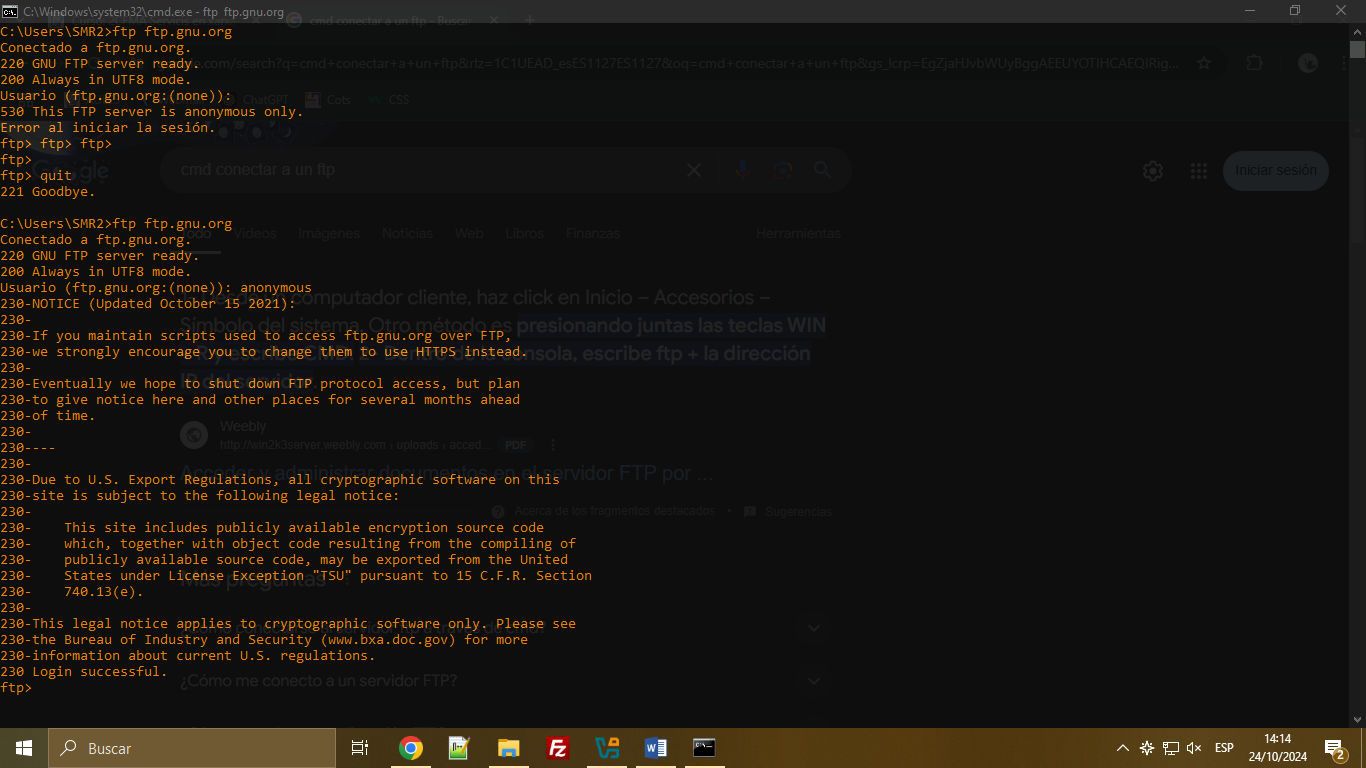
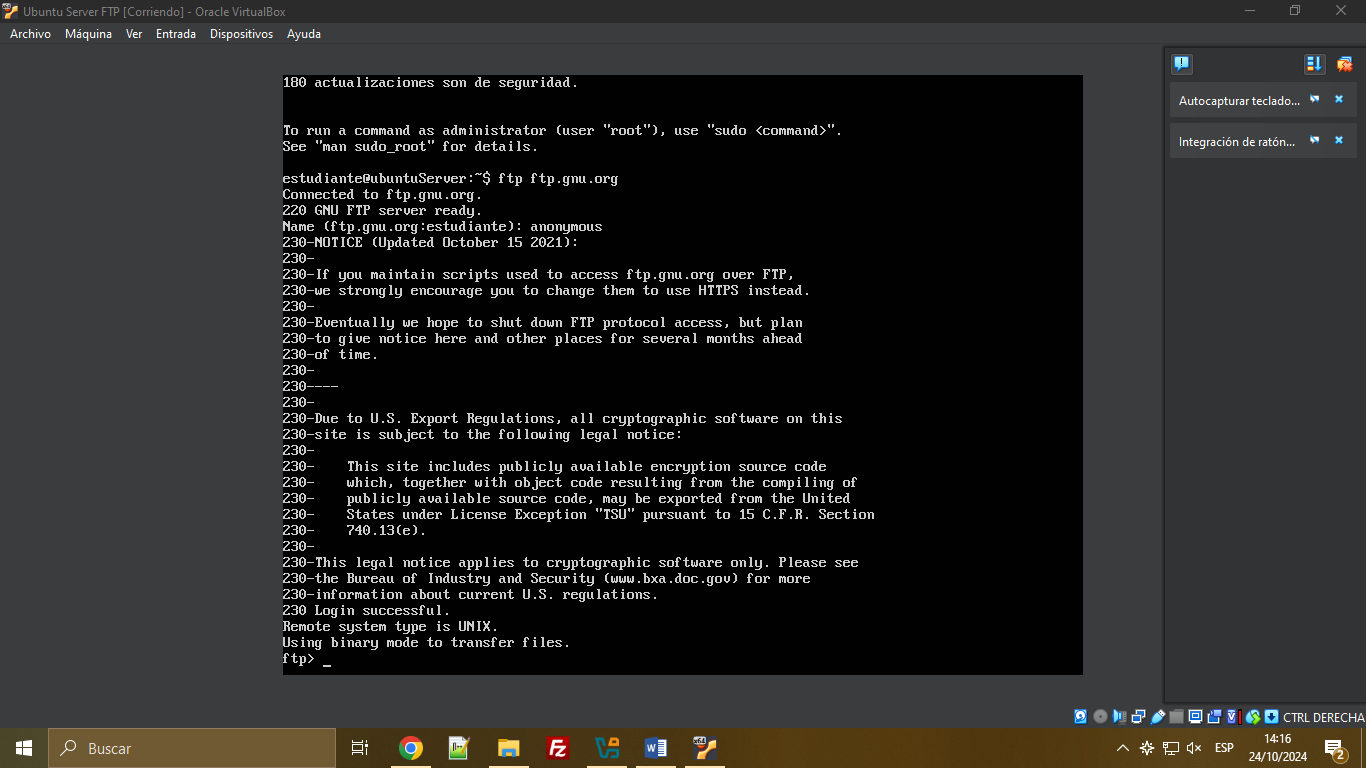
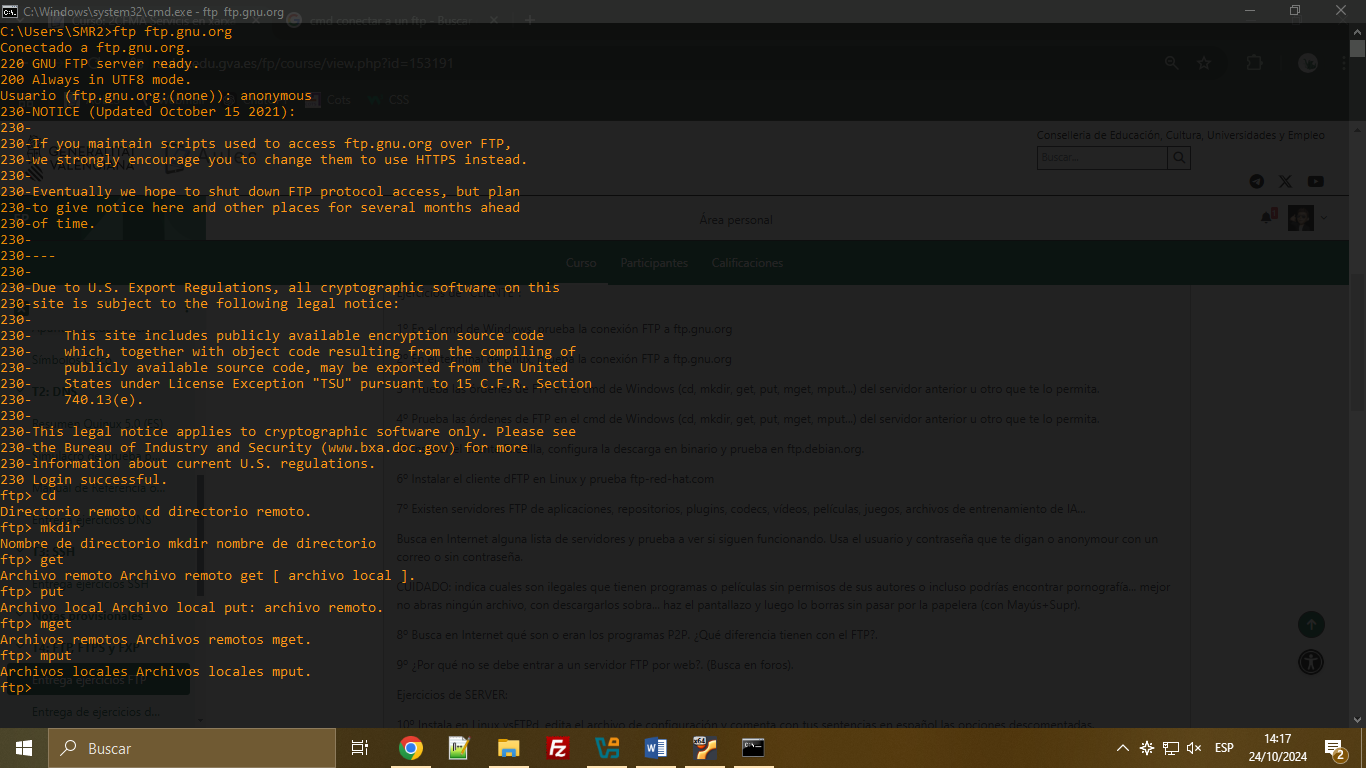
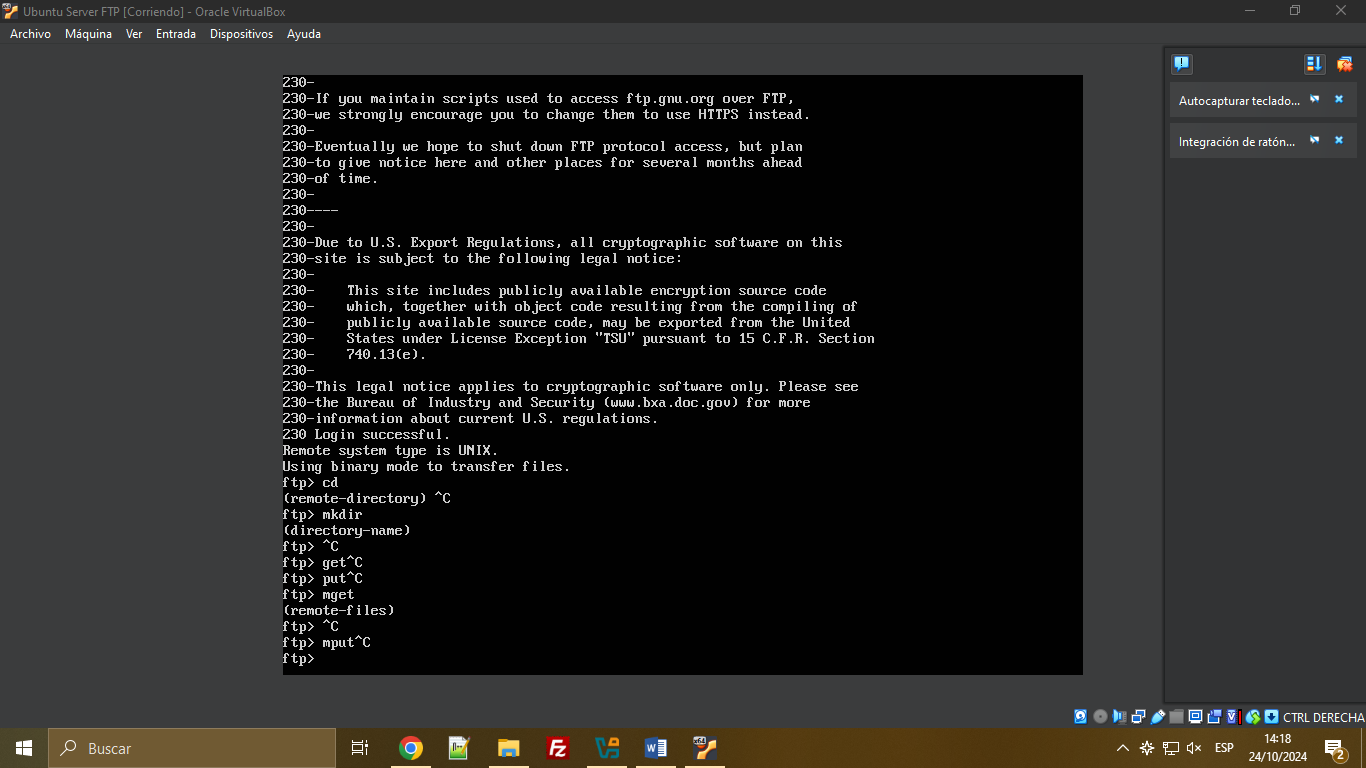
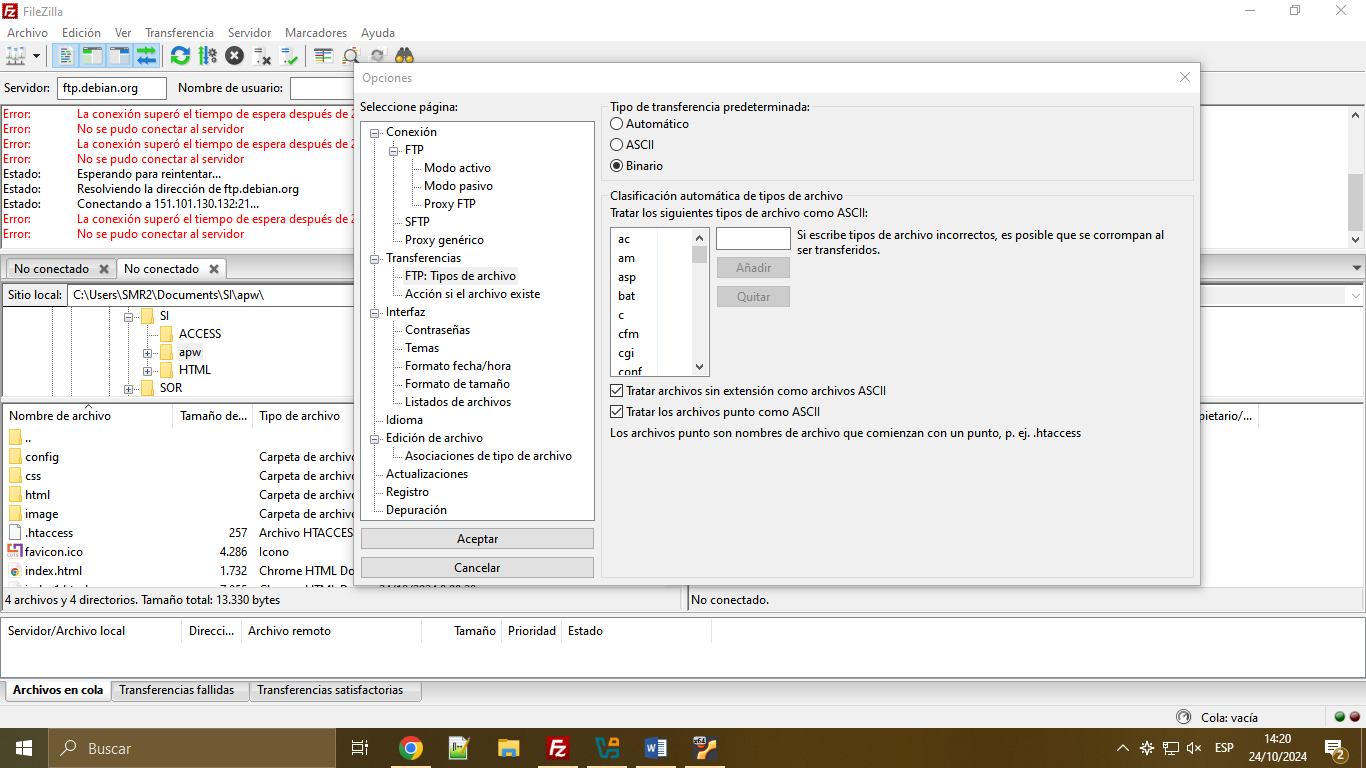
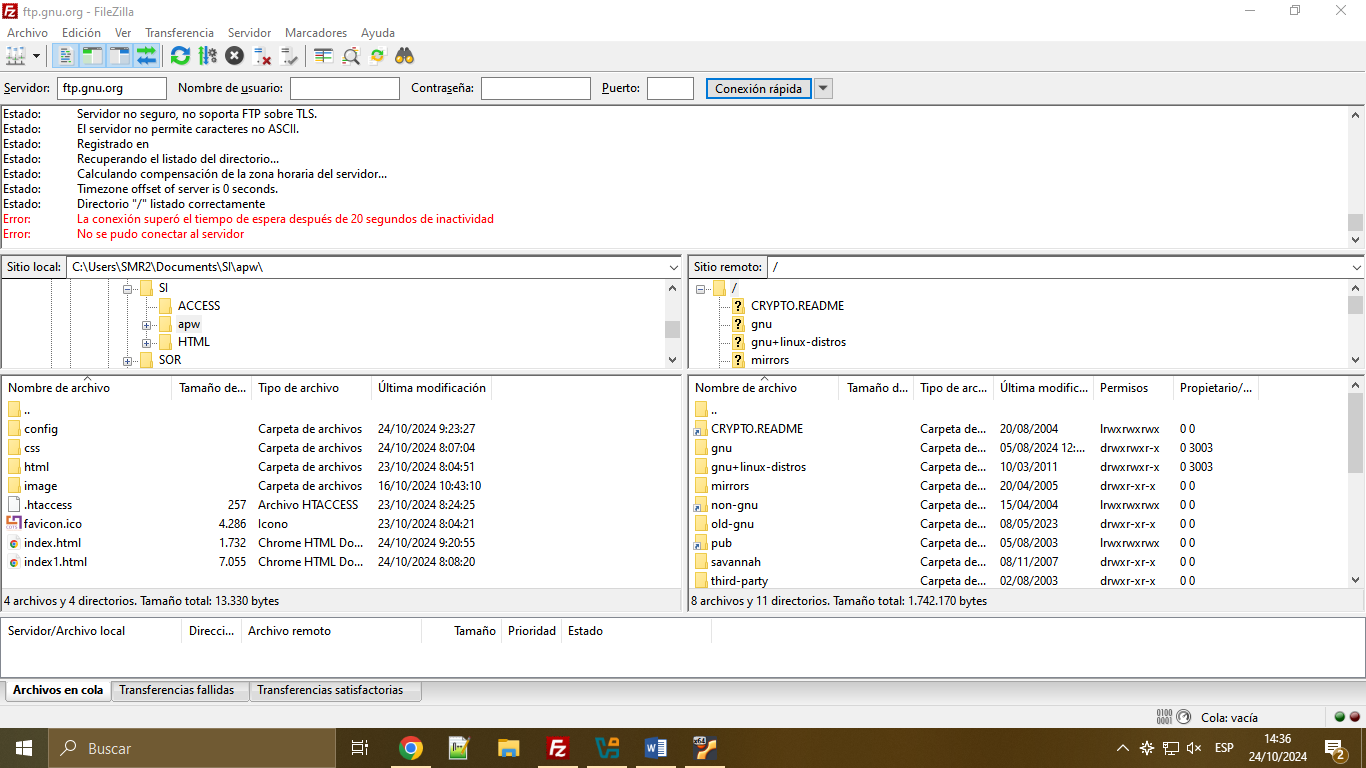
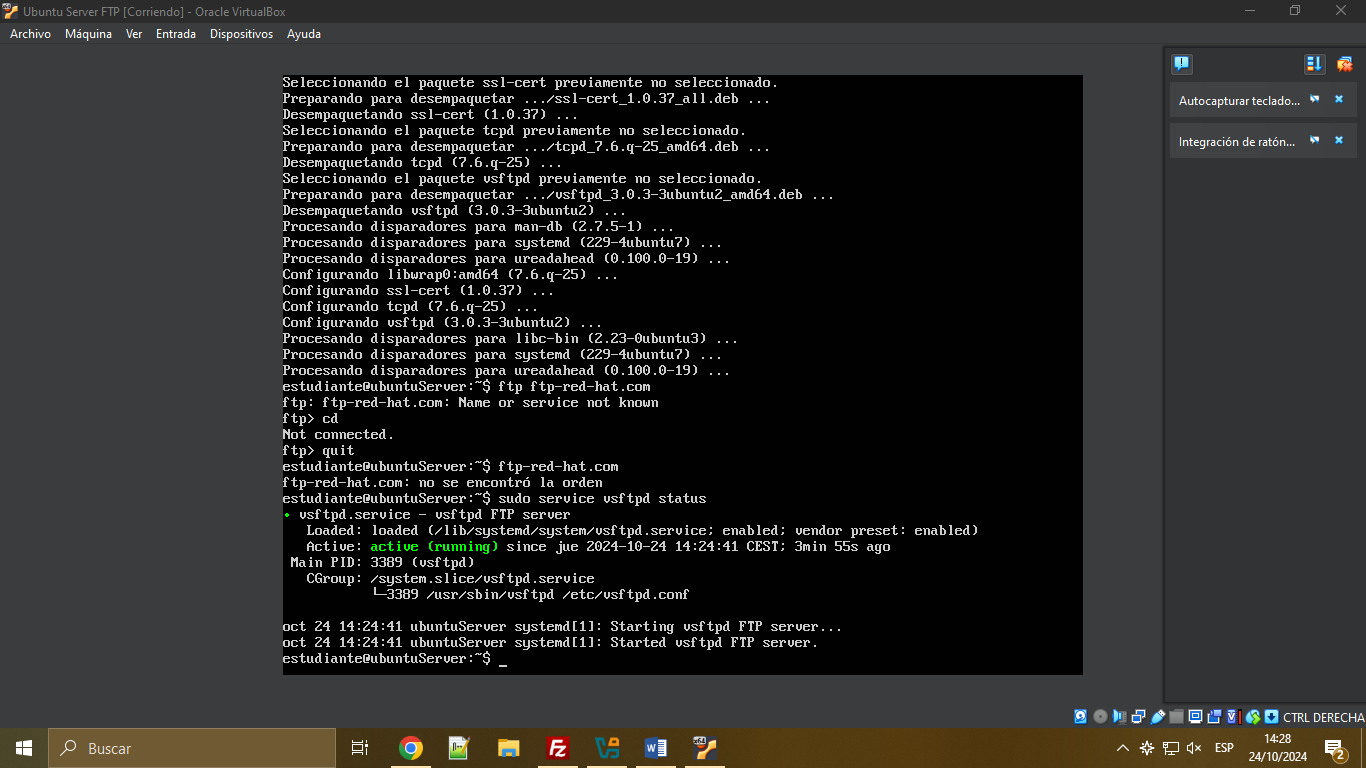
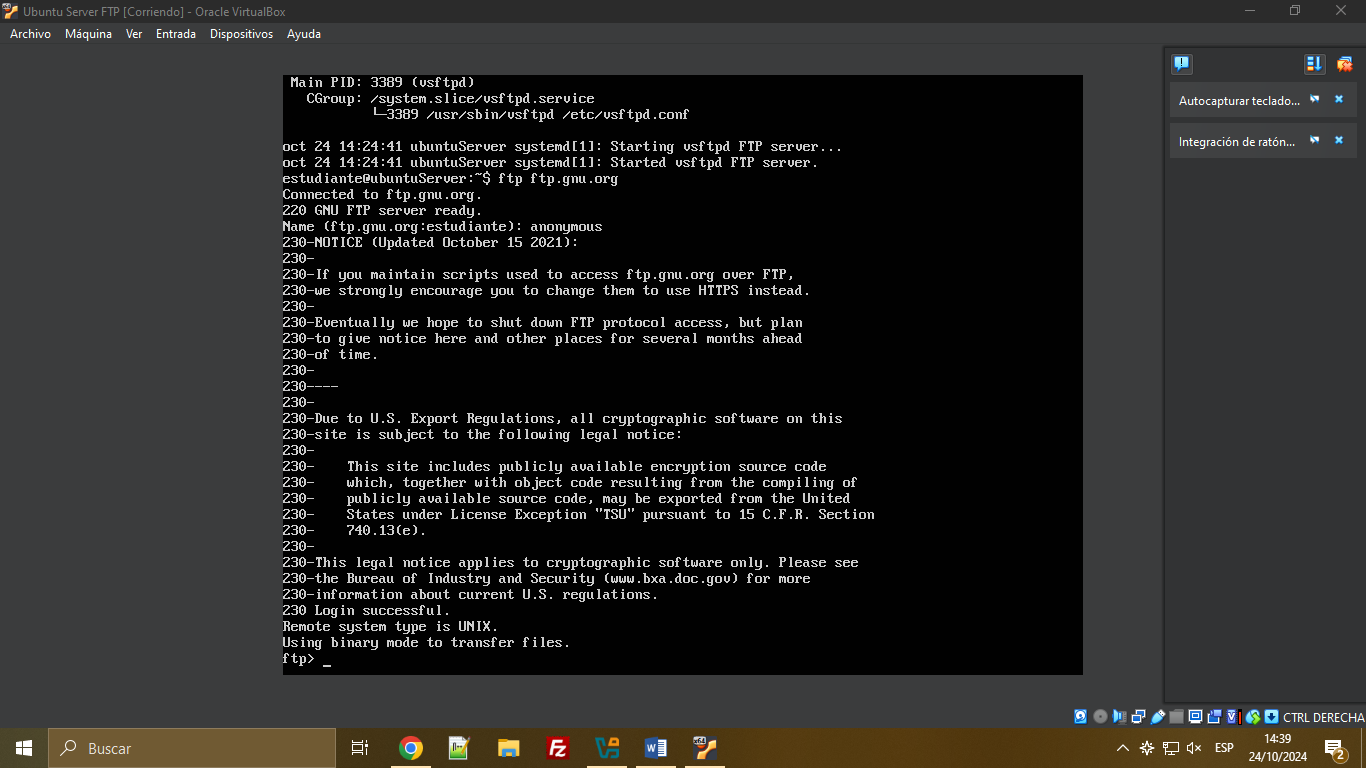
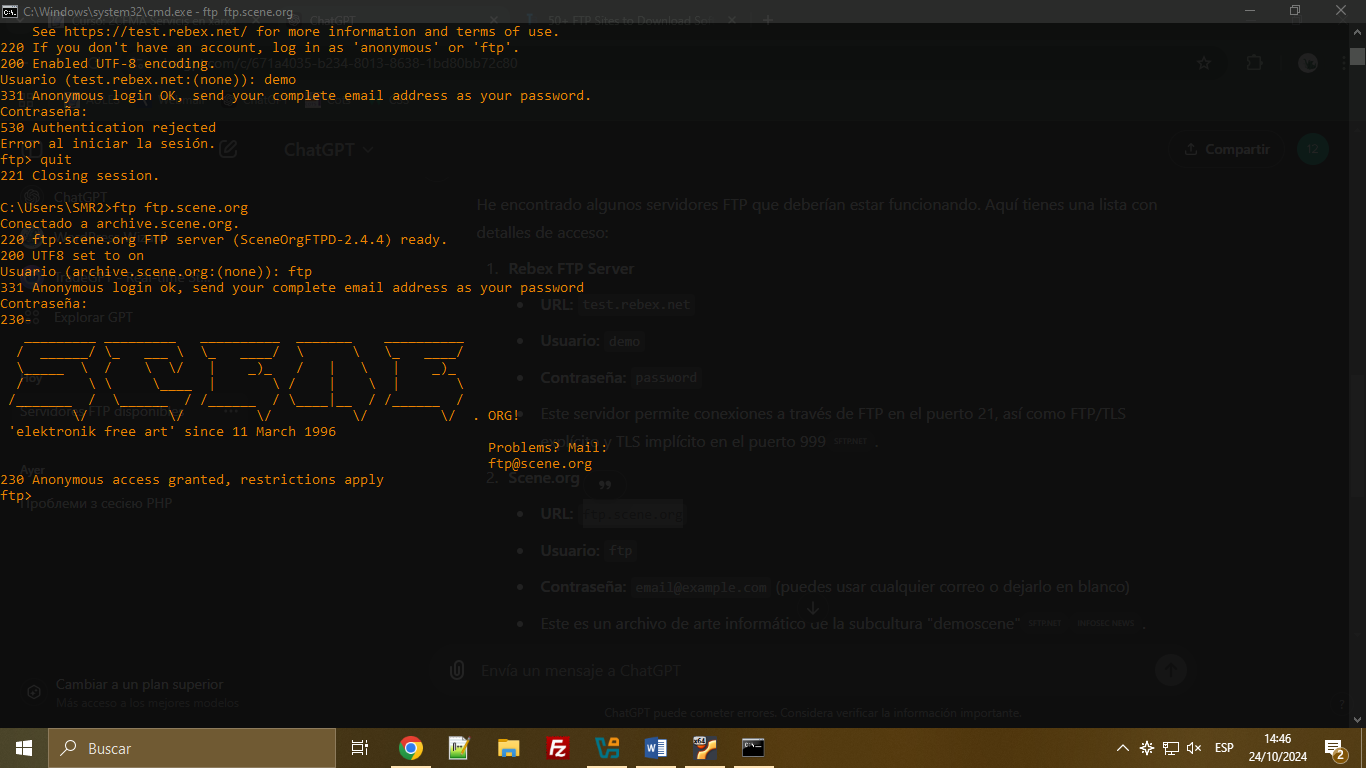
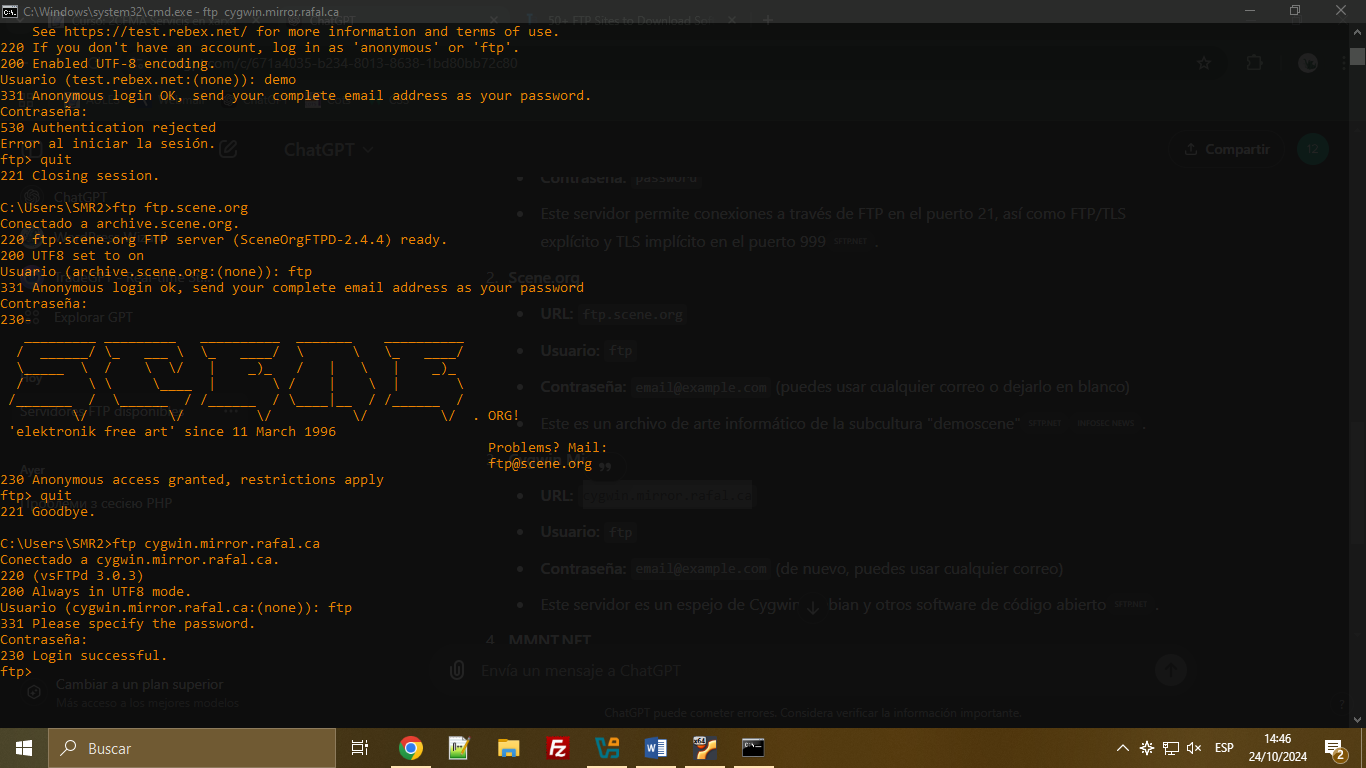
1. [ftp.gnu.org](ftp://ftp.gnu.org)
2. ftp.gnu.org 
3. ftp.gnu.org 
4. ftp.gnu.org 
5. FileZilla  ftp.gnu.org  
6. ftp.debian.org  
7. ftp.scene.org 

cygwin.mirror.rafal.ca 

1. P2P: No requiere un servidor central; los archivos se comparten directamente entre los usuarios.

FTP: Se basa en un modelo cliente-servidor, donde los archivos se almacenan en un servidor central al que los clientes se conectan para descargar o subir archivos.

1. Las conexiones FTP tradicionales no están encriptadas, lo que significa que los datos, incluyendo credenciales de inicio de sesión, se transmiten en texto plano. Esto puede ser interceptado por atacantes.
2. **listen=NO**: Esta opción desactiva el modo de escucha en IPv4. Esto significa que el servidor no escuchará conexiones FTP en direcciones IPv4. En su lugar, se utilizará listen\_ipv6.

**listen\_ipv6=YES**: Habilita el modo de escucha en IPv6, permitiendo que el servidor acepte conexiones FTP a través de direcciones IPv6.

**anonymous\_enable=NO**: Desactiva el acceso anónimo al servidor FTP, lo que significa que solo los usuarios registrados podrán iniciar sesión.

**local\_enable=YES**: Permite que los usuarios locales del sistema (es decir, aquellos que tienen cuentas en la máquina) inicien sesión en el servidor FTP.

**dirmessage\_enable=YES**: Habilita los mensajes de directorio. Esto muestra un mensaje personalizado a los usuarios cuando cambian a un nuevo directorio en el servidor FTP, si existe un archivo llamado .message en ese directorio.

**use\_localtime=YES**: Configura el servidor FTP para que use la hora local del sistema en lugar de la hora UTC. Esto es útil para asegurarse de que las marcas de tiempo de los archivos sean consistentes con la zona horaria local.

**xferlog\_enable=YES**: Habilita el registro de todas las transferencias de archivos realizadas a través del servidor FTP. Este registro se guarda en un archivo de log para auditorías y monitoreo.

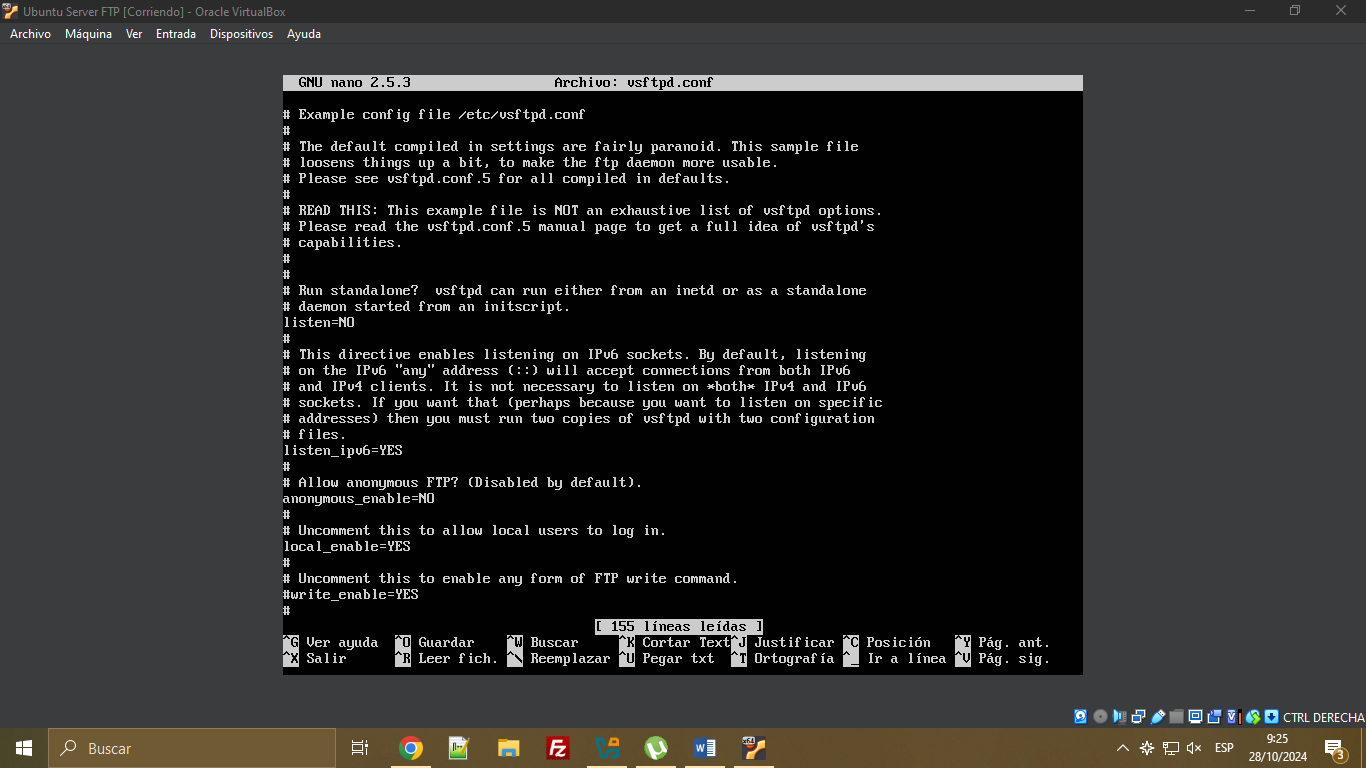
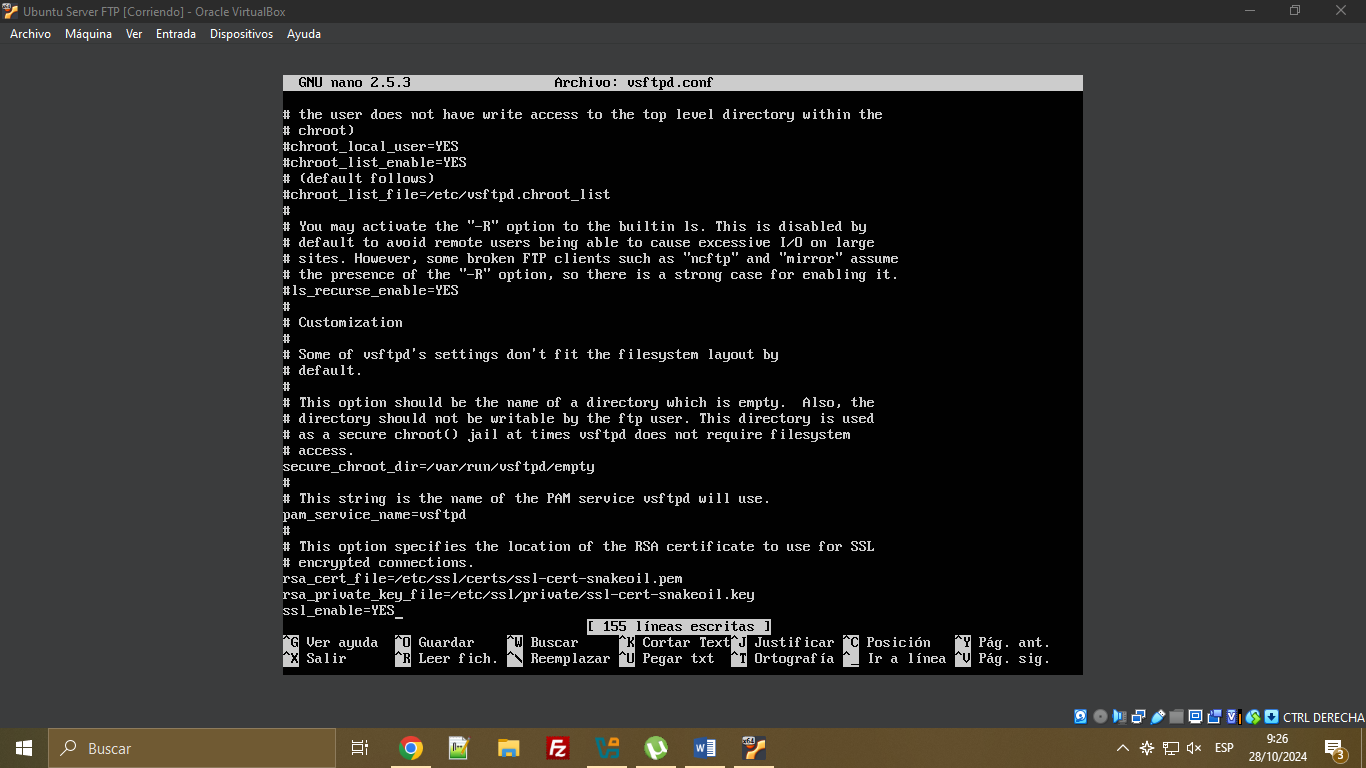
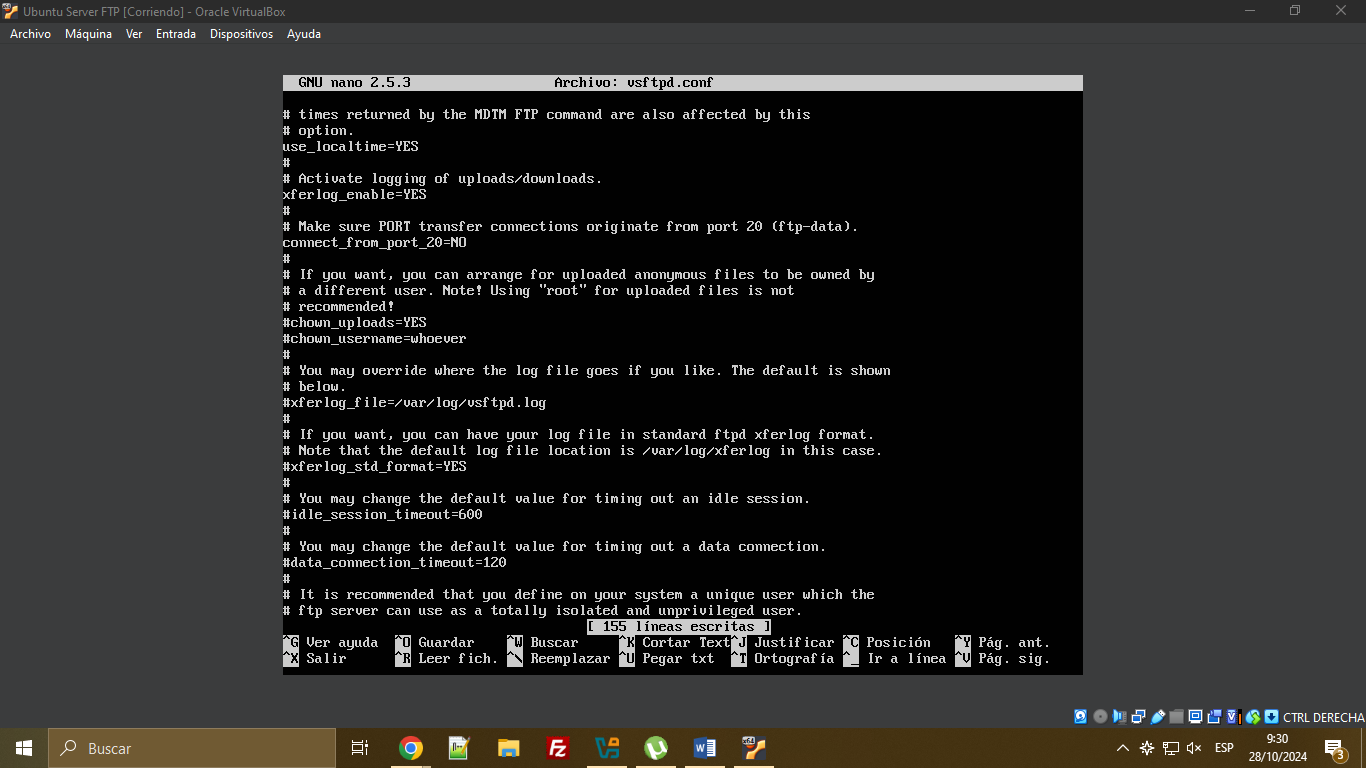
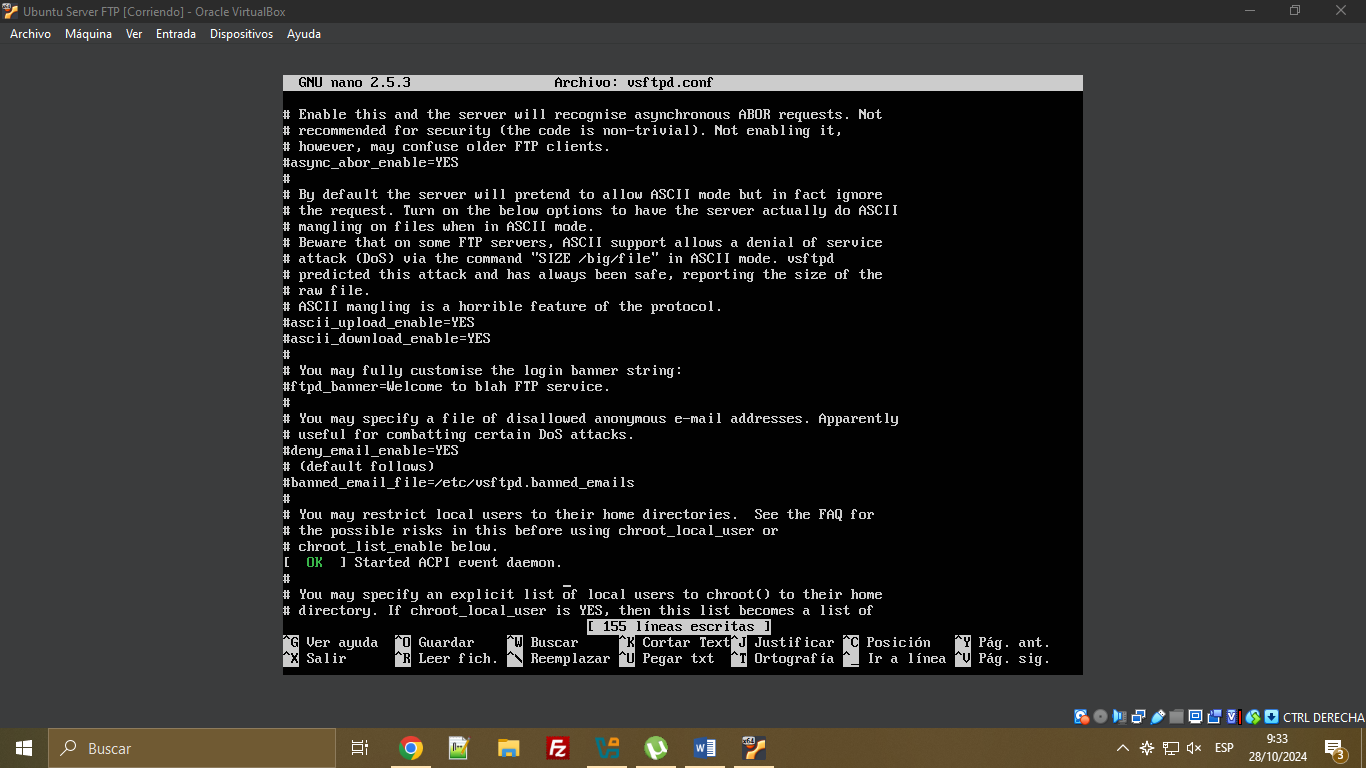
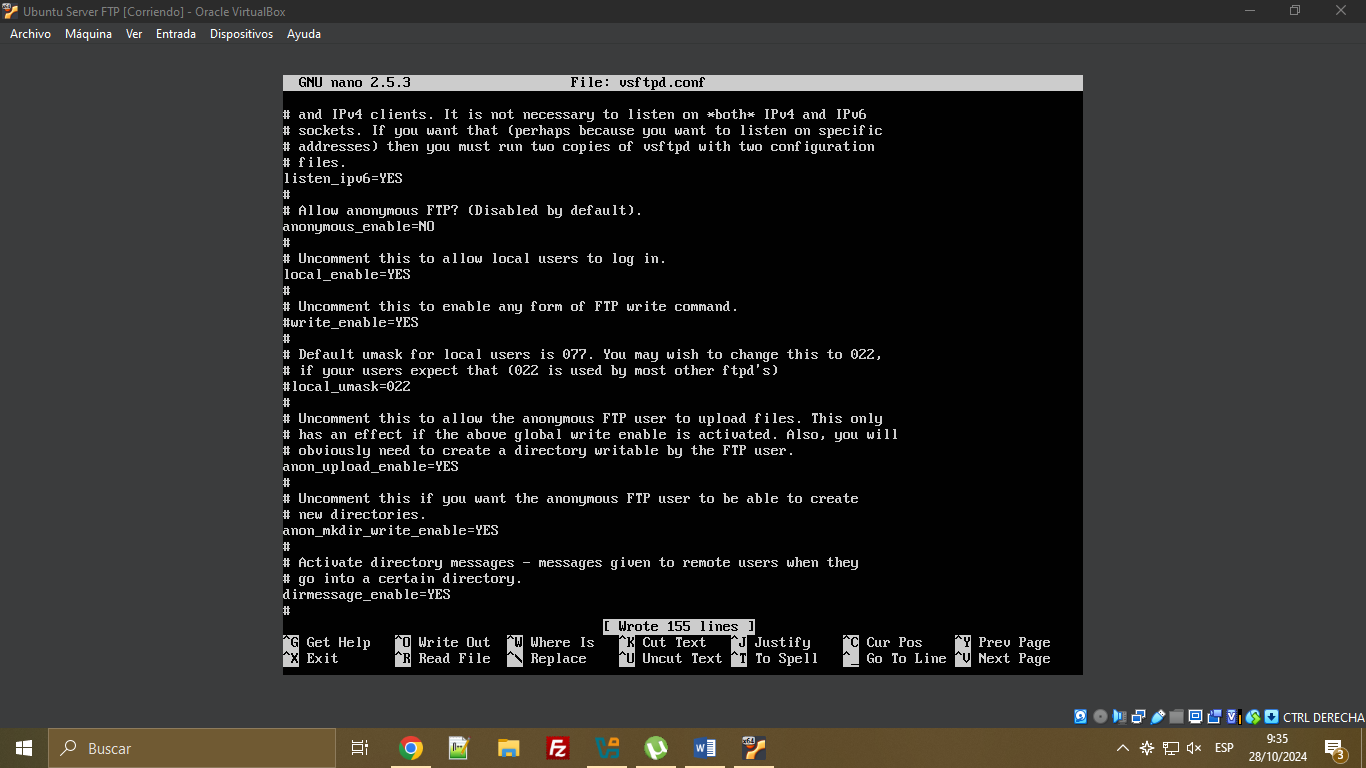
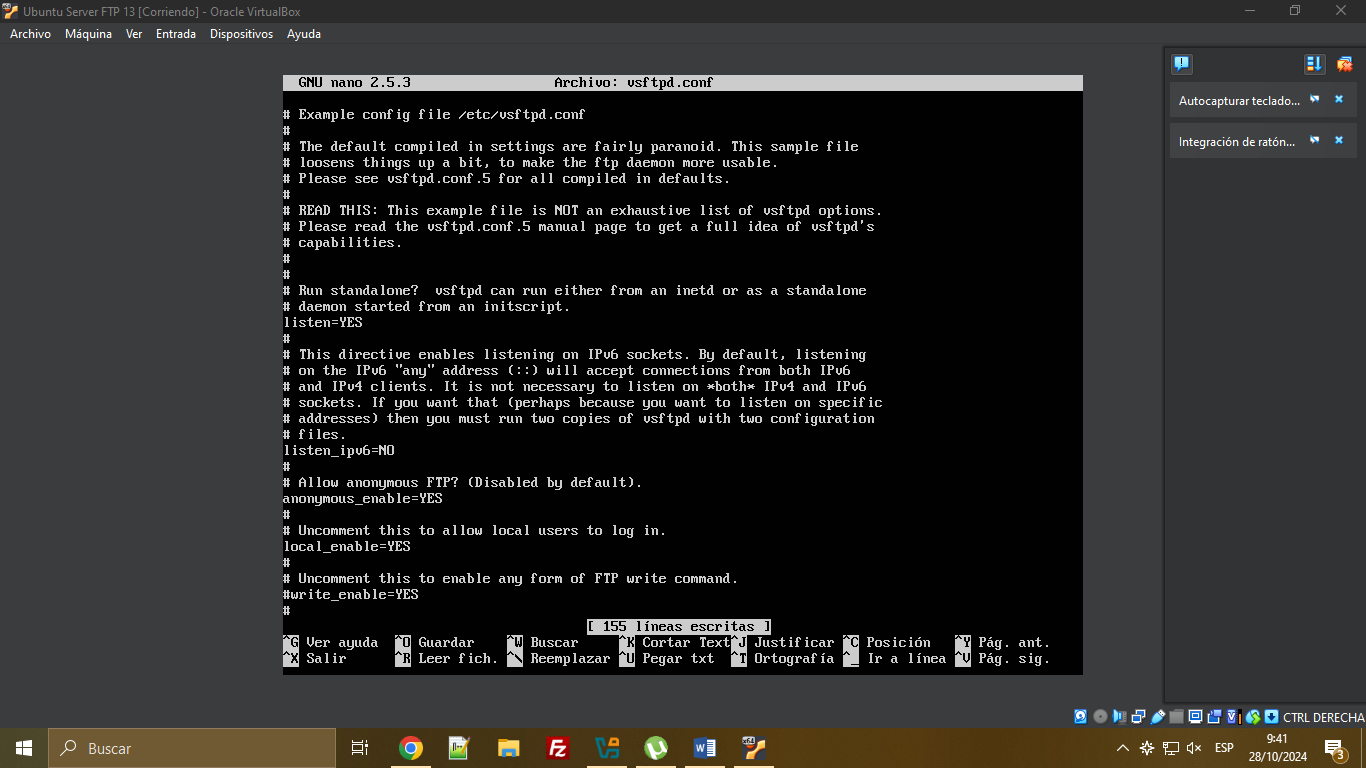
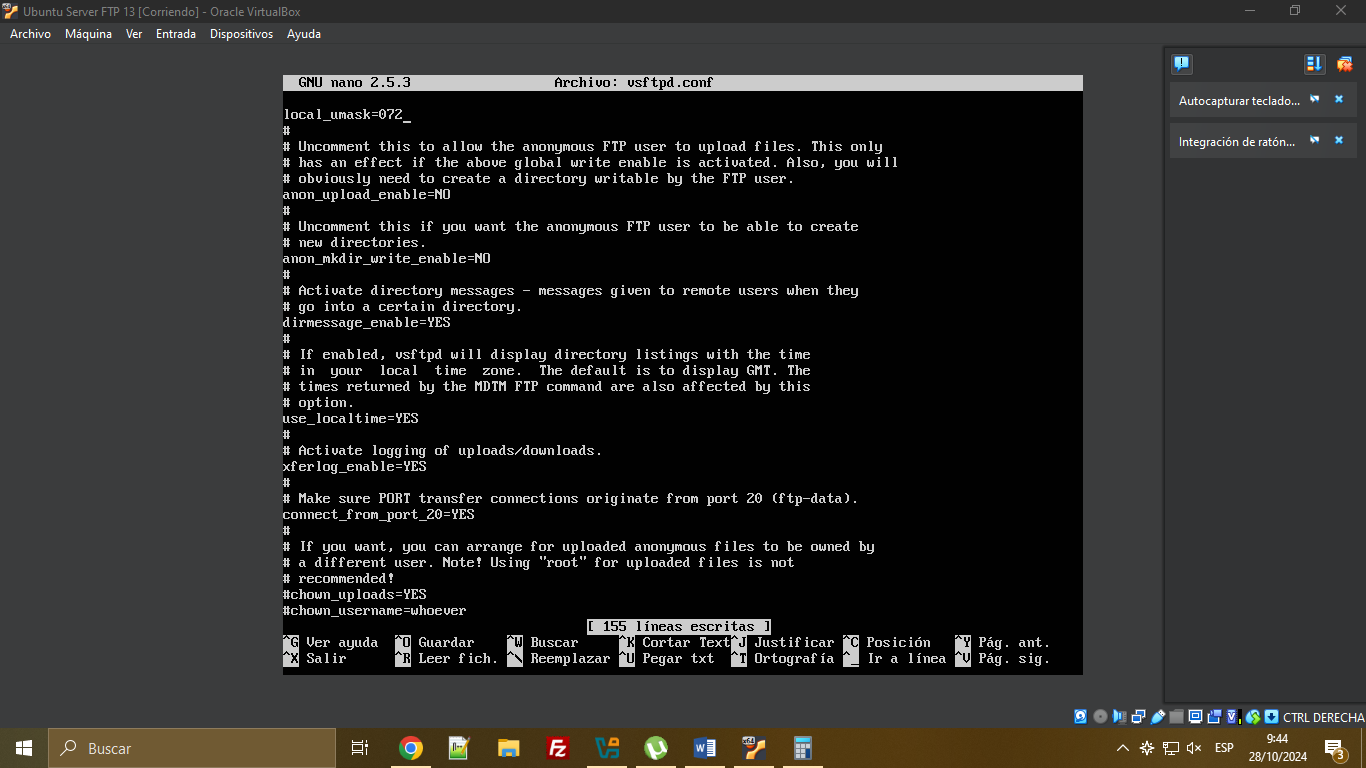
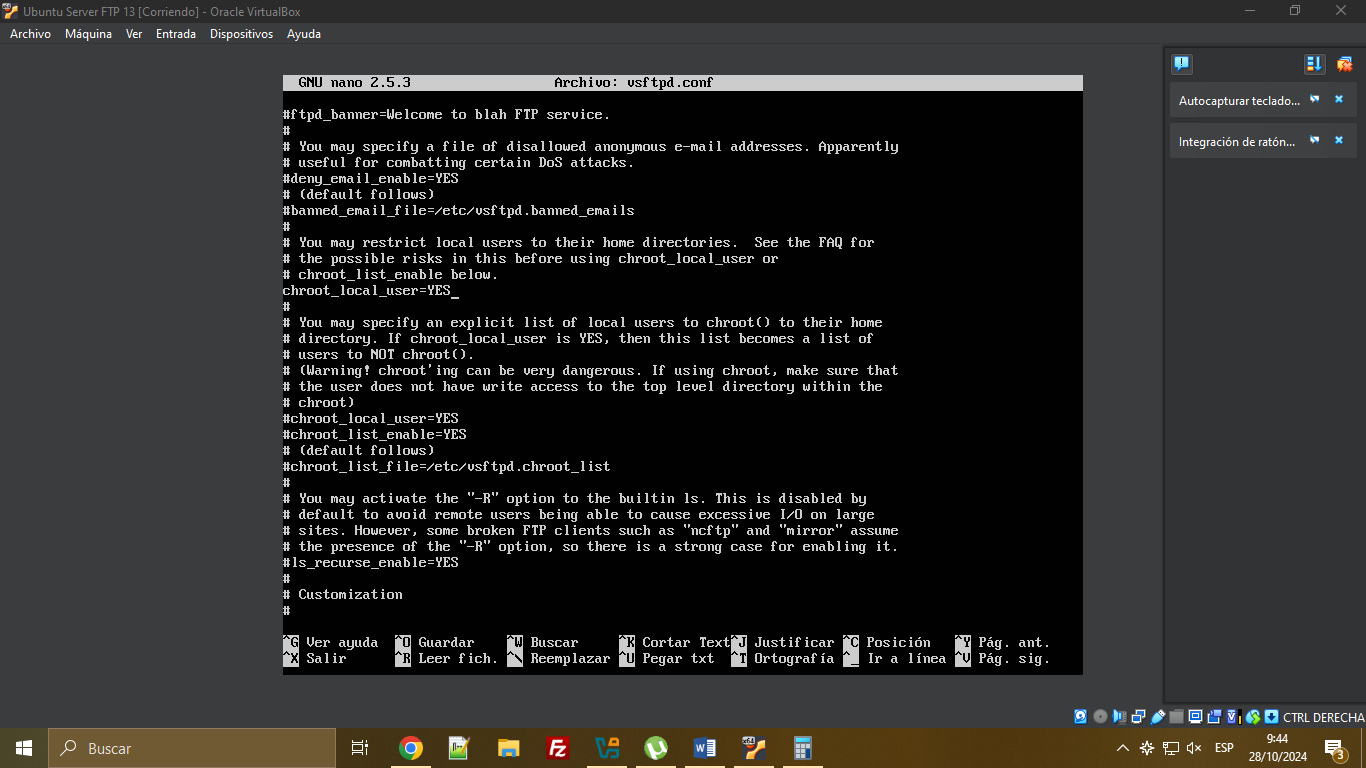
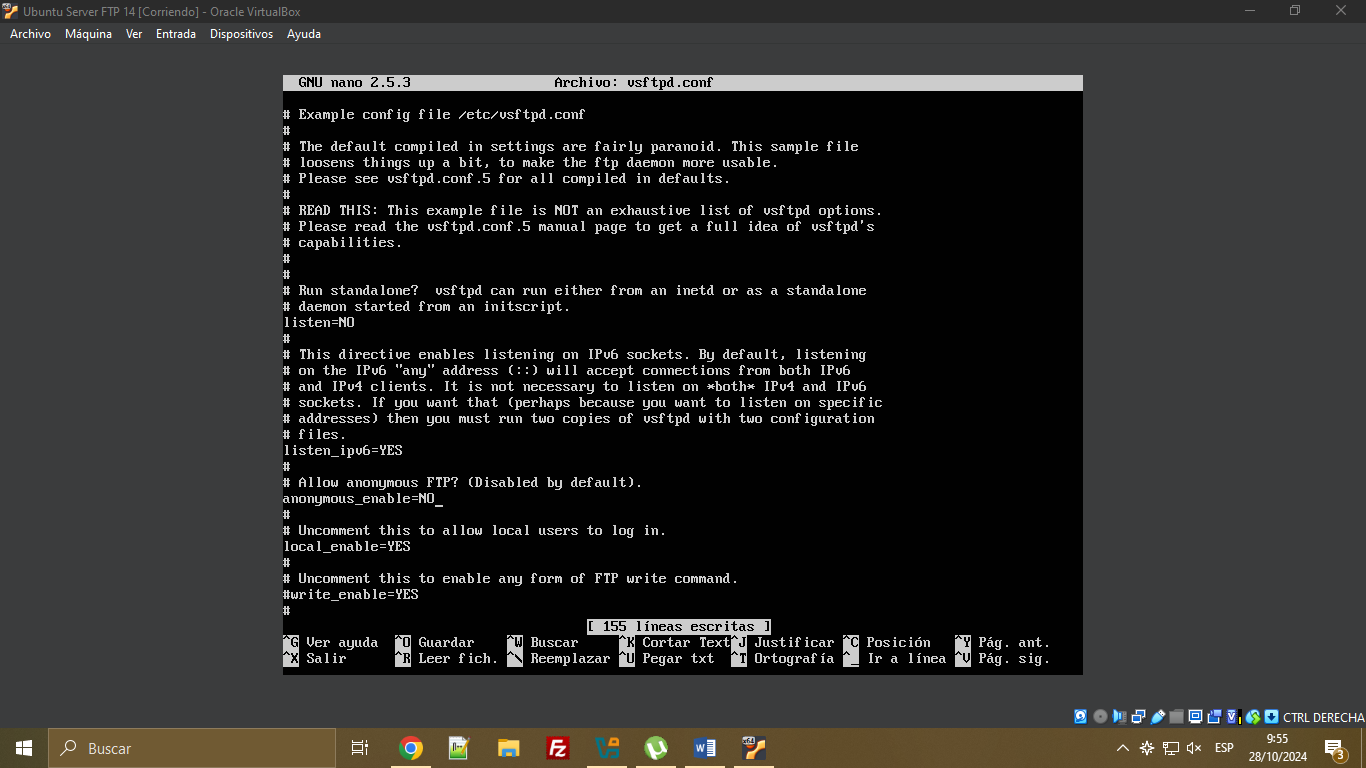
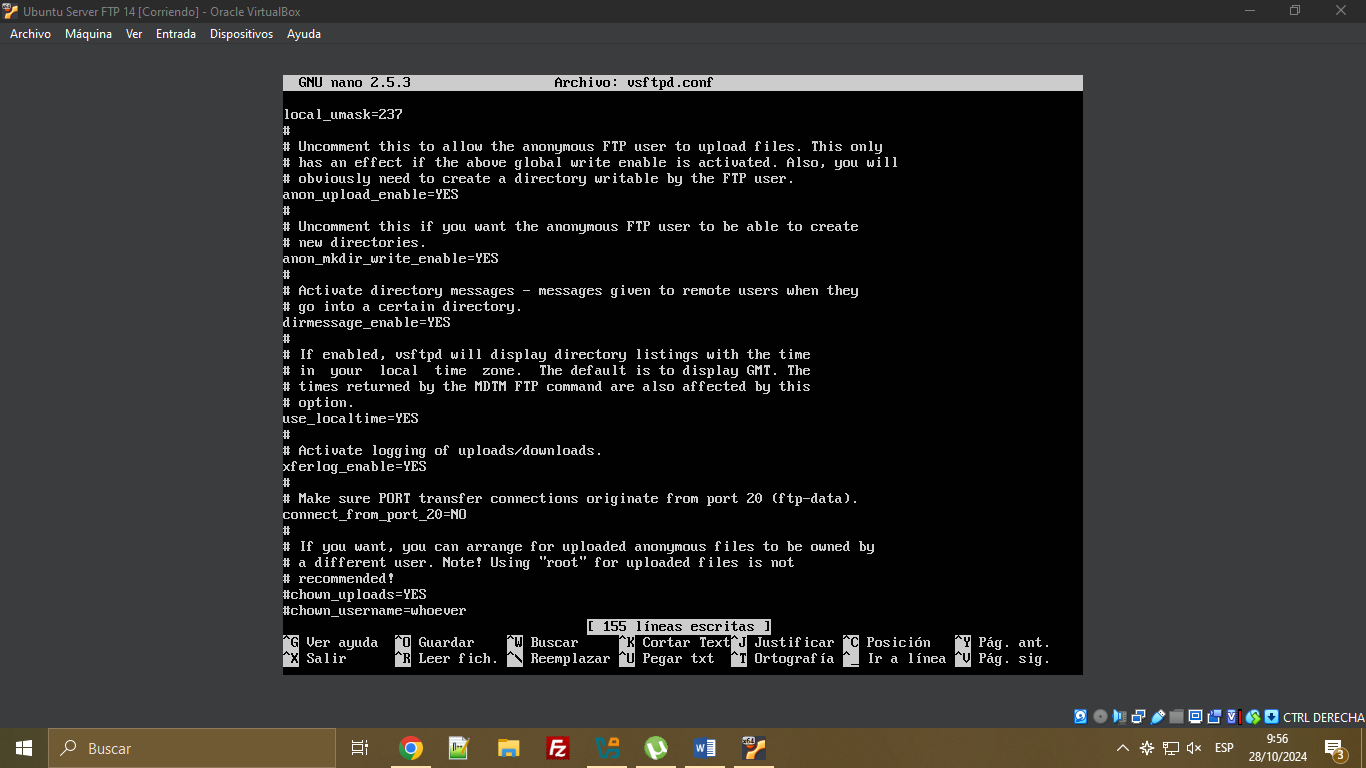
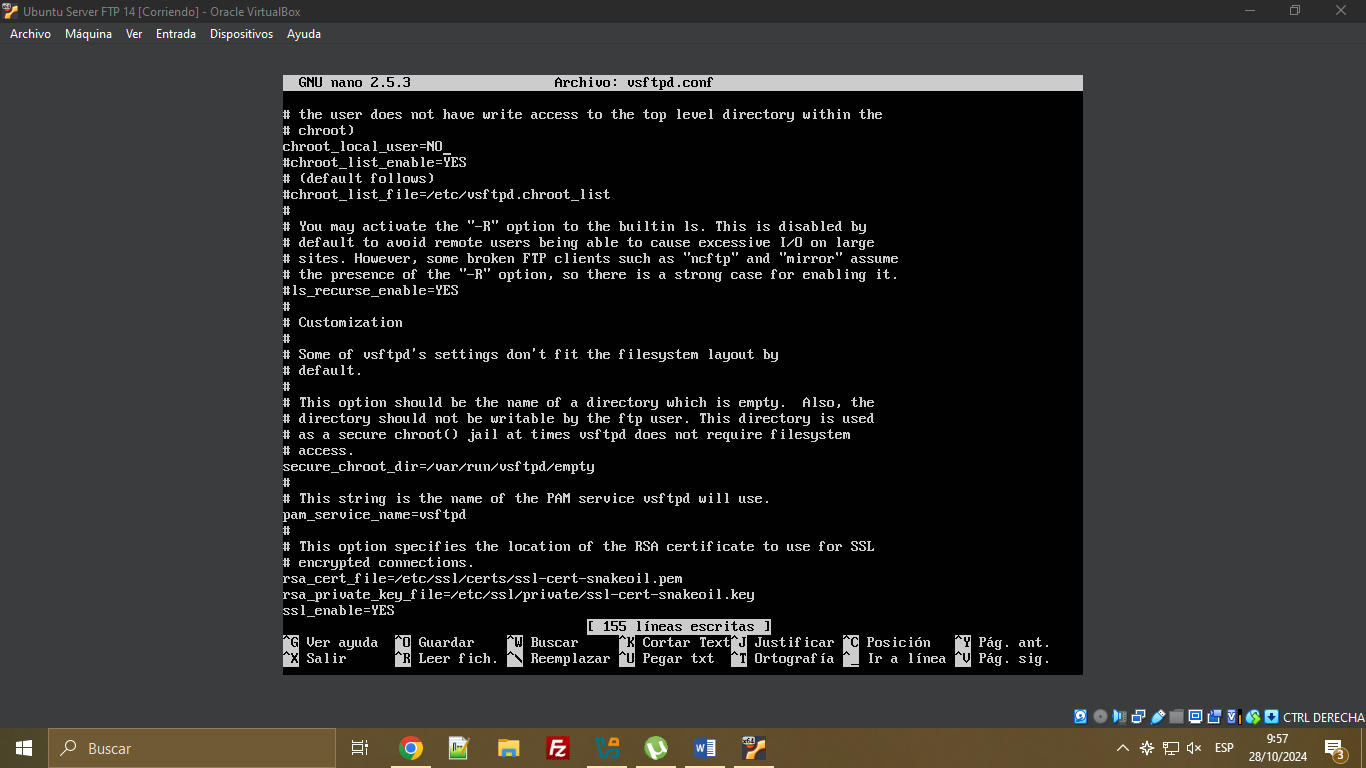
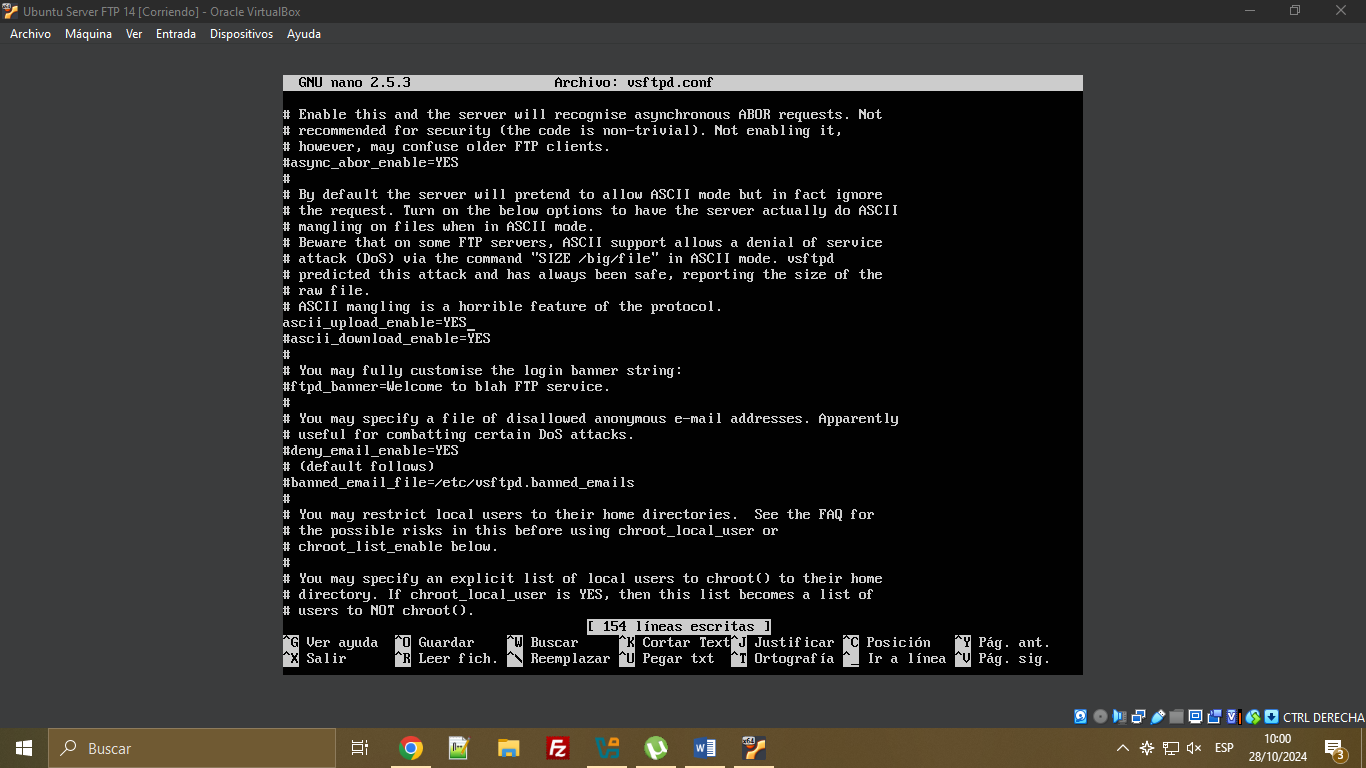
**connect\_from\_port\_20=YES**: Fuerza al servidor a usar el puerto 20 para las conexiones de datos FTP activas. Esto es parte del protocolo FTP estándar para mantener la compatibilidad.

**secure\_chroot\_dir=/var/run/vsftpd/empty**: Especifica un directorio seguro de "chroot" que el servidor utilizará para proteger el entorno del servidor FTP. El "chroot" restringe el acceso de los usuarios a un directorio específico, evitando que naveguen fuera de sus directorios asignados.

**rsa\_cert\_file=/etc/ssl/certs/ssl-cert-snakeoil.pem**: Indica la ruta al archivo del certificado RSA que se utilizará para conexiones SSL/TLS en el servidor FTP.

**rsa\_private\_key\_file=/etc/ssl/private/ssl-cert-snakeoil.key**: Indica la ruta al archivo de la clave privada RSA asociada con el certificado SSL/TLS.

**ssl\_enable=NO:** Desactiva el soporte SSL/TLS en el servidor FTP, lo que significa que todas las conexiones FTP serán no cifradas. Si se cambia a YES, se habilitaría el cifrado para conexiones seguras.

1. FTP Seguro    
2. Permisos para anonymous 
3. Servidor FTP   
4. Servidor FTP 2    
5. Optativo Configurar un servidor FTP