**PRACTICA 3**

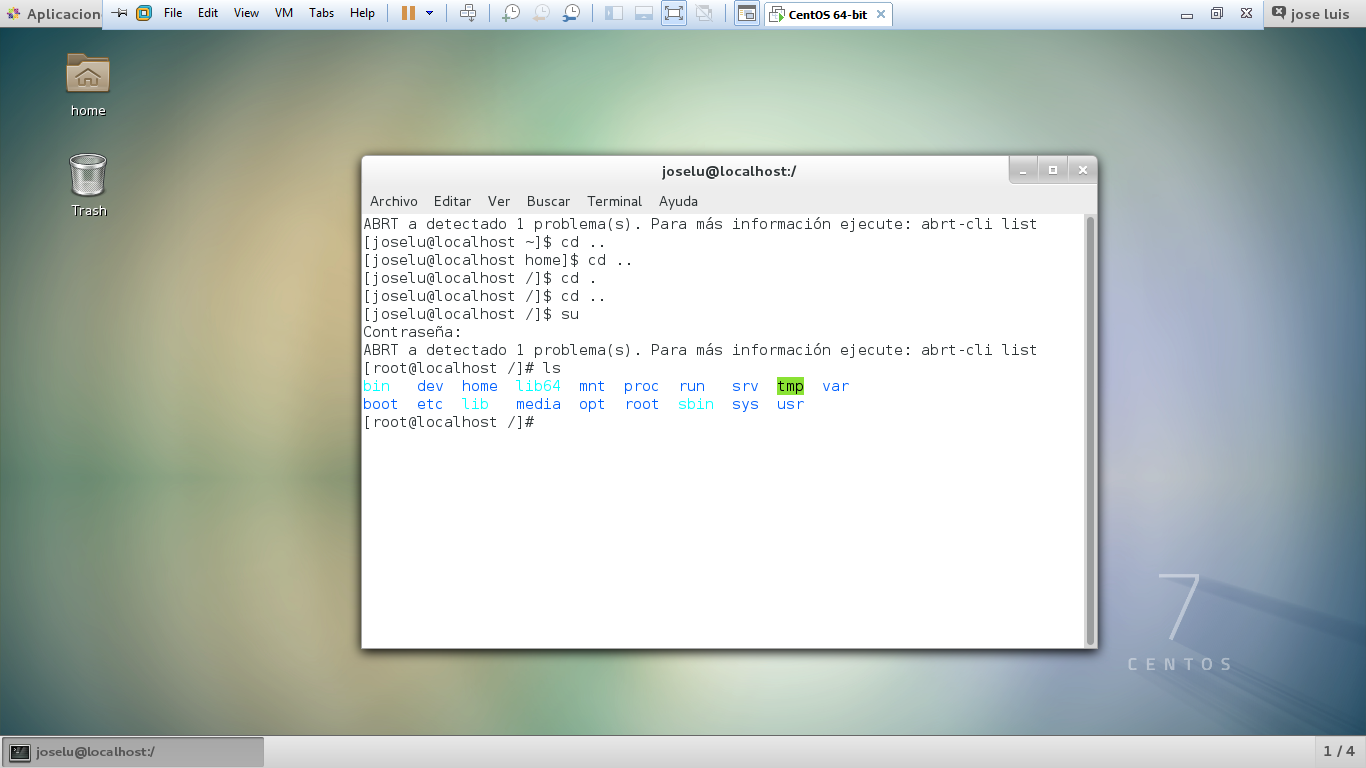
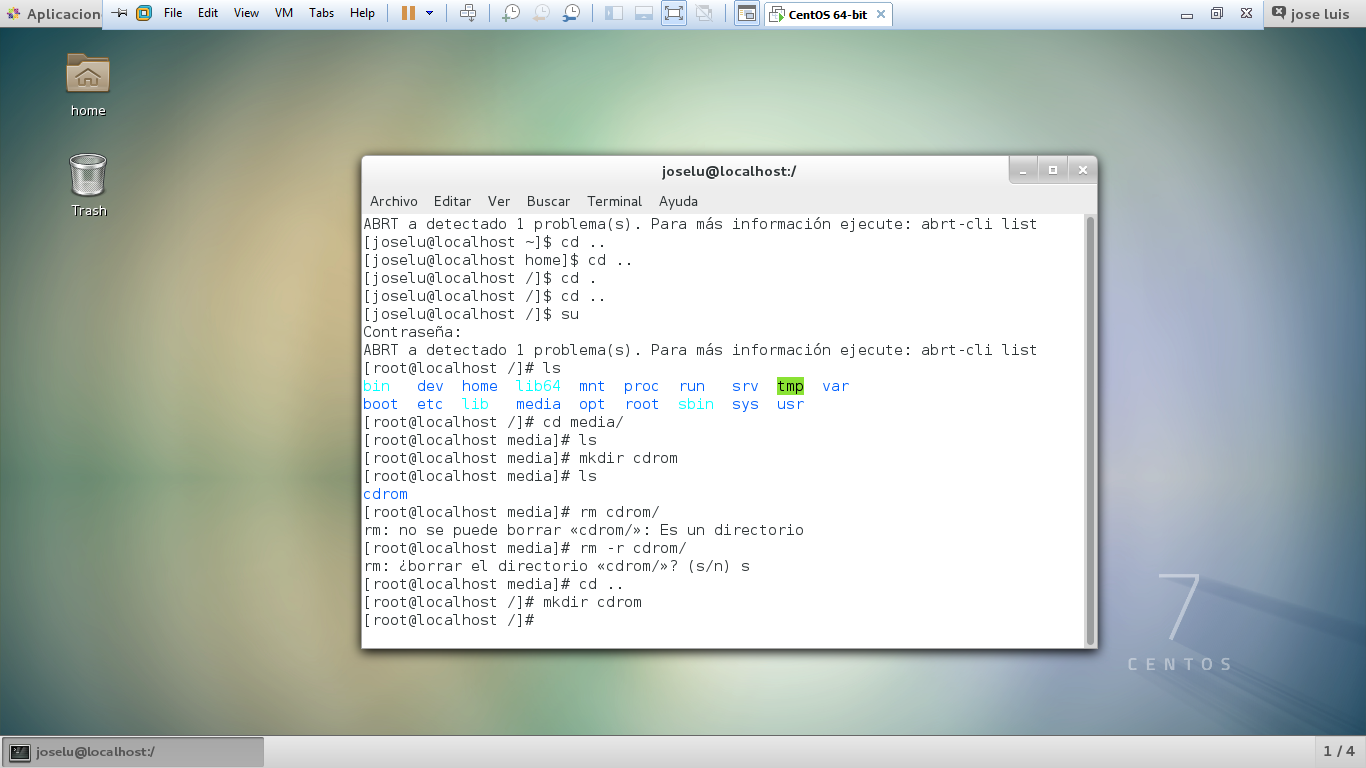
José Luis Arcos García-Verdugo

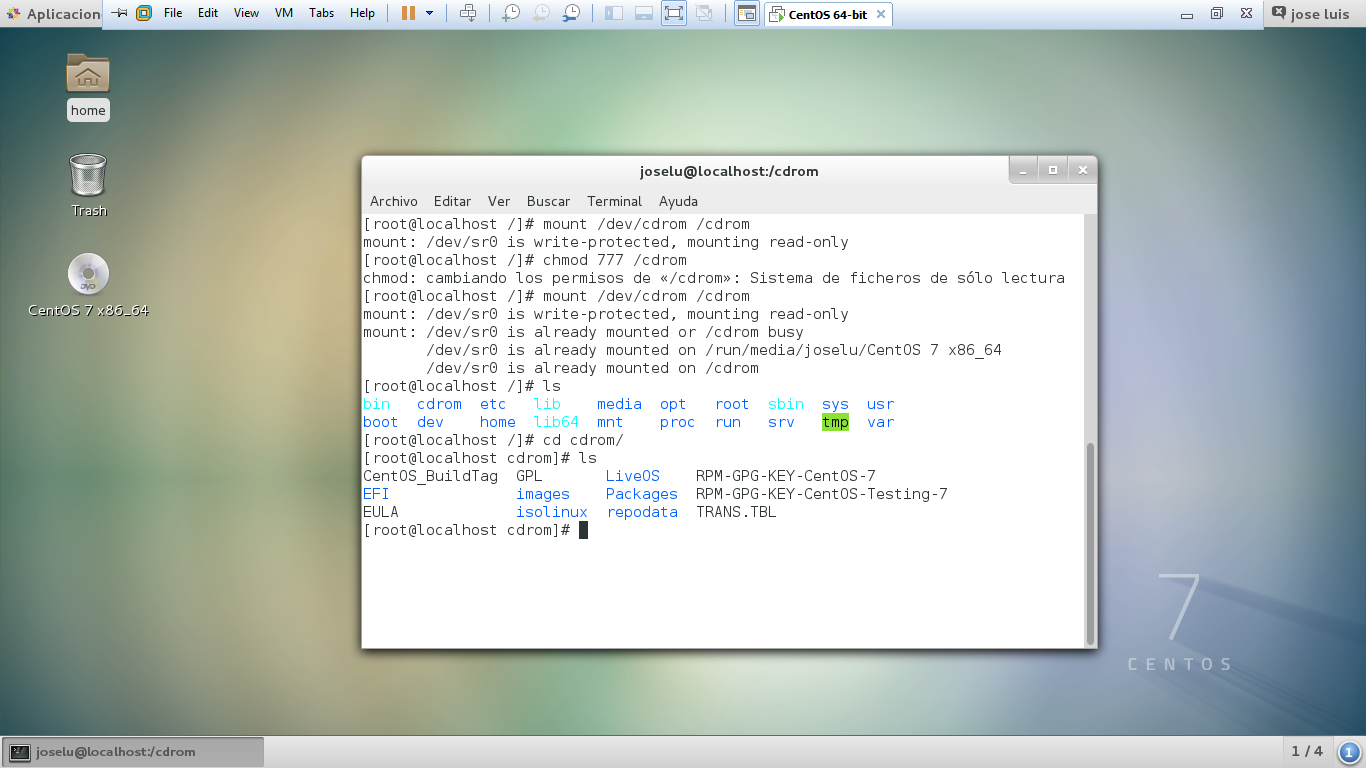
**Cuestiones**

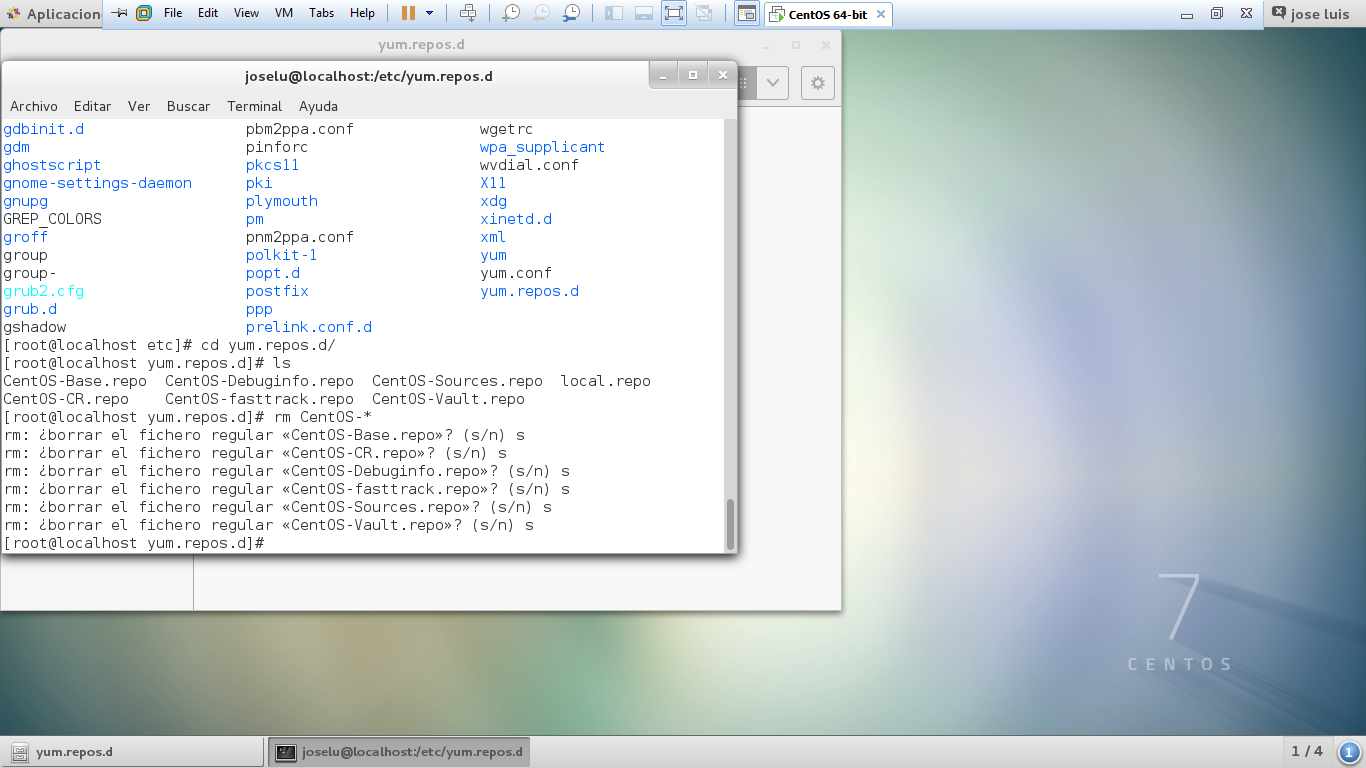
**Cuestión 1:**

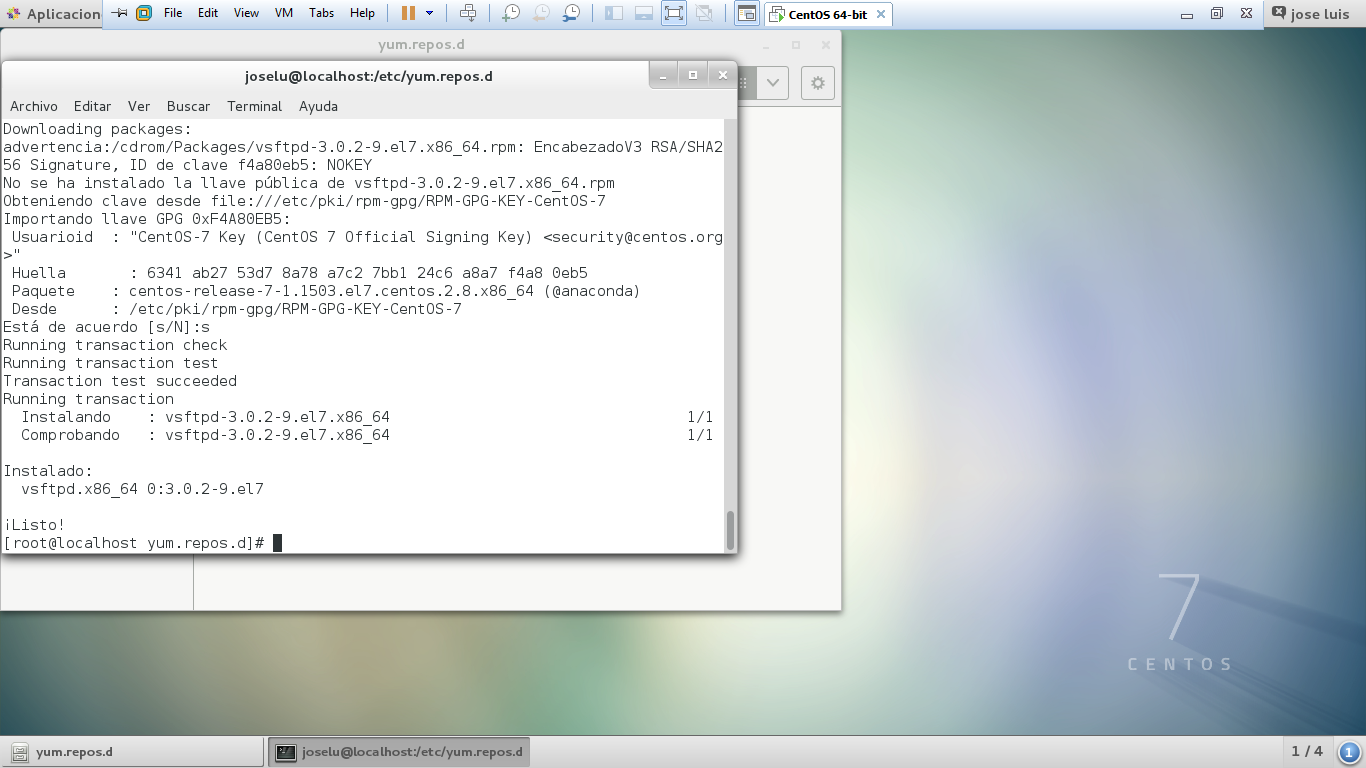
|  |  |  |
| --- | --- | --- |
| **Operaciones** | **Yum** | **Apt** |
| Instalar | yum install [paquete] | apt-get install [paquete] |
| Buscar | yum search [cadena] | apt-cache search paquete |
| Eliminar | yum remove [paquete] | apt remove paquete |

**Cuestión 2:**

****

****

****

****

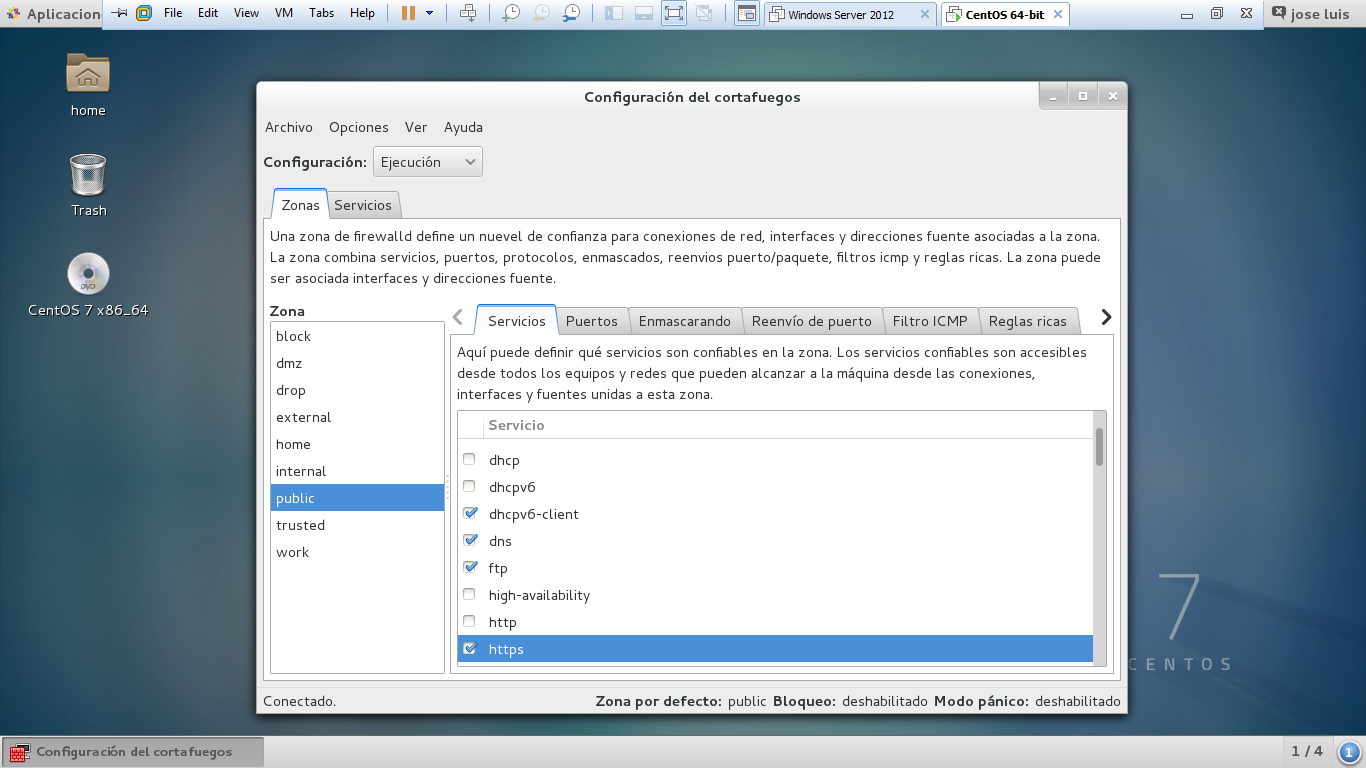
Instalamos vsftp, php y httpd con el comando yum install [paquete]. En Ubuntu seria lo mismo solo que en vez de usar yum usariamos apt.

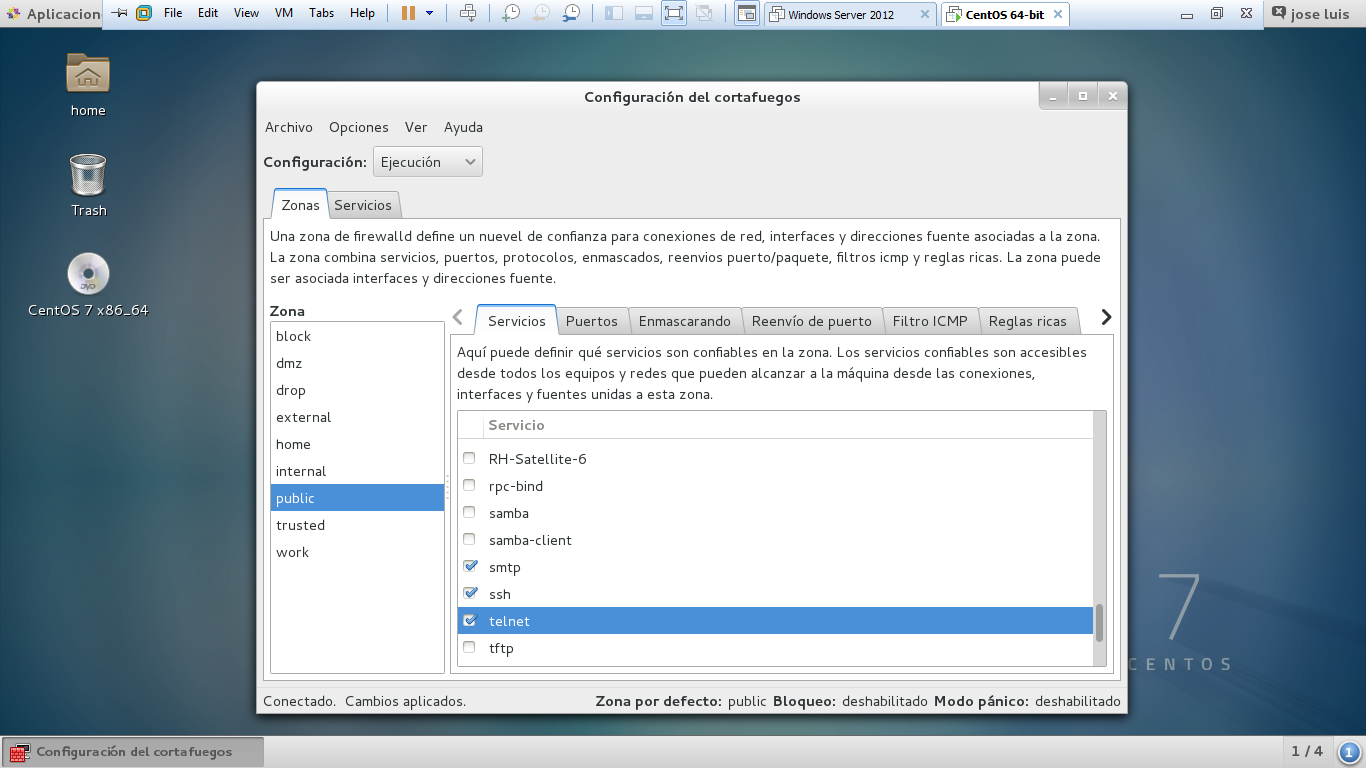
**Cuestión 3:**

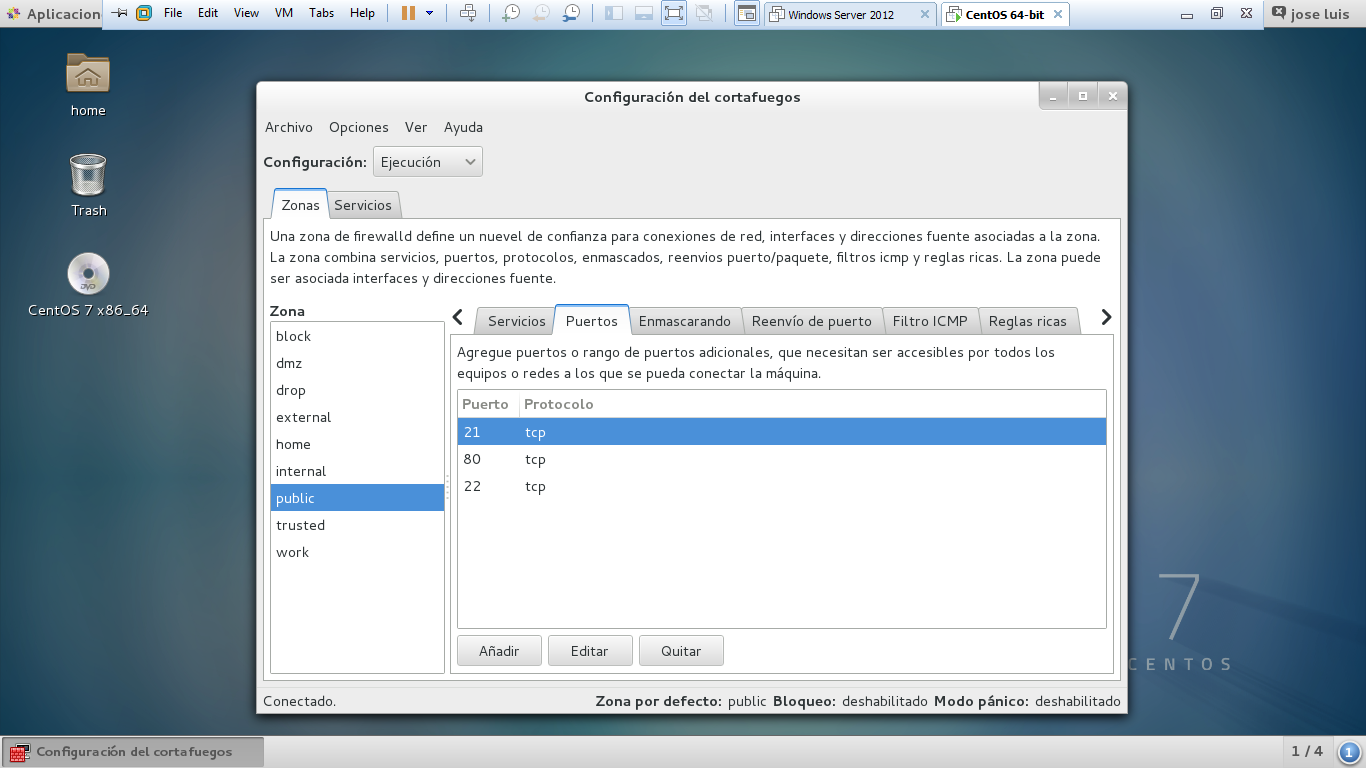
Los comprendidos entre 1024 (0400 en hexadecimal) y 49151 (BFFF en hexadecimal) son denominados "registrados" y pueden ser usados por cualquier aplicación. Los comprendidos entre los números 49152 (C000 en hexadecimal) y 65535 (FFFF en hexadecimal) son denominados dinámicos o privados, normalmente se asignan en forma dinámica a las aplicaciones de clientes al iniciarse la conexión. Son usados en conexiones peer to peer (P2P).

**Cuestión 4:**

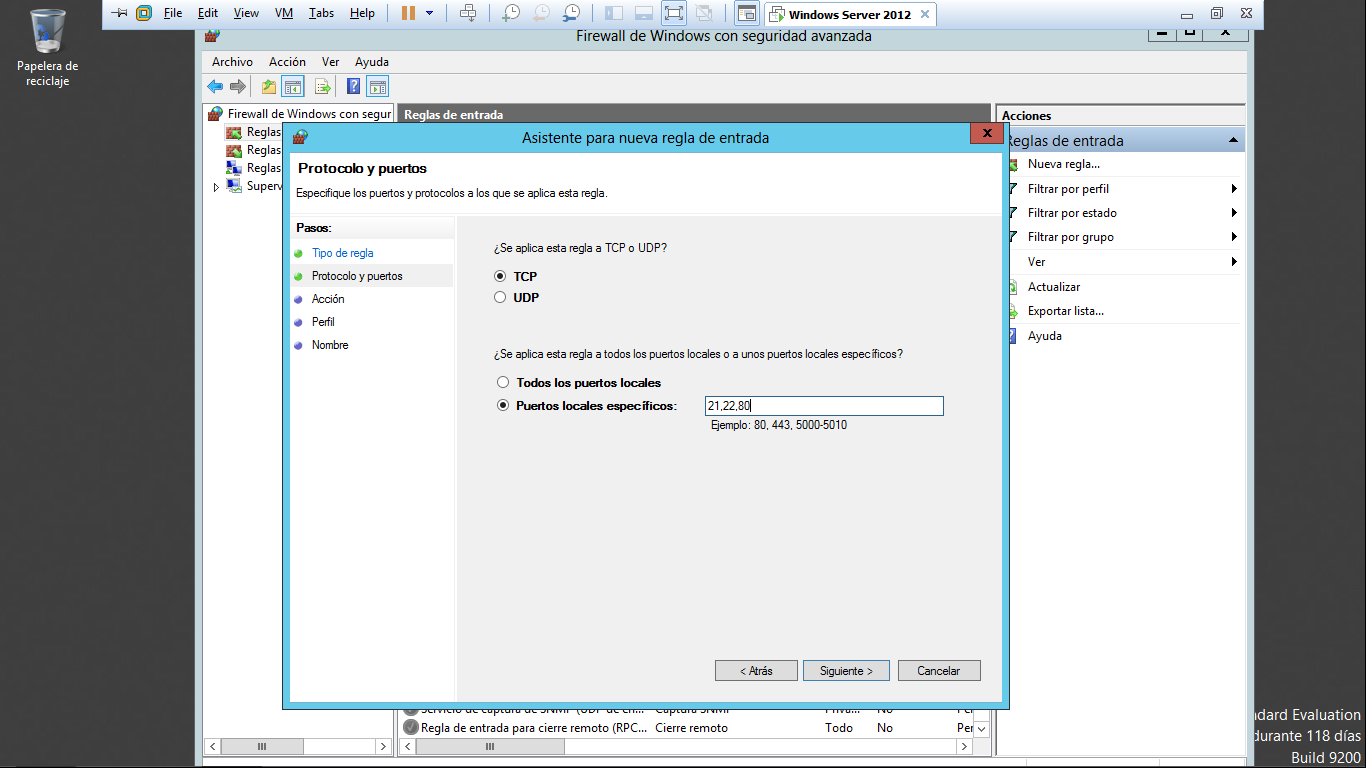
**CentOS:**







**Windows Server:**



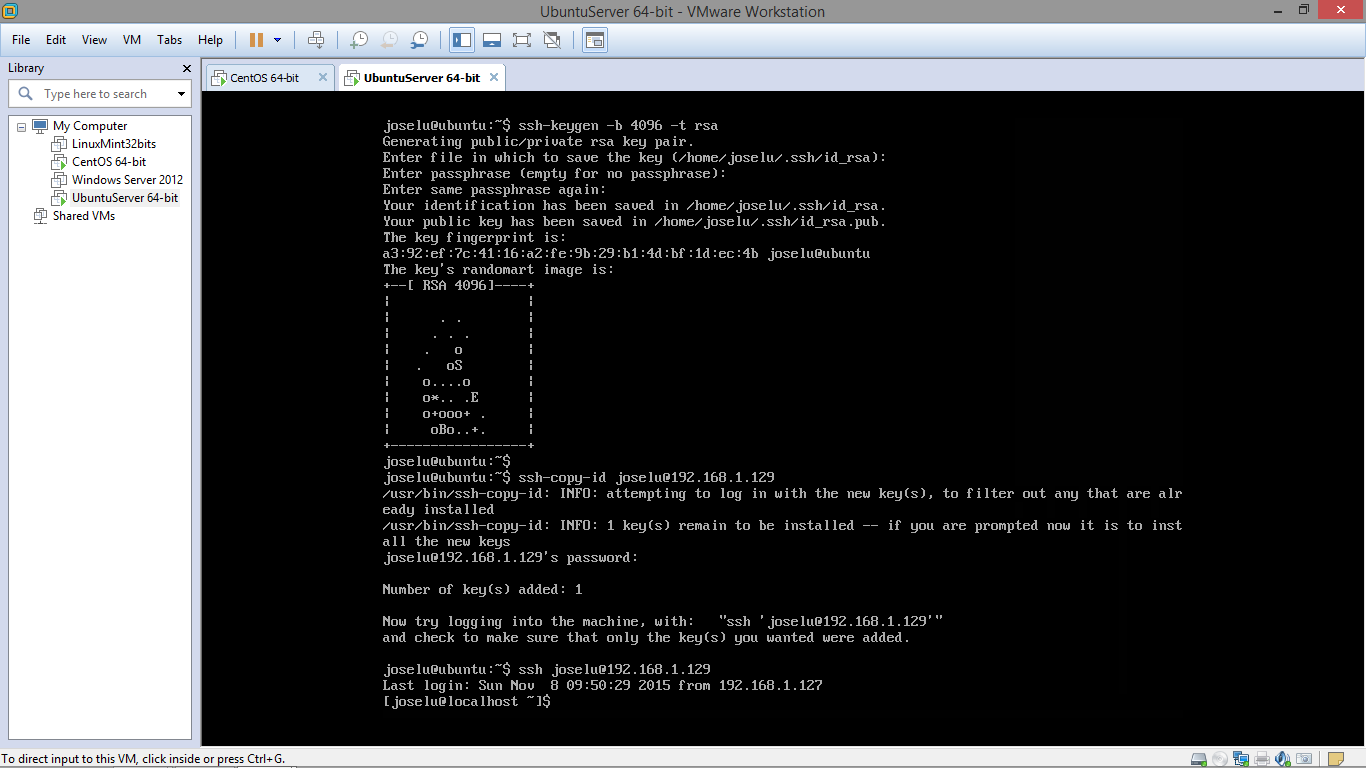
**Cuestión 5:**

Activa el X11, servidor grafico que sirve para poder ejecutar aplicaciones graficas de una maquina remota exportando el display a nuestro escritorio.

Si ejecutamos el comando gedit tal cual en el ssh no nos dejara abrir la aplicación pues pues no está la opción grafica activada. Para ello tienes que entrar al ssh con la opción -X para habilitar el entorno gráfico.

**Cuestión 6:**

Voy a conectarme por ssh de Ubuntu Server a CentOS:



**Cuestión 7:**

El archivo que contiene la configuración es ssh\_config y se encuentra en “/etc/ssh”.

**Cuestión 8:**

Si es necesario.

Para reiniciar un servicio en Ubuntu es tan sencillo como usar “restart” un ejemplo seria: sudo [servicio] restart

Para reiniciarlos en CentOS es al contrario: restart [servicio]

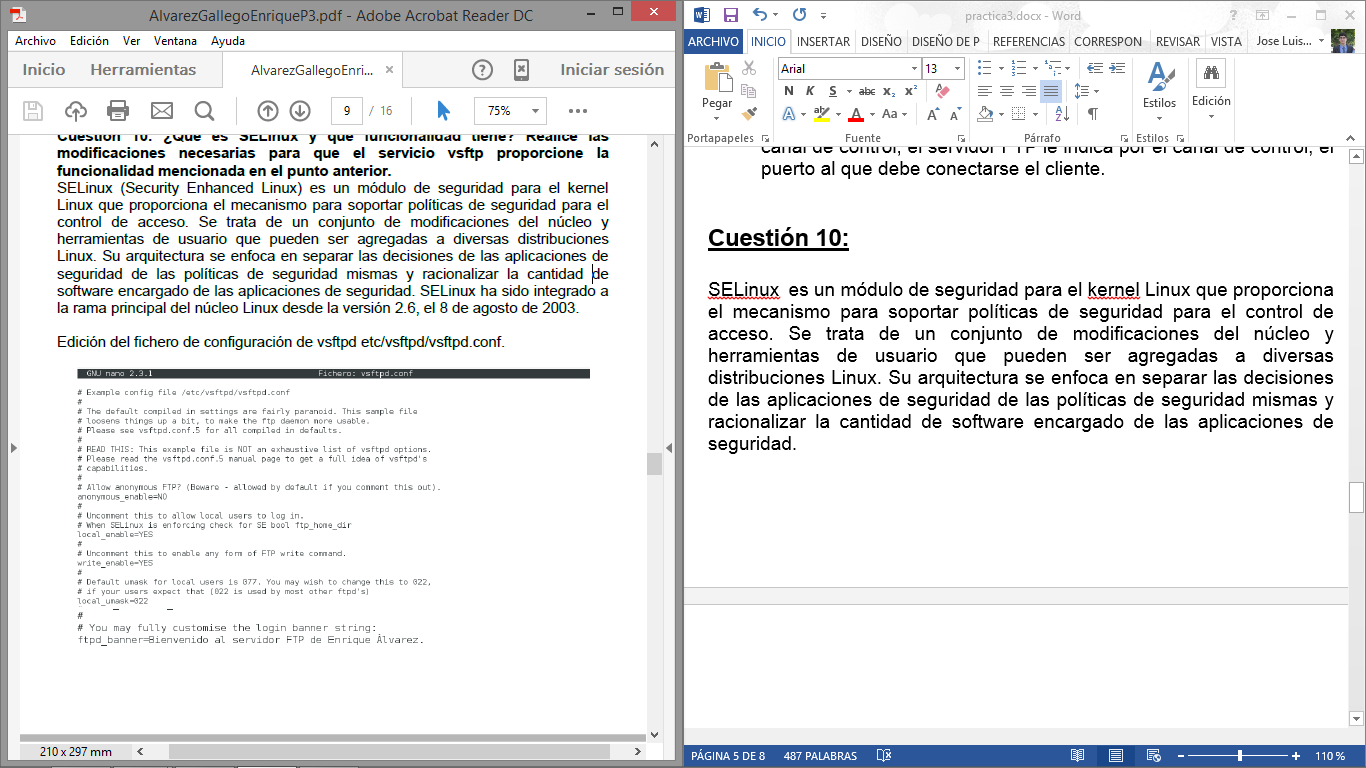
**Cuestión 9:**

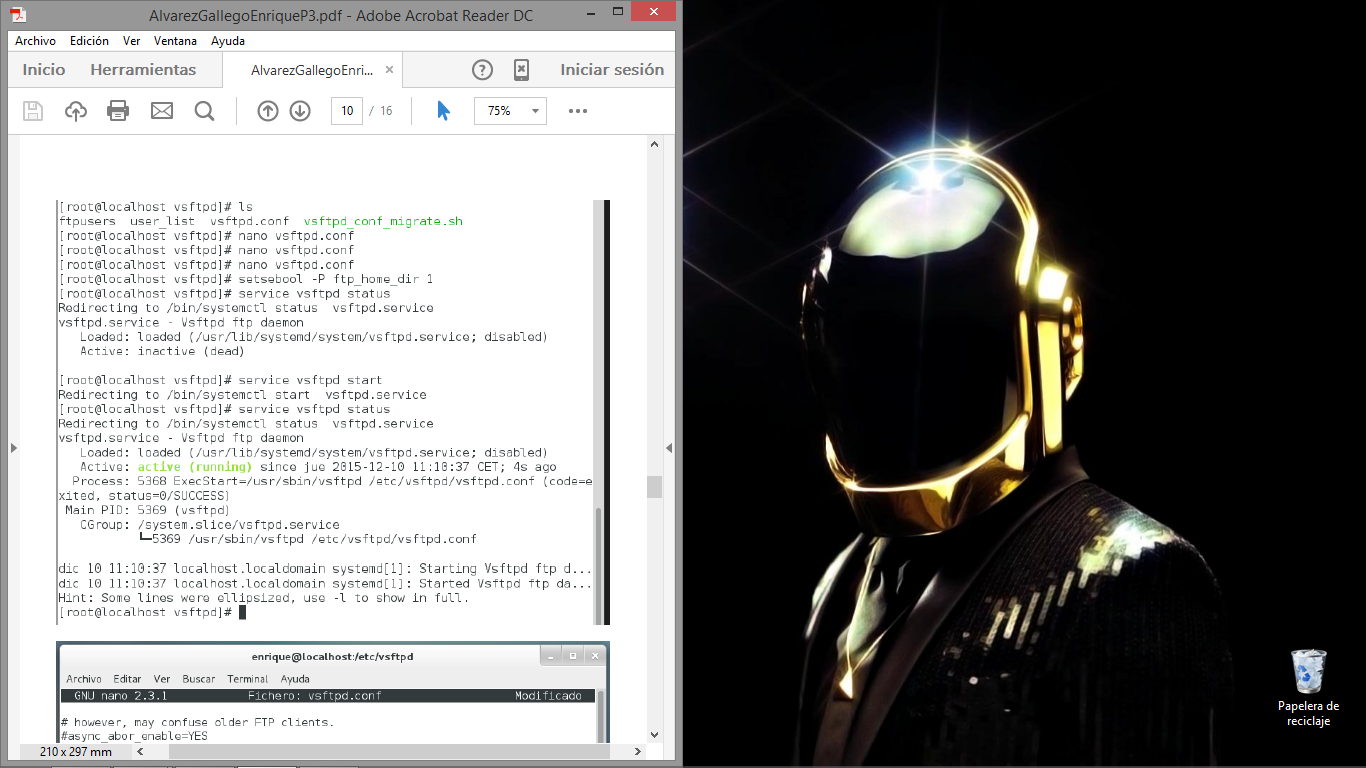
Existen dos modos:

* Modo activo: el servidor siempre crea el canal de datos en su puerto 20, mientras que en el lado del cliente el canal de datos se asocia a un puerto aleatorio mayor que el 1024.  Para ello, el cliente manda un comando PORT al servidor por el canal de control indicándole ese número de puerto, de manera que el servidor pueda abrirle una conexión de datos por donde se transferirán los archivos y los listados, en el puerto especificado.
* Modo pasivo: Cuando el cliente envía un comando PASV sobre el canal de control, el servidor FTP le indica por el canal de control, el puerto al que debe conectarse el cliente.

**Cuestión 10:**

SELinux  es un [módulo de seguridad](https://es.wikipedia.org/wiki/M%C3%B3dulo_de_n%C3%BAcleo#Seguridad) para el [kernel Linux](https://es.wikipedia.org/wiki/Linux_kernel) que proporciona el mecanismo para soportar políticas de seguridad para el control de acceso. Se trata de un conjunto de modificaciones del núcleo y herramientas de usuario que pueden ser agregadas a diversas distribuciones Linux. Su arquitectura se enfoca en separar las decisiones de las aplicaciones de seguridad de las políticas de seguridad mismas y racionalizar la cantidad de software encargado de las aplicaciones de seguridad.





**Cuestión 11:**

**Cuestión 12:**

**Cuestión 13:**

Otros 3 servidores comunes son:

* Cherokee
* Tomcat
* thttpd

**Cuestión 14:**

Accedemos al fichero de configuración del servidor apache “/etc/httpd/conf/httpd.conf” y escribimos:

Alias /practica3 “home/joselu/practica3”

Escribimos por terminal: “setsebool –P httpd\_read\_user\_content 1”. Damos permisos a los ficheros que contienen la web de apache y reiniciamos el servicio httpd con: “service httpd start” “service httpd stop” “service httpd restart”.

**Cuestión 15:**

Accedemos al fichero de configuración del servidor apache “/etc/apache2/apache2.conf” y escribimos:

DocumentRoot /practica2 “home/joselu/practica3”

Luego creamos nuestra propia entrada. Le damos permisos a los directorios que contengan la pagina web de apache e iniciamos el servido con “service apache2 start”

**Cuestión 16:**

**CentOS:**

* rmp –qi php

**Ubuntu:**

* dpkq –l | grep php

**Preguntas Breves:**

**Primera pregunta:**

¿Por qué es necesario reiniciar los servicios en los distintos sistemas operativos tras modificar los ficheros de configuración?

Porque los servicios funcionan a partir de un fichero de configuración. Si modificamos ese fichero, pero no reiniciamos el servicio, seguirá funcionando con respecto a fichero sin modificar. Una vez resteado el servicio coge el nuevo fichero de configuración.

**Segunda pregunta:**

¿Qué es y cuál es la función principal de un cortafuegos?

Un cortafuegos o firewall es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Los objetivos de un cortafuegos son permitir, limitar, cifrar y descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

**FUENTES:**

<http://blog.desdelinux.net/how-to-fedora-todo-lo-que-quisiste-saber-de-yum-y-no-te-atreviste-a-preguntar-parte-i/>

<https://mifedora.wordpress.com/2011/05/17/yum/>

<https://es.wikipedia.org/wiki/Puerto_de_red>

<http://www.openbsd.org/cgi-bin/man.cgi/OpenBSD-current/man1/slogin.1?query=ssh&sec=1>

<http://rm-rf.es/arrancar-parar-reiniciar-servicios-en-rhel-7-y-centos-7/>

<http://www.ubuntu-es.org/node/103287#.Vj47rLcve00>

<https://es.wikipedia.org/wiki/File_Transfer_Protocol>

<https://es.wikipedia.org/wiki/SELinux>

<https://es.wikipedia.org/wiki/Cortafuegos_(inform%C3%A1tica)>