Laboratorio 5
Dagoberto Rojas
2015127575

Preguntas Guía

1. Investigue para que se utiliza los comandos: useradd, userdel, passwd, así como los diferentes ID de usuarios
    a. **Useradd:** cuando se invoca sin la etiqueta **-D**, el comando useradd crea un nuevo usuario usando los valores especificados en la consola
    b. **Userdel:** remueve usuarios del sistema, elimina todos los archivos relacionados al usuario especificado
    c. **Passwd:** Cambia la contraseña para cuentas de usuario.
    d. **UID:** Identifica al usuario, utiliza un valor único para identificar al usuario, normalmente, la recomendación es utilizar el menor número posible mayor que 999 y mayor que cualquier otro usuario. Los ID entre 0 y 999 se reservan para usuarios del sistema
        i. **SYS_UID_MAX (number), SYS_UID_MIN (number)**: Rango de UserIDs usados en la creación de usuarios del sistema por **useradd** o **newusers**
        ii. **UID_MAX (number), UID_MIN (number):** Rango de UserIDs usados para la creación de usuarios regulares por **useradd** o **newusers**
2. ¿Qué son grupos primarios y grupos secundarios en Linux?
    a. El grupo primario de un usuario es el grupo por defecto con el que se asocia la cuenta, generalmente comparte el mismo nombre que el usuario. Los directorios y los archivos que el usuario crea tendrán asignados este grupo. Un grupo secundario es cualquier grupo adicional del que un usuario sea parte.
3. Realice un cuadro comparativo entre Inode y ACL

Inode	ACL
• Estructura de datos que tiene track de todos los archivos • Cada archivo o carpeta se identifica por su “inode number”	• Forma adicional de brindar permisos, a usuarios o grupos

4. Investigue el comando para cambiar permisos a un archivo. Coloque los métodos por medio de letras y de números.
    a. Se utiliza el comando chmod
    b. Chmod cambia los bits de modo de un archivo de acuerdo al modo, puede ser representación simbólica u octal
        i. Uso chmod (+/-) [modo (ugoa)]
            1. ugoa: 4 objetivos diferentes u(usuario dueño), g(usuarios en el grupo), o(otros usuarios en el grupo), a(todos los usuarios)
            2. representación simbólica: cada uno de los espacios de “ugoa” puede ser cambiado por uno de los caracteres de la representación (rwxXst)
                a. r: read
                b. w: write
                c. x: execute
                d. X: execute
                e. s: conjunto de usuarios o ID de grupo
                f. t: etiqueta de borrado (sticky bit)

Laboratorio 5
Dagoberto Rojas
2015127575

3. Representación octal: se componen por un número de bits, y los número s 4,2,1,:
    a. 4: UserID
    b. 2: groupID
    c. 1:sticky attribute

5. Explique cómo se administran los permisos especiales de directorios y archivos en un entorno Linux.
    a. Sticky bit: Permisos de acceso para directorios y archivos: solo el dueño del archio puede modificarlo o borrarlo
    b. SUID: Permite que cualquiera que ejecute un archivo tienen los permisos de el creador del archivo
    c. SGID: SUID pero a nivel de grupos de usuarios
6. Explique cuál es la implicación de utilizar FAT en un disco de gran capacidad (orden de los TB)
    a. El tamaño de registro para usar FAT (no FAT32) es de 8 bits, lo que el tamaño de archivos se ve muy limitado. Por ejemplo, para FAT32 es de 4 GB (aproximadamente), utilizando FAT el límite sería de 256 Bytes (aproximadamente)
    b. Actualmente se puede utilizar exFAT como una de las alternativas, por lo que los archivos pueden tener hasta casi 2 TB de tamaño.

Laboratorio 5
Dagoberto Rojas
2015127575

4. Creación de Usuarios

Para la siguiente sección se debe tomar captura de cada paso que se ejecuta.

1. Cree una máquina virtual nueva con el sistema operativo Centos. Los comandos pueden variar de una versión a otra, sin embargo, puede modificarlos en caso de que sea necesario. Observe que los comandos que inician con # es porque debe hacerlo con usuario privilegiado (sudo).

Basics

Subscription	
Resource group	
Virtual machine name	CentOS-dago
Region	East US 2
Availability options	Availability zone
Availability zone	1
Security type	Standard
Image	CentOS-based 7.9 - Gen2
VM architecture	x64
Size	Standard D2s v3 (2 vcpus, 8 GiB memory)
Authentication type	SSH public key
Username	
Key pair name	
Azure Spot	No

2. Conéctese por medio de ssh a la máquina recien creada.

Laboratorio 5
Dagoberto Rojas
2015127575

```
void@JOJO:~$ ssh -i ~/azure azureuser@20.69.237.227
The authenticity of host '20.69.237.227 (20.69.237.227)' can't be established.
ECDSA key fingerprint is SHA256:MQfOlWqJJ0KblfjfwChG3MtZgK24DlibLQsFJawuHYk.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '20.69.237.227' (ECDSA) to the list of known hosts.

Thank you for choosing this Microsoft sponsored CentOS image from OpenLogic!
 _______                        ______                 _____
 __  __ \_____________________  / _____________ ___(_)_______
 _  / / /__  __ \  _ \_  __ \_  /  _  __ \_  __ `/_  /_  ___/
 / /_/ /__  /_/ /  __/  / / /  /___/ /_/ /  /_/ /_  / / /__
 \____/ _  .___/\___//_/ /_//_____/\____/_\__, / /_/  \___/
        /_/                               /____/  by Perforce
                          ____                _    ___  ____    _____ ___
                         / ___|___ _ __ | |_ / _ \/ ___|  |___  / _ \
                        | |   / _ \ '_ \| __| | | \___ \     / / (_) |
                        | |__|  __/ | | | |_| |_| |___) |   / / \__, |
                         \____\___|_| |_|\__|\___/|____/   /_(_)  /_/
                                                            (2009)

While OpenLogic support is not including with this image, OpenLogic does
offer Silver (12x5) & Gold (24x7) support options and consulting for
enterprise and/or mission critical systems as well as over 400 open-source
packages.  If interested, email info@perforce.com or call +1 612.517.2100.

[azureuser@centos-dago ~]$
```

3. Agregue tres diferentes usuarios con contraseñas diferentes. Utilice el comando *# useradd < name >* y *# echo < password1 > — passwd –stdin < username1 >* .

```
[azureuser@centos-dago ~]$ sudo -i
[root@centos-dago ~]# useradd user1 && echo password - passwd -stdin user1
password - passwd -stdin user1
[root@centos-dago ~]# useradd user2 && echo password - passwd -stdin user2
seradd user3 && echo password - passwd -stdin user3password - passwd -stdin user2
[root@centos-dago ~]# useradd user3 && echo password - passwd -stdin user3
password - passwd -stdin user3
```

4. Confirme que cada usuarios se creó realizando los siguientes comandos. Note las diferencias en las salidas de datos.

   - *# id < username >*
   - *# yum install finger -y*
   - *# finger < username >*
   - *# cat /etc/passwd — grep < username >*

```
[root@centos-dago ~]# yum install finger -y
Failed to set locale, defaulting to C
Loaded plugins: langpacks
Package finger-0.17-52.el7.x86_64 already installed and latest version
Nothing to do
```

Laboratorio 5
Dagoberto Rojas
2015127575

```
[root@centos-dago ~]# id user1
uid=1001(user1) gid=1001(user1) groups=1001(user1)
[root@centos-dago ~]# id user2
uid=1002(user2) gid=1002(user2) groups=1002(user2)
[root@centos-dago ~]# id user3
uid=1003(user3) gid=1003(user3) groups=1003(user3)
```

```
[root@centos-dago ~]# finger user1
Login: user1                            Name:
Directory: /home/user1                  Shell: /bin/bash
Never logged in.
No mail.
No Plan.
[root@centos-dago ~]# finger user2
Login: user2                            Name:
Directory: /home/user2                  Shell: /bin/bash
Never logged in.
No mail.
No Plan.
[root@centos-dago ~]# finger user3
Login: user3                            Name:
Directory: /home/user3                  Shell: /bin/bash
Never logged in.
No mail.
No Plan.
```

```
[root@centos-dago ~]# cat /etc/passwd - grep user1
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:999:998:User for polkitd:/:/sbin/nologin
libstoragemgmt:x:998:996:daemon account for libstoragemgmt:/var/run/lsm:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
abrt:x:173:173::/etc/abrt:/sbin/nologin
```

Laboratorio 5
Dagoberto Rojas
2015127575

```
[root@centos-dago ~]# cat /etc/passwd - grep user2
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
```

```
[root@centos-dago ~]# clear
[root@centos-dago ~]# cat /etc/passwd - grep user3
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
```

5. Cree los grupos y usuarios que se muestran en la siguiente tabla. Utilice los comandos: # *groupadd* < *groupname* > y # *usermod -aG* < *groupname* >< *username* >

```
[root@centos-dago ~]# useradd Luis && useradd Diego && useradd Josue && useradd Viviana && useradd Steven && useradd Ped
ro && useradd Juan && useradd Harold
```

```
[root@centos-dago ~]# groupadd Professors && usermod -aG Professors Jason && usermod -aG Professors Luis && usermod -aG
Professors Diego
[root@centos-dago ~]# groupadd Assistents && usermod -aG Assistents Josue && usermod -aG Assistents Viviana && usermod -
aG Assistents Steven
[root@centos-dago ~]# groupadd Students && usermod -aG Students Pedro && usermod -aG Students Juan && usermod -aG Studen
ts Harold
```

Laboratorio 5
Dagoberto Rojas
2015127575

6. Valide que se hayan creado los grupos de usuario y sus respectivas listas. Además verifique la ruta */etc/groupfile*. Ejecute los siguientes comandos: *# id < username >* y *# cat /etc/group — grep < username >*

```
[root@centos-dago ~]# id Jason && cat /etc/group - grep Jason
uid=1004(Jason) gid=1005(Jason) groups=1005(Jason),1004(profesores),1014(Professors)
root:x:0:
bin:x:1:
daemon:x:2:
```

```
Professors:x:1014:Jason,Luis,Diego
Assistents:x:1015:Josue,Viviana,Steven
Students:x:1016:Pedro,Juan,Harold
cat: -: No such file or directory
cat: grep: No such file or directory
cat: Jason: No such file or directory
[root@centos-dago ~]#
```

5. Permisos

En esta sección se presentarán algunos comandos para establecer, verificar y cambiar los permisos de un archivo y directorio. De igual manera que el anterior debe aportar el screenshot para cada paso.

5.1. Archivos

1. Ejecute los comandos: *$ touch /tmp/test* y *$ ls -l /tmp/test*. Explique la función de cada uno de ellos, así como el resultado de de la ejecución. Muestre un screenshot. Debe explicar cada parte del resultado.

```
[azureuser@centos-dago ~]$ touch /tmp/test
test[azureuser@centos-dago ~]$ ls -l /tmp/test
-rw-rw-r--. 1 azureuser azureuser 0 Nov 11 21:49 /tmp/test
```

- touch: crea el archivo /tmp/test
- ls -l: lista información completa sobre /tmp/test

2. Ejecute, y explique el resultado de los siguientes comandos.
   - *$ chmod o+w /tmp/test.*
   - *$ chmod 666 /tmp/test.*
   - *$ chmod a-rwx /tmp/test.*
   - *$ cat /tmp/test .*
   - *$ chmod u+rw /tmp/test.*

Laboratorio 5
Dagoberto Rojas
2015127575

```
[azureuser@centos-dago ~]$ chmod o+w /tmp/test
est
chmod a-rwx /tmp/test
cat /tmp/test
chmod u+rw /tmp/test[azureuser@centos-dago ~]$ chmod 666 /tmp/test
[azureuser@centos-dago ~]$ chmod a-rwx /tmp/test
[azureuser@centos-dago ~]$ cat /tmp/test
cat: /tmp/test: Permission denied
[azureuser@centos-dago ~]$ chmod u+rw /tmp/test
[azureuser@centos-dago ~]$
```

- chmod o+w /tmp/test : da permisos de escritura a otros usuarios fuera del grupo
- chmod 666 /tmp/test: da permisos de lectura y escritura a el usuario, usuarios en el grupo y usuarios fuera del grupo
- chmod a-rwx /tmp/test: quita permisos de lectura, escritura y ejecución a todos los usuarios
- cat /tmp/test: intenta leer el archive, pero falla por no tener permisos de lectura
- chmod u+rw /tmp/test: Vuelve a brindar permisos de lectura y escritura al usuario duelo del archivo

5.2. Directorios

1. Cree un directorio con el siguiente comando: *$ mkdir -p /tmp/mydirectory/mydir2.*

```
[azureuser@centos-dago ~]$ mkdir -p /tmp/mydirectory/mydir2
```

2. Ejecute los siguientes comandos: *$ ls -l /tmp/mydirectory* y *$ ls -ld /tmp/mydirectory.* Describa el resultado que se muestra en consola.

```
[azureuser@centos-dago ~]$ ls -l /tmp/mydirectory
total 0
drwxrwxr-x. 2 azureuser azureuser 6 Nov 11 21:59 mydir2
[azureuser@centos-dago ~]$ ls -ld /tmp/mydirectory
drwxrwxr-x. 3 azureuser azureuser 20 Nov 11 21:59 /tmp/mydirectory
```

- ls -l: lista la información del archivo
- ls -ld: lista la información del directorio, no de su contenido

3. Si no permite que otros tengan permiso de ejecución en el directorio /tmp/mydirectory, no importa quién tenga acceso de lectura o escritura. Nadie puede acceder al directorio a menos que conozca el nombre exacto del archivo. Con el siguiente comando eliminas la ejecución de todos: *$ chmod a-x /tmp/mydirectory.*

```
[azureuser@centos-dago ~]$ chmod a-x /tmp/mydirectory
```

Laboratorio 5
Dagoberto Rojas
2015127575

4. ¿Qué ocurre si ejecuta el comando: *cd /tmp/mydirectory* ?

```
[azureuser@centos-dago ~]$  cd /tmp/mydirector
-bash: cd: /tmp/mydirectory: Permission denied
```

5. Restaure el acceso al directorio con el comando: *$ chmod ug+x /tmp/mydirectory.*

```
[azureuser@centos-dago ~]$ chmod ug+x /tmp/mydirectory
```

6. Verifique que otros no tengan permiso de acceso con el comando: *ls -ld /tmp/mydirectory*

```
[azureuser@centos-dago ~]$ ls -ld /tmp/mydirectory
drwxrwxr--. 3 azureuser azureuser 20 Nov 11 21:59 /tmp/mydirectory
```

7. Realice un archivo y un directorio, asigne, modifique y elimine permisos con representación numérica.

```
[azureuser@centos-dago ~]$ mkdir -p /tmp/mydirectory2/mydir
[azureuser@centos-dago ~]$ ls -l && ls -ld
total 0
drwx------. 5 azureuser azureuser 103 Nov 15  2022 .
[azureuser@centos-dago ~]$ ls
[azureuser@centos-dago ~]$  chmod a+777 /tmp/mydirectory2/mydir
```

```
[azureuser@centos-dago ~]$  chmod +700 /tmp/mydirectory2
```

```
[azureuser@centos-dago /]$  chmod -777 /tmp/mydirectory2
[azureuser@centos-dago /]$ cd /tmp/mydirectory2
-bash: cd: /tmp/mydirectory2: Permission denied
```

6. Lista de Control de Acceso

En esta sección se debe ejecutar los comandos y mostrar un screenshot de la consola con el resultado de los mismos.

1. Investigue el uso de los comandos: *getfacl* y *setfacl*. Muestre las diferentes sintaxis de uso.

- getfacl: para cada archivo muestra file name, owner, group, Access Control List
- setfacl: configura el ACL para archivos o directorios

2. Trate de editar el archivo */etc/motd*. Probablemente el un usuario no pueda editar y solo podrá leerlo. Ejecute el comando: *$ vim /etc/motd* (Note que el comando no se está ejecutando como root).

Laboratorio 5
Dagoberto Rojas
2015127575

```
~
~
~
~
E45: 'readonly' option is set (add ! to override)
```

3. Utilice el comando *setfacl* (punto 1, por ejemplo setfacl -m d:u:rootadmin:rw /etc/motd) y agregue una ACL que garantice que un usuario que no sea root pueda leer y escribir el archivo */etc/motd*.

```
[azureuser@centos-dago /]$ sudo setfacl -m 'u:1000:rw' /etc/motd
```

4. Ejecute el comando *getfacl /etc/motd*, verifique si la ACL que agregó en el punto anterior está correcta.

```
[azureuser@centos-dago /]$  getfacl /etc/motd
getfacl: Removing leading '/' from absolute path names
# file: etc/motd
# owner: root
# group: root
user::rw-
user:azureuser:rw-
group::r--
mask::rw-
other::r--
```

5. Como usuario no privilegiado (no root), ejecute el siguiente comando: *$ echo 'Welcome from rootadmin!' >> /etc/motd*.

```
[azureuser@centos-dago /]$ echo 'Welcome from rootadmin\!' >> /etc/motd
[azureuser@centos-dago /]$
```

6. Utilice otra terminal y conéctese por ssh a la máquina virtual, ¿Qué ocurre con respect al inicio ordinario?

- Se añade la línea “Welcome from rootadmin!” al final del inicio

Laboratorio 5
Dagoberto Rojas
2015127575

```
Holis
Thank you for choosing this Microsoft sponsored CentOS image from OpenLogic!
 _______                     ______                 _____
__  __ \_____________________ / ____________ ___(_)______
_  / / /__  __ \  _ \_  __ \_ /  _ \  __ \_  __ `/_  /_  ___/
/ /_/ /__  /_/ /  __/  / / /  /___/ /_/ /  /_/ /_  / / /__
\____/ _  .___/\___//_/ /_//_____/\____/_\__, / /_/  \___/
       /_/                                /____/  by Perforce
                          ____                _    ___  ____    _____ ___
                         / ___|___ _ __ | |_ / _ \/ ___|  |___  / _ \
                        | |    / _ \ '_ \| __| | | \___ \     / / (_) |
                        | |__|  __/ | | | |_| |_| |___) |   / / \__, |
                         \____\___|_| |_|\__|\___/|____/   /_(_)  /_/
                                                             (2009)

While OpenLogic support is not including with this image, OpenLogic does
offer Silver (12x5) & Gold (24x7) support options and consulting for
enterprise and/or mission critical systems as well as over 400 open-source
packages.  If interested, email info@perforce.com or call +1 612.517.2100.

'Welcome from rootadmin!'
[azureuser@centos-dago ~]$
```

al inicio ordinario.

7. Como root, cree el directorio *mkdir /var/tmp/collab.*

```
[root@centos-dago ~]# getfacl /var/tmp/collab
getfacl: Removing leading '/' from absolute path names
# file: var/tmp/collab
# owner: root
# group: root
user::rwx
group::r-x
other::r-x
```

9. Cree una ACL que permita que un usuario no root pueda leer y escribir todos los archivos creados bajo el directorio de */var/tmp/collab*. Para esto ejecute el comando: *# setfacl -m d:u:rootadmin:rw /var/tmp/collab.*

Laboratorio 5
Dagoberto Rojas
2015127575

```
'Welcome from rootadmin!'
[azureuser@centos-dago ~]$ sudo setfacl -m d:u:azureuser:rw /var/tmp/collab
[azureuser@centos-dago ~]$ gsetfacl /var/tmp/collab
-bash: gsetfacl: command not found
[azureuser@centos-dago ~]$ getfacl /var/tmp/collab
getfacl: Removing leading '/' from absolute path names
# file: var/tmp/collab
# owner: root
# group: root
user::rwx
group::r-x
other::r-x
default:user::rwx
default:user:azureuser:rw-
default:group::r-x
default:mask::rwx
default:other::r-x

[azureuser@centos-dago ~]$
```

10. Verifique la nueva ACL. *getfacl /var/tmp/collab.*

```
'Welcome from rootadmin!'
[azureuser@centos-dago ~]$ sudo setfacl -m d:u:azureuser:rw /var/tmp/collab
[azureuser@centos-dago ~]$ gsetfacl /var/tmp/collab
-bash: gsetfacl: command not found
[azureuser@centos-dago ~]$ getfacl /var/tmp/collab
getfacl: Removing leading '/' from absolute path names
# file: var/tmp/collab
# owner: root
# group: root
user::rwx
group::r-x
other::r-x
default:user::rwx
default:user:azureuser:rw-
default:group::r-x
default:mask::rwx
default:other::r-x

[azureuser@centos-dago ~]$
```

11. Ahora debe crear un archivo en el directorio creado llamado */var/tmp/collab/rootfile.* Ejecute el comando: *# echo rootfile contents > /var/tmp/collab/rootfile.*

```
[root@centos-dago ~]# echo "rootfile contents" > /var/tmp/collab/rootfile.
[root@centos-dago ~]#
```

12. Verifique el contenido con *cat /var/tmp/collab/rootfile*

```
[azureuser@centos-dago ~]$ cat /var/tmp/collab/rootfile
rootfile contents
```

13. Verifique la ACL del archivo. *getfacl /var/tmp/collab/rootfile.*

```
[azureuser@centos-dago ~]$  getfacl /var/tmp/collab/rootfile
getfacl: Removing leading '/' from absolute path names
# file: var/tmp/collab/rootfile
# owner: root
# group: root
user::rw-
user:azureuser:rw-
group::r-x                      #effective:r--
mask::rw-
other::r--
```

14. Ahora como usuario no root agregue una línea de texto en el archivo. Ejecute el comando *$ echo 'rootadmin was here' >> /var/tmp/collab/rootfile*

```
[azureuser@centos-dago ~]$ echo 'rootadmin was here' >> /var/tmp/collab/rootfile
[azureuser@centos-dago ~]$
```

15. Verifique el contenido. *# cat /var/tmp/collab/rootfile.*

```
[azureuser@centos-dago ~]$ sudo -i
[root@centos-dago ~]#  cat /var/tmp/collab/rootfile
rootfile contents
'rootadmin was here'
[root@centos-dago ~]#
```

Laboratorio 5
Dagoberto Rojas
2015127575

7. Práctica

Realice con líneas de comando la estructura de usuarios, ACL y archivos que muesta la figura 1.

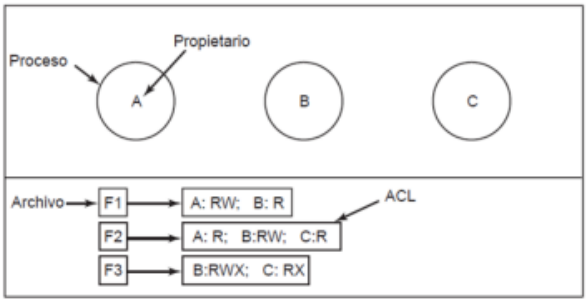

Figura 1: Estructura a realizar