

Instituto Politécnico Nacional

Centro de Investigación en  
Computación

Laboratorio de Ciberseguridad

UPIITA

Administración de Sistemas  
Operativos

Moisés Salinas Rosales  
msrosales@acm.org



INSTITUTO POLITÉCNICO NACIONAL  
LA TÉCNICA AL SERVICIO DE LA PATRIA



# Agenda

1. Fundamentos de Administración de Sistemas
2. Administración de usuarios



INSTITUTO POLITÉCNICO NACIONAL  
LA TÉCNICA AL SERVICIO DE LA PATRIA





# Fundamentos de Administración de Sistemas



INSTITUTO POLITÉCNICO NACIONAL  
LA TÉCNICA AL SERVICIO DE LA PATRIA



# Fundamentos de Administración de Sistemas

- Tareas asignadas al Administrador de sistemas y su equipo.
  - ❖ Al tanto de operaciones diarias
  - ❖ Administración de Servidores
  - ❖ Servidores 7 x 24



# Fundamentos de Administración de Sistemas

## □ Objetivos de la Administración eficaz:

- ❖ Prevención
- ❖ Actuación a tiempo
- ❖ Máxima prestación del servicio
- ❖ Evolución del sistema
  - Mejoras al funcionamiento
  - Nuevas funciones



# Fundamentos de Administración de Sistemas

## □ Administración de:

- ❖ Sistema de Archivos
- ❖ Procesos y estado del sistema
- ❖ Actividades de usuarios
- ❖ Servicios ofrecidos

## □ Comunicación con:

- ❖ Usuarios
- ❖ Otros administradores
- ❖ Desarrolladores de software



# Fundamentos de Administración de Sistemas

## □ Monitoreo de:

- ❖ Evolución del software
- ❖ Noticias de seguridad
- ❖ Esquemas de licenciamiento

## □ Difusión de:

- ❖ Políticas de uso
- ❖ Cultura de uso de recursos
- ❖ Nuevos servicios



# Administración de usuarios



INSTITUTO POLITÉCNICO NACIONAL  
LA TÉCNICA AL SERVICIO DE LA PATRIA



# Administración de usuarios

## □ Algunas definiciones

- ❖ User
- ❖ Password
- ❖ Grupo de Usuario
- ❖ UserID (UID)
- ❖ GroupID (GID)
- ❖ Home
- ❖ Shell



# Administración de usuarios

## □ Creación de cuentas de usuario

```
# adduser -c"Usuario 1" user1
```

```
# passwd user1
```

```
new password: ****
```

```
retype new password: ****
```



# Administración de usuarios

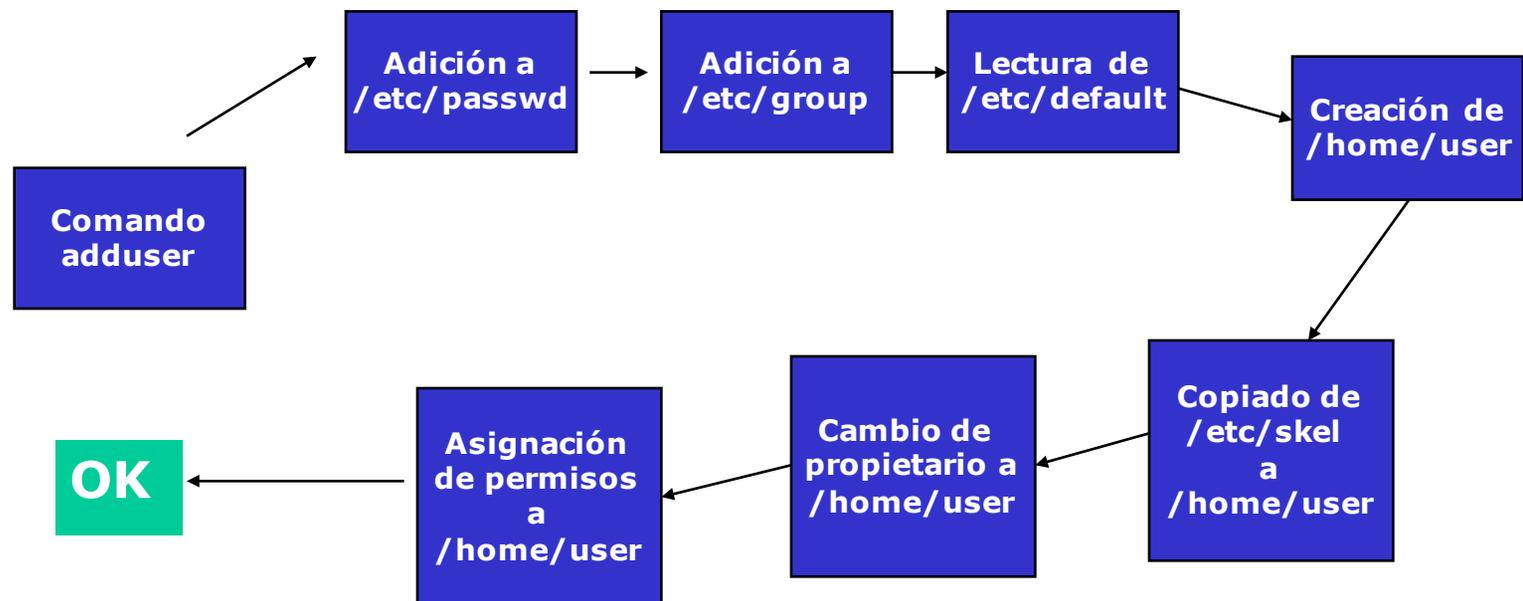
## □ Opciones del comando *adduser*

```
# adduser username  
    [-c "abcde"]  
    [-d /home/otro/]  
    [-k /etc/skel]  
    [-u UID]  
    [-g GID]  
    [-s /bin/shell]
```



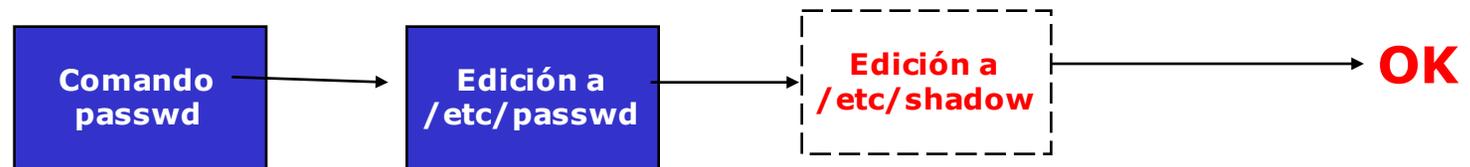
# Administración de usuarios

## □ Proceso de alta de cuentas de usuarios



# Administración de usuarios

- Proceso de asignación de password



# Administración de usuarios

## ❑ Eliminación de cuentas de usuario

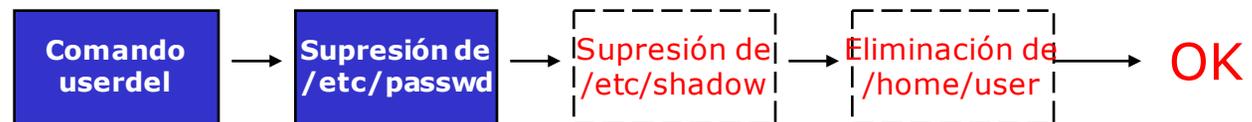
```
# userdel username  
[-f]
```

- ❖ Permite eliminar la cuenta **username** del sistema, y con la opción **-f** elimina el directorio home del usuario y sus archivos dependientes.



# Administración de usuarios

- Proceso de eliminación de cuenta de usuario



# Administración de usuarios

## □ Modificación de cuentas de usuario

```
# usermod username
```

```
[-u uid [-o]]
```

```
[-g group] [-G group,...]
```

```
[-d home [-m]] [-s shell]
```

```
[-c comment] [-l new_name]
```

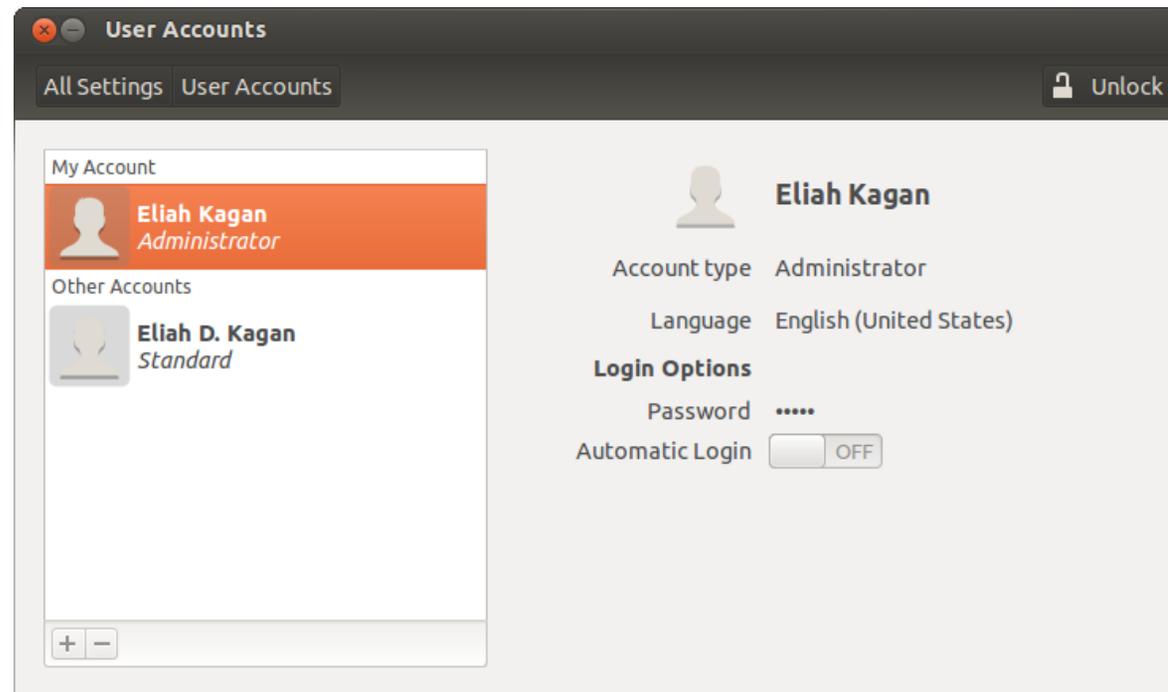
```
[-f inactive] [-e expire ]
```

```
[-p passwd]
```



# Administración de usuarios

- Modificación de cuentas de usuario (Gnome control center)



# Administración de usuarios

## □ El archivo /etc/passwd:

- ❖ Este archivo contiene la información acerca de las cuentas de usuarios del sistema.

```
moises:  
x:  
500:  
500:  
Moises Salinas Rosales:  
/home/moises:  
/bin/bash
```

# Administración de usuarios

## □ Monitoreo actividades

### ❖ Revisión de histórico de comandos:

➤ `~/.bash_history`

### ❖ Revisión de procesos actuales:

➤ `w`

➤ `ps aux |grep ttyX`

➤ `ps aux |grep user`



# Administración de usuarios

## □ Monitoreo actividades

❖ #cat ~/.bash\_history

```
psql moises
```

```
psql
```

```
psql
```

```
psql
```

```
halt
```

```
clear
```

```
ls
```

```
w
```

```
clear
```

```
w
```

```
clear
```

```
ls
```

```
w
```

```
clear
```

```
df
```

```
dmesg
```

```
clear
```

```
ls
```

```
df
```

```
psql
```

```
psql
```

```
clear
```

```
ls
```

```
cdp
```

```
clear
```

```
root
```

```
halt
```

```
balsa
```



# Administración de usuarios

## □ Monitoreo actividades

❖ # w

```
12:23pm up 1:30, 4 users, load average: 0.47, 0.44, 0.19
USER  TTY  FROM  LOGIN@  IDLE   JCPU   PCPU   WHAT
root  tty1  -     10:54am 1:14m 17.19s 0.01s  sh /usr/X11R6/
root  pts/0 :0    11:46am 2:59   0.14s 0.14s  bash
root  pts/1 :0    11:52am 11:34  0.19s 0.04s  vi muestras.txt
root  pts/2 :0    12:20pm 0.00s 0.15s 0.03s  w
```



# Administración de usuarios

## □ Monitoreo actividades

❖ #ps aux |grep tty1

```
root    605    0.0    4.3    5788 2548  tty1 S    11:09    0:00  magicdev
root    622    0.0    9.8    8080 5828  tty1 S    11:09    0:03  panel
root    624    0.0    9.1    7672 5420  tty1 S    11:09    0:01  gmc
root   2221    0.0    5.6    5568 3356  tty1 S    11:46    0:00  gnome
root   2222    0.0    0.9    1140   536  tty1 S    11:46    0:00  gnome-pty-
root   2240    0.0    5.6    5568 3356  tty1 S    11:52    0:00  gnome-
root   2241    0.0    0.9    1140   536  tty1 S    11:52    0:00  gnome-pty-
```



# Administración de usuarios

## □ Monitoreo actividades

❖ #ps aux |grep *user*

```
root  2221  0.0  5.6  5568 3356 tty1  S 11:46  0:00 gnome-terminal
root  2222  0.0  0.9  1140  536 tty1  S 11:46  0:00 gnome-pty-helper
root  2223  0.0  1.7  1840 1052 pts/0  S 11:46  0:00 bash
root  2240  0.0  5.6  5568 3356 tty1  S 11:52  0:00 gnome-terminal
root  2241  0.0  0.9  1140  536 tty1  S 11:52  0:00 gnome-pty-helper
root  2242  0.0  1.7  1840 1060 pts/1  S 11:52  0:00 bash
root  2292  0.0  1.7  1992 1008 pts/1  S 12:11  0:00 vi muestras.txt
```



# Administración de usuarios

## □ Generación de Perfiles:

- ❖ Dependientes del Shell
- ❖ Perfiles Generales
  - `/etc/profiles`
- ❖ Perfiles Individuales
  - `~/.bash_profiles`



# Administración de usuarios

## □ Generación de Perfiles:

```
# /etc/profile

PATH="$PATH:/usr/X11R6/bin"
PS1="[\u@\h \W]\$ "
ulimit -c 1000000
if [ `id -gn` = `id -un` -a `id -u` -gt 14 ]; then
    umask 002
else
    umask 022
fi
USER=`id -un`
LOGNAME=$USER
MAIL="/var/spool/mail/$USER"
```

# Administración de usuarios

## □ Generación de ACL's

- ❖ /etc/groups
- ❖ chmod
- ❖ chown



# Administración de sistemas de archivos

## □ Algunas definiciones

- ❖ Sistema de archivos
  - Características
  - Ventajas
  - Desventajas
- ❖ Particiones
- ❖ Archivos y directorios
- ❖ Archivos de dispositivo
- ❖ Enlaces (links)
- ❖ Incorporación de otros sistemas de archivos



# Administración de sistemas de archivos

- Exploración del sistema de archivos característicos de Linux.

/	/opt
/bin	/proc
/boot	/root
/dev	/sbin
/etc	/tmp
/home	/usr
/lib	/var
/lost+found	
/misc	
/mnt	



# Administración de sistemas de archivos

## □ Montaje de sistemas de archivos

- ❖ Incorpora sistemas de archivos residentes principalmente en dispositivos removibles (cdrom's, disquetes, cintas, zip's, etc)
- ❖ También se utiliza para incorporar sistemas de archivo compartidos vía red (nfs, samba)
- ❖ Una vez montado un sistema de archivos, es necesario desmontarlo para removerlo.



# Administración de sistemas de archivos

## □ Montaje de sistemas de archivos

❖ # mount `[/dev/xxx] [fs_type] mount_point`

❖ `/dev/xxx`

❖ `fs_type`

❖ `mount_point`



# Administración de sistemas de archivos

## □ Montaje de sistemas de archivos

Monitoreo de montajes en el sistema de archivos

❖ Archivo `/etc/mtab`

❖ `# df`



# Administración de sistemas de archivos

## □ Montaje de sistemas de archivos

❖ Para retirar un dispositivo removible, el cual contenga un sistema de archivos montado, es necesario primero desmontar este dispositivo.

❖ `#umount mount_point`



# Administración de sistemas de archivos

## □ Administración de espacio en particiones

❖ Revisión de espacio disponible en zonas críticas del sistema.

❖ `#df -k`

❖ `#du`



# Administración de sistemas de archivos

## □ Administración de espacio en particiones

### ❖ Liberación de espacio

- Zonas no críticas
- Documentación extra
- Información de usuarios no vigentes
- Histórico de bitácoras
- Colas de correo e impresión muertas
- Aplicaciones no utilizadas
- Bibliotecas no utilizadas



# Administración de sistemas de archivos

## □ Habilitación de nuevas particiones

### ❖ Objetivos

- Aumentar el espacio de almacenamiento en el sistema.
- Aislamiento de zonas de riesgos del FS.

### ❖ Procedimiento

- Disponer de espacio libre en un dispositivo.
- Crear la partición con fdisk.
- Dar formato a la nueva partición.
- Incorporar la nueva partición al FS.



# Administración de sistemas de archivos

## □ Habilitación de nuevas particiones

❖ Ubicación del dispositivo con espacio disponible.

➤ /dev/hdb ?

➤ /dev/hda ?

➤ /dev/scb ?

➤ /dev/sca ?



# Administración de sistemas de archivos

## □ Habilitación de nuevas particiones

- ❖ Creación de la nueva partición (fdisk)
- ❖ # fdisk /dev/dispositivo
- ❖ Opciones menu fdisk:
  - n definir nueva partición
  - d eliminar una partición
  - t definir el tipo de una partición
  - w salvar y salir
  - m mostrar el menu con la ayuda
- ❖ Parámetros necesarios:
  - Cilindro inicial (default)
  - Tamaño de la partición



# Administración de sistemas de archivos

## □ Habilitación de nuevas particiones

- ❖ Formato a nuevas particiones (formato para FS Linux)

- ❖ `# mkfs.ext2 /dev/hda[n]`

## □ Incorporación al FS original.

- ❖ El archivo `/etc/fstab`.
- ❖ Creación del punto de montaje.
- ❖ Migración de la información.



# Administración de sistemas de archivos

## □ Habilitación de nuevos dispositivos

### ❖ Tipos de dispositivos

➤ SATA

➤ IDE

➤ SCSI

### ❖ Identificación de estos en /dev/



# Administración de sistemas de archivos

## □ Configuración de cuotas de espacio (quotas)

- ❖ Aplicable a usuarios y a grupos

- ❖ Necesidad

- Limitar la cantidad de espacio que los usuarios utilizan o pueden llegar a utilizar dentro del sistema, para así evitar problemas de saturación de espacio en disco.
- Hacer cumplir políticas de uso de recursos.

- ❖ Requerimientos

- Kernel con soporte para Quotas.
- Instalación del Toolkit de Quotas.



# Administración de sistemas de archivos

## □ Configuración de cuotas de espacio (quotas)

- ❖ Definición. Una cuota es un límite sobre el espacio ocupado o bien sobre el número de archivos existentes dentro de una partición. Estas cuotas pueden definirse tanto como para usuarios, como para grupos de usuarios.
- ❖ Límite Flexible
- ❖ Límite Rígido



# Administración de sistemas de archivos

## □ Configuración de cuotas de espacio (quotas)

### ❖ Preparación del sistema de archivos

#### ➤ Configuración de la partición para uso de cuotas en /etc/fstab.

```
/dev/hda1 / ext2 default,usrquota,grpquota 1 1
```

#### ➤ Creación de archivos de cuotas en cada partición.

```
#touch /quota.usr
```

```
#touch /quota.group
```

```
#chmod 600 quota.usr quota.group
```

#### ➤ Reinicio del sistema

# Administración de sistemas de archivos

## ❑ Configuración de cuotas de espacio (quotas)

### ❖ Estableciendo cuotas para un usuario

➤ `#edquota user`

- ❑ Definición de límites: flexible y rígido
- ❑ Tipos de límites: bloques e inodos

➤ Por default `edquota` se aplica para un usuario (-u)

### ❖ Establecimiento de cuotas para un grupo

➤ `#edquota -g group`

- ❑ Definición de límites: flexible y rígido
- ❑ Tipos de límites: bloques e inodos



# Administración de sistemas de archivos

## □ Configuración de cuotas de espacio (quotas)

❖ Establecimiento de cuotas a partir de una cuenta muestra utilizando awk.

❖ `#edquota -p muestra `awk -F: '$3 > 499 {print $1}' /etc/passwd``



# Administración de sistemas de archivos

## □ Configuración de cuotas de espacio (quotas)

### ❖ Reportes sobre cuotas

➤ # quota user

➤ # repquota



# Administración de sistemas de archivos

## □ Herramientas de apoyo

### ❖ Midnight Commander

- #mc
- Visualización de archivos
- Edición de archivos
- Cambios de permisos/propietarios
- Copiado, Borrado y Movimiento de archivos
- Navegación entre ventanas
- Navegación dentro de contenedores

### ❖ which

### ❖ File



# Administración de sistemas de archivos

## □ Elaboración de respaldos.

### ❖ Definición de zonas críticas

- /etc
- /home
- /root
- /boot (en caso de recompilación de kernel)
- /var (datos de las aplicaciones y servicios)
- /var/spool/mail
- /var/spool/mqueue
- /var/log



# Administración de sistemas de archivos

## □ Elaboración de respaldos.

- ❖ Selección del dispositivo de respaldo
  - Disquete (no recomendado)
  - Cartucho ZIP o JAZZ
  - Cintas de datos
  - Unidades de Red
- ❖ Creación de contenedores y respaldos
  - tar
  - gzip
  - lha
  - zip



# Administración de sistemas de archivos

## ❑ Elaboración de respaldos.

### ❖ Creación de contenedores

➤ # `tar -cvf contenedor.tar datos.origen`

#### ➤ Opciones:

❑ C = CREAR EL CONTENEDOR

❑ V = VISUALIZAR EL ARCHIVADO DENTRO DEL CONTENEDOR

❑ F = DIRIGIR LA SALIDA A UN ARCHIVO

❑ Z = COMPRIMIR LA INFORMACION UTILIZANDO GZIP

❑ X = EXTRAER LA INFORMACION DEL CONTENEDOR

### ❖ Compresión de archivos

➤ # `gzip archivo.a.comprimir`

➤ # `gunzip archivo.a.comprimir.gz`