



**UNIVERSIDAD AUTÓNOMA DE
CHIAPAS**



**LICENCIATURA EN INGENIERIA EN
DESARROLLO DE TECNOLOGIAS DE SOFTWARE**

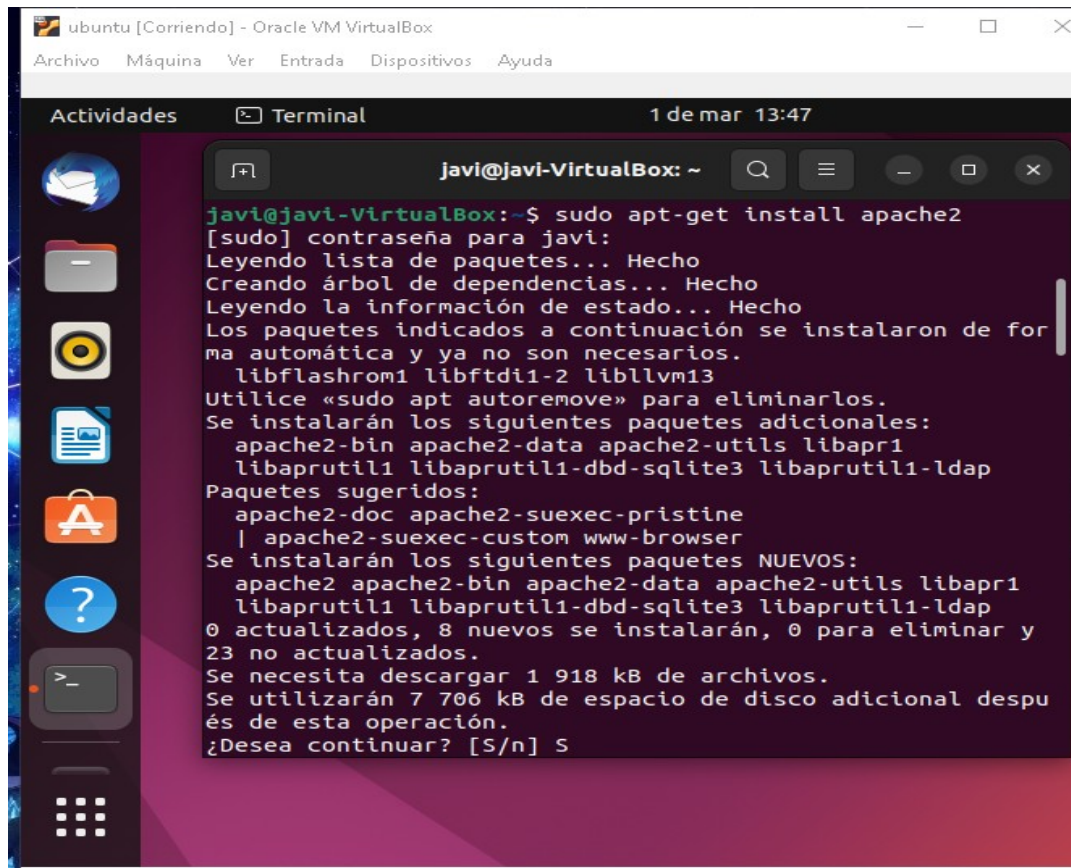
Unidad académica: Análisis de Vulnerabilidades

**Actividad: Proteger el servidor Web contra ataques DoS e instalar
el https con certificado**

Grado: 7 Grupo: M

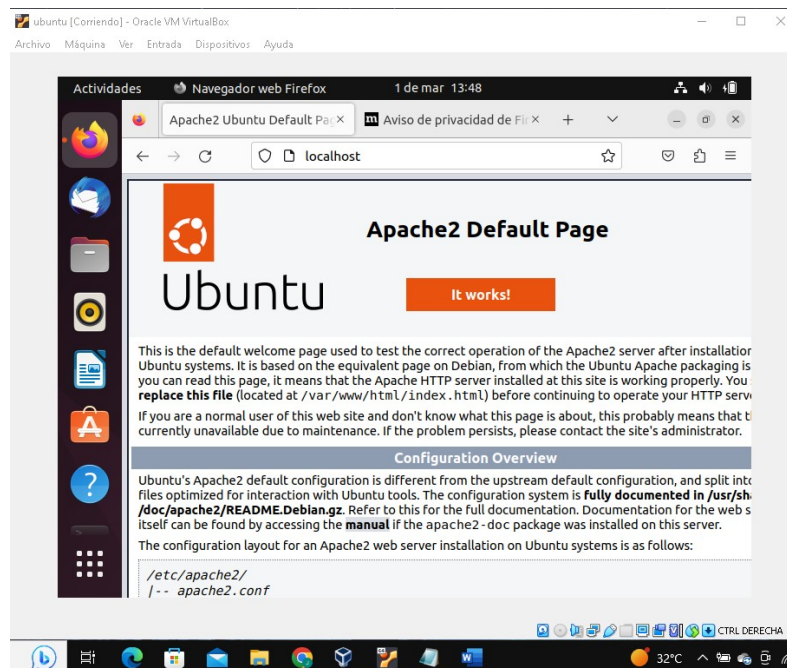
Alumno: Abel Alejandro Jimenez Camacho

1.- Activando el servidor apache sin el certificado ssl

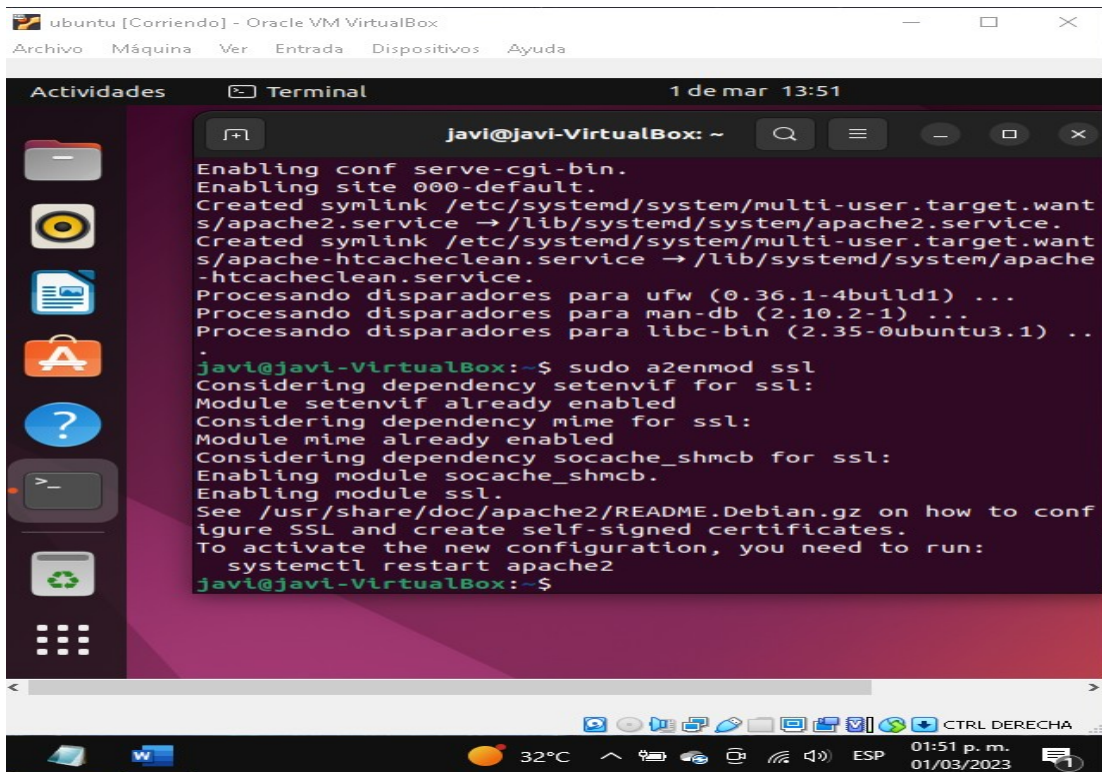


```
javi@javi-VirtualBox: ~  
javi@javi-VirtualBox:~$ sudo apt-get install apache2  
[sudo] contraseña para javi:  
Leyendo lista de paquetes... Hecho  
Creando árbol de dependencias... Hecho  
Leyendo la información de estado... Hecho  
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.  
libflashrom1 libftdi1-2 liblvm13  
Utilice «sudo apt autoremove» para eliminarlos.  
Se instalarán los siguientes paquetes adicionales:  
apache2-bin apache2-data apache2-utils libapr1  
libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap  
Paquetes sugeridos:  
apache2-doc apache2-suexec-pristine  
| apache2-suexec-custom www-browser  
Se instalarán los siguientes paquetes NUEVOS:  
apache2 apache2-bin apache2-data apache2-utils libapr1  
libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap  
0 actualizados, 8 nuevos se instalarán, 0 para eliminar y  
23 no actualizados.  
Se necesita descargar 1 918 kB de archivos.  
Se utilizarán 7 706 kB de espacio de disco adicional después de esta operación.  
¿Desea continuar? [S/n] S
```

Mostrando el servidor activo, pero sin el certificado.



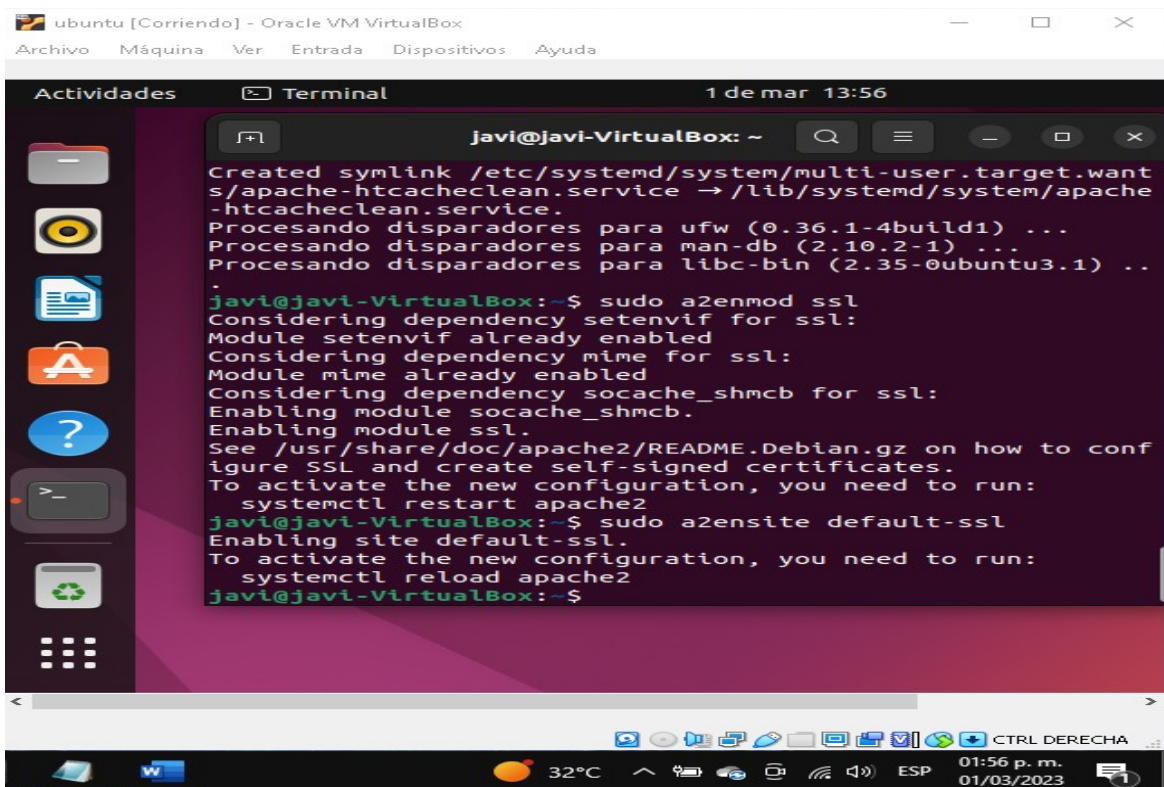
2.-Activando un módulo de ssl



The screenshot shows a terminal window titled 'javi@javi-VirtualBox: ~' with the following output:

```
Enabling conf serve-cgi-bin.
Enabling site 000-default.
Created symlink /etc/systemd/system/multi-user.target.wants/apache2.service → /lib/systemd/system/apache2.service.
Created symlink /etc/systemd/system/multi-user.target.wants/apache-htcacheclean.service → /lib/systemd/system/apache-htcacheclean.service.
Procesando disparadores para ufw (0.36.1-4build1) ...
Procesando disparadores para man-db (2.10.2-1) ...
Procesando disparadores para libc-bin (2.35-0ubuntu3.1) ..
.
javi@javi-VirtualBox:~$ sudo a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
    systemctl restart apache2
javi@javi-VirtualBox:~$
```

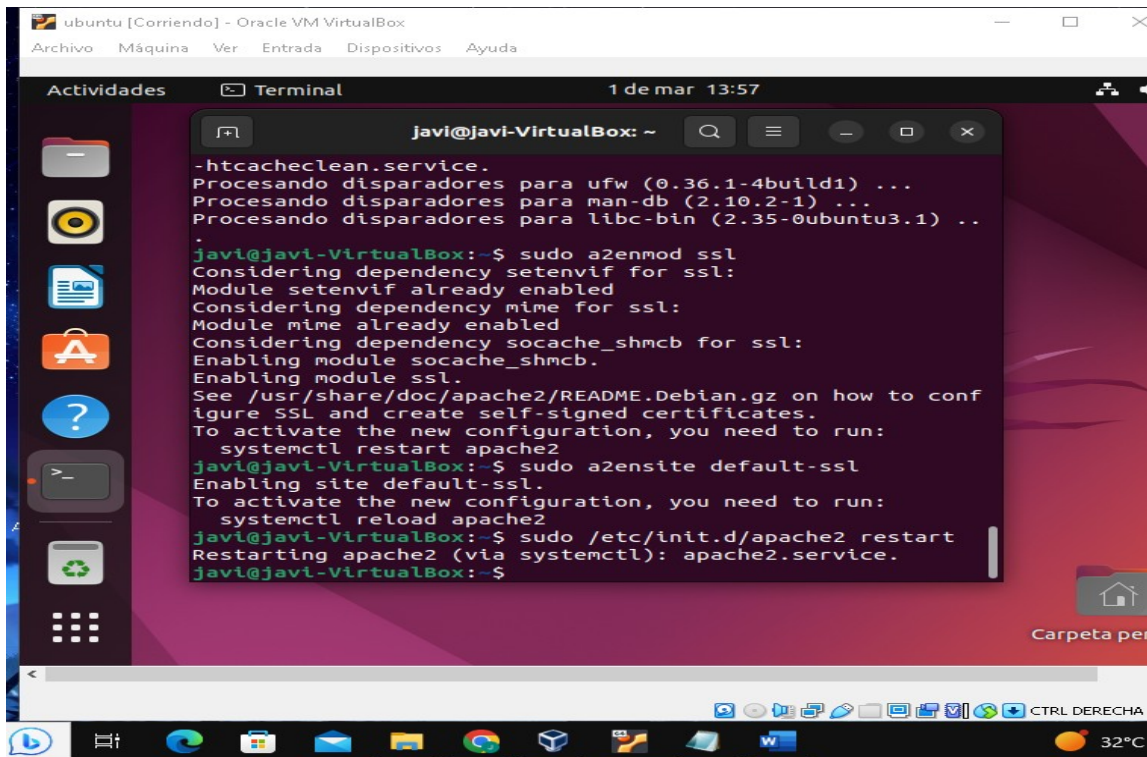
Activando https en Ubuntu



The screenshot shows a terminal window titled 'javi@javi-VirtualBox: ~' with the following output:

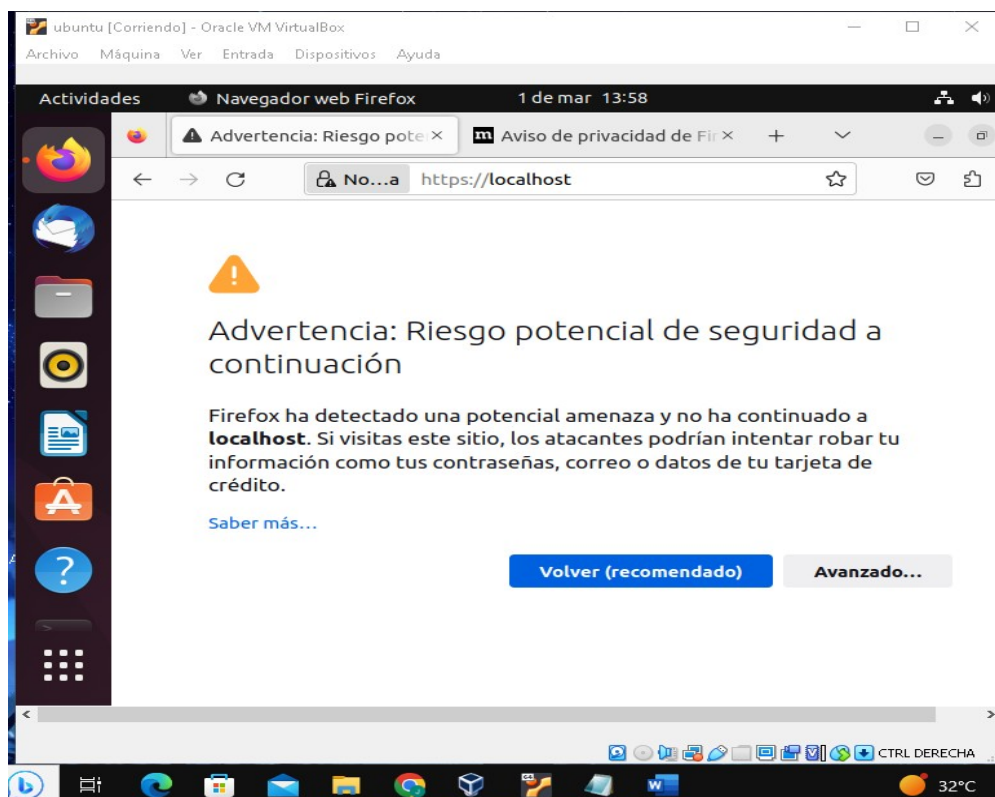
```
Created symlink /etc/systemd/system/multi-user.target.wants/apache-htcacheclean.service → /lib/systemd/system/apache-htcacheclean.service.
Procesando disparadores para ufw (0.36.1-4build1) ...
Procesando disparadores para man-db (2.10.2-1) ...
Procesando disparadores para libc-bin (2.35-0ubuntu3.1) ..
.
javi@javi-VirtualBox:~$ sudo a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
    systemctl restart apache2
javi@javi-VirtualBox:~$ sudo a2ensite default-ssl
Enabling site default-ssl.
To activate the new configuration, you need to run:
    systemctl reload apache2
javi@javi-VirtualBox:~$
```


Reiniciando servidor y mostrando que si funciona el https pero sin certificado aun

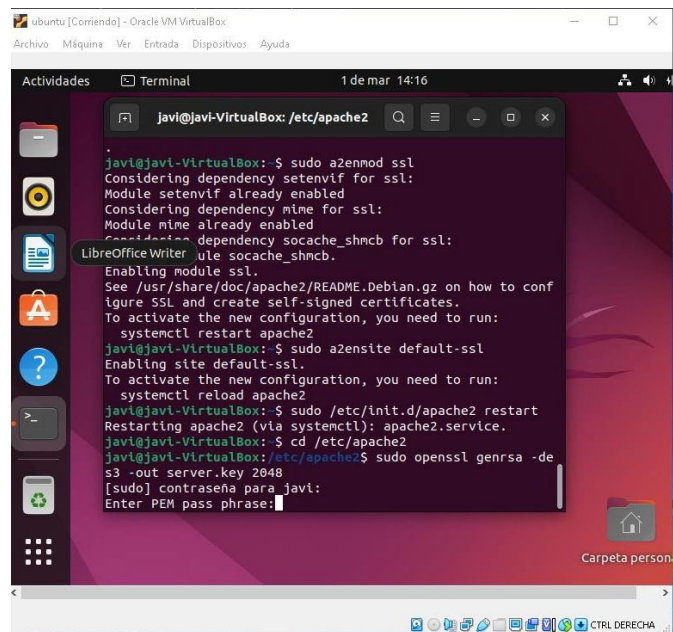


```
javi@javi-VirtualBox: ~  
-htcacheclean.service.  
Procesando disparadores para ufw (0.36.1-4build1) ...  
Procesando disparadores para man-db (2.10.2-1) ...  
Procesando disparadores para libc-bin (2.35-0ubuntu3.1) ..  
.  
javi@javi-VirtualBox:~$ sudo a2enmod ssl  
Considering dependency setenvif for ssl:  
Module setenvif already enabled  
Considering dependency mime for ssl:  
Module mime already enabled  
Considering dependency socache_shmcb for ssl:  
Enabling module socache_shmcb.  
Enabling module ssl.  
See /usr/share/doc/apache2/README.Debian.gz on how to conf  
figure SSL and create self-signed certificates.  
To activate the new configuration, you need to run:  
systemctl restart apache2  
javi@javi-VirtualBox:~$ sudo a2ensite default-ssl  
Enabling site default-ssl.  
To activate the new configuration, you need to run:  
systemctl reload apache2  
javi@javi-VirtualBox:~$ sudo /etc/init.d/apache2 restart  
Restarting apache2 (via systemctl): apache2.service.  
javi@javi-VirtualBox:~$
```

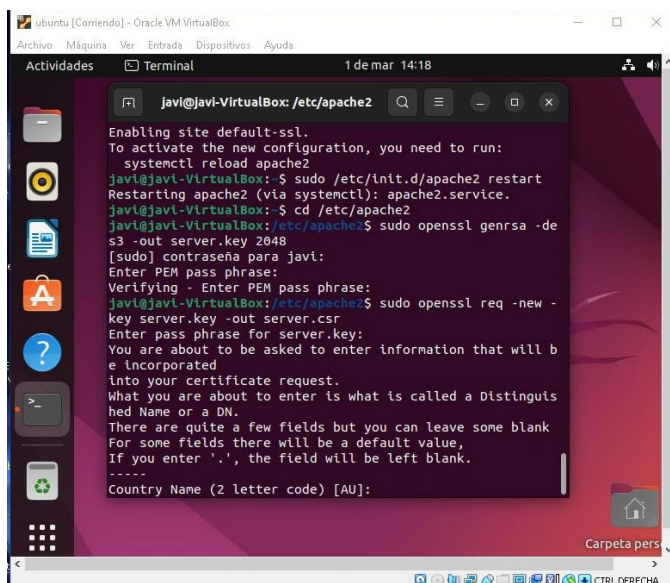
Mostrando https



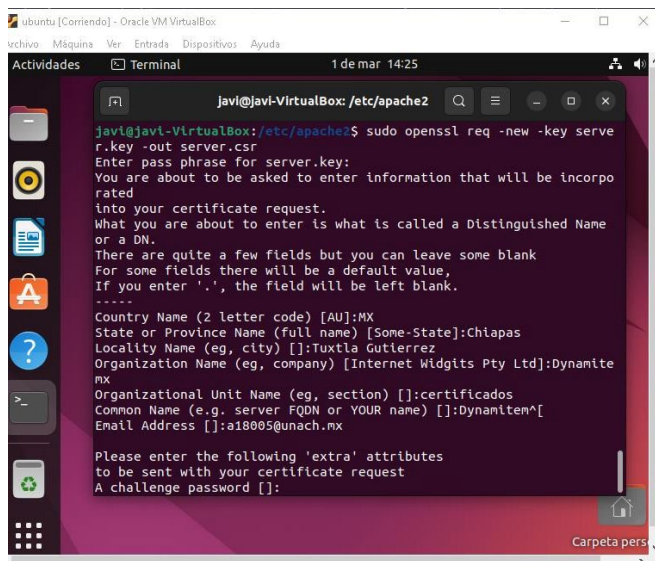
3.-Agregando datos de compañía, correo y nombres para poder crear el certificado



```
jav@jav-VirtualBox: /etc/apache2
jav@jav-VirtualBox:~$ sudo a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Module socache_shmcb already enabled.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
systemctl restart apache2
jav@jav-VirtualBox:~$ sudo a2ensite default-ssl
Enabling site default-ssl.
To activate the new configuration, you need to run:
systemctl reload apache2
jav@jav-VirtualBox:~$ sudo /etc/init.d/apache2 restart
Restarting apache2 (via systemctl): apache2.service.
jav@jav-VirtualBox:~$ cd /etc/apache2
jav@jav-VirtualBox:/etc/apache2$ sudo openssl genrsa -des3 -out server.key 2048
[sudo] contraseña para jav:
Enter PEM pass phrase:
```



```
jav@jav-VirtualBox:/etc/apache2$ sudo openssl req -new -key server.key -out server.csr
[sudo] contraseña para jav:
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
jav@jav-VirtualBox:/etc/apache2$ sudo openssl req -new -key server.key -out server.csr
Enter pass phrase for server.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
```

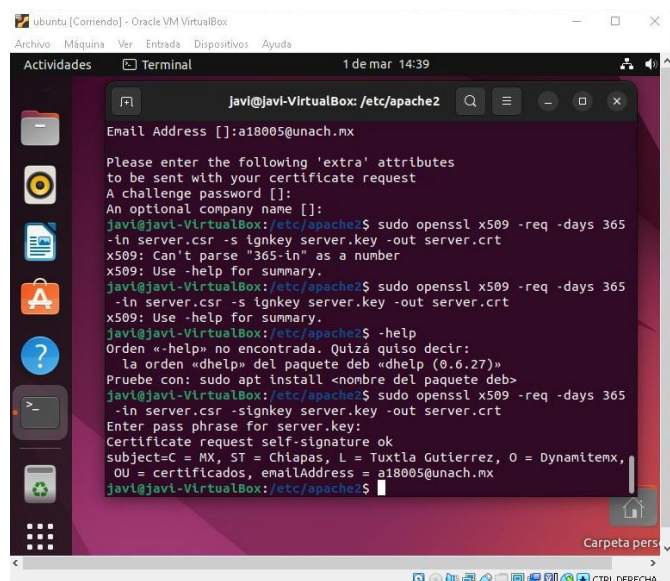


A terminal window titled 'javi@javi-VirtualBox: /etc/apache2' showing the execution of the command `sudo openssl req -new -key server.key -out server.csr`. The prompt 'Enter pass phrase for server.key:' is shown. The user is then prompted to enter information for a Distinguished Name (DN). The following fields are entered: Country Name (2 letter code) [AU]:MX, State or Province Name (full name) [Some-State]:Chiapas, Locality Name (eg, city) []:Tuxtla Gutierrez, Organization Name (eg, company) [Internet Widgits Pty Ltd]:Dynamitemx, Organizational Unit Name (eg, section) []:certificados, Common Name (e.g. server FQDN or YOUR name) []:Dynamitemx, and Email Address []:a18005@unach.mx. The prompt 'Please enter the following 'extra' attributes to be sent with your certificate request' is shown, followed by 'A challenge password []:'.

```
javi@javi-VirtualBox: /etc/apache2$ sudo openssl req -new -key server
r.key -out server.csr
Enter pass phrase for server.key:
You are about to be asked to enter information that will be incorpo
rated
into your certificate request.
What you are about to enter is what is called a Distinguished Name
or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:MX
State or Province Name (full name) [Some-State]:Chiapas
Locality Name (eg, city) []:Tuxtla Gutierrez
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Dynamitem
x
Organizational Unit Name (eg, section) []:certificados
Common Name (e.g. server FQDN or YOUR name) []:Dynamitemx[
Email Address []:a18005@unach.mx

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
```

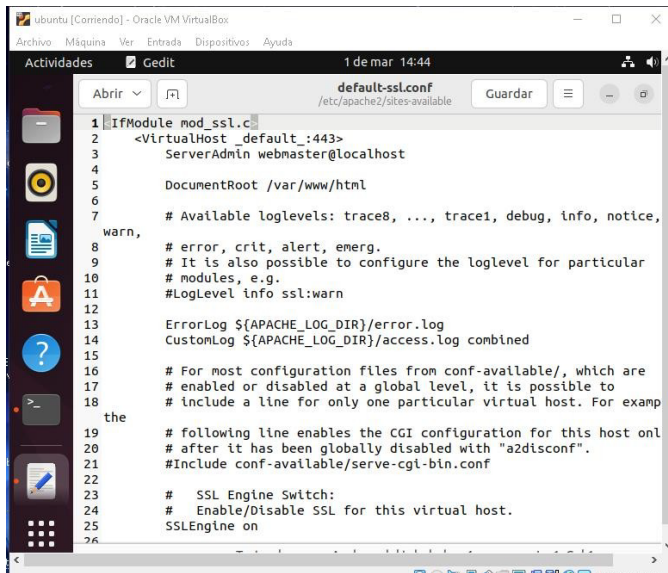
4.-Confirmamos que creo el certificado con los datos



A terminal window titled 'javi@javi-VirtualBox: /etc/apache2' showing the execution of the command `sudo openssl x509 -req -days 365 -in server.csr -s ignkey server.key -out server.crt`. The prompt 'Enter pass phrase for server.key:' is shown. The user is then prompted to enter the following 'extra' attributes to be sent with the certificate request: 'A challenge password []:', 'An optional company name []:', and 'Orden «-help» no encontrada. Quizá quiso decir: la orden «dhelp» del paquete deb «dhelp (0.6.27)»'. The user then enters the command `sudo openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt`. The prompt 'Enter pass phrase for server.key:' is shown. The user is then prompted to enter the following 'extra' attributes to be sent with the certificate request: 'subject=C = MX, ST = Chiapas, L = Tuxtla Gutierrez, O = Dynamitemx, OU = certificados, emailAddress = a18005@unach.mx'.

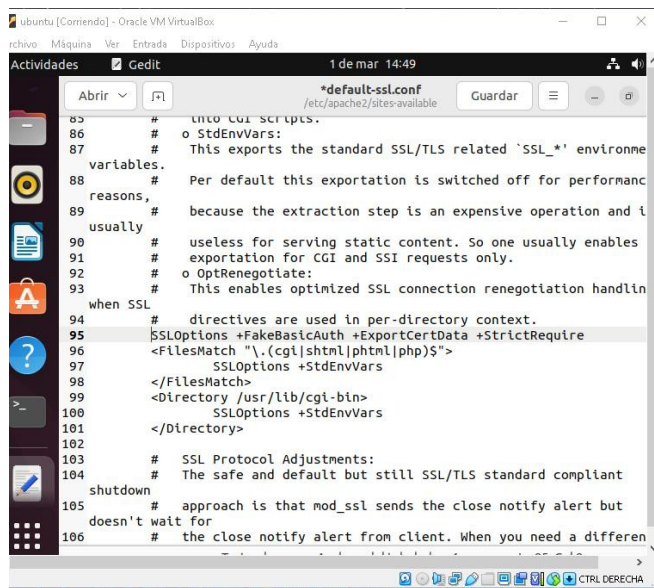
```
javi@javi-VirtualBox: /etc/apache2$ sudo openssl x509 -req -days 365
-in server.csr -s ignkey server.key -out server.crt
x509: Can't parse "365-in" as a number
x509: Use -help for summary.
javi@javi-VirtualBox: /etc/apache2$ sudo openssl x509 -req -days 365
-in server.csr -s ignkey server.key -out server.crt
x509: Use -help for summary.
javi@javi-VirtualBox: /etc/apache2$ -help
Orden «-help» no encontrada. Quizá quiso decir:
la orden «dhelp» del paquete deb «dhelp (0.6.27)»
Pruebe con: sudo apt install <nombre del paquete deb>
javi@javi-VirtualBox: /etc/apache2$ sudo openssl x509 -req -days 365
-in server.csr -signkey server.key -out server.crt
Enter pass phrase for server.key:
Certificate request self-signature ok
subject=C = MX, ST = Chiapas, L = Tuxtla Gutierrez, O = Dynamitemx,
OU = certificados, emailAddress = a18005@unach.mx
javi@javi-VirtualBox: /etc/apache2$
```

5.-Ahora copiaremos los archivos en la carpeta correspondiente



The screenshot shows a Gedit window titled 'default-ssl.conf' with the file path '/etc/apache2/sites-available'. The editor displays the configuration for the default SSL virtual host. The code includes comments for log levels, error logs, and SSL engine settings. The SSL engine is set to 'on'.

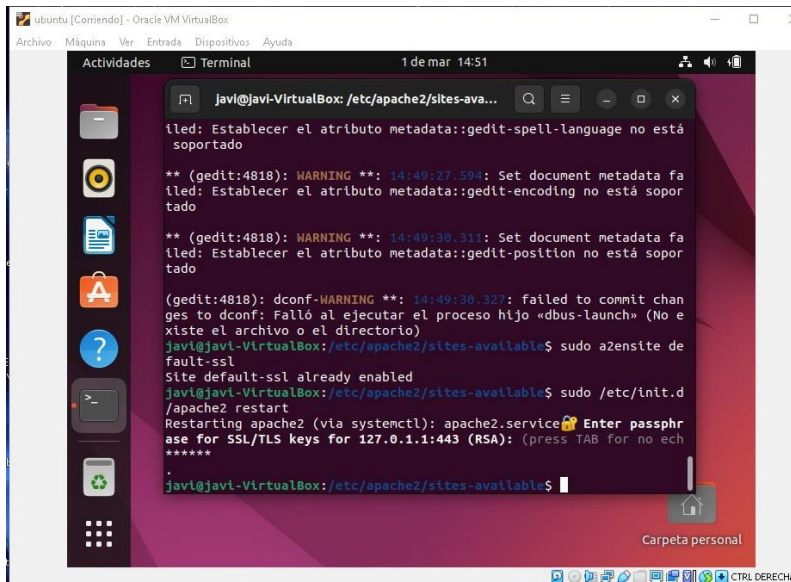
```
1 #IfModule mod_ssl.c
2 <VirtualHost _default_:443>
3     ServerAdmin webmaster@localhost
4
5     DocumentRoot /var/www/html
6
7     # Available loglevels: trace8, ..., trace1, debug, info, notice,
8     warn,
9     # error, crit, alert, emerg.
10    # It is also possible to configure the loglevel for particular
11    # modules, e.g.
12    #LogLevel info ssl:warn
13
14    ErrorLog ${APACHE_LOG_DIR}/error.log
15    CustomLog ${APACHE_LOG_DIR}/access.log combined
16
17    # For most configuration files from conf-available/, which are
18    # enabled or disabled at a global level, it is possible to
19    # include a line for only one particular virtual host. For example
20    # the following line enables the CGI configuration for this host only
21    # after it has been globally disabled with "a2disconf".
22    #Include conf-available/serve-cgi-bin.conf
23
24    # SSL Engine Switch:
25    # Enable/Disable SSL for this virtual host.
26    SSLEngine on
```



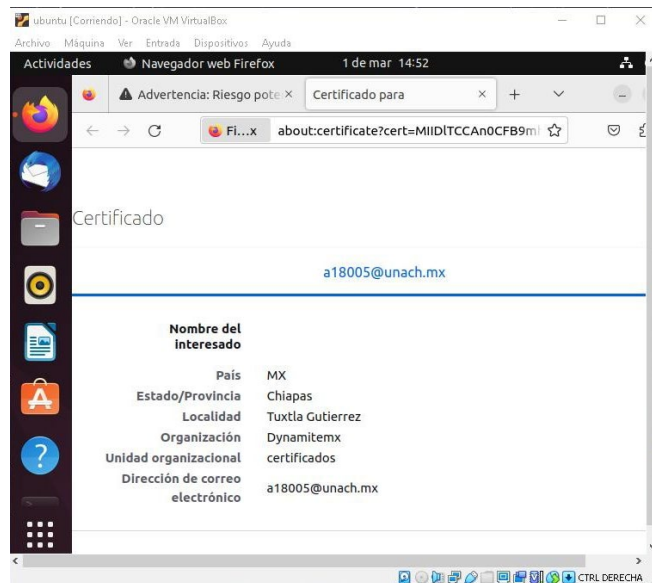
The screenshot shows a Gedit window titled '*default-ssl.conf' with the file path '/etc/apache2/sites-available'. The editor displays the configuration for the default SSL virtual host, including SSL options and protocol adjustments. The code includes comments for SSL options, protocol adjustments, and shutdown settings.

```
85 # into CGI scripts.
86 # o StdEnvVars:
87 # This exports the standard SSL/TLS related 'SSL_*' environme
88 variables.
89 # Per default this exportation is switched off for performanc
90 reasons,
91 # because the extraction step is an expensive operation and i
92 usually
93 # useless for serving static content. So one usually enables
94 # exportation for CGI and SSI requests only.
95 # o OptRenegotiate:
96 # This enables optimized SSL connection renegotiation handle
97 when SSL
98 # directives are used in per-directory context.
99 #SSLOptions +FakeBasicAuth +ExportCertData +StrictRequire
100 <FilesMatch "\.(cgi|shtml|phtml|php)$">
101     SSLOptions +StdEnvVars
102 </FilesMatch>
103 <Directory /usr/lib/cgi-bin>
104     SSLOptions +StdEnvVars
105 </Directory>
106
107 # SSL Protocol Adjustments:
108 # The safe and default but still SSL/TLS standard compliant
109 shutdown
110 # approach is that mod_ssl sends the close notify alert but
111 doesn't wait for
112 # the close notify alert from client. When you need a differen
```

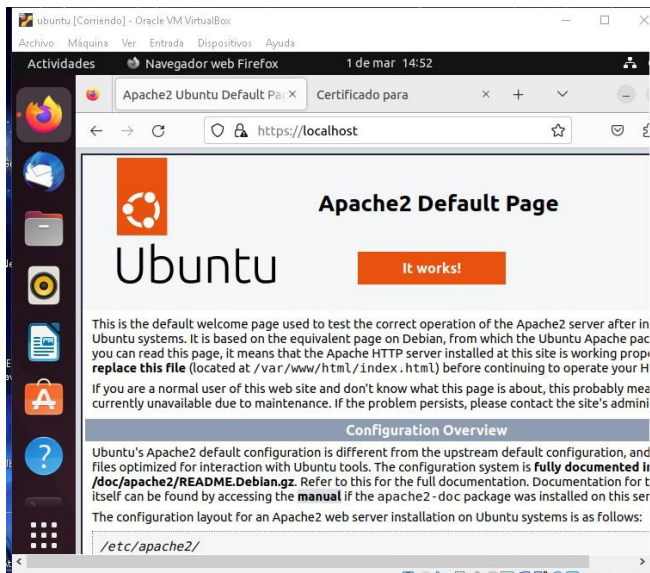
6.-Para finalizar comprobamos si esta activo el https y el certificado SSL



7.-Comprobamos que tiene el certificado nuestros datos

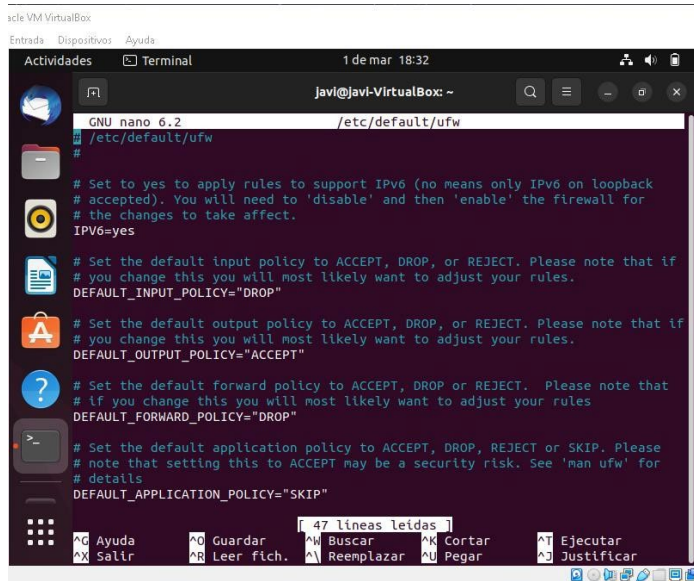


8.-Cargamos la página con https

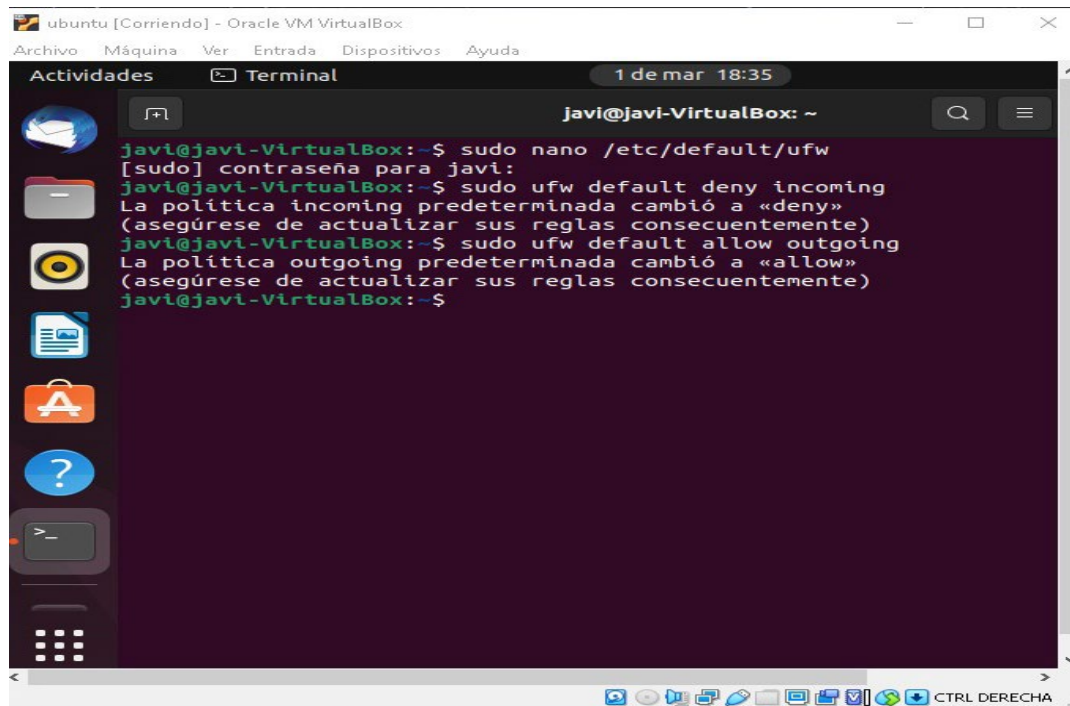


Configuramos el firewall ufw

1.-Activamos el IPv6



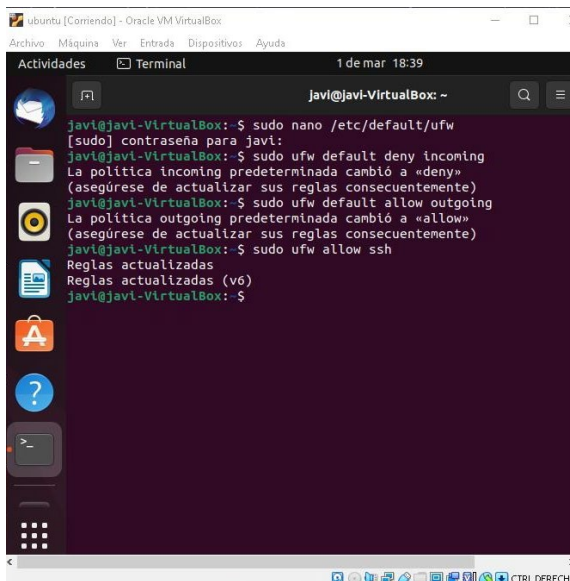
2.-Configurando políticas



The screenshot shows a terminal window titled "ubuntu [Corriendo] - Oracle VM VirtualBox". The terminal output is as follows:

```
javi@javi-VirtualBox:~$ sudo nano /etc/default/ufw
[sudo] contraseña para javi:
javi@javi-VirtualBox:~$ sudo ufw default deny incoming
La política incoming predeterminada cambió a «deny»
(asegúrese de actualizar sus reglas consecuentemente)
javi@javi-VirtualBox:~$ sudo ufw default allow outgoing
La política outgoing predeterminada cambió a «allow»
(asegúrese de actualizar sus reglas consecuentemente)
javi@javi-VirtualBox:~$
```

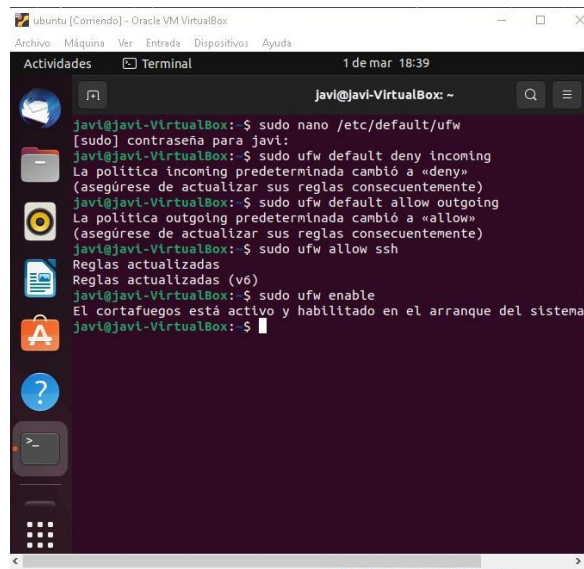
3.-Habilitar conexiones SSH



The screenshot shows a terminal window titled "ubuntu [Corriendo] - Oracle VM VirtualBox". The terminal output is as follows:

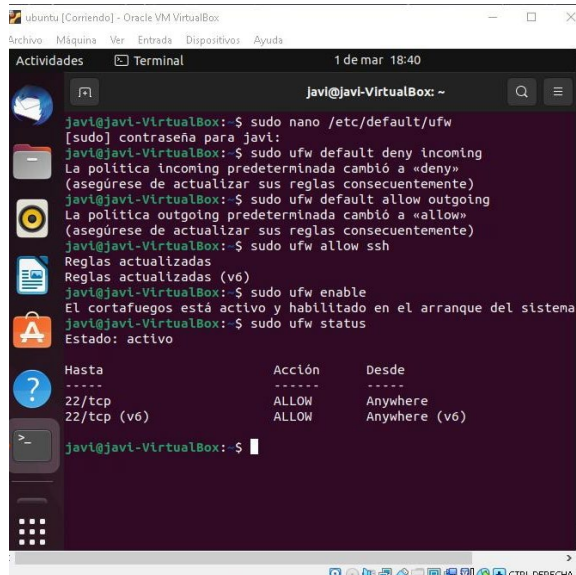
```
javi@javi-VirtualBox:~$ sudo nano /etc/default/ufw
[sudo] contraseña para javi:
javi@javi-VirtualBox:~$ sudo ufw default deny incoming
La política incoming predeterminada cambió a «deny»
(asegúrese de actualizar sus reglas consecuentemente)
javi@javi-VirtualBox:~$ sudo ufw default allow outgoing
La política outgoing predeterminada cambió a «allow»
(asegúrese de actualizar sus reglas consecuentemente)
javi@javi-VirtualBox:~$ sudo ufw allow ssh
Reglas actualizadas
Reglas actualizadas (v6)
javi@javi-VirtualBox:~$
```

4.-Por ultimo confirmamos ufw



```
javi@javi-VirtualBox: ~  
$ sudo nano /etc/default/ufw  
[sudo] contraseña para javi:  
javi@javi-VirtualBox: $ sudo ufw default deny incoming  
La política incoming predeterminada cambió a «deny»  
(asegúrese de actualizar sus reglas consecuentemente)  
javi@javi-VirtualBox: $ sudo ufw default allow outgoing  
La política outgoing predeterminada cambió a «allow»  
(asegúrese de actualizar sus reglas consecuentemente)  
javi@javi-VirtualBox: $ sudo ufw allow ssh  
Reglas actualizadas  
Reglas actualizadas (v6)  
javi@javi-VirtualBox: $ sudo ufw enable  
El cortafuegos está activo y habilitado en el arranque del sistema  
javi@javi-VirtualBox: $
```

5.-Corta fuegos en el puerto 22



```
javi@javi-VirtualBox: ~  
$ sudo nano /etc/default/ufw  
[sudo] contraseña para javi:  
javi@javi-VirtualBox: $ sudo ufw default deny incoming  
La política incoming predeterminada cambió a «deny»  
(asegúrese de actualizar sus reglas consecuentemente)  
javi@javi-VirtualBox: $ sudo ufw default allow outgoing  
La política outgoing predeterminada cambió a «allow»  
(asegúrese de actualizar sus reglas consecuentemente)  
javi@javi-VirtualBox: $ sudo ufw allow ssh  
Reglas actualizadas  
Reglas actualizadas (v6)  
javi@javi-VirtualBox: $ sudo ufw enable  
El cortafuegos está activo y habilitado en el arranque del sistema  
javi@javi-VirtualBox: $ sudo ufw status  
Estado: activo  


| Hasta       | Acción | Desde         |
|-------------|--------|---------------|
| 22/tcp      | ALLOW  | Anywhere      |
| 22/tcp (v6) | ALLOW  | Anywhere (v6) |

  
javi@javi-VirtualBox: $
```