LDAP SEGURO:

Antes de nada, voy a cambiar el nombre de la máquina para no liarnos con el del dominio, la llamaremos maquina00.

```
sudo hostnamectl set-hostname maquina00
```

Configuración en el servidor LDAP

Preparativos

1 crearemos el directorio donde dejaremos los certificados.

```
mkdir ssl-ldap
cd ssl-ldap
```

2Generar certificados SSL autofirmados

2.1 generar certificado ssl

```
sudo openssl genrsa -aes128 -out maquina00.comercio.com.key 4096
```

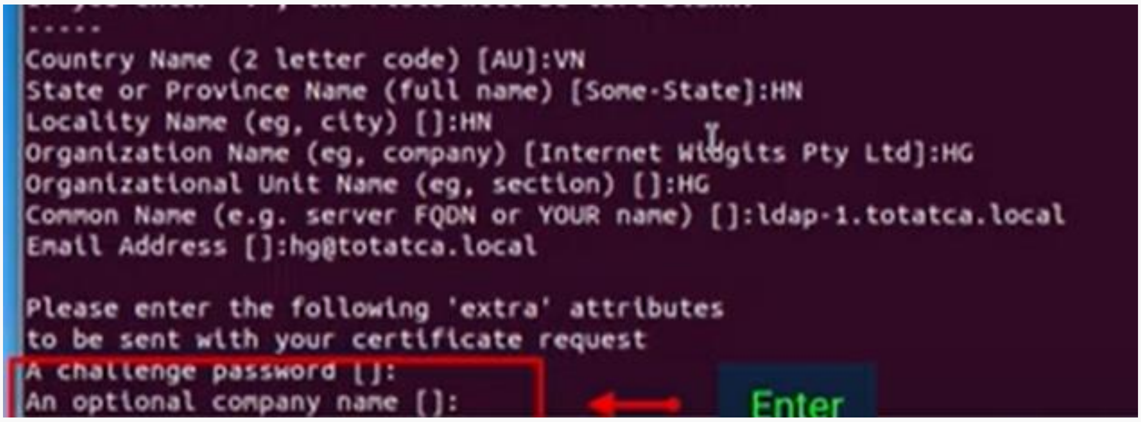
2.2 Quitar la contraseña de la clave privada generada

```
sudo openssl rsa -in maquina00.comercio.com.key -out
maquina00.comercio.com.key
```

meter la clave del paso 2.1

Generamos la clave csr

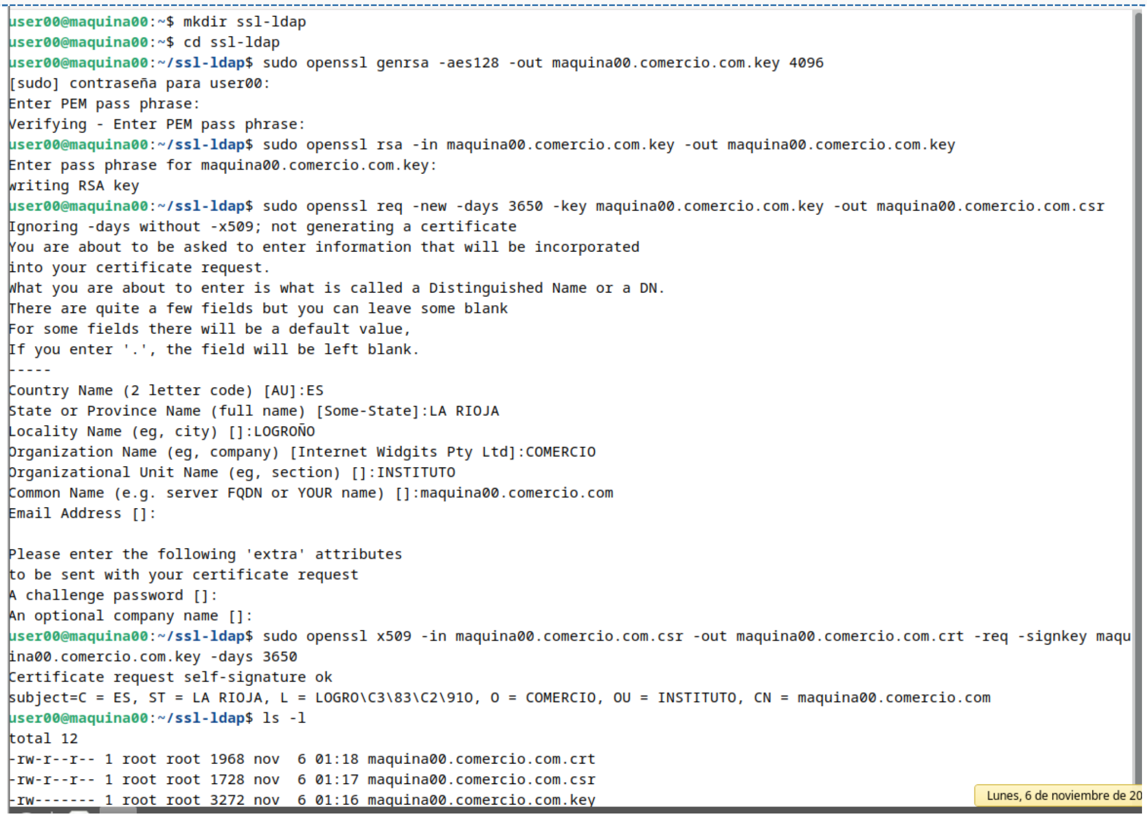
```
sudo openssl req -new -days 3650 -key maquina00.comercio.com.key -out
maquina00.comercio.com.csr
```



```
-----
Country Name (2 letter code) [AU]:VN
State or Province Name (full name) [Some-State]:HN
Locality Name (eg, city) []:HN
Organization Name (eg, company) [Internet Widgits Pty Ltd]:HG
Organizational Unit Name (eg, section) []:HG
Common Name (e.g. server FQDN or YOUR name) []:ldap-1.totatca.local
Email Address []:hg@totatca.local

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

2.4 firmar el certificado

```
sudo openssl x509 -in maquina00.comercio.com.csr -out
maquina00.comercio.com.crt -req -signkey maquina00.comercio.com.key -
days 3650

ls -l
```

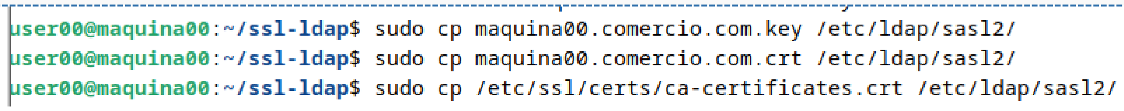


```
user00@maquina00:~$ mkdir ssl-ldap
user00@maquina00:~$ cd ssl-ldap
user00@maquina00:~/ssl-ldap$ sudo openssl genrsa -aes128 -out maquina00.comercio.com.key 4096
[sudo] contraseña para user00:
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
user00@maquina00:~/ssl-ldap$ sudo openssl rsa -in maquina00.comercio.com.key -out maquina00.comercio.com.key
Enter pass phrase for maquina00.comercio.com.key:
writing RSA key
user00@maquina00:~/ssl-ldap$ sudo openssl req -new -days 3650 -key maquina00.comercio.com.key -out maquina00.comercio.com.csr
Ignoring -days without -x509; not generating a certificate
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]:ES
State or Province Name (full name) [Some-State]:LA RIOJA
Locality Name (eg, city) []:LOGROÑO
Organization Name (eg, company) [Internet Widgits Pty Ltd]:COMERCIO
Organizational Unit Name (eg, section) []:INSTITUTO
Common Name (e.g. server FQDN or YOUR name) []:maquina00.comercio.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
user00@maquina00:~/ssl-ldap$ sudo openssl x509 -in maquina00.comercio.com.csr -out maquina00.comercio.com.crt -req -signkey maqu
ina00.comercio.com.key -days 3650
Certificate request self-signature ok
subject=C = ES, ST = LA RIOJA, L = LOGRO\C3\83\C2\91O, O = COMERCIO, OU = INSTITUTO, CN = maquina00.comercio.com
user00@maquina00:~/ssl-ldap$ ls -l
total 12
-rw-r--r-- 1 root root 1968 nov  6 01:18 maquina00.comercio.com.crt
-rw-r--r-- 1 root root 1728 nov  6 01:17 maquina00.comercio.com.csr
-rw------- 1 root root 3272 nov  6 01:16 maquina00.comercio.com.key
```

Configurar SSL en el servidor LDAP

3.1 copiar los certificados y claves en /etc/ldap/sasl2

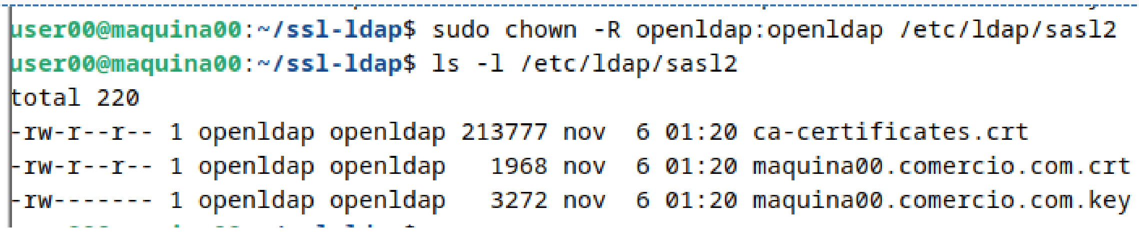
```
sudo cp maquina00.comercio.com.key /etc/ldap/sasl2/
sudo cp maquina00.comercio.com.crt /etc/ldap/sasl2/
sudo cp /etc/ssl/certs/ca-certificates.crt /etc/ldap/sasl2/
```



```
user00@maquina00:~/ssl-ldap$ sudo cp maquina00.comercio.com.key /etc/ldap/sasl2/
user00@maquina00:~/ssl-ldap$ sudo cp maquina00.comercio.com.crt /etc/ldap/sasl2/
user00@maquina00:~/ssl-ldap$ sudo cp /etc/ssl/certs/ca-certificates.crt /etc/ldap/sasl2/
```

Cambiar el propietario:

```
sudo chown -R openldap:openldap /etc/ldap/sasl2
ls -l /etc/ldap/sasl2
```

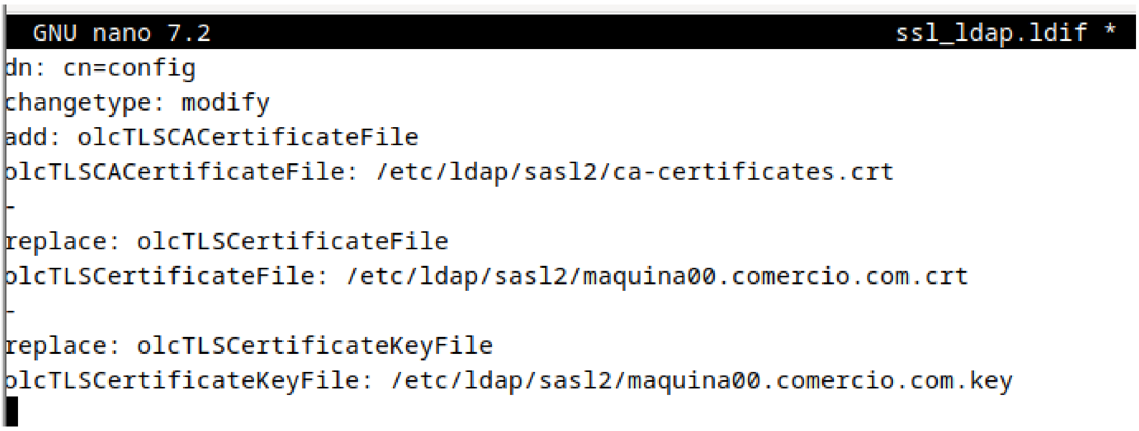


```
user00@maquina00:~/ssl-ldap$ sudo chown -R openldap:openldap /etc/ldap/sasl2
user00@maquina00:~/ssl-ldap$ ls -l /etc/ldap/sasl2
total 220
-rw-r--r-- 1 openldap openldap 213777 nov  6 01:20 ca-certificates.crt
-rw-r--r-- 1 openldap openldap   1968 nov  6 01:20 maquina00.comercio.com.crt
-rw------- 1 openldap openldap   3272 nov  6 01:20 maquina00.comercio.com.key
```

3.3 crear fichero .ldif de configuración

```
sudo nano ssl_ldap.ldif
```

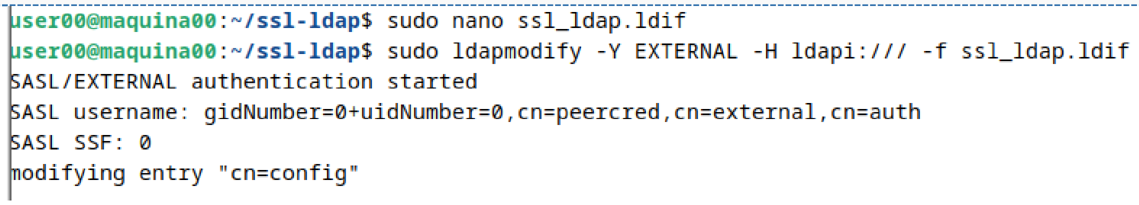
```
dn: cn=config
changetype: modify
add: olcTLSCACertificateFile
olcTLSCACertificateFile: /etc/ldap/sasl2/ca-certificates.crt

replace: olcTLSCertificateFile
olcTLSCertificateFile: /etc/ldap/sasl2/maquina00.comercio.com.crt

replace: olcTLSCertificateKeyFile
olcTLSCertificateKeyFile: /etc/ldap/sasl2/maquina00.comercio.com.key
```



```
GNU nano 7.2                                              ssl_ldap.ldif *
dn: cn=config
changetype: modify
add: olcTLSCACertificateFile
olcTLSCACertificateFile: /etc/ldap/sasl2/ca-certificates.crt
-
replace: olcTLSCertificateFile
olcTLSCertificateFile: /etc/ldap/sasl2/maquina00.comercio.com.crt
-
replace: olcTLSCertificateKeyFile
olcTLSCertificateKeyFile: /etc/ldap/sasl2/maquina00.comercio.com.key
```

3.4 configurar el servidor LDAP para usar certificados SSL

```
sudo ldapmodify -Y EXTERNAL -H ldapi:/// -f ssl_ldap.ldif
```

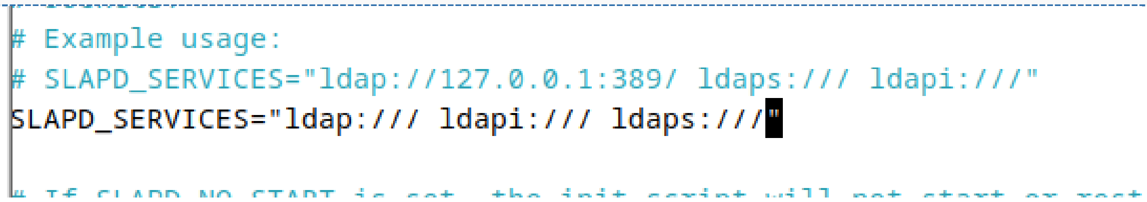


```
user00@maquina00:~/ssl-ldap$ sudo nano ssl_ldap.ldif
user00@maquina00:~/ssl-ldap$ sudo ldapmodify -Y EXTERNAL -H ldapi:/// -f ssl_ldap.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "cn=config"
```

```
sudo ldapmodify -Y EXTERNAL -H ldap:/// -f ssl_ldap.ldif
```

3.5 Editar /etc/default/slapd

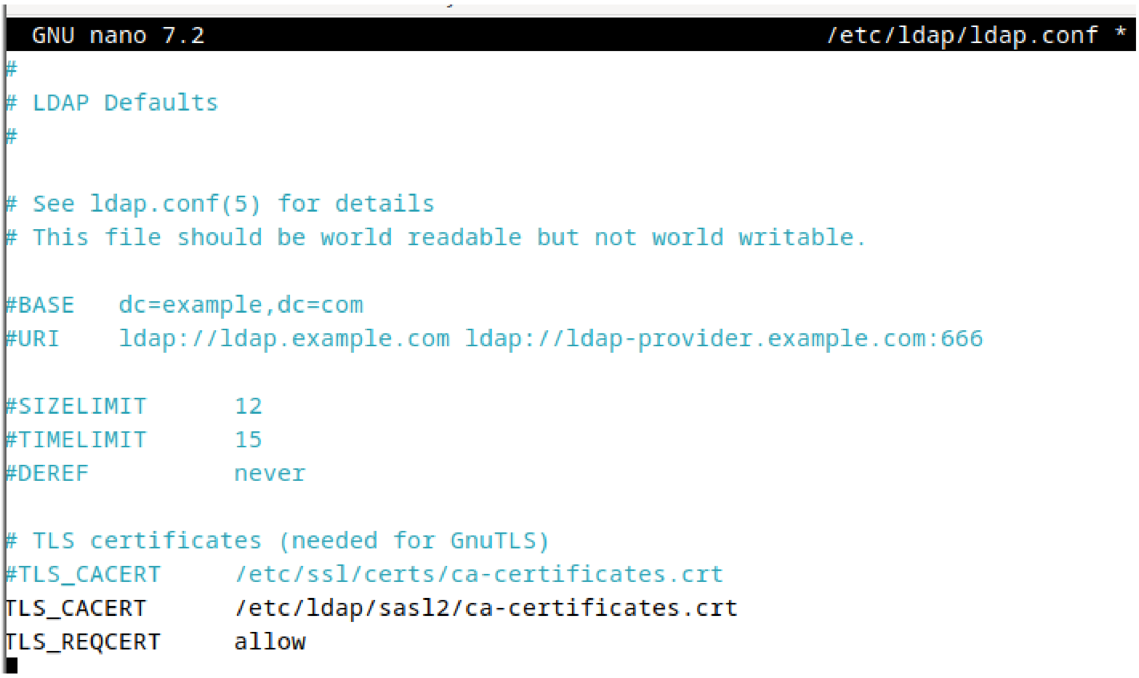
```
sudo nano /etc/default/slapd
```



```
# Example usage:
# SLAPD_SERVICES="ldap://127.0.0.1:389/ ldaps:/// ldapi:///"
SLAPD_SERVICES="ldap:/// ldapi:/// ldaps:///"

# If SLAPD_NO_START is set, the init script will not start or rest
```

3.6 Ediatr /etc/ldap/ldap.conf

```
sudo nano /etc/ldap/ldap.conf
```



```
 GNU nano 7.2                                              /etc/ldap/ldap.conf *
#
# LDAP Defaults
#

# See ldap.conf(5) for details
# This file should be world readable but not world writable.

#BASE   dc=example,dc=com
#URI    ldap://ldap.example.com ldap://ldap-provider.example.com:666

#SIZELIMIT      12
#TIMELIMIT      15
#DEREF          never

# TLS certificates (needed for GnuTLS)
#TLS_CACERT     /etc/ssl/certs/ca-certificates.crt
TLS_CACERT      /etc/ldap/sasl2/ca-certificates.crt
TLS_REQCERT     allow
```

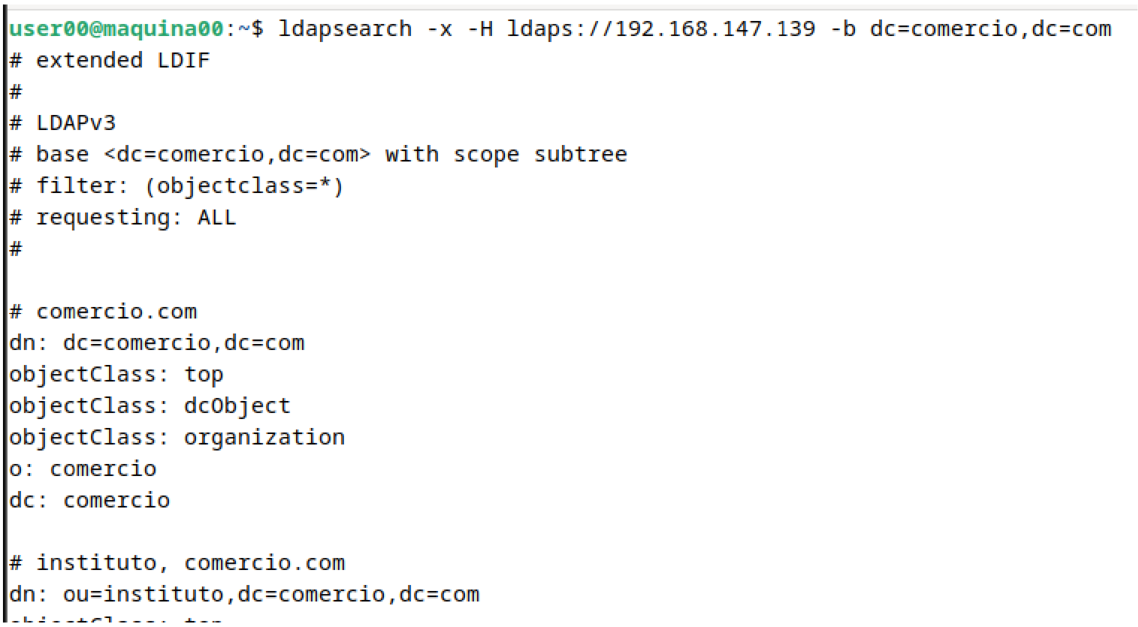
```
TLS_CACERT      /etc/ldap/sasl2/ca-certificates.crt
TLS_REQCERT     allow
```

3.7 reiniciar el servidor ldap

```
sudo systemctl restart slapd
```

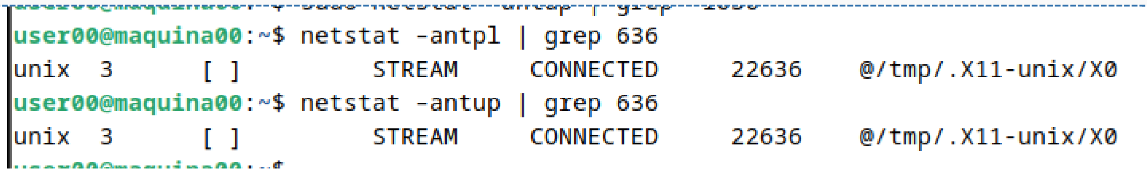
4. Verificar

```
sudo ldapsearch -x -H ldaps://192.168.147.139 –b dc=comercio,dc=com
```



```
user00@maquina00:~$ ldapsearch -x -H ldaps://192.168.147.139 -b dc=comercio,dc=com
# extended LDIF
#
# LDAPv3
# base <dc=comercio,dc=com> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# comercio.com
dn: dc=comercio,dc=com
objectClass: top
objectClass: dcObject
objectClass: organization
o: comercio
dc: comercio

# instituto, comercio.com
dn: ou=instituto,dc=comercio,dc=com
```

```
netstat -antup | grep 636
```



```
user00@maquina00:~$ netstat -antpl | grep 636
unix  3      [ ]         STREAM     CONNECTED     22636    @/tmp/.X11-unix/X0
user00@maquina00:~$ netstat -antup | grep 636
unix  3      [ ]         STREAM     CONNECTED     22636    @/tmp/.X11-unix/X0
```

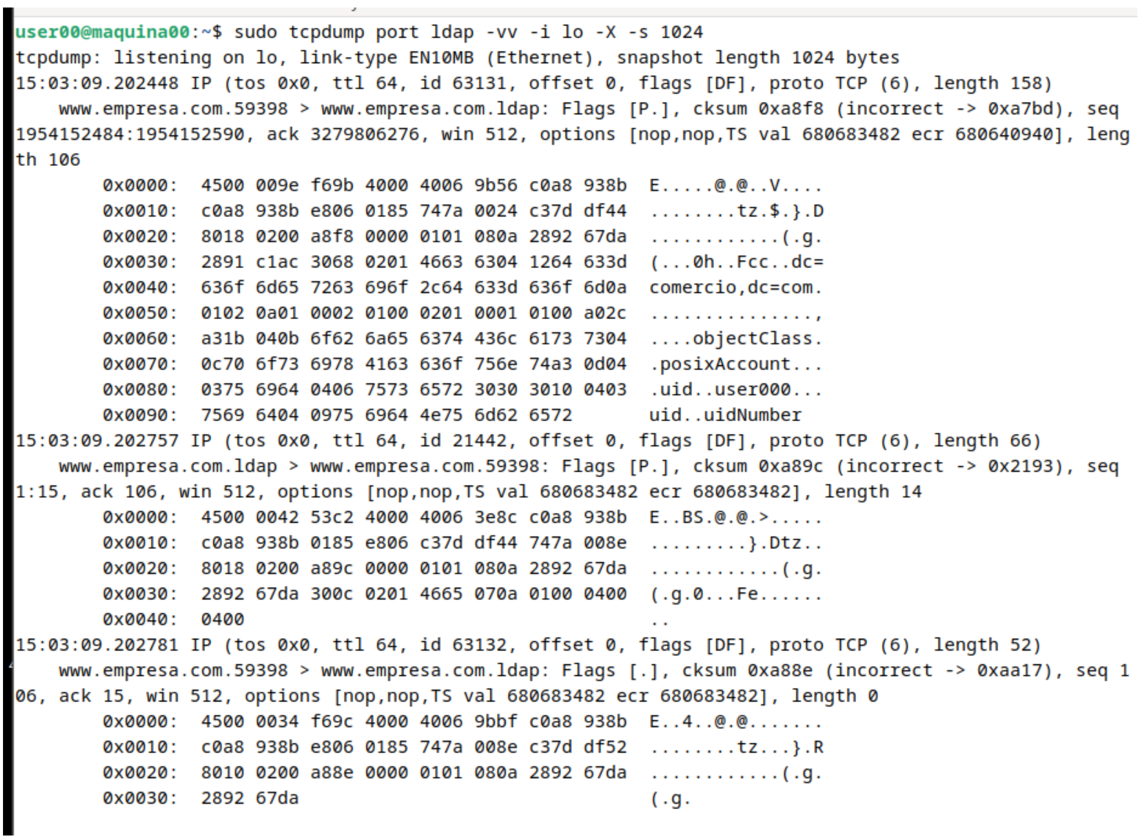
También podemos probarlo abriendo una segunda consola y ejecutando:

```
sudotcpdump port ldap -vv -i lo -X -s 1024
```

A continuación, en la otra consola:

```
sudo ldapsearch -x -H ldaps://192.168.147.139 -b dc=comercio,dc=com
```

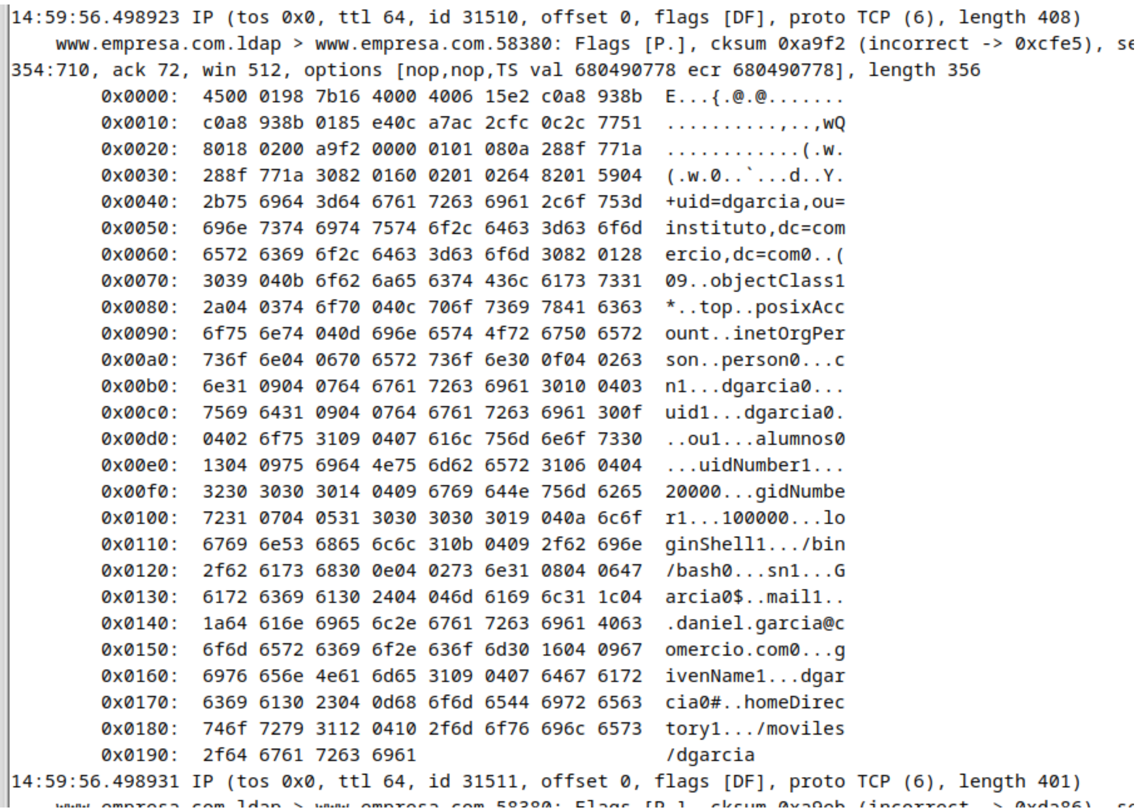
y observamos los resultados de tcpdump:



```
user00@maquina00:~$ sudo tcpdump port ldap -vv -i lo -X -s 1024
tcpdump: listening on lo, link-type EN10MB (Ethernet), snapshot length 1024 bytes
15:03:09.202448 IP (tos 0x0, ttl 64, id 63131, offset 0, flags [DF], proto TCP (6), length 158)
    www.empresa.com.59398 > www.empresa.com.ldap: Flags [P.], cksum 0xa8f8 (incorrect -> 0xa7bd), seq
1954152484:1954152590, ack 3279806276, win 512, options [nop,nop,TS val 680683482 ecr 680640940], leng
th 106
        0x0000:  4500 009e f69b 4000 4006 9b56 c0a8 938b  E.....@.@..V....
        0x0010:  c0a8 938b e806 0185 747a 0024 c37d df44  ........tz.$.}.D
        0x0020:  8018 0200 a8f8 0000 0101 080a 2892 67da  ............(.g.
        0x0030:  2891 c1ac 3068 0201 4663 6304 1264 633d  (...0h..Fcc..dc=
        0x0040:  636f 6d65 7263 696f 2c64 633d 636f 6d0a  comercio,dc=com.
        0x0050:  0102 0a01 0002 0100 0201 0001 0100 a02c  ...............,
        0x0060:  a31b 040b 6f62 6a65 6374 436c 6173 7304  ....objectClass.
        0x0070:  0c70 6f73 6978 4163 636f 756e 74a3 0d04  .posixAccount...
        0x0080:  0375 6964 0406 7573 6572 3030 3010 0403  .uid..user000...
        0x0090:  7569 6404 0975 6964 4e75 6d62 6572       uid..uidNumber
15:03:09.202757 IP (tos 0x0, ttl 64, id 21442, offset 0, flags [DF], proto TCP (6), length 66)
    www.empresa.com.ldap > www.empresa.com.59398: Flags [P.], cksum 0xa89c (incorrect -> 0x2193), seq
1:15, ack 106, win 512, options [nop,nop,TS val 680683482 ecr 680683482], length 14
        0x0000:  4500 0042 53c2 4000 4006 3e8c c0a8 938b  E..BS.@.@.>.....
        0x0010:  c0a8 938b 0185 e806 c37d df44 747a 008e  .........}.Dtz..
        0x0020:  8018 0200 a89c 0000 0101 080a 2892 67da  ............(.g.
        0x0030:  2892 67da 300c 0201 4665 070a 0100 0400  (.g.0...Fe......
        0x0040:  0400                                     ..
15:03:09.202781 IP (tos 0x0, ttl 64, id 63132, offset 0, flags [DF], proto TCP (6), length 52)
    www.empresa.com.59398 > www.empresa.com.ldap: Flags [.], cksum 0xa88e (incorrect -> 0xaa17), seq 1
06, ack 15, win 512, options [nop,nop,TS val 680683482 ecr 680683482], length 0
        0x0000:  4500 0034 f69c 4000 4006 9bbf c0a8 938b  E..4..@.@.......
        0x0010:  c0a8 938b e806 0185 747a 008e c37d df52  ........tz...}.R
        0x0020:  8010 0200 a88e 0000 0101 080a 2892 67da  ............(.g.
        0x0030:  2892 67da                                (.g.
```

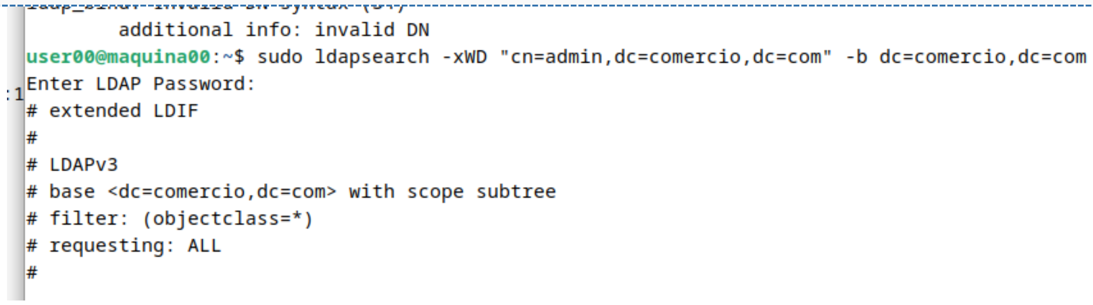
Ahora probamos con:

```
sudo ldapsearch -x -H ldap://192.168.147.139 –b dc=comercio,dc=com
```



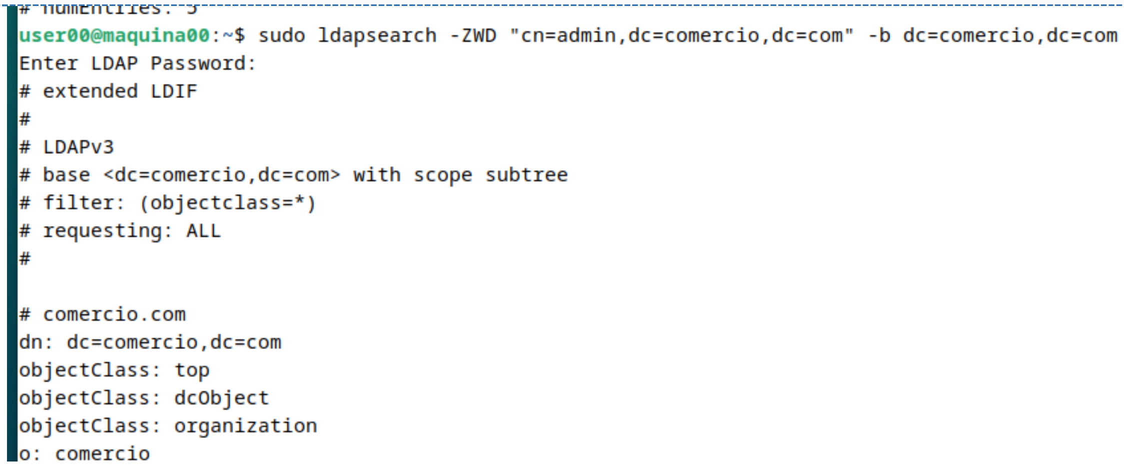
```
14:59:56.498923 IP (tos 0x0, ttl 64, id 31510, offset 0, flags [DF], proto TCP (6), length 408)
    www.empresa.com.ldap > www.empresa.com.58380: Flags [P.], cksum 0xa9f2 (incorrect -> 0xcfe5), se
354:710, ack 72, win 512, options [nop,nop,TS val 680490778 ecr 680490778], length 356
        0x0000:  4500 0198 7b16 4000 4006 15e2 c0a8 938b  E...{.@.@.......
        0x0010:  c0a8 938b 0185 e40c a7ac 2cfc 0c2c 7751  ..........,..,wQ
        0x0020:  8018 0200 a9f2 0000 0101 080a 288f 771a  ............(.w.
        0x0030:  288f 771a 3082 0160 0201 0264 8201 5904  (.w.0..`...d..Y.
        0x0040:  2b75 6964 3d64 6761 7263 6961 2c6f 753d  +uid=dgarcia,ou=
        0x0050:  696e 7374 6974 7574 6f2c 6463 3d63 6f6d  instituto,dc=com
        0x0060:  6572 6369 6f2c 6463 3d63 6f6d 3082 0128  ercio,dc=com0..(
        0x0070:  3039 040b 6f62 6a65 6374 436c 6173 7331  09..objectClass1
        0x0080:  2a04 0374 6f70 040c 706f 7369 7841 6363  *..top..posixAcc
        0x0090:  6f75 6e74 040d 696e 6574 4f72 6750 6572  ount..inetOrgPer
        0x00a0:  736f 6e04 0670 6572 736f 6e30 0f04 0263  son..person0...c
        0x00b0:  6e31 0904 0764 6761 7263 6961 3010 0403  n1...dgarcia0...
        0x00c0:  7569 6431 0904 0764 6761 7263 6961 300f  uid1...dgarcia0.
        0x00d0:  0402 6f75 3109 0407 616c 756d 6e6f 7330  ..ou1...alumnos0
        0x00e0:  1304 0975 6964 4e75 6d62 6572 3106 0404  ...uidNumber1...
        0x00f0:  3230 3030 3014 0409 6769 644e 756d 6265  20000...gidNumbe
        0x0100:  7231 0704 0531 3030 3030 3019 040a 6c6f  r1...100000...lo
        0x0110:  6769 6e53 6865 6c6c 310b 0409 2f62 696e  ginShell1.../bin
        0x0120:  2f62 6173 6830 0e04 0273 6e31 0804 0647  /bash0...sn1...G
        0x0130:  6172 6369 6130 2404 046d 6169 6c31 1c04  arcia0$..mail1..
        0x0140:  1a64 616e 6965 6c2e 6761 7263 6961 4063  .daniel.garcia@c
        0x0150:  6f6d 6572 6369 6f2e 636f 6d30 1604 0967  omercio.com0...g
        0x0160:  6976 656e 4e61 6d65 3109 0407 6467 6172  ivenName1...dgar
        0x0170:  6369 6130 2304 0d68 6f6d 6544 6972 6563  cia0#..homeDirec
        0x0180:  746f 7279 3112 0410 2f6d 6f76 696c 6573  tory1.../moviles
        0x0190:  2f64 6761 7263 6961                      /dgarcia
14:59:56.498931 IP (tos 0x0, ttl 64, id 31511, offset 0, flags [DF], proto TCP (6), length 401)
    www.empresa.com.ldap > www.empresa.com.58380: Flags [P.], cksum 0xa9eb (incorrect -> 0xda86), se
```

```
sudo ldapsearch -xWD “cn=admin,dc=comercio,dc=com” -b
dc=comercio,dc=com
```



```
ldap_bind: Invalid DN syntax (34)
        additional info: invalid DN
user00@maquina00:~$ sudo ldapsearch -xWD "cn=admin,dc=comercio,dc=com" -b dc=comercio,dc=com
Enter LDAP Password:
# extended LDIF
#
# LDAPv3
# base <dc=comercio,dc=com> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
```

```
sudo ldapsearch -ZWD “cn=admin,dc=comercio,dc=com” -b
dc=comercio,dc=com
```



```
# numEntries: 3
user00@maquina00:~$ sudo ldapsearch -ZWD "cn=admin,dc=comercio,dc=com" -b dc=comercio,dc=com
Enter LDAP Password:
# extended LDIF
#
# LDAPv3
# base <dc=comercio,dc=com> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# comercio.com
dn: dc=comercio,dc=com
objectClass: top
objectClass: dcObject
objectClass: organization
o: comercio
```

Configuararel firewall