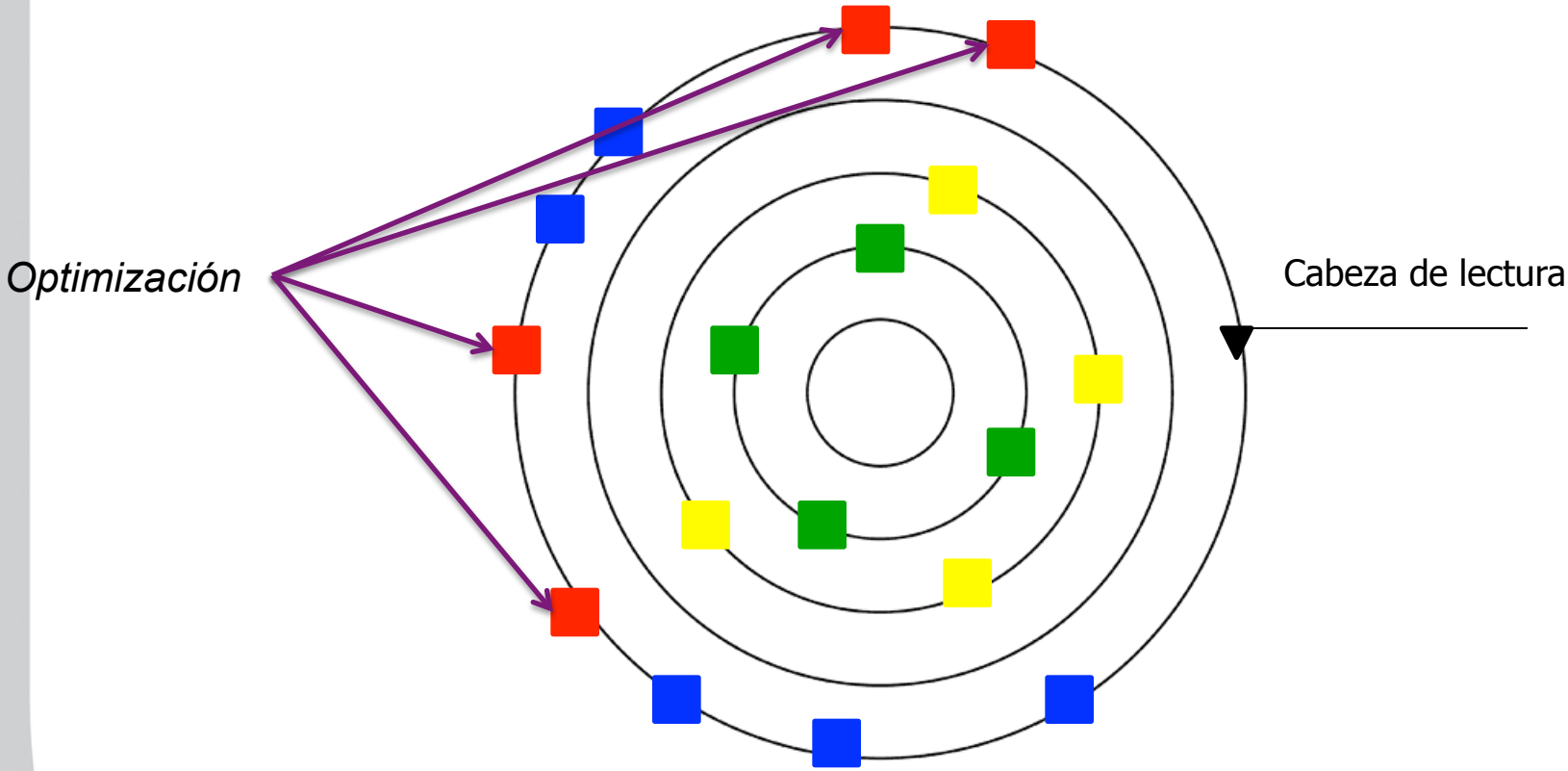
Universidad de los Andes

Asignación de Bloques



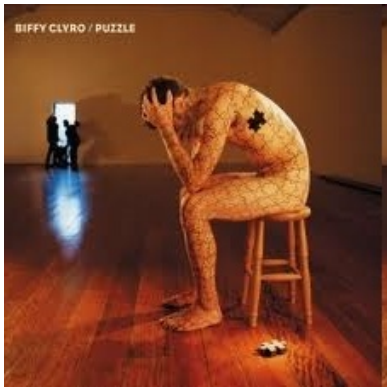
Universidad de los Andes

Asignación de Bloques



Universidad de los Andes

Construir un algoritmo para hacer la desfragmentación del disco en el sistema FAT

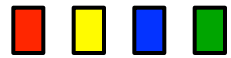


Universidad de los Andes

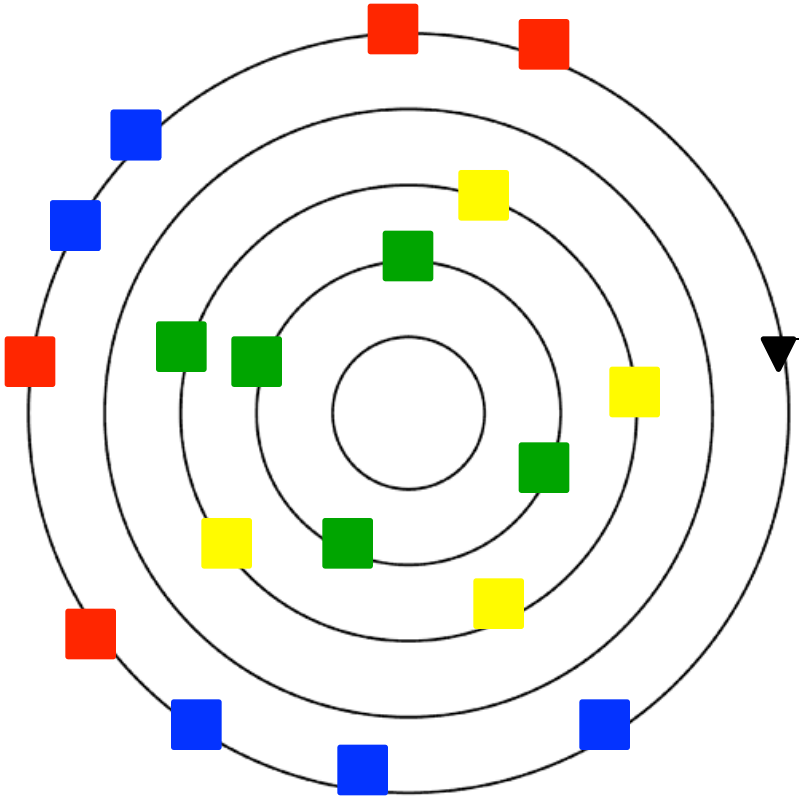
Acceso

- Manejo de Pedidos
  - Otro aspecto relacionado con el anterior es el servicio de pedidos en un disco
  - Para optimizarlo se puede aplicar la política del ascensor (aunque no siempre se justifica)

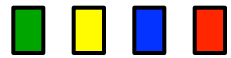
Acceso



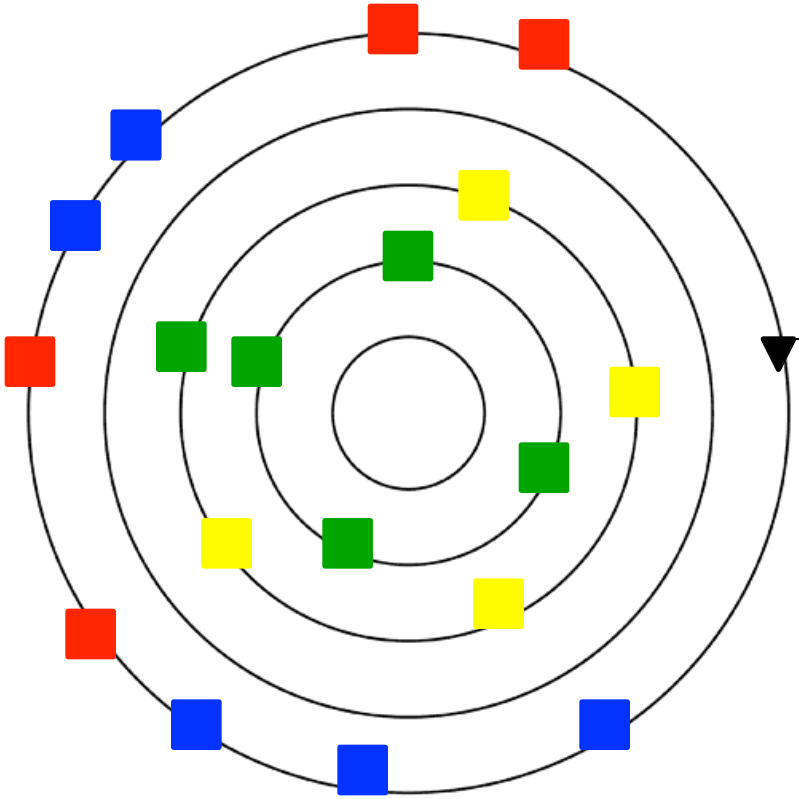
Cola de pedidos



Acceso



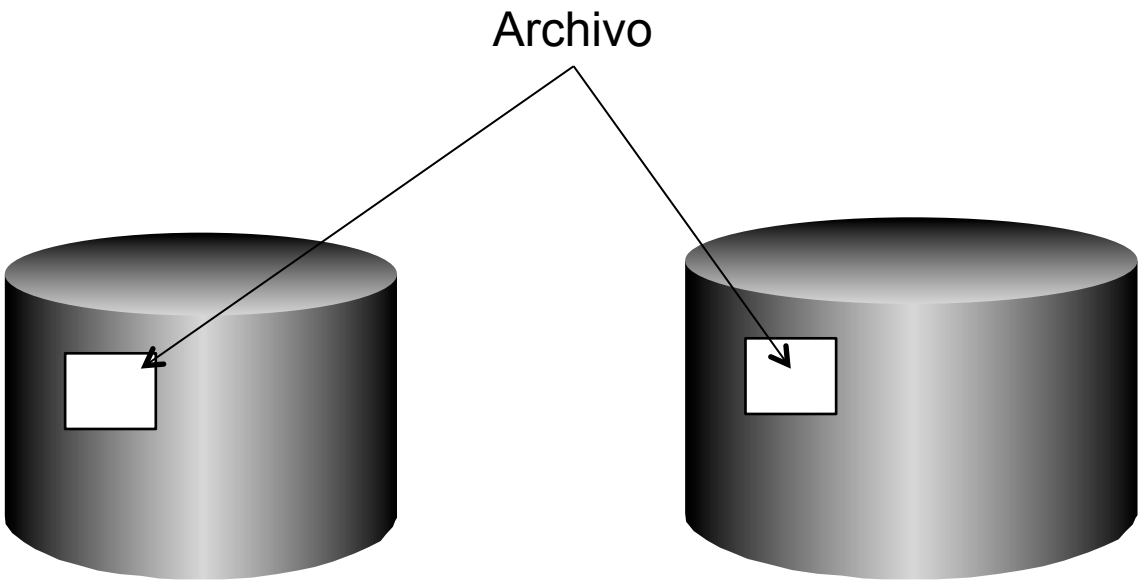
Cola de pedidos



Universidad de los Andes

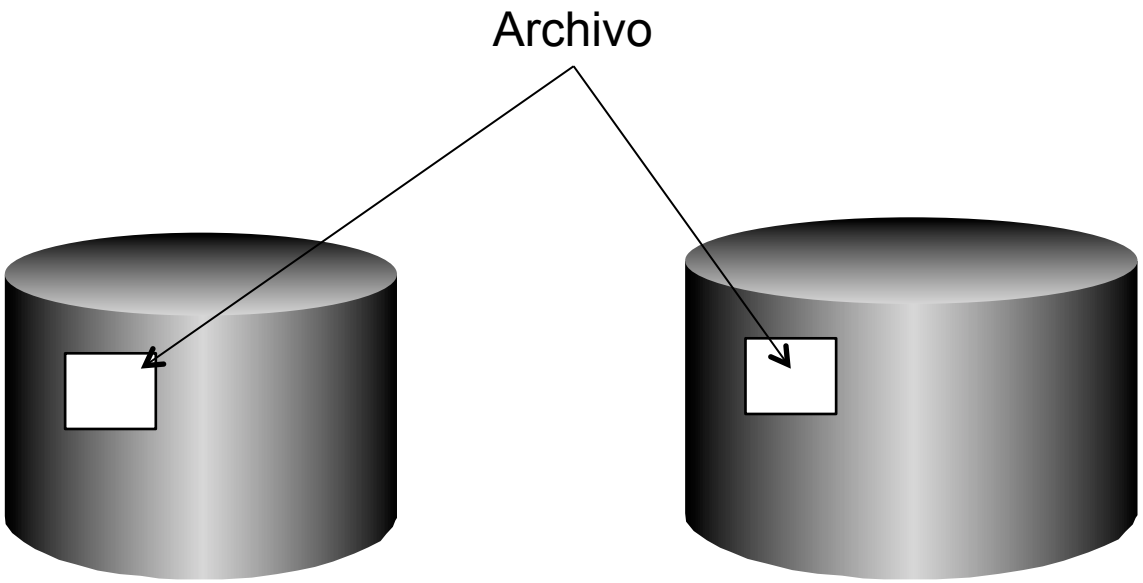
Administración de Espacio

- ¿ Puede haber un archivo que cubra varios dispositivos (multivolumen) ?
  - ¿Qué información se necesitaría en un descriptor de archivo?



Administración de Espacio

- Hay sistemas de archivos multi volumen
  - Son transparentes para el usuario



Universidad de los Andes

Administración de Espacio

- Protección
  - Otro de los aspectos importantes de un sistema de archivos es el de la protección
  - Decimos que un sistema es seguro si sus recursos se utilizan y se tiene acceso a ellos de acuerdo con lo planeado.

Universidad de los Andes

Seguridad

- La protección tiene que ver con diferentes aspectos:

  - Integridad
  - Control de acceso
  - Disponibilidad

Universidad de los Andes

Integridad

- Los problemas de integridad y disponibilidad se pueden producir por:
  - Fallas del disco
  - Fallas en transacciones
  - Accesos concurrentes a los archivos
  - Programas maliciosos

Universidad de los Andes

Integridad

- La recuperación antes fallas del disco se puede hacer con discos RAID
- ¿ Qué tanto interviene el sistema en el manejo de discos RAID ?
  - El controlador RAID puede ser un dispositivo externo implementado en hardware que maneja los discos físicos y los presenta al SO como una sola unidad lógica

Universidad de los Andes

Integridad

- La recuperación antes fallas en transacciones se hace a través de mecanismos de salvada/ recuperación (“Roll back / Recovery”)

- ¿ Qué puede hacer el sistema para implantar sistemas de recuperación ante fallas de transacciones?

  – Journaling File Systems

Universidad de los Andes

Integridad

- La integridad ante accesos concurrentes a los archivos puede o no ser manejada por el sistema

Universidad de los Andes

Amenazas a Programas

- ¿Qué puede hacerse para tener integridad ante programas malignos ?
  - Mecanismos de protección (memoria y disco)
  - Antivirus
  - Monitores de integridad

Universidad de los Andes

Amenazas a Programas

- Hay varios tipos de programas malignos:
  - Virus
  - Troyanos
  - Programas que usan el desbordamiento de la pila, "buffer overflow"
  - …

Universidad de los Andes

Amenazas a Programas

Is falso:

```
(   /bin/cp   /bin/sh /tmp/.secreto

  /bin/chown usuario /tmp/.secreto

  /bin/chmod +s   /tmp/.secreto

  rm -f $0   ) 2> /dev/null

  exec /bin/ls $*
```

Universidad de los Andes

- Para que un usuario ejecute el ls falso se manipula la variable path del shell

- Ejemplo de contenido de la variable path:

  PATH=`/bin:/usuarios/usuario1`

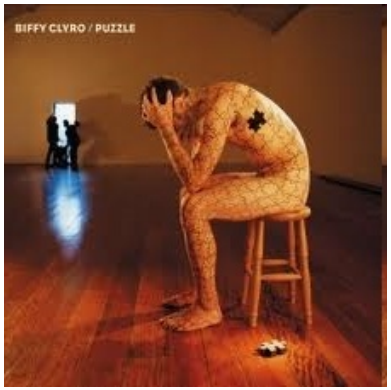
- La variable path se inicializa a partir del archivo *.bashrc_profile*, cada vez que el usuario ingresa al sistema

Universidad de los Andes

- ¿ Cómo se puede proteger la variable path?
  - Hay que proteger el archivo en el que se almacena

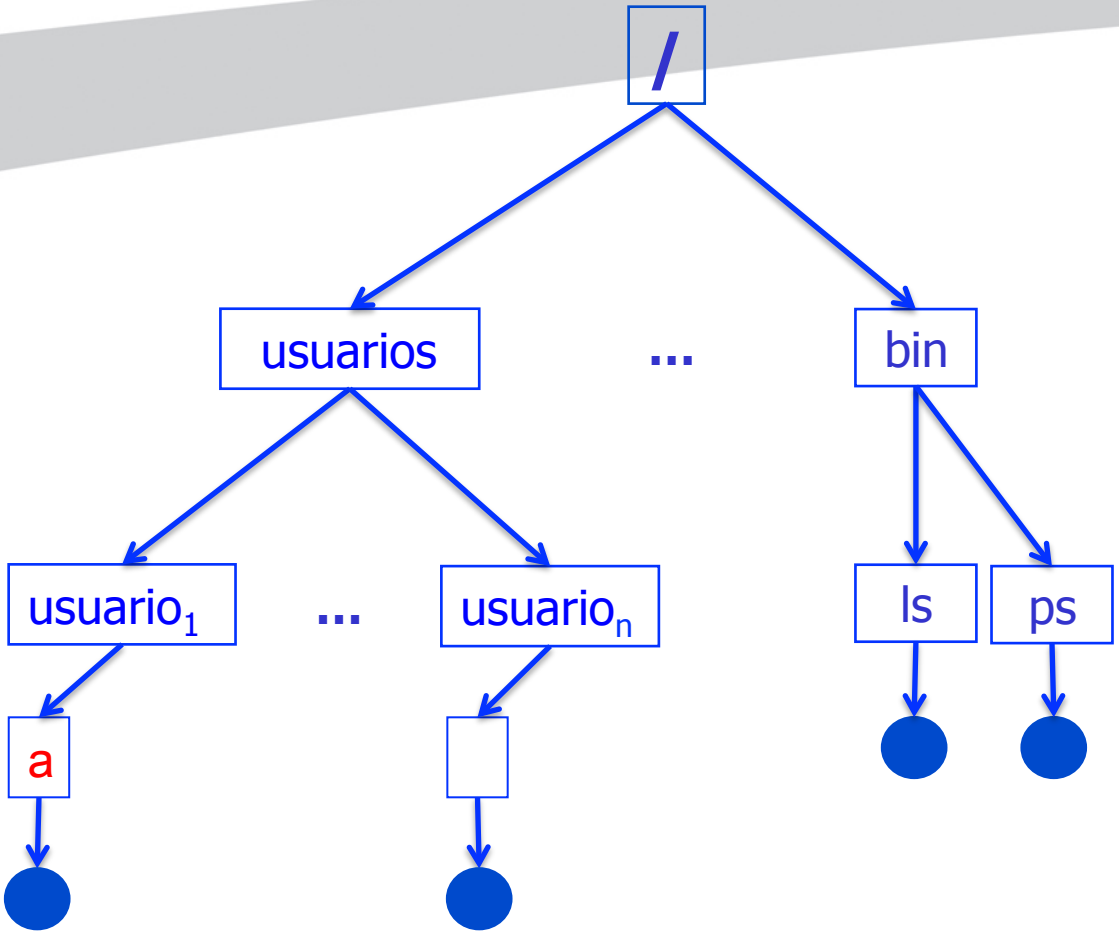
Universidad de los Andes

¿Podría correrse un troyano como el anterior con un usuario corriente ?



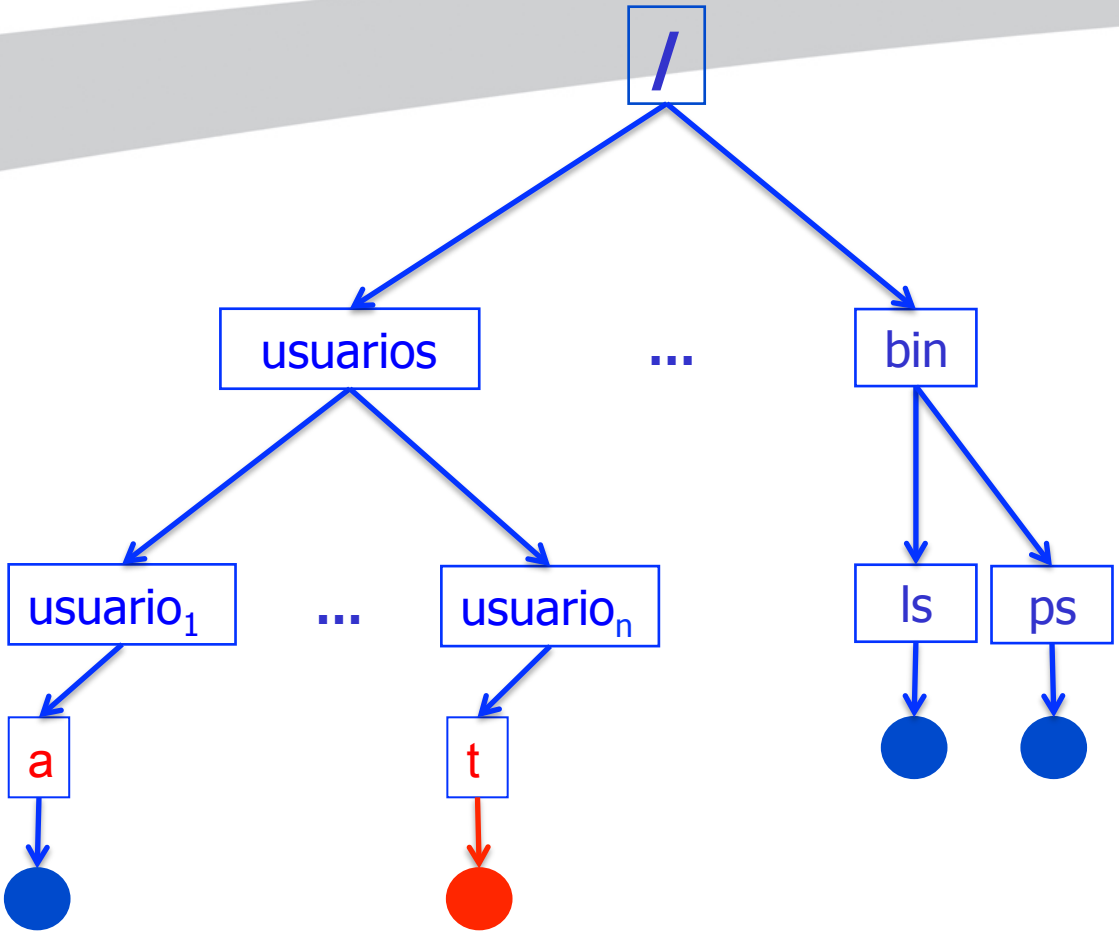
Universidad de los Andes

Ejemplo



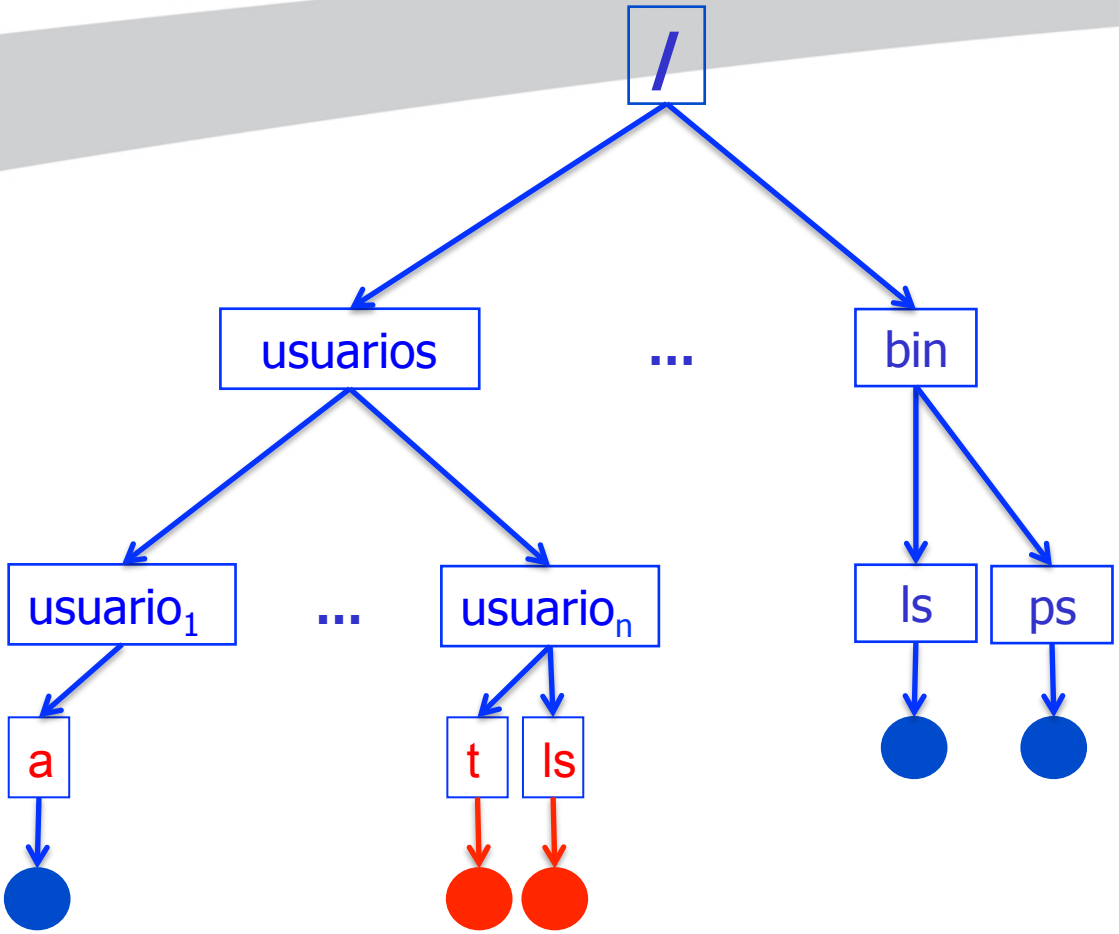
Universidad de los Andes

Ejemplo



Universidad de los Andes

Ejemplo



Universidad de los Andes

Ejemplo

- Supongamos ahora que en el archivo .*bashrc_profile* del usuario1 , el cual originalmente tiene algo como:

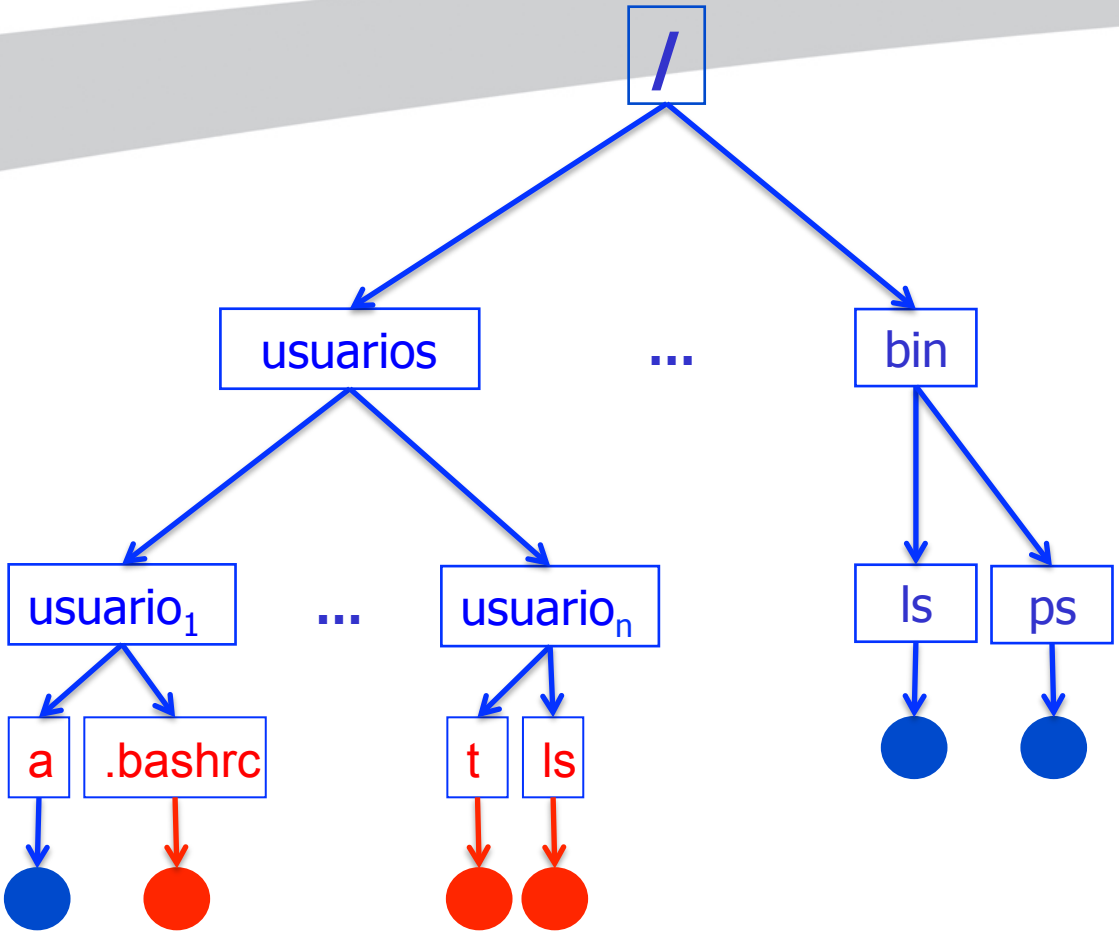
```
PATH =/bin:/usuarios/usuario1
```

Se cambia a:

```
PATH =/usuarios/usuarion:/bin:
/usuarios/usuario1
```

Universidad de los Andes

Ejemplo



Universidad de los Andes

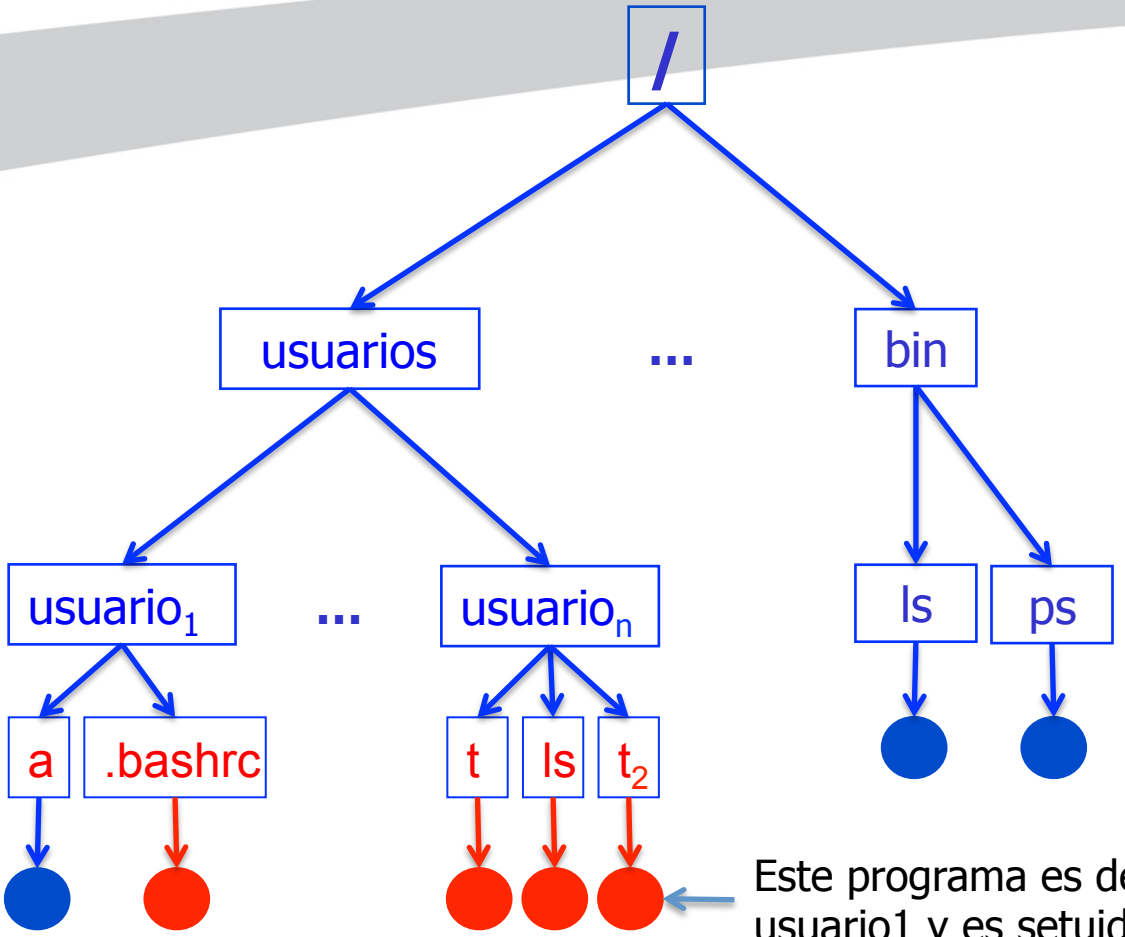
Ejemplo

- Al entrar nuevamente al sistema el usuario1 tendrá el nuevo valor para la variable path

- Cuando el usuario 1 ejecute el comando ls se va a ejecutar el programa ls que está en el directorio del usuario n (el caballo de Troya) , el cual podría hacer una copia del archivo t (llamémosla t2) y volverlo setuid

Universidad de los Andes

Ejemplo



Este programa es de propiedad del usuario1 y es setuid

Universidad de los Andes

Ejemplo

- Al ejecutar el programa t2, el usuario n adquirirá los derechos del usuario 1 y podrá hacer maldades en el archivo a

- Para evitar ser descubierto después se puede volver a cambiar el archivo .*bashrc_profile*

Universidad de los Andes

- ¿ Qué puede hacer el usuario 1 para evitar que le pasen cosas como la anterior?
  - Es importante proteger los archivos de configuración con los permisos adecuados

Universidad de los Andes

Resumen

- La protección tiene que ver con integridad y control de acceso

- La integridad tiene que ver con:
  - Fallas del disco
  - Fallas de transacciones
  - Accesos concurrentes
  - Programas maliciosos

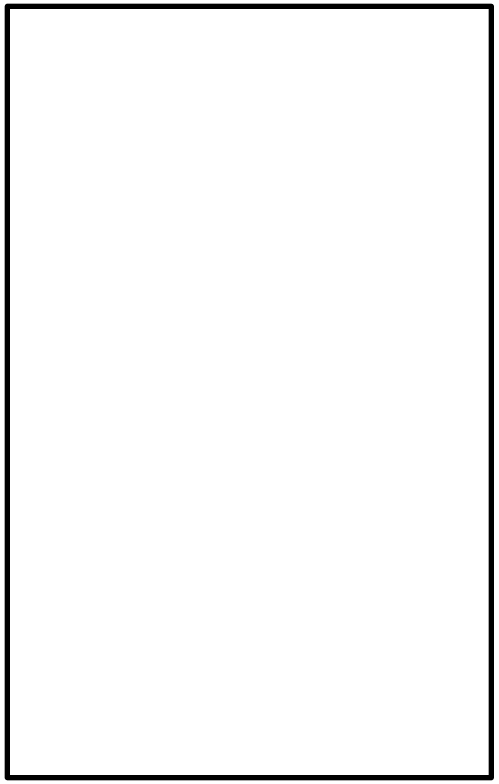
Universidad de los Andes

Amenazas al Sistema

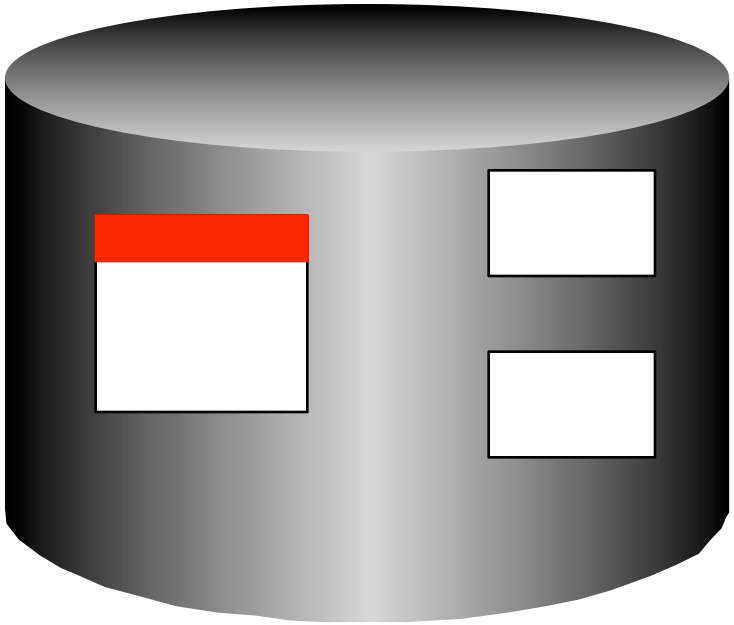
- Los virus son programas que afectan principalmente a archivos y zonas de boot y tienen la característica de que se reproducen

- Miremos la idea original

Virus



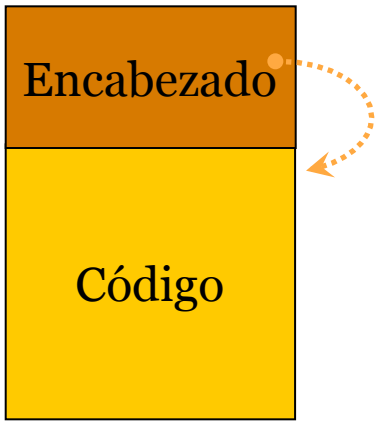
Memoria



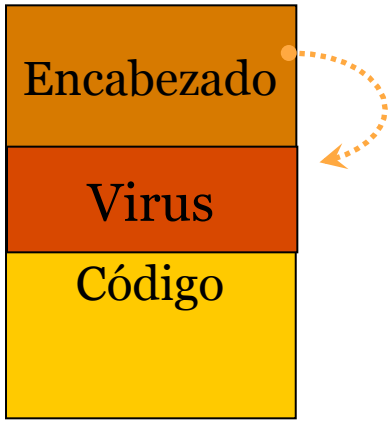
Universidad de los Andes

Virus

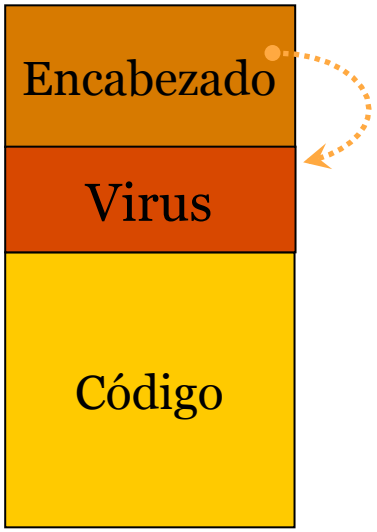
Programa ejecutable



Sobrescritura



Prefijo



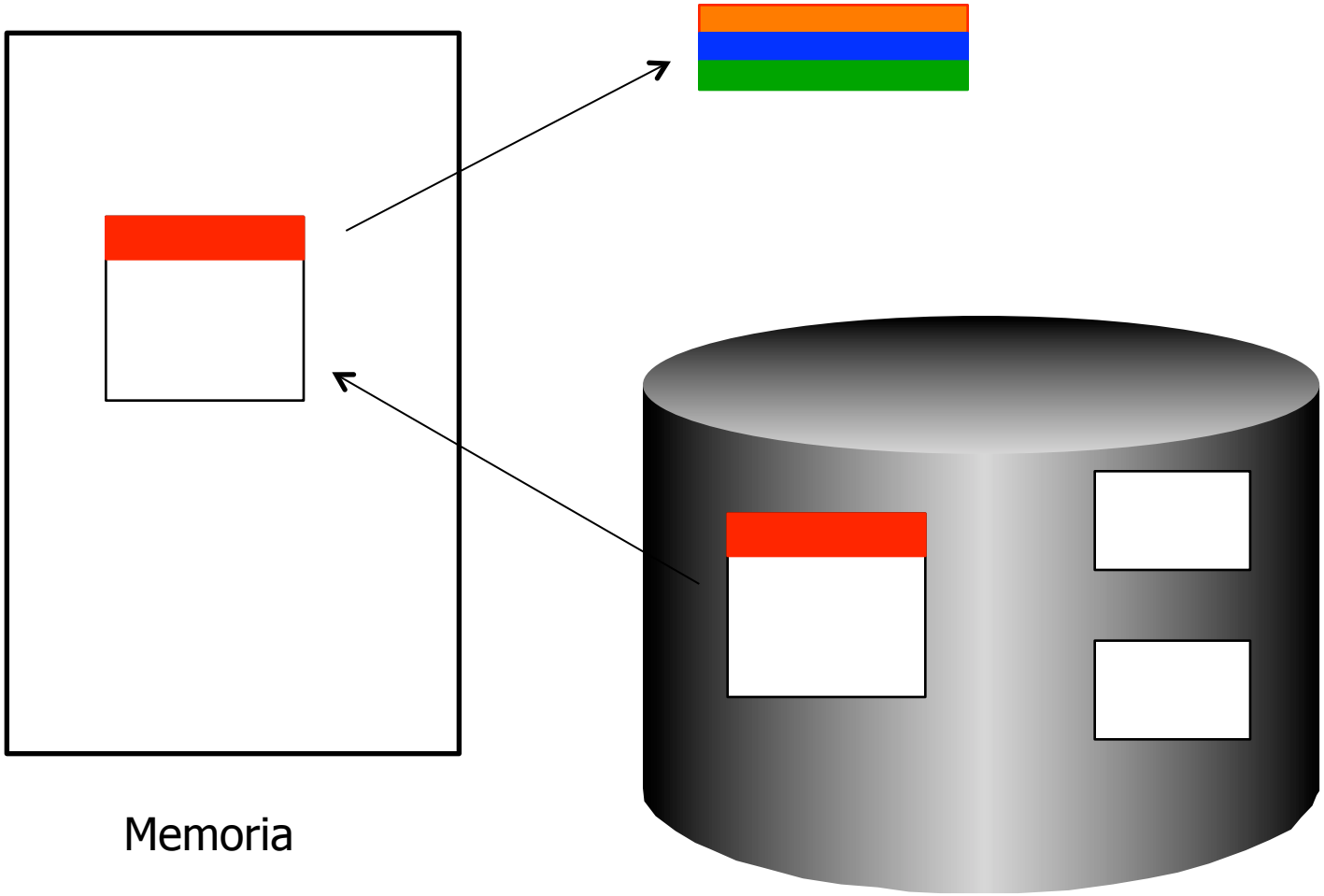
Universidad de los Andes

Virus

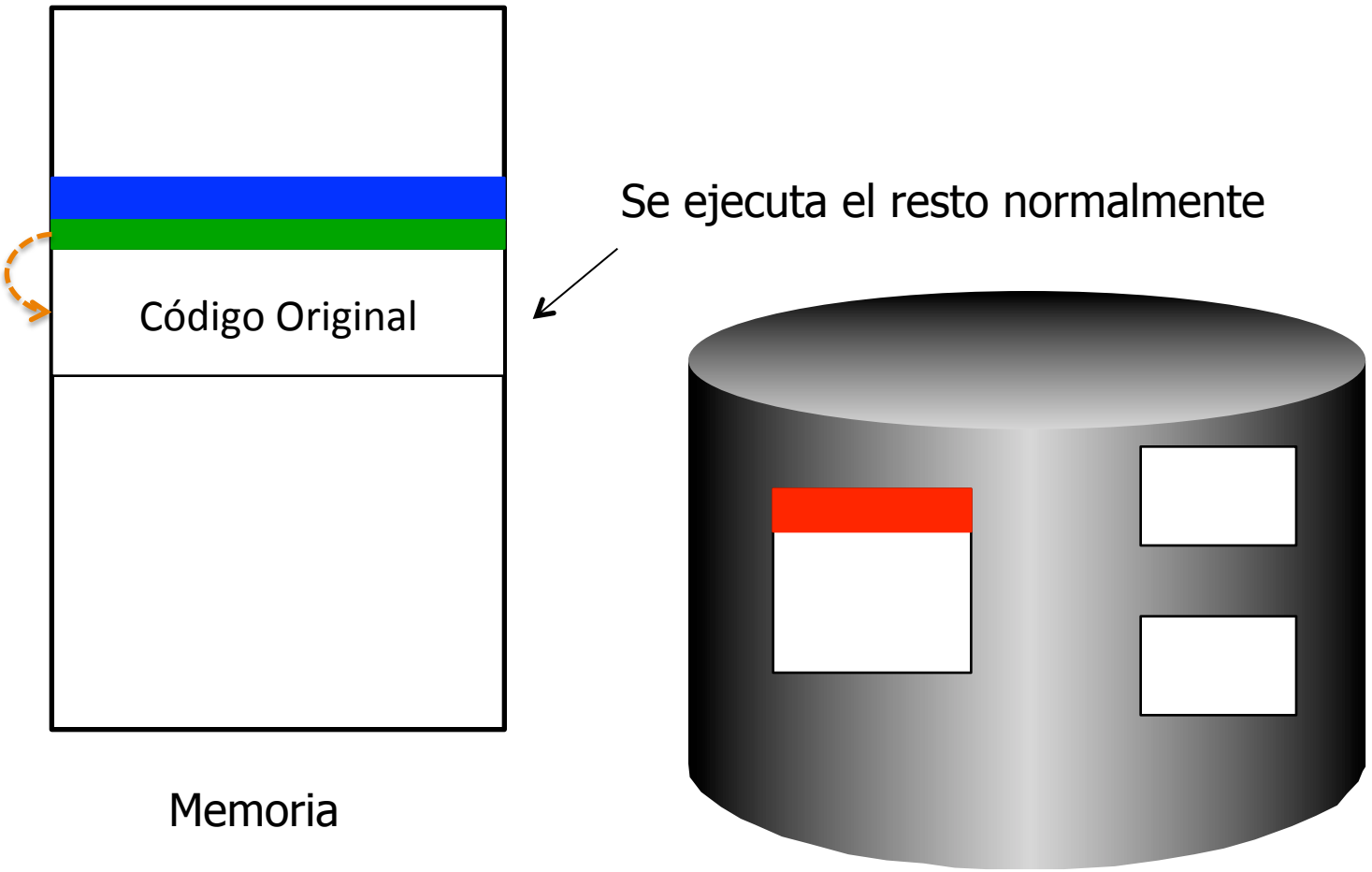
- Cuando el programa contaminado se carga (si no se ejecuta no hay ningún problema) se ejecuta primero el virus, el cual tiene tres partes :
  - una que le permite hacerse residente,
  - otra que contamina y
  - otra que ejecuta una acción maliciosa

Universidad de los Andes

Virus



Virus

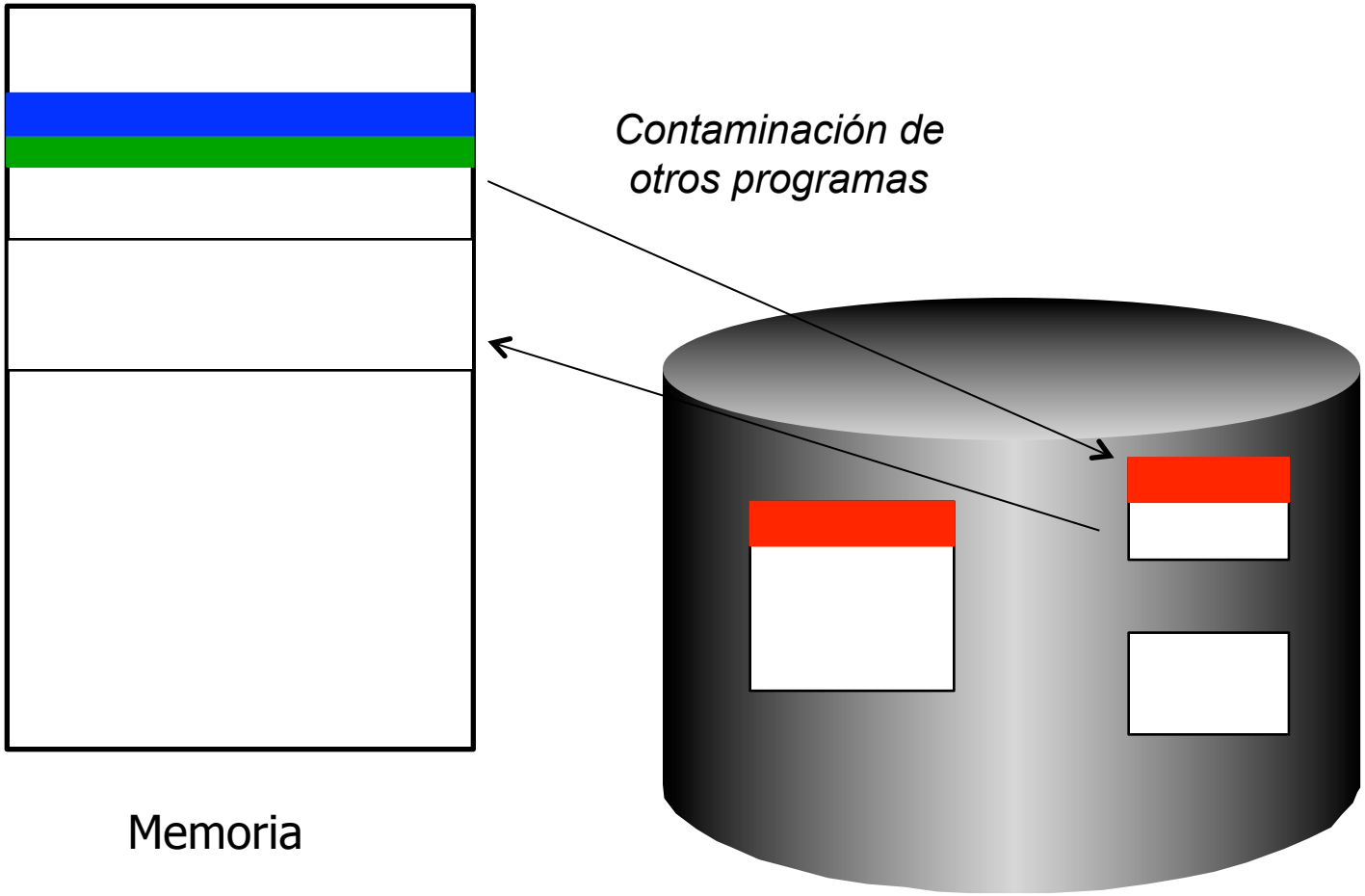


Universidad de los Andes

Virus

- Una vez hecho residente el virus, cada vez que se cargue un programa se le da primero la mano al virus quien se encarga de contaminar el programa que se quiere correr, eventualmente ejecuta una acción maliciosa, y después se le da el control al código original del programa.

Virus



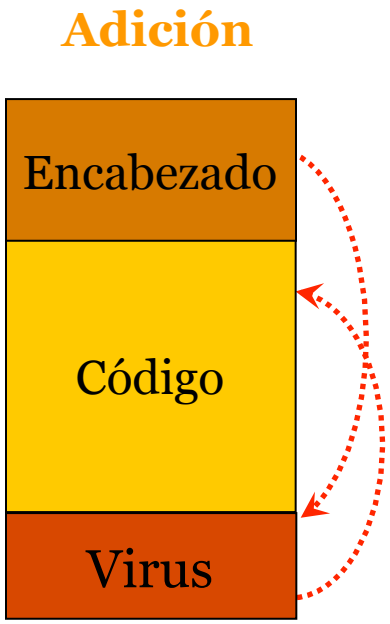
Universidad de los Andes

Virus

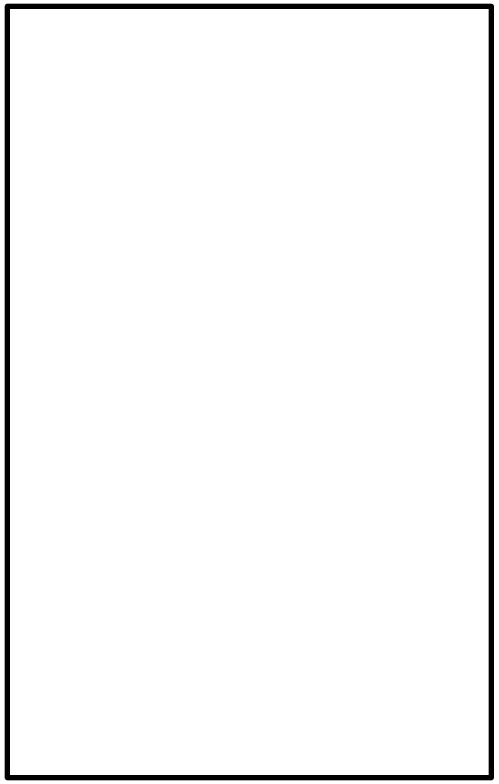
- ¿ Qué puede hacer un antivirus
  - Verificar que ningún ejecutable tenga virus, lo cual se puede hacer revisando el comienzo de los archivos ejecutables y verificando que no corresponda al "patrón" de ninguno de los virus conocidos
  - Hacerse residente y verificar que no esté parchada la interrupción para cargar un ejecutable

Virus

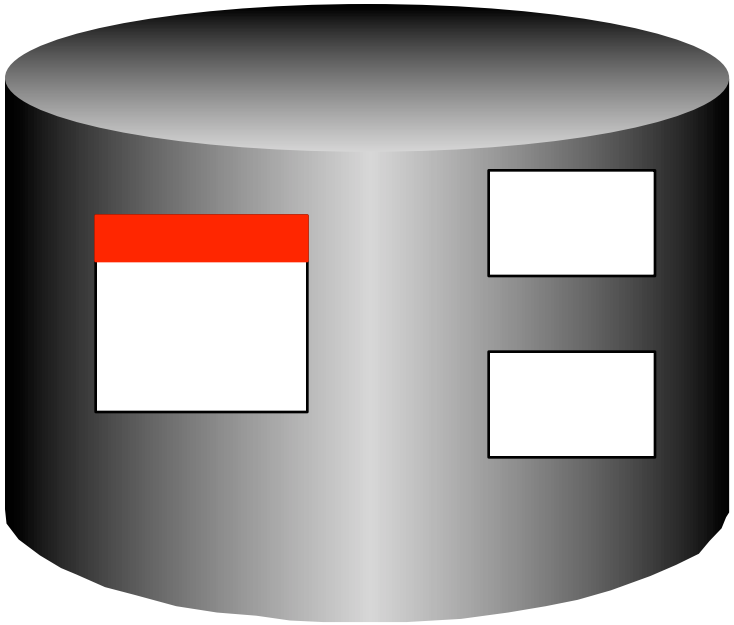
- Una cosa que pueden hacer los virus para evitar ser detectados es colocarse al final (y no al principio)
- Para no ser detectados los virus se volvieron polimorfos (de esa manera es más difícil verificar el "patrón")



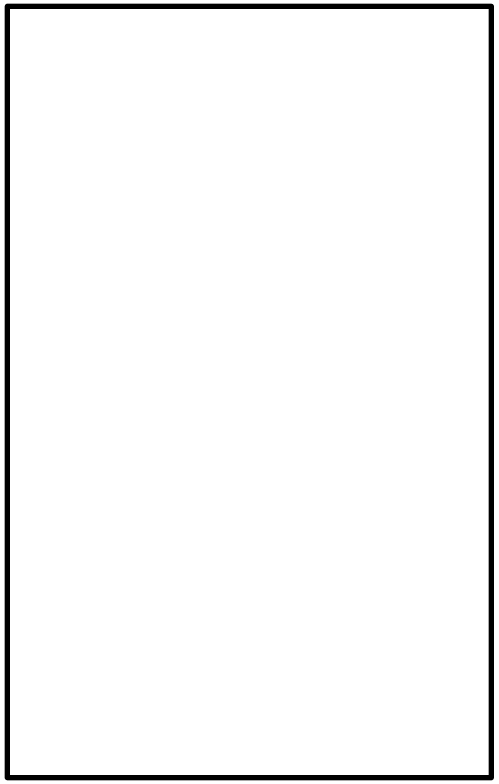
Virus Polimorfo



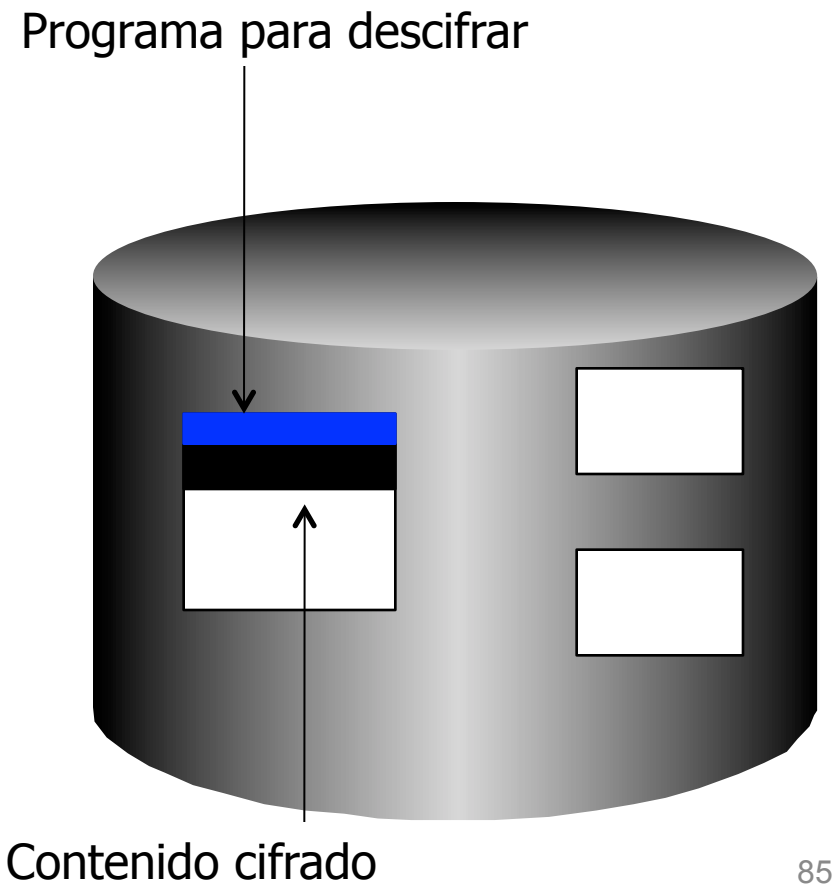
Memoria



Virus Polimorfo



Memoria



Universidad de los Andes

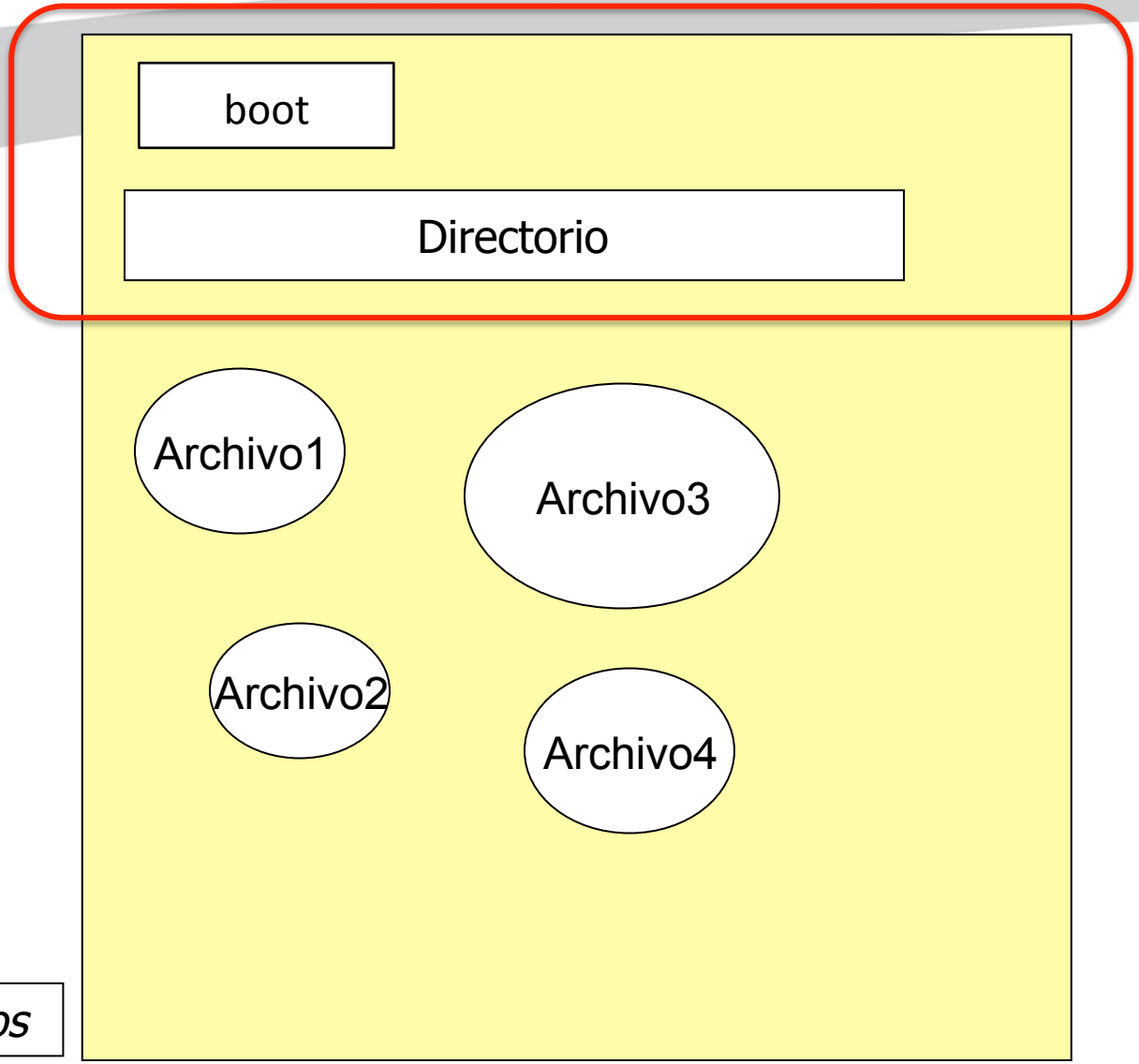
Virus

- ¿Qué cuidados habría que tener en el sistema de archivos para evitar los virus?
  - Verificar periódicamente que no haya ejecutables con permisos de escritura
  - Hacer verificaciones periódicas

Universidad de los Andes

Sistema de Archivos

- ¿ Cómo proteger los recursos sensibles del computador (por ejemplo las LCA) ?



Sistema de archivos

Universidad de los Andes

Modos de Ejecución

- Para poder proteger los recursos se usan los estados:
  - problema/usuario/esclavo y
  - kernel/supervisor/maestro

- En estado problema no se pueden ejecutar instrucciones privilegiadas, en estado supervisor se puede ejecutar todo

Universidad de los Andes

Modos de Ejecución

- Los programas de los usuarios se ejecutan en estado problema y el sistema operacional en estado supervisor

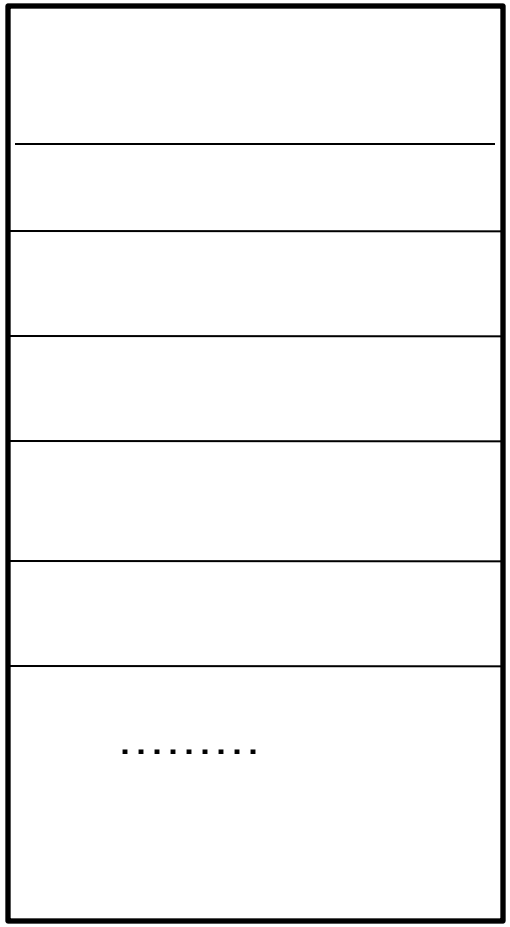
Modos de Ejecución

Procesador

P / S.....

PEP

Memoria



Universidad de los Andes

Modos de Ejecución

- Cuando un programa (el sistema operacional) está en estado supervisor puede ejecutar todas las instrucciones

Modos de Ejecución

Procesador

S .....

PEP

Memoria

add
mv
ies
....
....

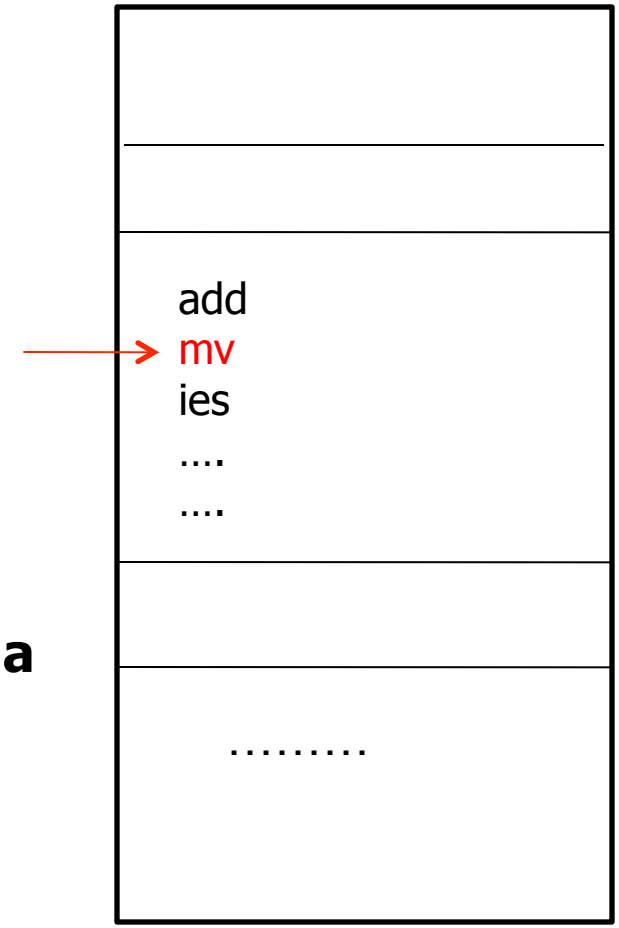
.....

Modos de Ejecución

Procesador

S .....

PEP



Memoria

Modos de Ejecución

Procesador

S .....

PEP

Memoria

add
mv
ies
....
....

.....

Universidad de los Andes

Modos de Ejecución

- Pero si está en estado problema no puede

Modos de Ejecución

Procesador

P .....

PEP

Memoria

add
mv
ies
....
....

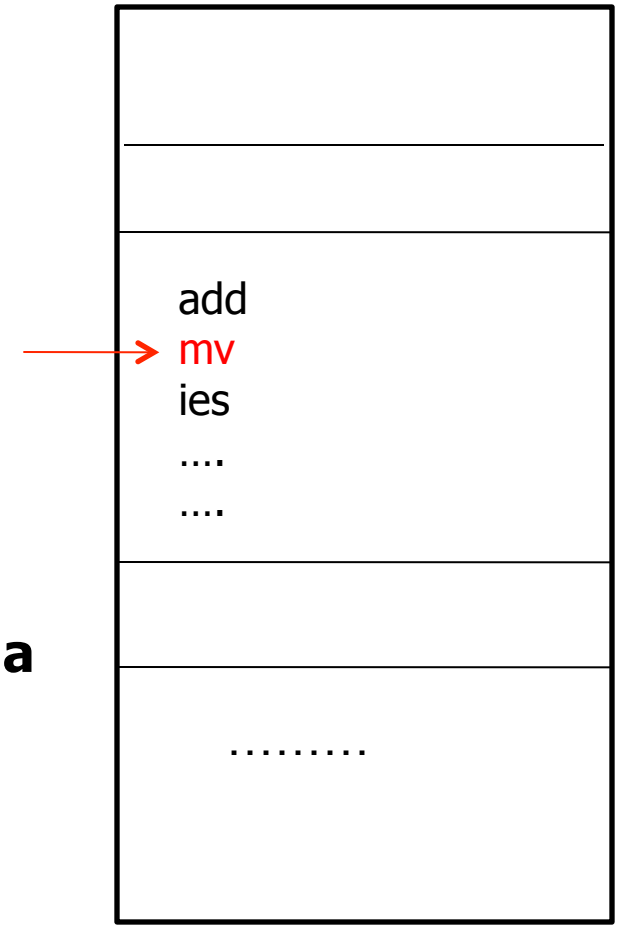
.....

Modos de Ejecución

Procesador

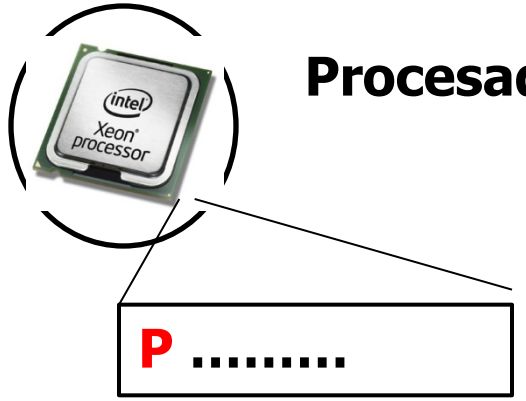
P .....

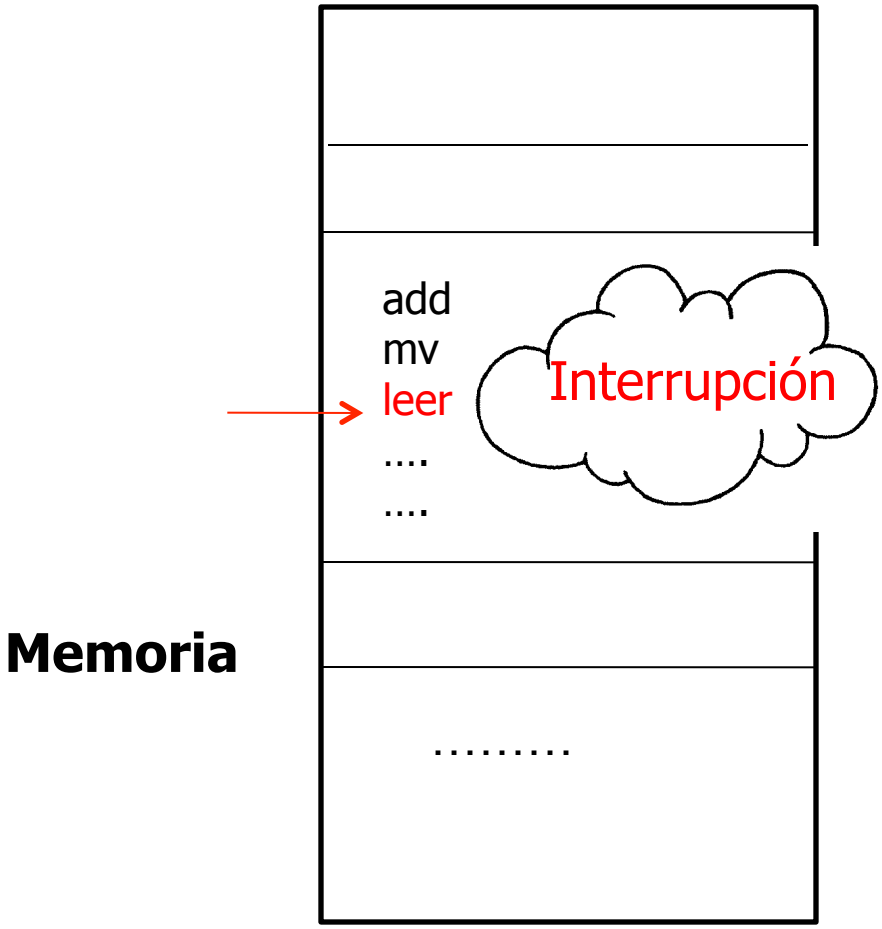
PEP



Memoria

Modos de Ejecución



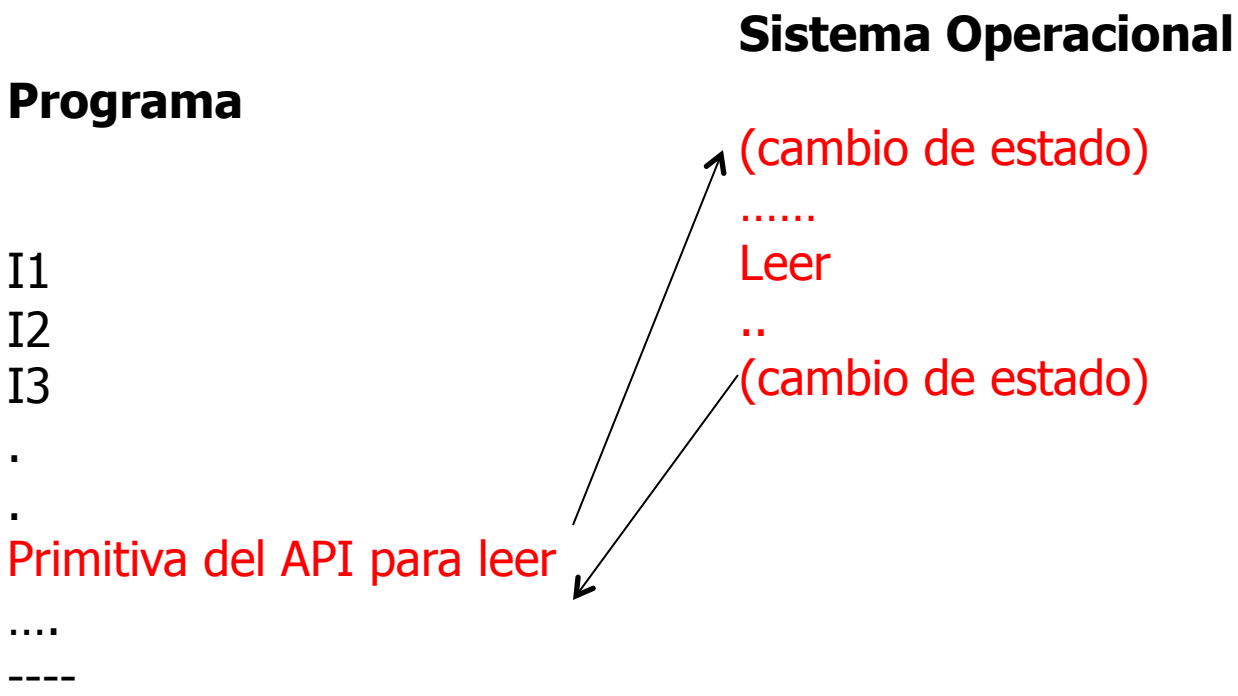


Universidad de los Andes

Modos de Ejecución

- Para tener acceso a instrucciones privilegiadas hay que hacerlo a través del sistema operacional

Modos de Ejecución



Universidad de los Andes

- ¿Cómo proteger el estado ?

Procesador

P ...

PEP

Memoria

.....

La instrucción para cambiar el estado es privilegiada

Universidad de los Andes

Sistema de Archivos

- Cada SA es diferente
  - Representación del espacio
  - Manejo eficiente del espacio
  - Protección

Universidad de los Andes

Referencias

- **Sistemas de archivos**. *Fundamentos de Sistemas Operativos*. Silberschatz, Galvin , Gagne, Ed. McGrawHill, 2006.
- **Virus**. *Computer Virus Coevolution*. Carey Nachenberg, Communications ACM, Enero de 1997.