

Infraestructura Computacional

# **Protección**

Sandra Rueda

# Protección

- Cualquier mecanismo para controlar el acceso de programas, procesos o usuarios a recursos definidos en un sistema.

# Metas de la Protección

- En un sistema operativo con múltiples usuarios es necesario controlar el acceso de usuarios y procesos a los recursos
- Soportar la confiabilidad de cualquier sistema completo que maneja recursos compartidos

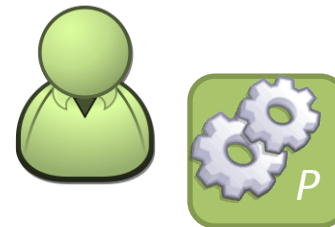
# Evolución

- Multiusuario vs. Multiproceso



# Elementos

- Procesos
  - elementos activos
- Objetos
  - elementos pasivos
    - memoria, archivos, impresoras, discos, programas



# Control de Acceso

- Un mecanismo de control de acceso tiene dos componentes fundamentales

- medio para la especificación

- medio para hacer cumplir la especificación

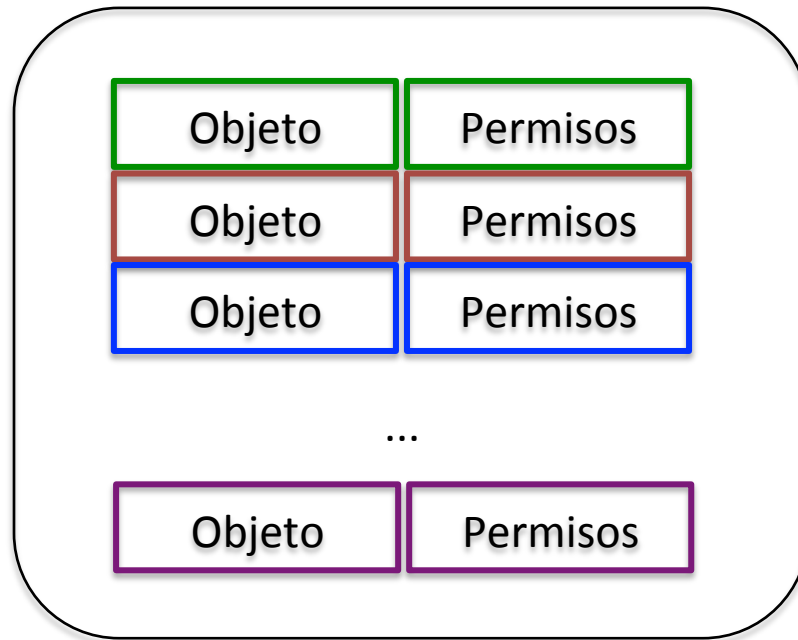
*Política*



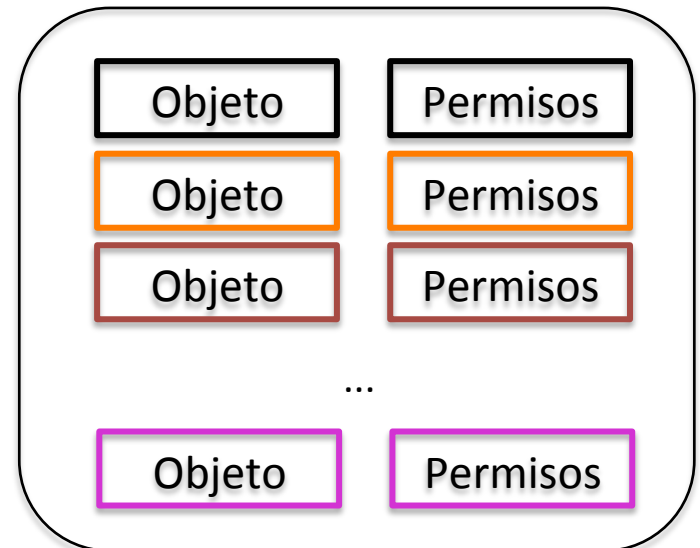
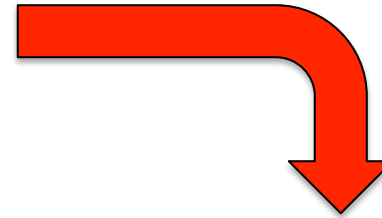
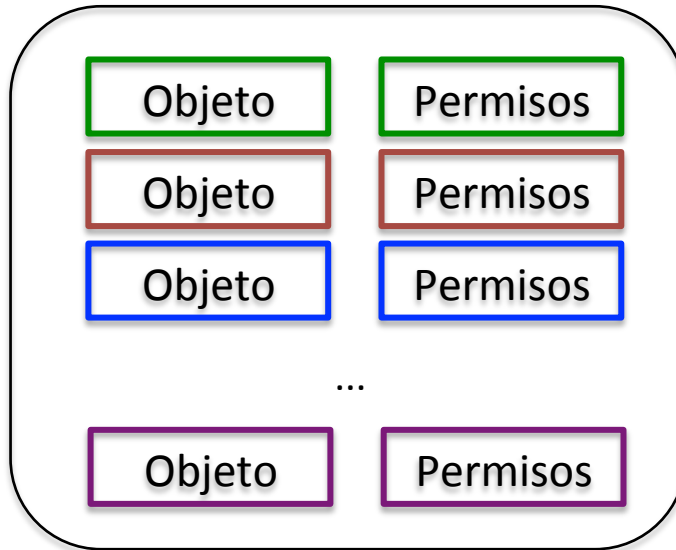
*Mecanismo*

# Dominio de protección

- Conjunto de derechos de acceso



# Cambio de Dominio





# Especificación

- Matriz de Control de Acceso
  - Representación abstracta de la política de un sistema de control de acceso

	archivo1	archivo2	programa1	programa2
proceso1	read,write,own	read	read,write, execute,own	write
proceso2	append	read,own	read	read,write, execute,own

# Implementación

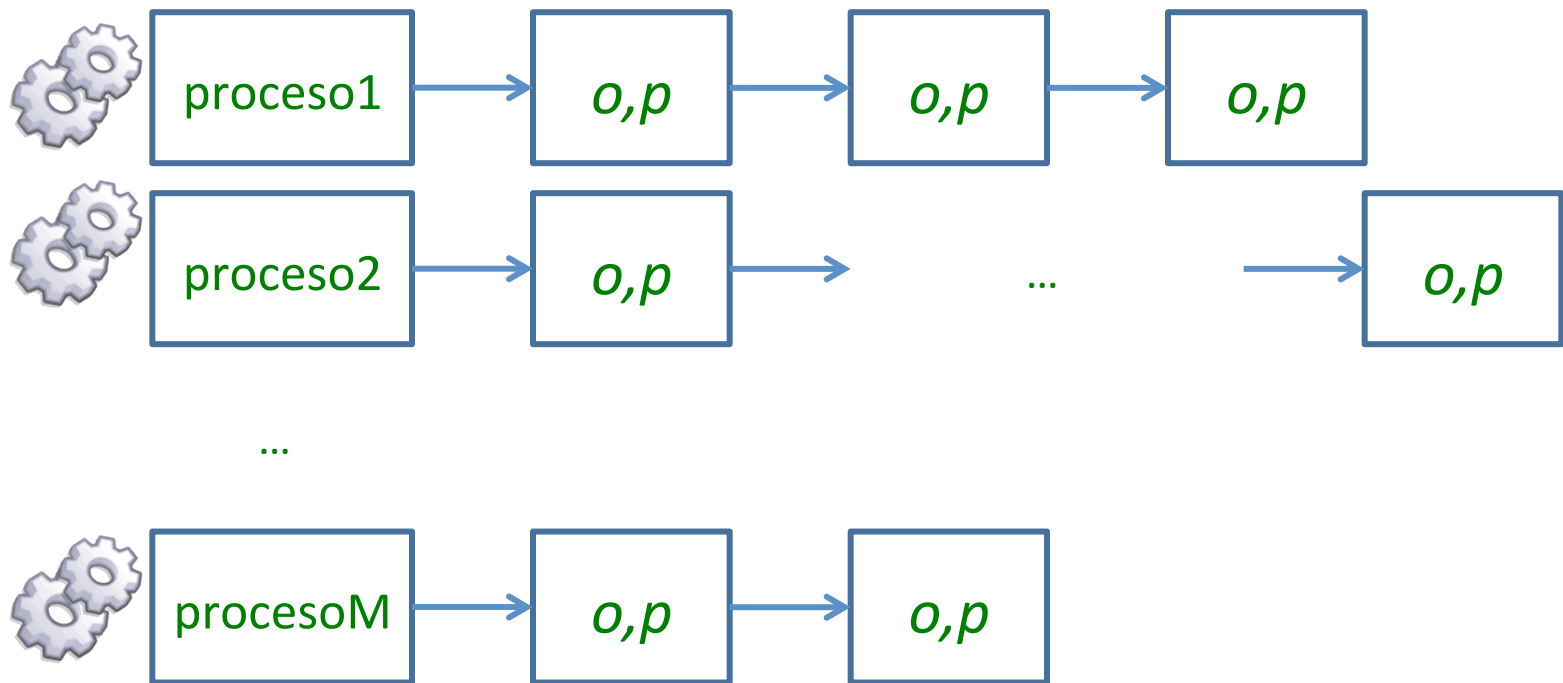
- Tabla Global

	archivo1	archivo2	programa1	programa2
proceso1	read,write,own	read	read,write, execute,own	write
proceso2	append	read,own	read	read,write, execute,own

...

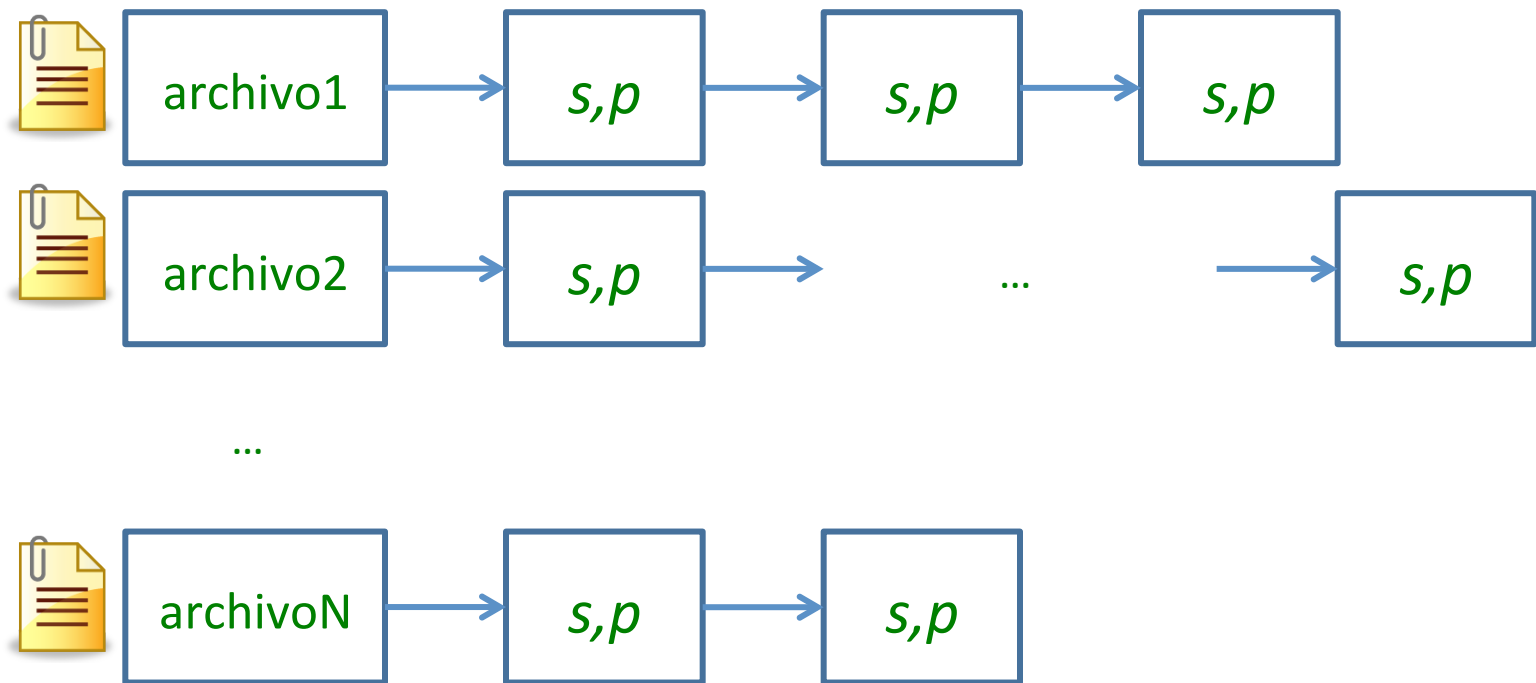

# Implementación

- Lista de capacidades



# Implementación

- Lista de acceso



# Listas de Acceso

- Implementación más común
  - Sistemas operativos (Linux y Windows)
  - Firewalls
  - Aplicaciones web

# Tabla vs. Listas

- Suponga que se tiene un sistema con 1000 recursos y 100 usuarios (en cierto momento). 1% de los recursos son accesibles (r,w,x o una combinación) para todos los usuarios. 10% son accesibles para dos usuarios y 89% son accesibles para un usuario. Se requiere una unidad de espacio para almacenar un permiso de acceso (o una combinación de permisos), o un identificador de usuario o un identificador de recurso.
- ¿Cuánto espacio se requiere para almacenar toda la matriz de acceso? ¿la lista de control de acceso? ¿La lista de capacidades?

# Lista de Acceso vs. Lista de Capacidades

	Lista de Acceso	Lista de Capacidades
Ventajas		
Desventajas		

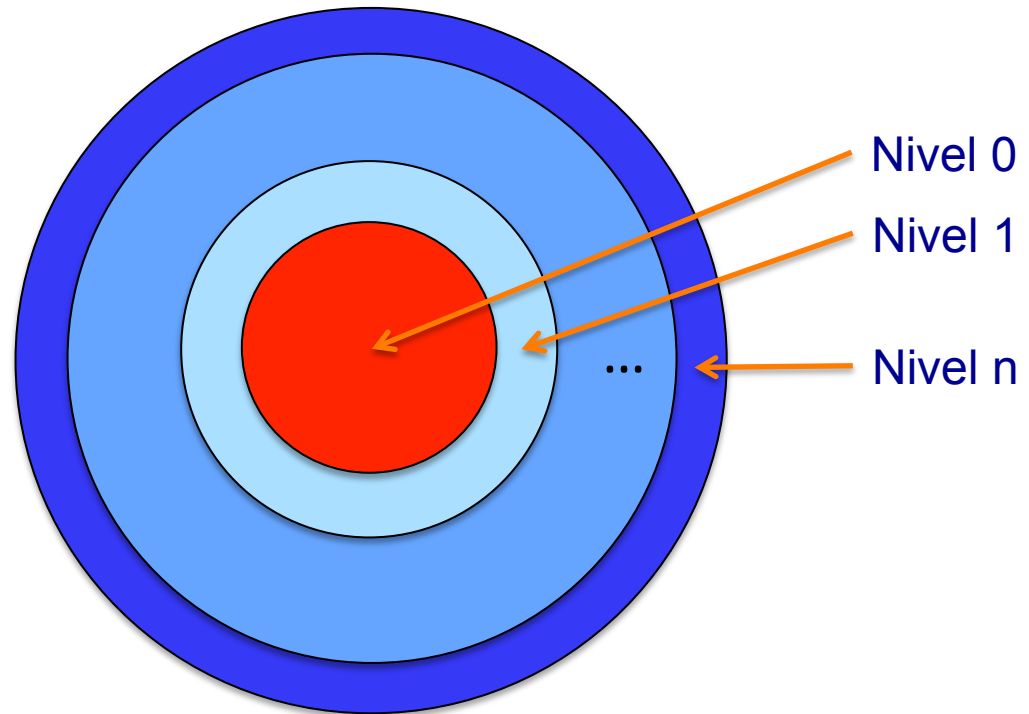
# Ejercicio

- Suponga que se tiene un sistema en el que es posible etiquetar un archivo como sensible. Cuando se borra uno de estos archivos, su área de almacenamiento se sobrescribe con bits aleatorios.
  - ¿Por qué? [SGG]



# Protección en Anillos

- En MULTICS (1964) los dominios de protección están organizados jerárquicamente en una estructura de anillo. Los anillos están numerados del 0 al 7, siendo 0 el anillo con más privilegios. Los privilegios en otros niveles son subconjuntos de los privilegios de niveles anteriores.

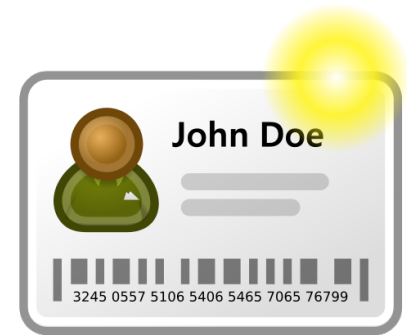


# Ejercicio

- En un sistema de protección de anillo, el nivel 0 tiene mayor acceso y el nivel  $n$  tiene menos derechos de acceso. Los derechos de acceso de un programa en un nivel particular en la estructura de anillo se consideran como un conjunto de capacidades.
  - ¿Cuál es la relación entre las capacidades de un programa en el nivel  $j$  y un programa en el nivel  $i$  para un objeto, con  $j > i$ ? [SGG]

# Autenticación

- Proveer evidencia que pruebe que alguien es quien dice ser
  - Algo que se tiene
  - Algo que se es
  - Algo que se conoce



# Autenticación

- UNIX
  - Login/clave
  - ¿Cómo mantener la clave secreta?
    - El sistema tiene una función de hash  $f$  que no tiene inversa, pero que es sencilla de calcular
    - El sistema aplica  $f$  a la clave de cada usuario y almacena  $f(clave)$
    - Ataques de diccionario

# Autenticación

- Cajeros
  - Tarjeta
  - Número de identificación personal

# Autenticación

- Biométricos
  - Huellas digitales
  - Scan de retina
  - Reconocimiento facial
  - Lector de mano
  - Reconocimiento de voz
  - Firma

# Clasificación

	Ser	Saber	Tener
Clave			
PIN			
Dirección en un paquete IP			
Llave criptográfica simétrica			
Llave criptográfica asimétrica			
Huella digital			

# Autorización

- Definición de los permisos asignados a cada usuario
  - Quién
  - Qué
  - Cómo



# Autenticación y Autorización

- La etapa de autenticación establece la identidad de un usuario o proceso
- La etapa de autorización asigna permisos con base en la identidad del usuario o proceso

# Autorización y Control de Acceso

- Un usuario o proceso solicita acceso a un objeto en un modo determinado
- El manejador del control de acceso autoriza o rechaza la solicitud
  - recibe la solicitud
  - consulta la política definida (los permisos establecidos)
  - informa la decisión



# Control de Acceso

- ¿Cuándo tomar decisiones de control de acceso?
  - La primera vez que se solicita acceso a un recurso, por ejemplo al abrir un archivo para lectura
  - Cada vez que se ejecute una operación relevante para la seguridad del sistema, por ejemplo al abrir un archivo y cada vez que se realice una lectura sobre el mismo

# Autorización

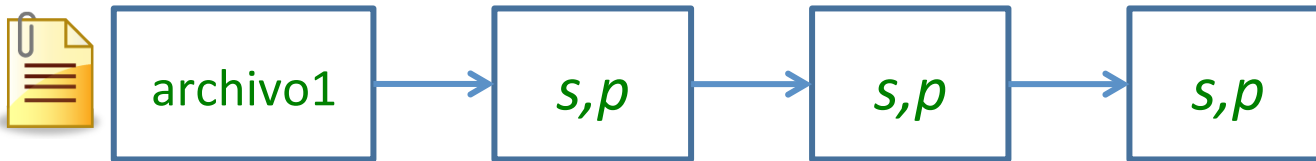
	Primera Vez	Cada Vez
Ventajas		
Desventajas		

# Caso MS-DOS

- No maneja un sistema de control de acceso
- Sistema operativo diseñado para computadores personales
  - individuos

# Caso Unix/Linux

- Implementa una versión simplificada de listas de acceso



# UNIX/Linux

- UNIX/Linux
  - Cada usuario
    - uid
    - gid



```
infracomp@seguridad1:~$ id -u infracomp
1004
infracomp@seguridad1:~$ id -g infracomp
1004
infracomp@seguridad1:~$ █
```

# UNIX/Linux

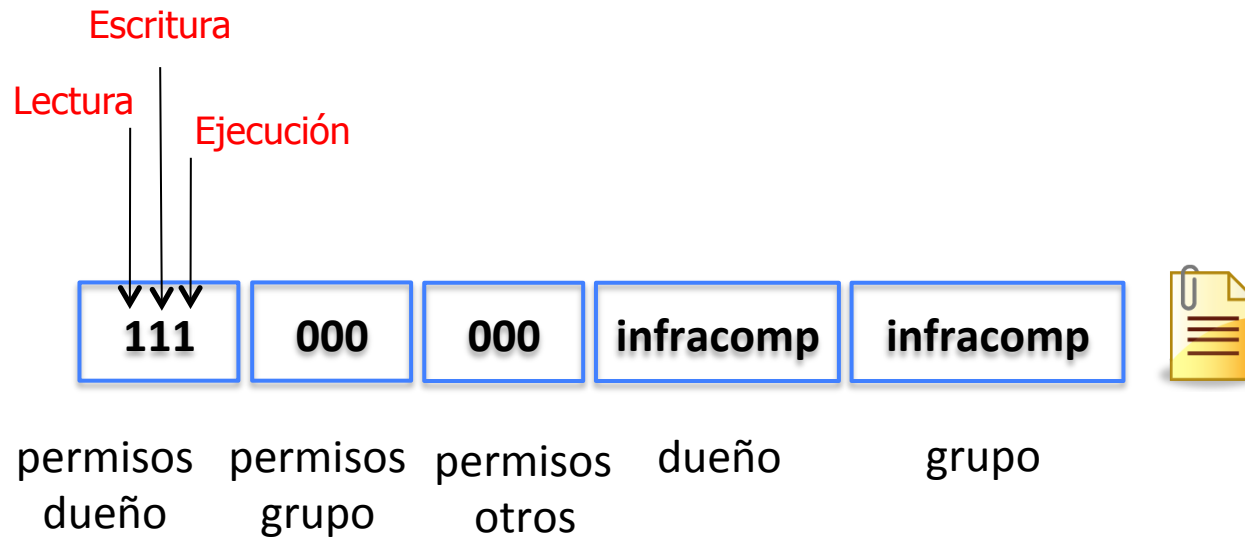
- UNIX/Linux
  - Cada archivo
    - id del propietario
    - gid del propietario



```
infracomp@seguridad1:~$ ls -l
total 8
drwxr-xr-x 2 infracomp infracomp 4096 Jan 17 22:22 apps
-rw-r--r-- 1 infracomp infracomp   0 Jan 17 22:22 archivo1
-rw-r--r-- 1 infracomp infracomp   0 Jan 17 22:22 archivo2
-rw-r--r-- 1 infracomp infracomp 179 Jan 17 22:21 examples.desktop
infracomp@seguridad1:~$
```

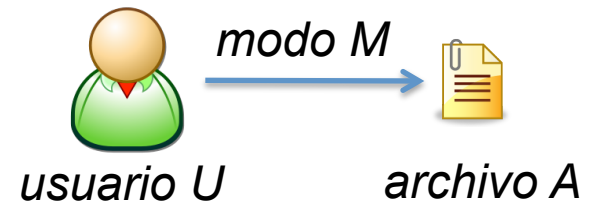


# Manejo de Permisos



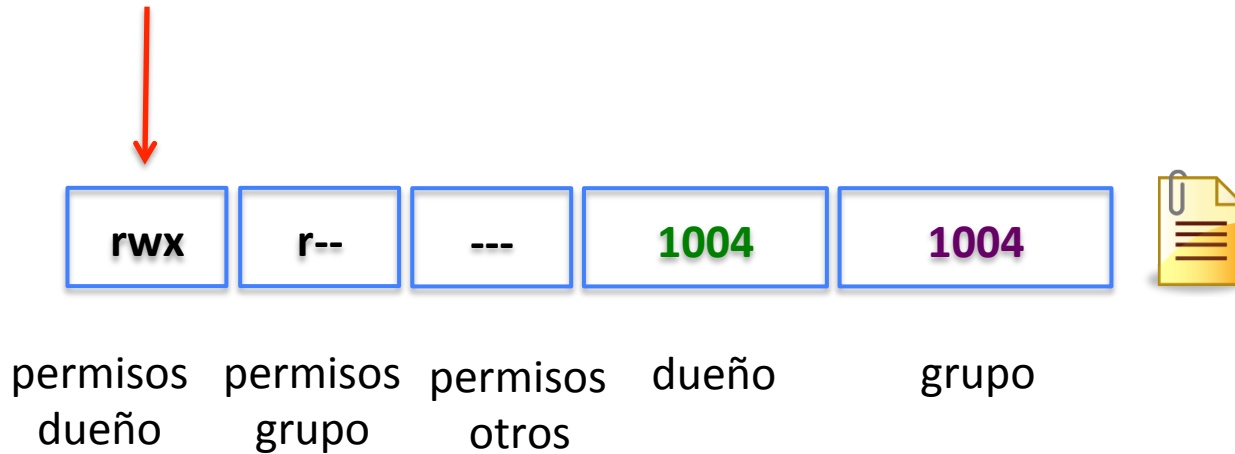
```
infracomp@seguridad1:~$ ls -l
total 8
drwxr-xr-x 2 infracomp infracomp 4096 Jan 17 22:22 apps
-rw-r--r-- 1 infracomp infracomp  0 Jan 17 22:22 archivo1
-rw-r--r-- 1 infracomp infracomp  0 Jan 17 22:22 archivo2
-rw-r--r-- 1 infracomp infracomp 179 Jan 17 22:21 examples.desktop
infracomp@seguridad1:~$
```

# Evaluación de Permisos

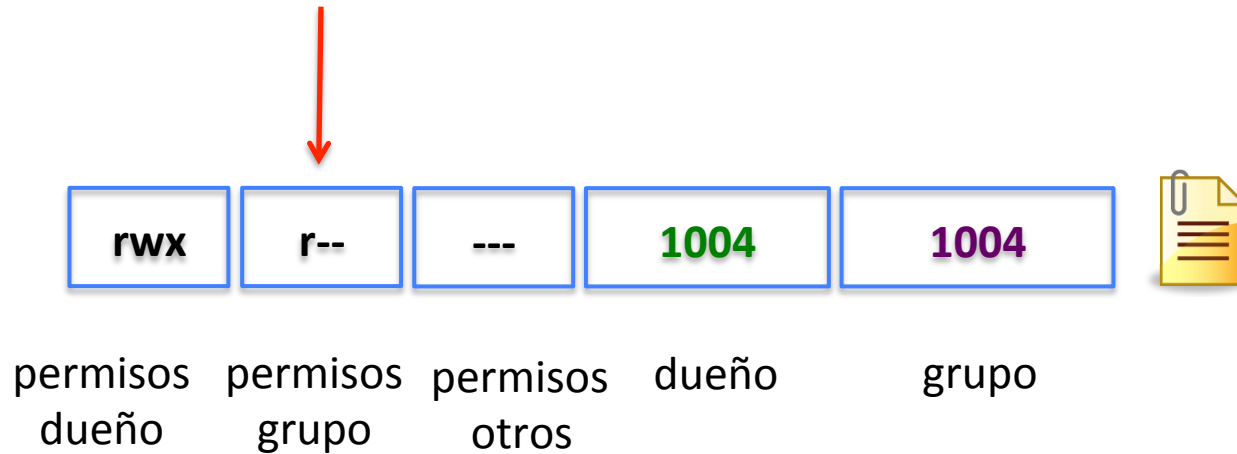


```
si ( UID usuario = UID archivo )  
    permisos = bits usuario  
si_no si ( algún GID usuario = GID archivo )  
    permisos = bits grupo  
si_no permisos = bits otros  
  
si ( acción en permisos )  
    efectuar acción
```

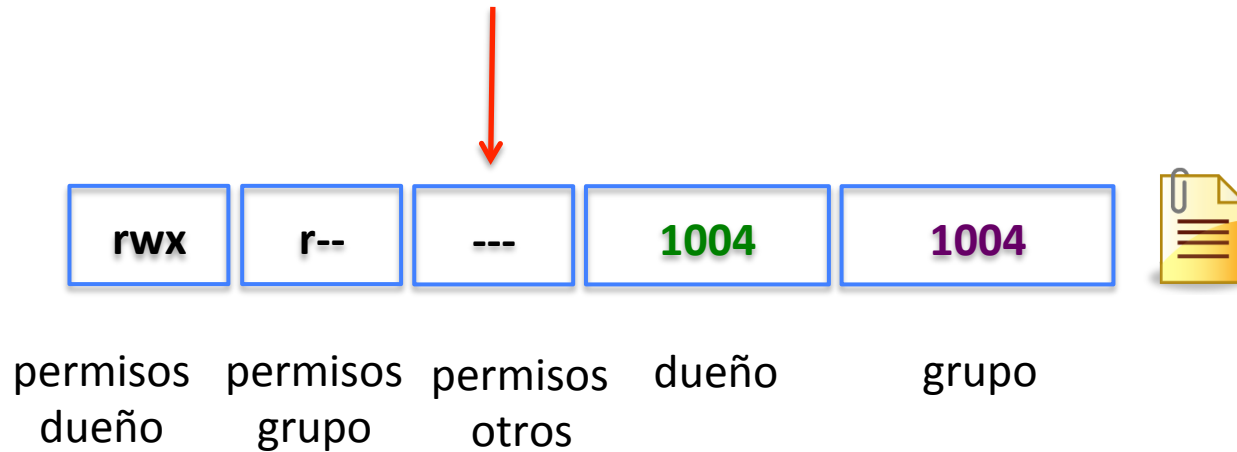
# Evaluación de Permisos



# Evaluación de Permisos



# Evaluación de Permisos



1005  
1010

# UNIX/Linux

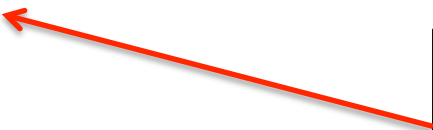
- Procesos
  - Los procesos se crean con UID del usuario
  - Los procesos hijos heredan UID del padre
  - Los procesos pueden efectuar las mismas acciones que su propietario
  - Los permisos de acceso dependen de
    - quién lanzó el proceso y
    - del propietario del archivo

# UNIX/Linux

- Atributos de los procesos
  - 2 UID (y 2 GID):
    - UID real (RUID): UID del usuario que lo lanzó
    - UID efectivo (EUID):
      - UID del usuario que lo lanzó O
      - UID del archivo binario que se ejecutó, Si este tiene activo el bit setuid
        - » Permite cambio de dominio (en particular, root)
  - Los permisos de acceso se revisan contra el EUID

# Archivos

- Tipos de acceso a los archivos
  - Los archivos también tienen especificado si son un directorio o no
  - Hay 3 bits “misceláneos”:
    - su = setuid
    - sg = setgid
    - t = sticky



Permite cambio de dominio  
(en particular, root)



# Ejercicio

- Elabore una lista de seis mecanismos de protección relacionados con la seguridad del sistema de cómputo de un banco.
  - Para cada uno indique si éste se relaciona con seguridad física, seguridad humana o seguridad del sistema operativo.

# Referencias

- *[SGG] Sistemas Operativos*. Siberschatz, Galvin y Gagne. Editorial Wiley.
- *Sistemas Operativos Modernos*. Andrew Tanenbaum.