

9. Acceso remoto: SSH

- Secure Shell (SSH) es un protocolo que facilita la comunicación cliente-servidor y permite que los clientes accedan de forma remota. SSH asegura la conexión. El cliente transmite su información de autenticación al servidor de firma encriptada, y todos los datos enviados y recibidos durante una sesión se transmiten también bajo encriptación.
- SSH permite que los usuarios se autentifiquen sin contraseña, mediante una pareja de claves pública-privada

9. Formas de autenticación SSH

- **Con password:** Una vez establecido el canal cifrado por SSH, se envían login y password hacia el servidor. El servidor comprueba que el usuario existe, y que la contraseña es correcta comparándola con la entrada correspondiente del fichero de `/etc/passwd` o `/etc/shadow`. Este sistema hace necesario que el usuario rescriba su contraseña cada vez que desea establecer una sesión.
- **Con clave pública:** El usuario o cliente debe generar una pareja de claves pública/privada. Después debe copiar la clave pública en el servidor. Cuando se ha establecido la comunicación segura por SSH y el cliente debe autenticarse, el servidor generará un número aleatorio, conocido como “desafío”, y utilizará la clave pública del cliente que tiene almacenada para cifrar este número. Ese número cifrado se envía al cliente, que lo descifra con su clave privada y lo devuelve al servidor, demostrando que es quien dice ser. Las ventajas que aporta este método son evitar que el usuario tenga que recordar y escribir contraseñas, y evitar que la contraseña del usuario viaje hacia el servidor, ni tan siquiera viajando encriptada.

9. Pasos en una conexión SSH

- Cuando un cliente de SSH se conecta al servidor, se realizan los siguientes pasos:
 - 1. El cliente abre una conexión TCP al puerto 22 del host servidor.
 - 2. El cliente y el servidor negocian la versión a usar en función de su configuración y capacidad.
 - 3. El servidor posee una pareja de claves pública/privada generadas mediante el algoritmo RSA. El servidor envía la clave pública al cliente.
 - 4. Si es la primera vez que ese cliente se conecta al servidor, el usuario recibe un mensaje donde se le pregunta si está seguro de que la clave pública del servidor es esa. Si el usuario contesta que sí, el sistema cliente guarda esta clave y no repite más la pregunta. En conexiones posteriores, el cliente recibe de nuevo la clave pública del servidor, y la compara con la que tiene almacenada, verificando así su autenticidad.
 - 5. El cliente genera una clave de sesión aleatoria y selecciona un algoritmo de cifrado simétrico. Después, cifra el algoritmo seleccionado y la clave simétrica generada mediante RSA y la clave pública del servidor. Envía este paquete cifrado al servidor.
 - 6. El servidor recibe un paquete cifrado, que descifra mediante la clave privada, que sólo él conoce. En el paquete se le informa del algoritmo y la clave simétricas elegidas para el resto de la comunicación.
 - 7. Finalmente, se realiza la autenticación del usuario. Si esta es correcta, comienza la sesión interactiva, siempre dentro de un canal cifrado.

9. Instalación de un servidor OpenSSH

- Se instala el paquete **openssh-server**
- Se inicia el daemon **sshd** y se configura el inicio automático:
systemctl start sshd
systemctl enable sshd
- Para especificar direcciones diferentes de 0.0.0.0 (IPv4) o :: (IPv6) se usa la directiva **ListenAddress** en **/etc/ssh/sshd_config**
- Para que sshd no arranque antes de que toda la red esté disponible (necesario si se ha modificado la directiva ListenAddress) se añade la dependencia de la unidad **network-online.target** en el fichero de unidad **sshd.service**. Para esto, se crea el archivo **/etc/systemd/system/sshd.service.d/local.conf** con el contenido siguiente:

[Unit]

Wants=network-online.target

After=network-online.target

9.L Instalación de un servidor OpenSSH

- Para cambiar el mensaje de bienvenida del servidor se modifica el fichero /etc/issue (y para cambiar el mensaje tras el login, /etc/motd)
- Para comprobar que el servicio está corriendo, `systemctl status sshd`

```
[root@localhost ~]# systemctl status sshd
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; vendor preset: enabled)
   Drop-In: /etc/systemd/system/sshd.service.d
            └─local.conf
   Active: active (running) since Wed 2020-03-25 12:32:26 CET; 38s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
  Main PID: 1477 (sshd)
    Tasks: 1 (limit: 8020)
   Memory: 2.4M
   CGroup: /system.slice/sshd.service
           └─1477 /usr/sbin/sshd -D -oCiphers=aes256-gcm@openssh.com,chacha20-poly1305@openss

Mar 25 12:32:26 localhost.localdomain systemd[1]: Starting OpenSSH server daemon...
Mar 25 12:32:26 localhost.localdomain sshd[1477]: Server listening on 0.0.0.0 port 22.
Mar 25 12:32:26 localhost.localdomain sshd[1477]: Server listening on :: port 22.
Mar 25 12:32:26 localhost.localdomain systemd[1]: Started OpenSSH server daemon.
lines 1-17/17 (END)
```

9.L SSH sin contraseña

- Para mejorar la seguridad del sistema, la configuración recomendada consiste en acceder mediante claves y deshabilitar la autenticación por contraseña. La configuración es como sigue:
- Se cambia la directiva **PasswordAuthentication** a "no" en **/etc/ssh/sshd_config**, y se comprueba que las directivas **PubKeyAuthentication** y **ChallengeResponseAuthentication** estén puestas a "yes". Si se está haciendo la configuración del servidor desde una máquina remota, no deshabitar **PasswordAuthentication** hasta que funcione el acceso por claves
- Si el directorio **/home** estuviese en NFS, hacer **setsebool -P use_nfs_home_dirs 1**
- Recargar los cambios con **systemctl reload sshd**

9.L SSH sin contraseña: acceso desde otro Linux

- Las claves SSH se generan con **ssh-keygen** en la máquina desde la que se vaya a acceder, empleando el usuario que vaya a conectarse. Una vez generadas, se debe copiar la clave pública del cliente al directorio ~/.ssh del usuario correspondiente en la máquina remota:

```
[root@localhost ~]# ssh-keygen -t ecdsa
Generating public/private ecdsa key pair.
Enter file in which to save the key (/root/.ssh/id_ecdsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_ecdsa.
Your public key has been saved in /root/.ssh/id_ecdsa.pub.
The key fingerprint is:
SHA256:g+y2AXwSroYwZUnpbmfc5oSJHHYF6SOIGY/jRsnqtk0 root@localhost.localdomain
The key's randomart image is:
+---[ECDSA 256]---+
|      ...0      |
| .  0. . . .    |
| .*=0.. .       |
| =*00=0+.       |
| *,  +=*+=S     |
| 0= .==* +.     |
| + 0E 0++       |
| +0   . 0.      |
| .....         |
+----[SHA256]-----+
| 101 111 121 131 141 151 161 171 181 191 201 211 221 231 241 251 261 271 281 291 301 311 321 331 341 351 361 371 381 391 401 411 421 431 441 451 461 471 481 491 501 511 521 531 541 551 561 571 581 591 601 611 621 631 641 651 661 671 681 691 701 711 721 731 741 751 761 771 781 791 801 811 821 831 841 851 861 871 881 891 901 911 921 931 941 951 961 971 981 991 1001 1011 1021 1031 1041 1051 1061 1071 1081 1091 1101 1111 1121 1131 1141 1151 1161 1171 1181 1191 1201 1211 1221 1231 1241 1251 1261 1271 1281 1291 1301 1311 1321 1331 1341 1351 1361 1371 1381 1391 1401 1411 1421 1431 1441 1451 1461 1471 1481 1491 1501 1511 1521 1531 1541 1551 1561 1571 1581 1591 1601 1611 1621 1631 1641 1651 1661 1671 1681 1691 1701 1711 1721 1731 1741 1751 1761 1771 1781 1791 1801 1811 1821 1831 1841 1851 1861 1871 1881 1891 1901 1911 1921 1931 1941 1951 1961 1971 1981 1991 2001 2011 2021 2031 2041 2051 2061 2071 2081 2091 2101 2111 2121 2131 2141 2151 2161 2171 2181 2191 2201 2211 2221 2231 2241 2251 2261 2271 2281 2291 2301 2311 2321 2331 2341 2351 2361 2371 2381 2391 2401 2411 2421 2431 2441 2451 2461 2471 2481 2491 2501 2511 2521 2531 2541 2551 2561 2571 2581 2591 2601 2611 2621 2631 2641 2651 2661 2671 2681 2691 2701 2711 2721 2731 2741 2751 2761 2771 2781 2791 2801 2811 2821 2831 2841 2851 2861 2871 2881 2891 2901 2911 2921 2931 2941 2951 2961 2971 2981 2991 3001 3011 3021 3031 3041 3051 3061 3071 3081 3091 3101 3111 3121 3131 3141 3151 3161 3171 3181 3191 3201 3211 3221 3231 3241 3251 3261 3271 3281 3291 3301 3311 3321 3331 3341 3351 3361 3371 3381 3391 3401 3411 3421 3431 3441 3451 3461 3471 3481 3491 3501 3511 3521 3531 3541 3551 3561 3571 3581 3591 3601 3611 3621 3631 3641 3651 3661 3671 3681 3691 3701 3711 3721 3731 3741 3751 3761 3771 3781 3791 3801 3811 3821 3831 3841 3851 3861 3871 3881 3891 3901 3911 3921 3931 3941 3951 3961 3971 3981 3991 4001 4011 4021 4031 4041 4051 4061 4071 4081 4091 4101 4111 4121 4131 4141 4151 4161 4171 4181 4191 4201 4211 4221 4231 4241 4251 4261 4271 4281 4291 4301 4311 4321 4331 4341 4351 4361 4371 4381 4391 4401 4411 4421 4431 4441 4451 4461 4471 4481 4491 4501 4511 4521 4531 4541 4551 4561 4571 4581 4591 4601 4611 4621 4631 4641 4651 4661 4671 4681 4691 4701 4711 4721 4731 4741 4751 4761 4771 4781 4791 4801 4811 4821 4831 4841 4851 4861 4871 4881 4891 4901 4911 4921 4931 4941 4951 4961 4971 4981 4991 5001 5011 5021 5031 5041 5051 5061 5071 5081 5091 5101 5111 5121 5131 5141 5151 5161 5171 5181 5191 5201 5211 5221 5231 5241 5251 5261 5271 5281 5291 5301 5311 5321 5331 5341 5351 5361 5371 5381 5391 5401 5411 5421 5431 5441 5451 5461 5471 5481 5491 5501 5511 5521 5531 5541 5551 5561 5571 5581 5591 5601 5611 5621 5631 5641 5651 5661 5671 5681 5691 5701 5711 5721 5731 5741 5751 5761 5771 5781 5791 5801 5811 5821 5831 5841 5851 5861 5871 5881 5891 5901 5911 5921 5931 5941 5951 5961 5971 5981 5991 6001 6011 6021 6031 6041 6051 6061 6071 6081 6091 6101 6111 6121 6131 6141 6151 6161 6171 6181 6191 6201 6211 6221 6231 6241 6251 6261 6271 6281 6291 6301 6311 6321 6331 6341 6351 6361 6371 6381 6391 6401 6411 6421 6431 6441 6451 6461 6471 6481 6491 6501 6511 6521 6531 6541 6551 6561 6571 6581 6591 6601 6611 6621 6631 6641 6651 6661 6671 6681 6691 6701 6711 6721 6731 6741 6751 6761 6771 6781 6791 6801 6811 6821 6831 6841 6851 6861 6871 6881 6891 6901 6911 6921 6931 6941 6951 6961 6971 6981 6991 7001 7011 7021 7031 7041 7051 7061 7071 7081 7091 7101 7111 7121 7131 7141 7151 7161 7171 7181 7191 7201 7211 7221 7231 7241 7251 7261 7271 7281 7291 7301 7311 7321 7331 7341 7351 7361 7371 7381 7391 7401 7411 7421 7431 7441 7451 7461 7471 7481 7491 7501 7511 7521 7531 7541 7551 7561 7571 7581 7591 7601 7611 7621 7631 7641 7651 7661 7671 7681 7691 7701 7711 7721 7731 7741 7751 7761 7771 7781 7791 7801 7811 7821 7831 7841 7851 7861 7871 7881 7891 7901 7911 7921 7931 7941 7951 7961 7971 7981 7991 8001 8011 8021 8031 8041 8051 8061 8071 8081 8091 8101 8111 8121 8131 8141 8151 8161 8171 8181 8191 8201 8211 8221 8231 8241 8251 8261 8271 8281 8291 8301 8311 8321 8331 8341 8351 8361 8371 8381 8391 8401 8411 8421 8431 8441 8451 8461 8471 8481 8491 8501 8511 8521 8531 8541 8551 8561 8571 8581 8591 8601 8611 8621 8631 8641 8651 8661 8671 8681 8691 8701 8711 8721 8731 8741 8751 8761 8771 8781 8791 8801 8811 8821 8831 8841 8851 8861 8871 8881 8891 8901 8911 8921 8931 8941 8951 8961 8971 8981 8991 9001 9011 9021 9031 9041 9051 9061 9071 9081 9091 9101 9111 9121 9131 9141 9151 9161 9171 9181 9191 9201 9211 9221 9231 9241 9251 9261 9271 9281 9291 9301 9311 9321 9331 9341 9351 9361 9371 9381 9391 9401 9411 9421 9431 9441 9451 9461 9471 9481 9491 9501 9511 9521 9531 9541 9551 9561 9571 9581 9591 9601 9611 9621 9631 9641 9651 9661 9671 9681 9691 9701 9711 9721 9731 9741 9751 9761 9771 9781 9791 9801 9811 9821 9831 9841 9851 9861 9871 9881 9891 9901 9911 9921 9931 9941 9951 9961 9971 9981 9991 10001 10011 10021 10031 10041 10051 10061 10071 10081 10091 10101 10111 10121 10131 10141 10151 10161 10171 10181 10191 10201 10211 10221 10231 10241 10251 10261 10271 10281 10291 10301 10311 10321 10331 10341 10351 10361 10371 10381 10391 10401 10411 10421 10431 10441 10451 10461 10471 10481 10491 10501 10511 10521 10531 10541 10551 10561 10571 10581 10591 10601 10611 10621 10631 10641 10651 10661 10671 10681 10691 10701 10711 10721 10731 10741 10751 10761 10771 10781 10791 10801 10811 10821 10831 10841 10851 10861 10871 10881 10891 10901 10911 10921 10931 10941 10951 10961 10971 10981 10991 11001 11011 11021 11031 11041 11051 11061 11071 11081 11091 11101 11111 11121 11131 11141 11151 11161 11171 11181 11191 11201 11211 11221 11231 11241 11251 11261 11271 11281 11291 11301 11311 11321 11331 11341 11351 11361 11371 11381 11391 11401 11411 11421 11431 11441 11451 11461 11471 11481 11491 11501 11511 11521 11531 11541 11551 11561 11571 11581 11591 11601 11611 11621 11631 11641 11651 11661 11671 11681 11691 11701 11711 11721 11731 11741 11751 11761 11771 11781 11791 11801 11811 11821 11831 11841 11851 11861 11871 11881 11891 11901 11911 11921 11931 11941 11951 11961 11971 11981 11991 12001 12011 12021 12031 12041 12051 12061 12071 12081 12091 12101 12111 12121 12131 12141 12151 12161 12171 12181 12191 12201 12211 12221 12231 12241 12251 12261 12271 12281 12291 12301 12311 12321 12331 12341 12351 12361 12371 12381 12391 12401 12411 12421 12431 12441 12451 12461 12471 12481 12491 12501 12511 12521 12531 12541 12551 12561 12571 12581 12591 12601 12611 12621 12631 12641 12651 12661 12671 12681 12691 12701 12711 12721 12731 12741 12751 12761 12771 12781 12791 12801 12811 12821 12831 12841 12851 12861 12871 12881 12891 12901 12911 12921 12931 12941 12951 12961 12971 12981 12991 13001 13011 13021 13031 13041 13051 13061 13071 13081 13091 13101 13111 13121 13131 13141 13151 13161 13171 13181 13191 13201 13211 13221 13231 13241 13251 13261 13271 13281 13291 13301 13311 13321 13331 13341 13351 13361 13371 13381 13391 13401 13411 13421 13431 13441 13451 13461 13471 13481 13491 13501 13511 13521 13531 13541 13551 13561 13571 13581 13591 13601 13611 13621 13631 13641 13651 13661 13671 13681 13691 13701 13711 13721 13731 13741 13751 13761 13771 13781 13791 13801 13811 13821 13831 13841 13851 13861 13871 13881 13891 13901 13911 13921 13931 13941 13951 13961 13971 13981 13991 14001 14011 14021 14031 14041 14051 14061 14071 14081 14091 14101 14111 14121 14131 14141 14151 14161 14171 14181 14191 14201 14211 14221 14231 14241 14251 14261 14271 14281 14291 14301 14311 14321 14331 14341 14351 14361 14371 14381 14391 14401 14411 14421 14431 14441 14451 14461 14471 14481 14491 14501 14511 14521 14531 14541 14551 14561 14571 14581 14591 14601 14611 14621 14631 14641 14651 14661 14671 14681 14691 14701 14711 14721 14731 14741 14751 14761 14771 14781 14791 14801 14811 14821 14831 14841 14851 14861 14871 14881 14891 14901 14911 14921 14931 14941 14951 14961 14971 14981 14991 15001 15011 15021 15031 15041 15051 15061 15071 15081 15091 15101 15111 15121 15131 15141 15151 15161 15171 15181 15191 15201 15211 15221 15231 15241 15251 15261 15271 15281 15291 15301 15311 15321 15331 15341 15351 15361 15371 15381 15391 15401 15411 15421 15431 15441 15451 15461 15471 15481 15491 15501 15511 15521 15531 15541 15551 15561 15571 15581 15591 15601 15611 15621 15631 15641 15651 15661 15671 15681 15691 15701 15711 15721 15731 15741 15751 15761 15771 15781 15791 15801 15811 15821 15831 15841 15851 15861 15871 15881 15891 15901 15911 15921 15931 15941 15951 15961 15971 15981 15991 16001 16011 16021 16031 16041 16051 16061 16071 16081 16091 16101 16111 16121 16131 16141 16151 16161 16171 16181 16191 16201 16211 16221 16231 16241 16251 16261 16271 16281 16291 16301 16311 16321 16331 16341 16351 16361 16371 16381 16391 16401 16411 16421 16431 16441 16451 16461 16471 16481 16491 16501 16511 16521 16531 16541 16551 16561 16571 16581 16591 16601 16611 16621 16631 16641 16651 16661 16671 16681 16691 16701 16711 16721 16731 16741 16751 16761 16771 16781 16791 16801 16811 16821 16831 16841 16851 16861 16871 16881 16891 16901 16911 16921 16931 16941 16951 16961 16971 16981 16991 17001 17011 17021 17031 17041 17051 17061 17071 17081 17091 17101 17111 17121 17131 17141 17151 17161 17171 17181 17191 17201 17211 17221 17231 17241 17251 17261 17271 17281 17291 17301 17311 17321 17331 17341 17351 17361 17371 17381 17391 17401 17411 17421 17431 17441 17451 17461 17471 17481 17491 17501 17511 17521 17531 17541 17551 17561 17571 17581 17591 17601 17611 17621 17631 17641 17651 17661 17671 17681 17691 17701 17711 17721 17731 17741 17751 17761 17771 17781 17791 17801 17811 17821 17831 17841 17851 17861 17871 17881 17891 17901 17911 17921 17931 17941 17951 17961 17971 17981 17991 18001 18011 18021 18031 18041 18051 18061 18071 18081 18091 18101 18111 18121 18131 18141 18151 18161 18171 18181 18191 18201 18211 18221 18231 18241 18251 18261 18271 18281 18291 18301 18311 18321 18331 18341 18351 18361 18371 18381 18391 18401 18411 18421 18431 18441 18451 18461 18471 18481 18491 18501 18511 18521 18531 18541 18551 18561 18571 18581 18591 18601 18611 18621 18631 18641 18651 18661 18671 18681 18691 18701 18711 18721 18731 18741 18751 18761 18771 18781 18791 18801 18811 18821 18831 18841 18851 18861 18871 18881 18891 18901 18911 18921 18931 18941 18951 18961 18971 18981 18991 19001 19011 19021 19031 19041 19051 19061 19071 19081 19091 19101 19111 19121 19131 19141 19151 19161 19171 19181 19191 19201 19211 19221 19231 19241 19251 19261 19271 19281 19291 19301 19311 19321 19331 19341 19351 19361 19371 19381 19391 19401 19411 19421 19431 19441 19451 19461 19471 19481 19491 19501 19511 19521 19531 19541 19551 19561 19571 19581 19591 19601 19611 19621 19631 19641 19651 19661 19671 19681 19691 19701 19711 19721 19731 19741 19751 19761 19771 19781 19791 19801 19811 19821 19831 19841 19851 19861 19871 19881 19891 19901 19911 19921 19931 19941 19951 19961 19971 19981 19991 20001 20011 20021 20031 20041 20051 20061 20071 20081 20091 20101 20111 20121 20131 20141 20151 20161 20171 20181 20191 20201 20211 20221 20231 20241 20251 20261 20271 20281 20291 20301 20311 20321 20331 20341 20351 20361 20371 20381 20391 20401 20411 20421 20431 20441 20451 20461 20471 20481 20491 20501 20511 20521 20531 20541 20551 20561 20571 20581 20591 20601 20611 20621 20631 20641 20651 20661 20671 20681 20691 20701 20711 20721 20731 20741 20751 20761 20771 20781 20791 20801 20811 20821 20831 20841 20851 20861 20871 20881 20891 20901 20911 20921 20931 20941 20951 20961 20971 20981 20991 21001 21011 21021 21031 21041 21051 21061 21071 21081 21091 21101 21111 21121 21131 21141 21151 21161 21171 21181 21191 21201 21211 21221 21231 21241 21251 21261 21271 21281 21291 21301 21311 21321 21331 21341 21351 21361 21371 21381 21391 21401 21411 21421 21431 21441 21451 21461 21471 21481 21491 21501 21511 21521 21531 21541 21551 21561 21571 21581 21591 21601 21611 21621 21631 21641 21651 21661 21671 21681 21691 21701 21711 21721 21731 21741 21751 21761 21771 21781 21791 21801 21
```

9.L SSH sin contraseña: acceso desde otro Linux

- Se usa la orden `ssh-copy-id` para copiar la clave generada a la máquina remota. Este paso copia el archivo `id_ecdsa.pub` al directorio `.ssh` del usuario del servidor

```
root@localhost ~]# ssh-copy-id root@localhost
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_ecdsa.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
root@localhost's password:

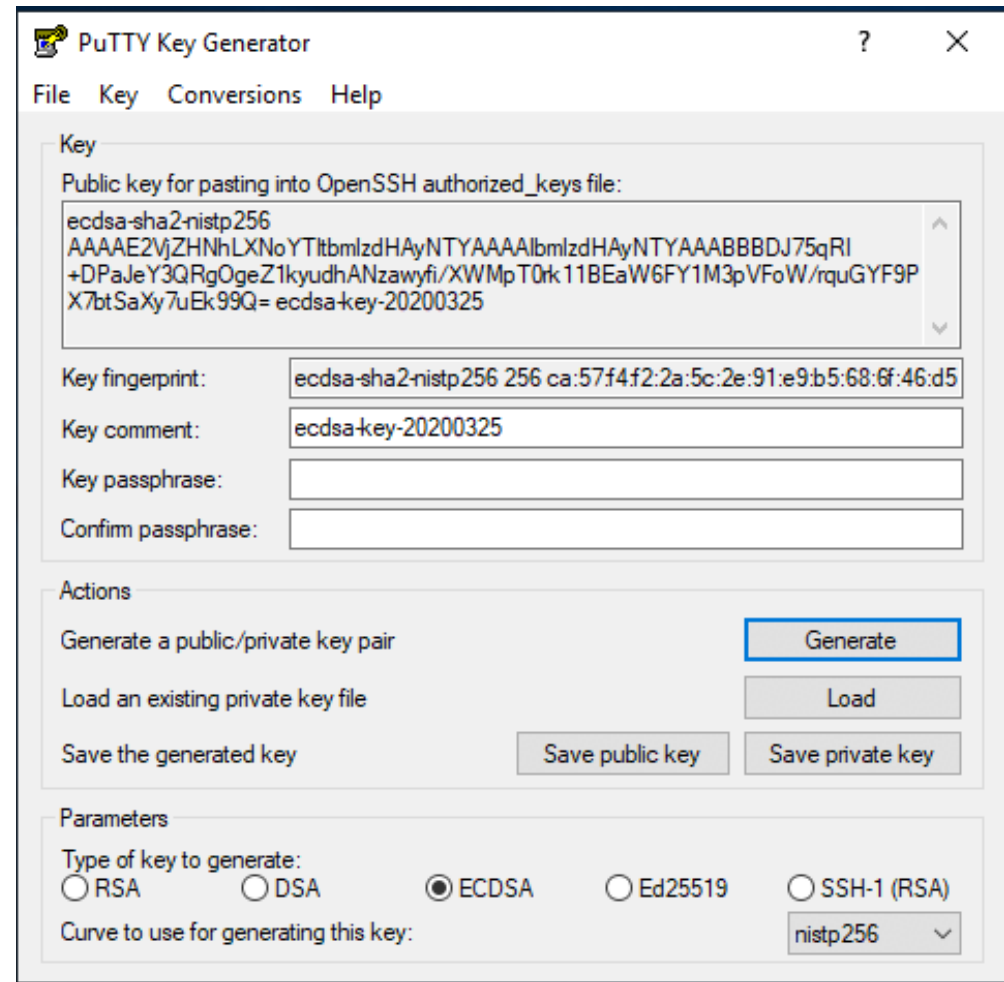
Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'root@localhost'"
and check to make sure that only the key(s) you wanted were added.

root@localhost ~]# cat .ssh/
authorized_keys  id_ecdsa          id_ecdsa.pub      known_hosts
root@localhost ~]# cat .ssh/id_ecdsa.pub
ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBAUywoIhwWiPSaEUGp6g00w1+Hf atRi0yJLqdv0Dk91NF3
eQEmMC0T1UMb3UmPkrK0PgKhbAcKGY4= root@localhost.localdomain
root@localhost ~]# cat .ssh/known_hosts
localhost ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBAG9xDjoZZEUmtHU31xRdGDdSzPWTb40AN6
ECayC+kvCTuub9wQb8NeJPoRwFSa.jyLSwftoAfa/k=
root@localhost ~]#
```

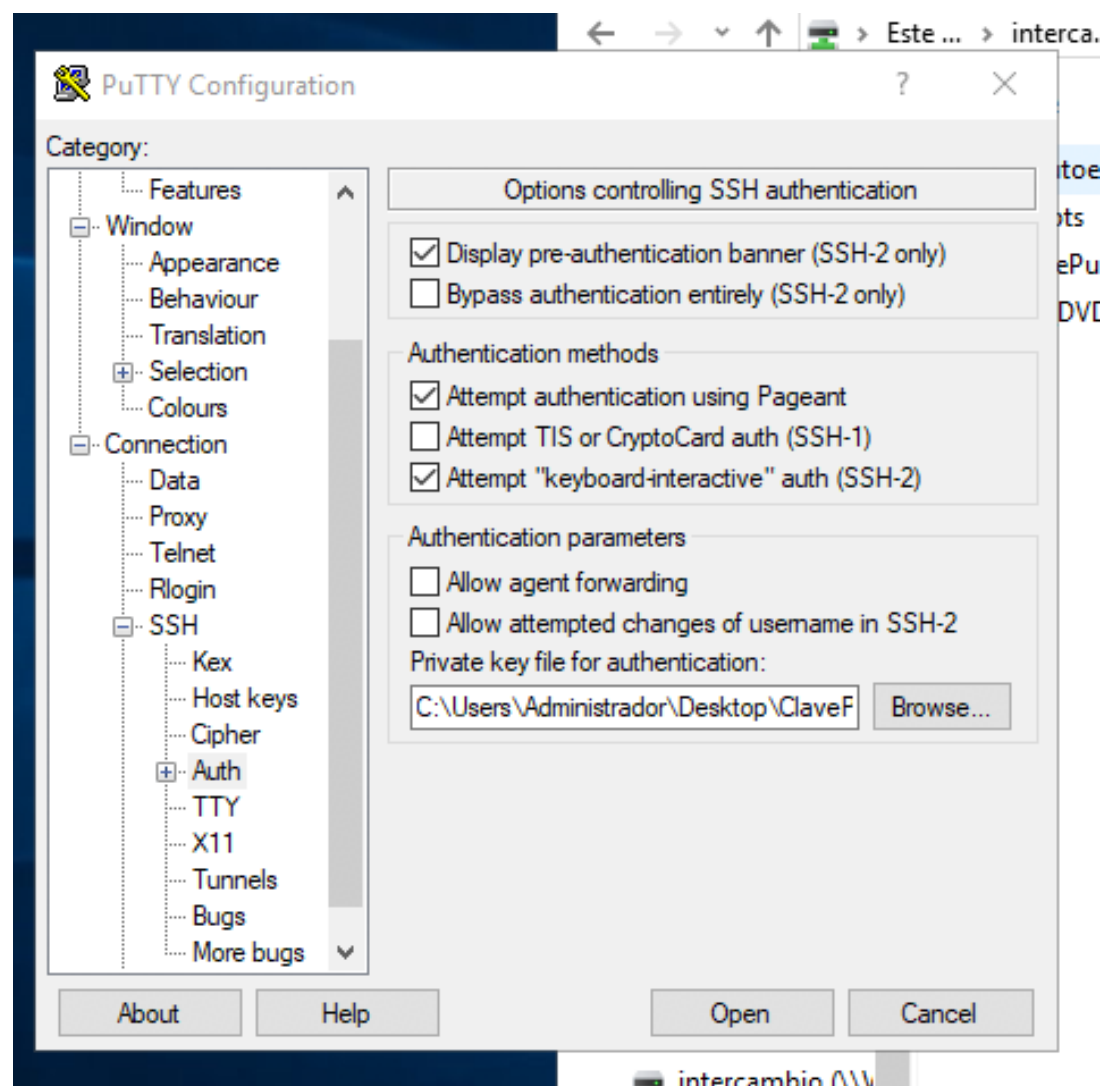

9.W SSH sin contraseña: acceso desde PuTTY

- La pareja de claves pública/privada se generan con PuTTY Generator. Se le puede indicar una contraseña (recomendable para guardar la clave privada)
- La clave pública debe convertirse al formato **OpenSSH con `ssh-keygen -i -f clavePutty.pub > claveOpenSSH.pub`**
- La clave convertida se debe añadir al final del archivo **`.ssh/authorized_keys`**

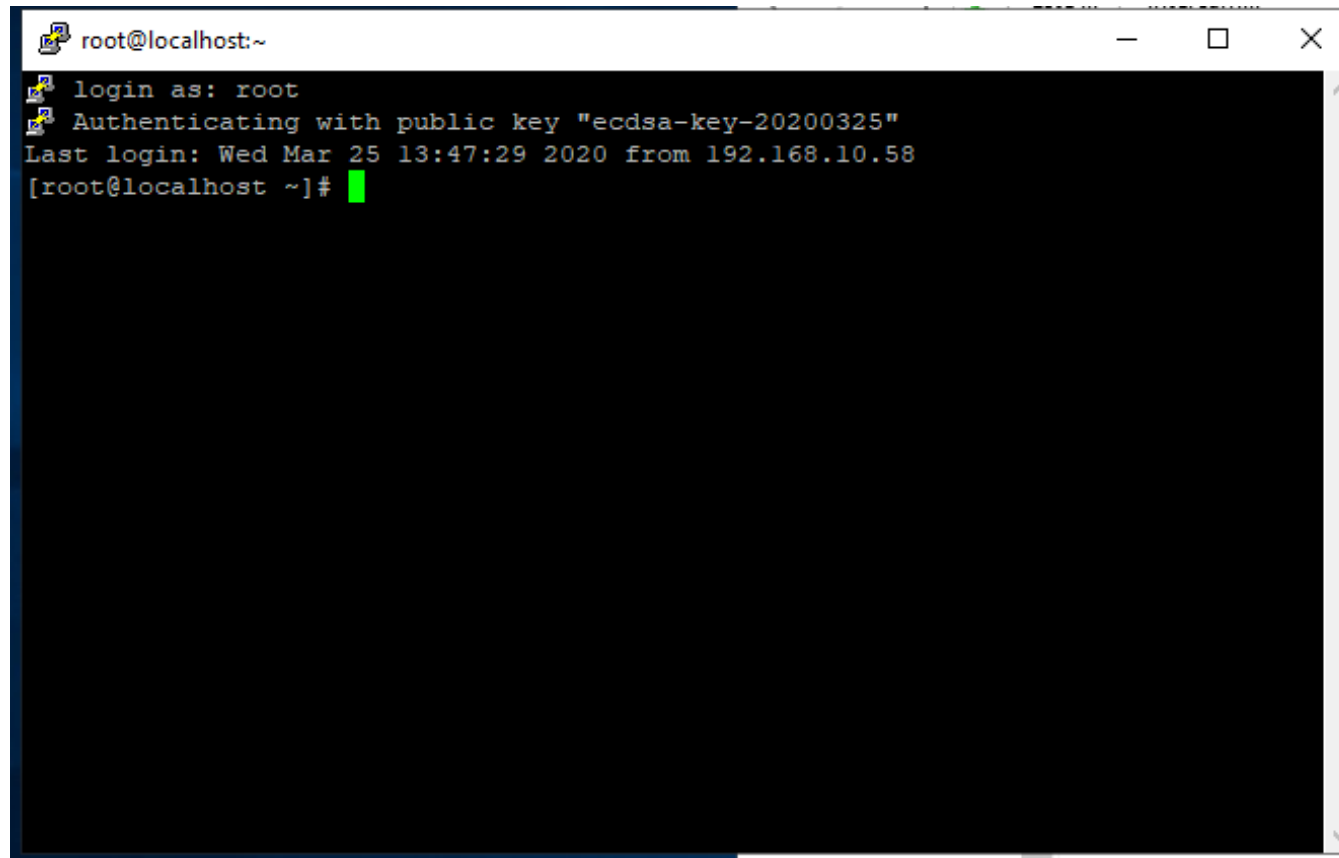


9. SSH sin contraseña: acceso desde PuTTY

- Para conectarse al host se indica el fichero con la clave privada de la máquina windows (la que se ha generado con PuTTY Generator) en la sección Auth de SSH



9.W SSH sin contraseña: acceso desde PuTTY



A screenshot of a PuTTY terminal window titled 'root@localhost:~'. The terminal shows the following text: 'login as: root', 'Authenticating with public key "ecdsa-key-20200325"', and 'Last login: Wed Mar 25 13:47:29 2020 from 192.168.10.58'. The prompt is '[root@localhost ~]#' followed by a green cursor. The window has standard window controls (minimize, maximize, close) in the top right corner.

```
root@localhost:~  
login as: root  
Authenticating with public key "ecdsa-key-20200325"  
Last login: Wed Mar 25 13:47:29 2020 from 192.168.10.58  
[root@localhost ~]#
```

- La conexión no solicita contraseña; se emplea la clave pública del cliente windows y se compara con la almacenada en **authorized_keys**

9.L Tunel SSH

- `ssh -f usuario@servidor -L 2000:servidor:25 -N`
 - `-f`: ir a background
 - `-L 2000:servidor:25` es de la forma `puertolocal:host:puertoremoto`
 - `-N`: no ejecutar un intérprete de comandos en el sistema remoto
- Reenvía el puerto 2000 del ordenador local al puerto 25 del servidor, encriptando la comunicación
- Permite acceder al puerto 25 del servidor si estamos tras un firewall que no bloquee el puerto 22

9.W. Servidor OpenSSH en Windows Server 2019

- Desde interfaz de usuario de configuración:

Configuración/Aplicaciones/Aplicaciones y características/Administrar funciones opcionales

Agregar una característica

Seleccionar "Servidor de OpenSSH" y click a "Instalar"

La instalación creará y habilitará una regla de firewall denominada "OpenSSH-Server-In-TCP", que permite tráfico entrante en el puerto 22

9.W. Servidor OpenSSH en Windows Server 2019

- Desde powershell: Comprobar si está instalado e instalar característica:

```
PS C:\Users\Administrador> Get-WindowsCapability -Online | ? Name -like 'OpenSSH*'

Name : OpenSSH.Client~~~~0.0.1.0
State : Installed

Name : OpenSSH.Server~~~~0.0.1.0
State : NotPresent
```

```
PS C:\Users\Administrador> Add-WindowsCapability -Online -Name OpenSSH.Server

Path      :
Online    : True
RestartNeeded : False
```

9.W Configuración del servidor SSH

```
PS C:\Users\Administrador> Start-Service sshd
PS C:\Users\Administrador> Set-Service -Name sshd -StartupType 'Automatic'
PS C:\Users\Administrador> Get-NetFirewallRule -Name *ssh*

Name                           : OpenSSH-Server-In-TCP
DisplayName                     : OpenSSH SSH Server (sshd)
Description                     : Inbound rule for OpenSSH SSH Server (sshd)
DisplayGroup                    : OpenSSH Server
Group                           : OpenSSH Server
Enabled                         : True
Profile                         : Any
Platform                       : {}
Direction                      : Inbound
Action                         : Allow
EdgeTraversalPolicy             : Block
LooseSourceMapping              : False
LocalOnlyMapping               : False
Owner                           :
PrimaryStatus                   : OK
Status                         : Se analizó la regla correctamente desde el almacén. (65536)
EnforcementStatus              : NotApplicable
PolicyStoreSource               : PersistentStore
PolicyStoreSourceType           : Local
```

- A partir de este punto se puede conectar desde cualquier host remoto con ssh administrador@xx.xx.xx.xx

9.W Servidor SSH

```
Microsoft Windows [Versión 10.0.17763.1098]
(c) 2018 Microsoft Corporation. Todos los derechos reservados.

administrador@WIN-1RAA0711J1U C:\Users\Administrador>dir
El volumen de la unidad C no tiene etiqueta.
El número de serie del volumen es: C423-DFB5

Directorio de C:\Users\Administrador

25/03/2020  12:24    <DIR>          .
25/03/2020  12:24    <DIR>          ..
25/03/2020  20:20    <DIR>          3D Objects
25/03/2020  20:20    <DIR>          Contacts
25/03/2020  20:20    <DIR>          Desktop
25/03/2020  20:20    <DIR>          Documents
25/03/2020  20:20    <DIR>          Downloads
25/03/2020  20:20    <DIR>          Favorites
25/03/2020  20:20    <DIR>          Links
25/03/2020  20:20    <DIR>          Music
25/03/2020  20:20    <DIR>          Pictures
25/03/2020  20:20    <DIR>          Saved Games
25/03/2020  20:20    <DIR>          Searches
25/03/2020  20:20    <DIR>          Videos
                0 archivos                0 bytes
                14 dirs 16.956.723.200 bytes libres

administrador@WIN-1RAA0711J1U C:\Users\Administrador>
```

- El shell que se usa en el servidor de OpenSSH de Windows es el mismo que el shell de comandos de windows

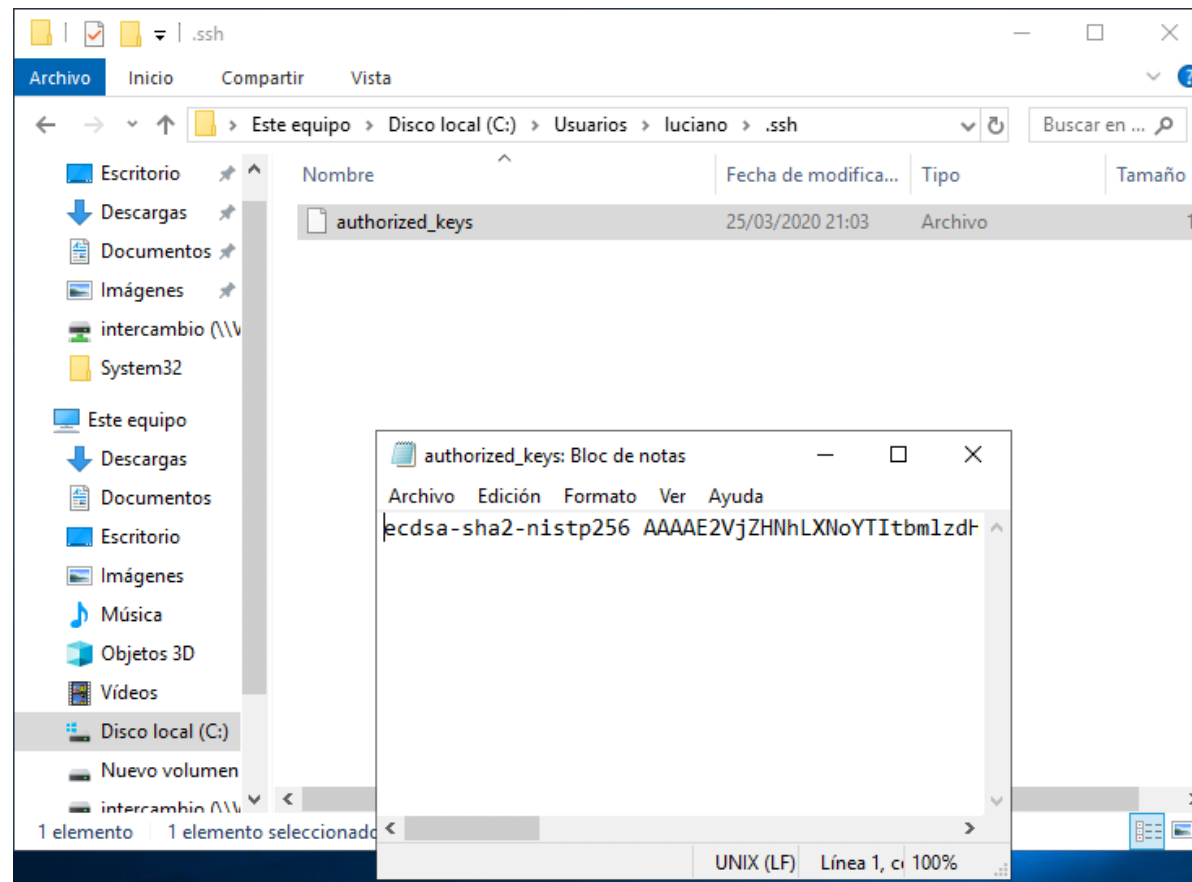
9.W Servidor SSH

- Para acceder con claves públicas/privadas: si se desea utilizar el **cliente** OpenSSH de Windows, el comando `ssh-keygen` crea dos archivos en la carpeta `.ssh` del usuario
- Si se accede desde Linux o con PuTTY, este paso no es necesario

```
PS C:\Users\Administrador>
PS C:\Users\Administrador> ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (C:\Users\Administrador\.ssh/id_rsa):
Created directory 'C:\Users\Administrador\.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in C:\Users\Administrador\.ssh/id_rsa.
Your public key has been saved in C:\Users\Administrador\.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:u207S6IJGvYrIvKduFGqGwwfdCwakBliAIjZZG6sOjc administrador@WIN-1RAA0711J1V
The key's randomart image is:
+---[RSA 2048]-----+
|@Oo
|X+..
|. * o
| * o
|+ . S
|. + .
|o E o o .
|++ .B * o =o
|oo=+O++ ..++
+---[SHA256]-----+
PS C:\Users\Administrador>
```

9.W Servidor SSH

- La clave pública del cliente debe añadirse manualmente al archivo `.ssh\authorized_keys`, excepto si el usuario está en el grupo de administradores.



9.W Servidor SSH

- Si el usuario está en el grupo de administradores, el archivo correcto es C:\ProgramData\ssh\administrators_authorized_keys
- Este archivo solamente puede ser accesible por los usuarios del grupo de Administradores y por la cuenta SYSTEM (ver siguiente transparencia)

```
PS C:\ProgramData\ssh> dir

Directorio: C:\ProgramData\ssh

Mode                LastWriteTime         Length Name
----                -
d-----          25/03/2020    20:23             logs
-a----          25/03/2020    21:03             188 administrators_authorized_keys
-a----          25/03/2020    20:23              6 sshd.pid
-a----          25/03/2020    20:08          2253 sshd_config
-a----          25/03/2020    20:23           672 ssh_host_dsa_key
-a----          25/03/2020    20:23           626 ssh_host_dsa_key.pub
-a----          25/03/2020    20:23           227 ssh_host_ecdsa_key
-a----          25/03/2020    20:23           198 ssh_host_ecdsa_key.pub
-a----          25/03/2020    20:23           432 ssh_host_ed25519_key
-a----          25/03/2020    20:23           118 ssh_host_ed25519_key.pub
-a----          25/03/2020    20:23          1679 ssh_host_rsa_key
-a----          25/03/2020    20:23           418 ssh_host_rsa_key.pub

c|
PS C:\ProgramData\ssh> 
```

9.W Servidor SSH

- El siguiente script de PowerShell pone los permisos correctos al archivo (si está instalado en inglés debe cambiarse la línea

```
$administratorsRule = New-Object  
system.security.accesscontrol.filesystemaccessrule("Administradores","FullControl","Allow")
```

```
cPS C:\ProgramData\ssh> $administratorsRule = New-Object system.security.accesscontrol.filesystemaccessrule("Administradores","FullControl","Allow")  
PS C:\ProgramData\ssh> $acl.SetAccessRule($administratorsRule)  
PS C:\ProgramData\ssh> $acl.SetAccessRule($systemRule)  
PS C:\ProgramData\ssh> $acl | Set-Acl  
PS C:\ProgramData\ssh> $acl = Get-Acl C:\ProgramData\ssh\administrators_authorized_keys  
PS C:\ProgramData\ssh> $acl.SetAccessRuleProtection($true,$false)  
PS C:\ProgramData\ssh> $administratorsRule = New-Object system.security.accesscontrol.filesystemaccessrule("Administradores","FullControl","Allow")  
PS C:\ProgramData\ssh> $systemRule = New-Object system.security.accesscontrol.filesystemaccessrule("SYSTEM","FullControl","Allow")  
PS C:\ProgramData\ssh> $acl.SetAccessRule($administratorsRule)  
PS C:\ProgramData\ssh> $acl.SetAccessRule($systemRule)  
PS C:\ProgramData\ssh> $acl | Set-Acl  
PS C:\ProgramData\ssh>
```

9.L VNC

- Servidor VNC: atiende peticiones en el puerto 5900 y siguientes
- Se elige una contraseña con `vncpasswd`
- Se edita `/etc/sysconfig/vncservers`, se activa con `service vncserver start`
- Se edita `/home/nombre-usuario/.vnc/xstartup` para configurar la sesión X
- Debería usarse siempre con un túnel ssh

```
# Uncomment the line below to start a VNC server on display :1
# as my 'myusername' (adjust this to your own). You will also
# need to set a VNC password; run 'man vncpasswd' to see how
# to do that.
#
# DO NOT RUN THIS SERVICE if your local area network is
# untrusted!  For a secure way of using VNC, see
# <URL:http://www.uk.research.att.com/vnc/sshvnc.html>.
```

```
VNCSERVERS="1:fred 2:joe"
```

```
# fred's VNC options
VNCSERVERARGS[1]="-geometry 1024x768"
```

```
# joe's VNC options
VNCSERVERARGS[2]="-geometry 1280x1024"
```

9.L VNC en Centos 8

- En primer lugar debemos de instalar el cliente grafico

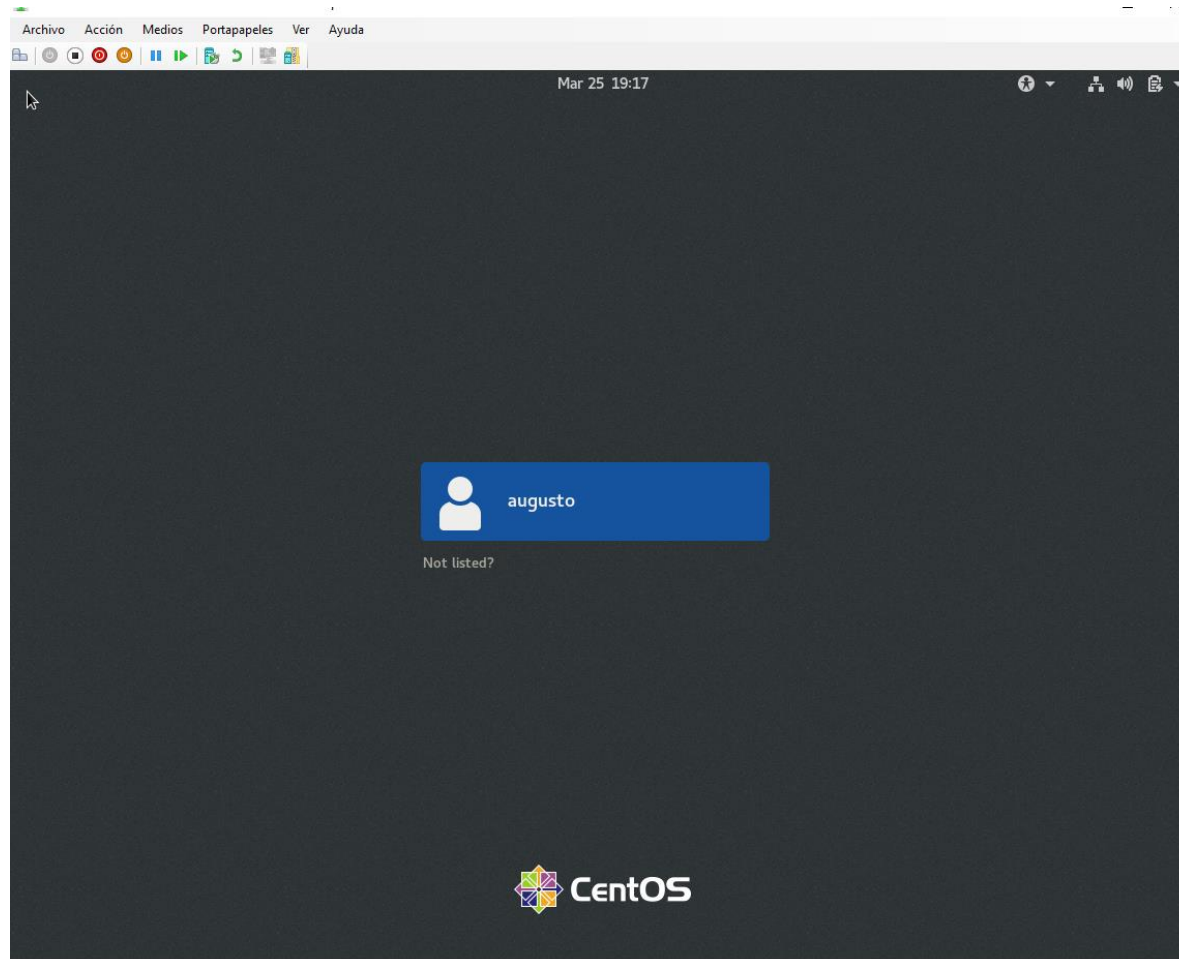
```
[root@MiWiFi-R3P-srv ~]# sudo dnf groupinstall "Server with GUI"
```

```
[root@MiWiFi-R3P-srv ~]# systemctl set-default graphical.target  
Removed /etc/systemd/system/default.target.  
Created symlink /etc/systemd/system/default.target → /usr/lib/systemd/system/graphical.target.  
[root@MiWiFi-R3P-srv ~]#
```

- Reiniciamos la maquina y veremos como se inicia con interfaz grafica.

9.L VNC en Centos 8

- Interfaz Grafica



9.L VNC en Centos 8

- Una vez instalado el entorno grafico instalamos un servidor VNC , por ejemplo TIGER VNC, que es open Source

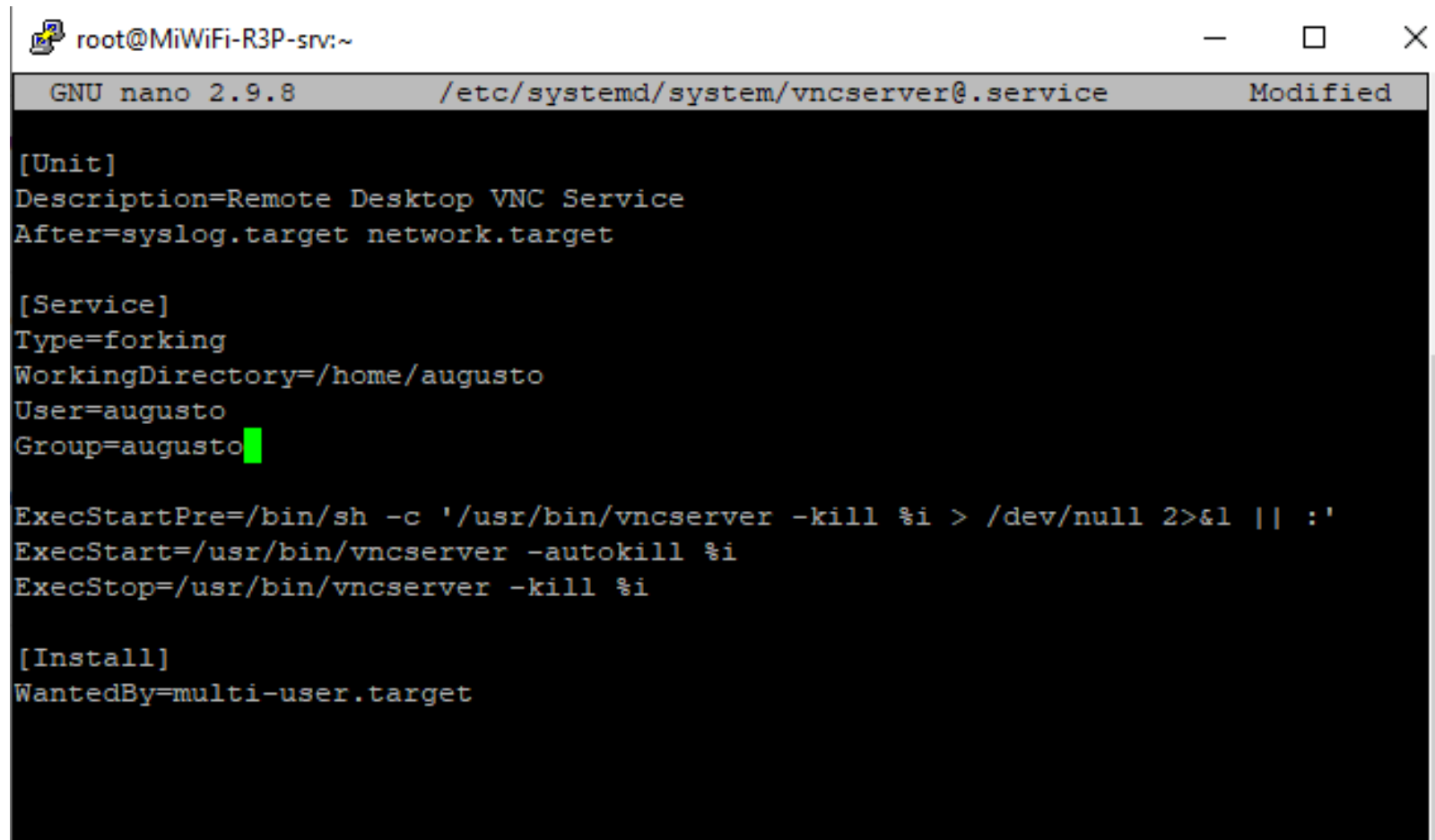
```
augusto@MiWiFi-R3P-srv ~]$ su root
root@MiWiFi-R3P-srv agosto)# dnf install tigervnc-server tigervnc-server-module -y
```

- Una vez instalado nos logeamos con el usuario que accedera al escritorio, en este caso agosto y cambiamos su contraseña

```
Installed:
  tigervnc-server-1.9.0-12.el8_1.x86_64      tigervnc-server-module-1.9.0-12.el8_1.x86_64
Complete!
[root@MiWiFi-R3P-srv agosto]# su agosto
[augusto@MiWiFi-R3P-srv ~]$ vncpasswd
Password:
Verify:
Would you like to enter a view-only password (y/n)? n
A view-only password is not used
[augusto@MiWiFi-R3P-srv ~]$
```


9.L VNC en Centos 8

- Creamos el fichero de configuración en [/etc/systemd/vncserver@.service](#)



```
root@MiWiFi-R3P-srv:~  
GNU nano 2.9.8 /etc/systemd/system/vncserver@.service Modified  
[Unit]  
Description=Remote Desktop VNC Service  
After=syslog.target network.target  
  
[Service]  
Type=forking  
WorkingDirectory=/home/augusto  
User=augusto  
Group=augusto  
  
ExecStartPre=/bin/sh -c '/usr/bin/vncserver -kill %i > /dev/null 2>&1 || :'  
ExecStart=/usr/bin/vncserver -autokill %i  
ExecStop=/usr/bin/vncserver -kill %i  
  
[Install]  
WantedBy=multi-user.target
```

9.L VNC en Centos 8

- Reiniciamos y habilitamos el servicio VNC en la display 1

```
[root@MiWiFi-R3P-srv ~]# systemctl daemon-reload
[root@MiWiFi-R3P-srv ~]# systemctl start vncserver@:1.service
[root@MiWiFi-R3P-srv ~]# systemctl enable vncserver@:1.service
Created symlink /etc/systemd/system/multi-user.target.wants/vncserver@:1.service
→ /etc/systemd/system/vncserver@.service.
[root@MiWiFi-R3P-srv ~]#
```

- Comprobamos que todo esta correcto

```
root@MiWiFi-R3P-srv:~
● vncserver@:1.service - Remote Desktop VNC Service
   Loaded: loaded (/etc/systemd/system/vncserver@.service; enabled; vendor preset: disabled)
   Active: active (running) since Wed 2020-03-25 19:32:22 EDT; 5min ago
     Tasks: 158 (limit: 23890)
    Memory: 217.6M
    CGroup: /system.slice/system-vncserver.slice/vncserver@:1.service
            └─4788 /usr/bin/Xvnc :2 -auth /home/augusto/.Xauthority -desktop MiWiFi-R3P-srv:2 (augusto) -fp
            └─4796 sh -c (/home/augusto/.vnc/xstartup; /usr/bin/vncserver -kill :2) >> '/home/augusto/.vnc/
            └─4797 /bin/sh /home/augusto/.vnc/xstartup
            └─4798 /usr/libexec/gnome-session-binary
            └─4807 dbus-launch --sh-syntax --exit-with-session
            └─4808 /usr/bin/dbus-daemon --syslog --fork --print-pid 6 --print-address 8 --session
            └─4817 /usr/bin/ssh-agent /etc/X11/xinit/Xclients
```

9.L VNC en Centos 8

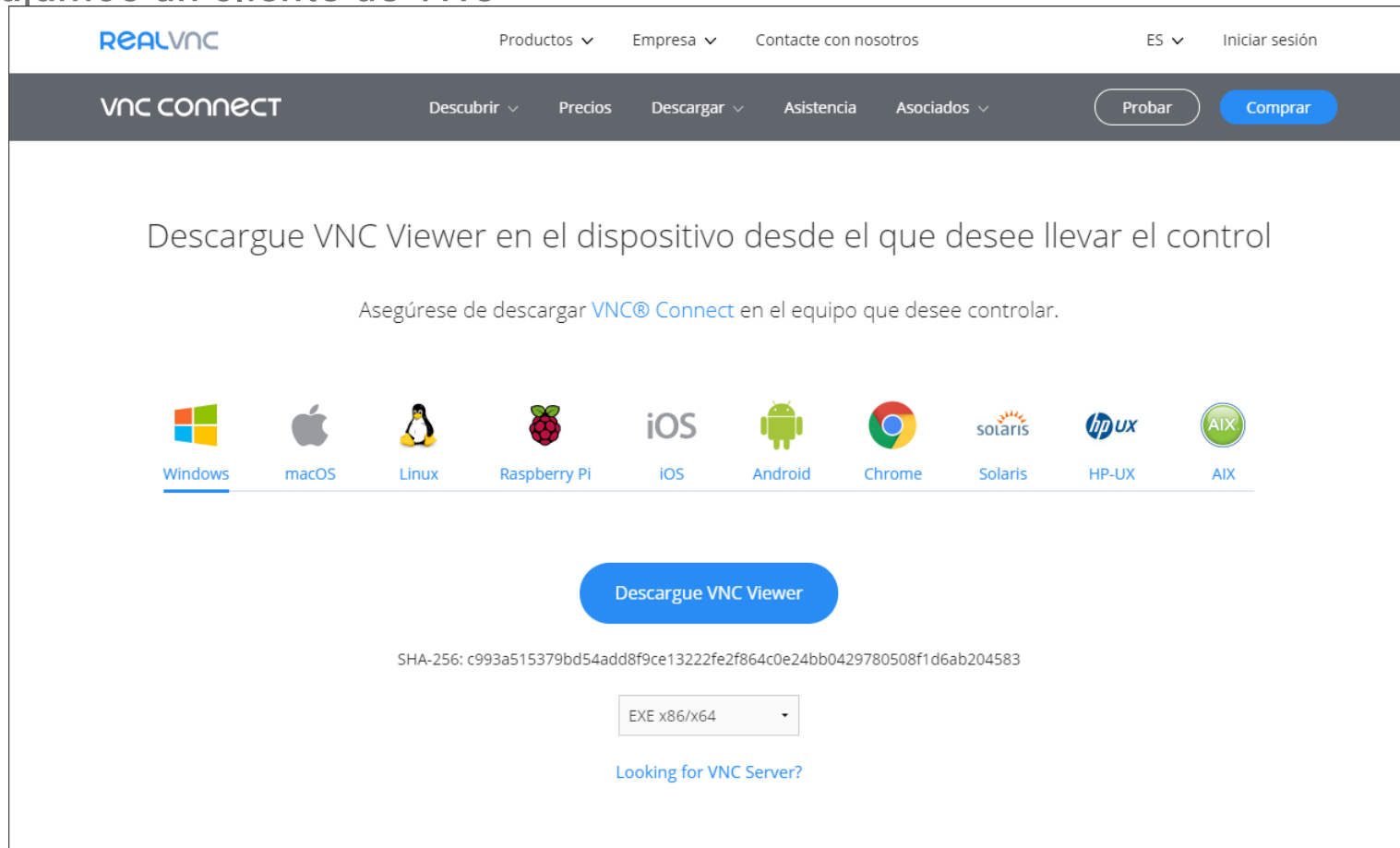
- Creamos las reglas de firewall pertinentes y lo reiniciamos

```
root@MiWiFi-R3P-srv:~  
[root@MiWiFi-R3P-srv ~]# firewall-cmd --permanent --add-port=5901/tcp  
success  
[root@MiWiFi-R3P-srv ~]# firewall-cmd --reload  
success  
[root@MiWiFi-R3P-srv ~]#
```

- VNC por defecto escucha en el puerto 5900+n , siendo n el número de pantalla, en este caso seria el 5901

9.L VNC en Centos 8

- Nos bajamos un cliente de VNC



The screenshot shows the RealVNC website's download page. At the top, there is a navigation bar with the RealVNC logo and links for 'Productos', 'Empresa', 'Contacte con nosotros', 'ES', and 'Iniciar sesión'. Below this is a secondary navigation bar with 'vnc connect' and links for 'Descubrir', 'Precios', 'Descargar', 'Asistencia', and 'Asociados', along with 'Probar' and 'Comprar' buttons. The main content area features the text 'Descargue VNC Viewer en el dispositivo desde el que desee llevar el control' and 'Asegúrese de descargar VNC® Connect en el equipo que desee controlar.' Below this is a row of icons for various operating systems: Windows, macOS, Linux, Raspberry Pi, iOS, Android, Chrome, Solaris, HP-UX, and AIX. A large blue button labeled 'Descargue VNC Viewer' is centered below the icons. Underneath the button is the SHA-256 hash: 'c993a515379bd54add8f9ce13222fe2f864c0e24bb0429780508f1d6ab204583'. A dropdown menu shows 'EXE x86/x64'. At the bottom, there is a link that says 'Looking for VNC Server?'.

REALVNC

Productos ▾ Empresa ▾ Contacte con nosotros ES ▾ Iniciar sesión

vnc connect Descubrir ▾ Precios Descargar ▾ Asistencia Asociados ▾ Probar Comprar

Descargue VNC Viewer en el dispositivo desde el que desee llevar el control

Asegúrese de descargar VNC® Connect en el equipo que desee controlar.

Windows macOS Linux Raspberry Pi iOS Android Chrome Solaris HP-UX AIX

Descargue VNC Viewer

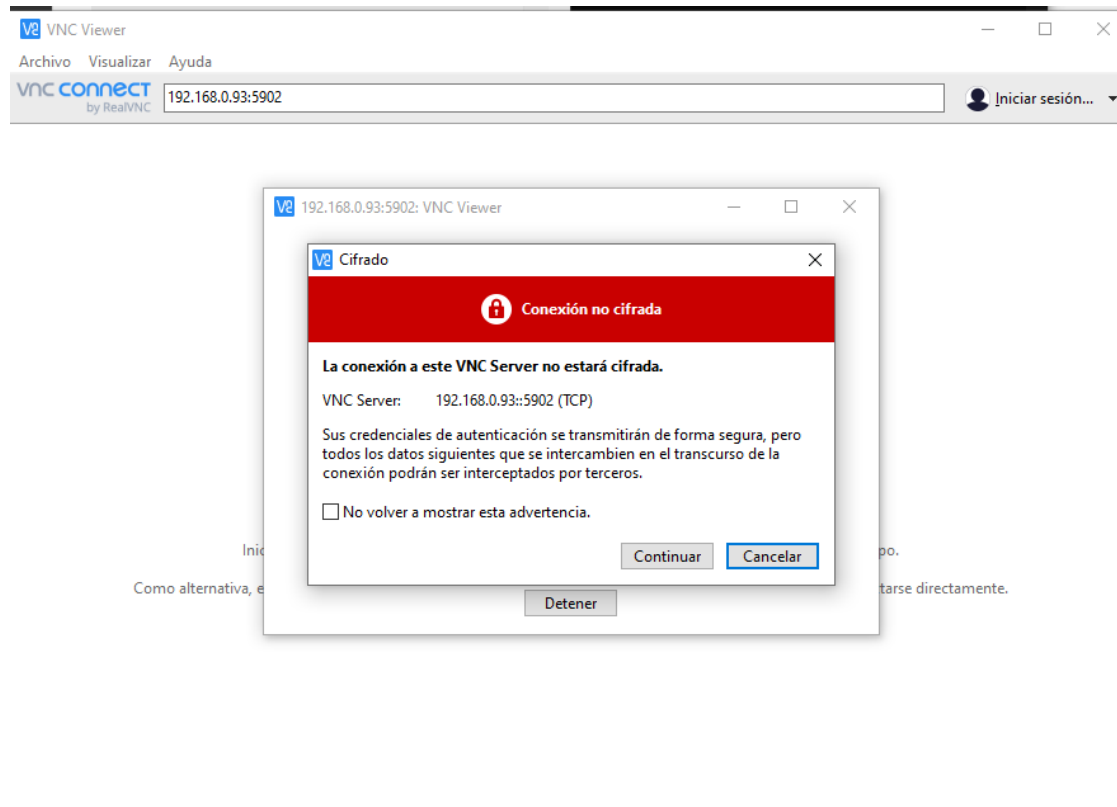
SHA-256: c993a515379bd54add8f9ce13222fe2f864c0e24bb0429780508f1d6ab204583

EXE x86/x64 ▾

[Looking for VNC Server?](#)

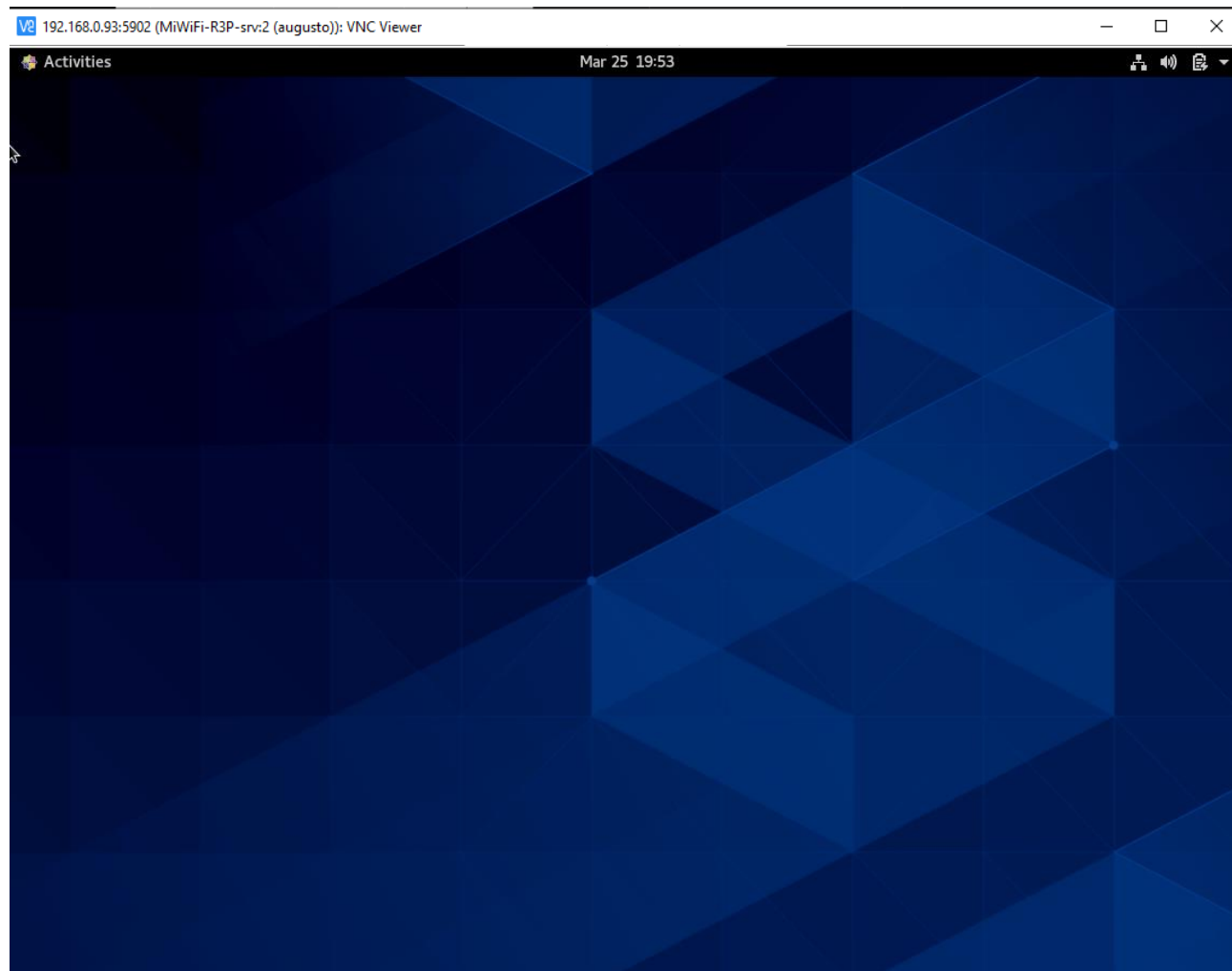
9.L VNC en Centos 8

- Nos salta un aviso de conexión sin cifrar (lo solucionaremos ahora)



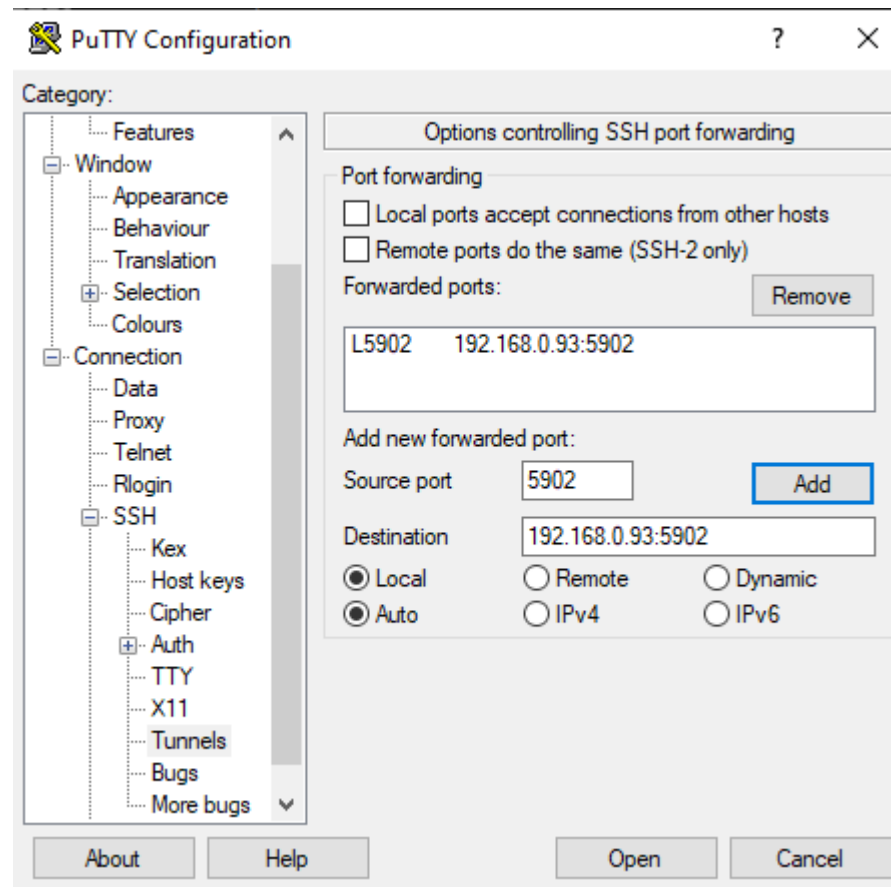
9.L VNC en Centos 8

- Nos salta un aviso de conexión sin cifrar (lo solucionaremos ahora)



9.L VNC en Centos 8

- Para solucionar el aviso de cifrado, bastaría con pasar la conexión por un túnel ssh , seria tan sencillo como ir al Putty y Crearlo



9.W Servidor Remote Desktop

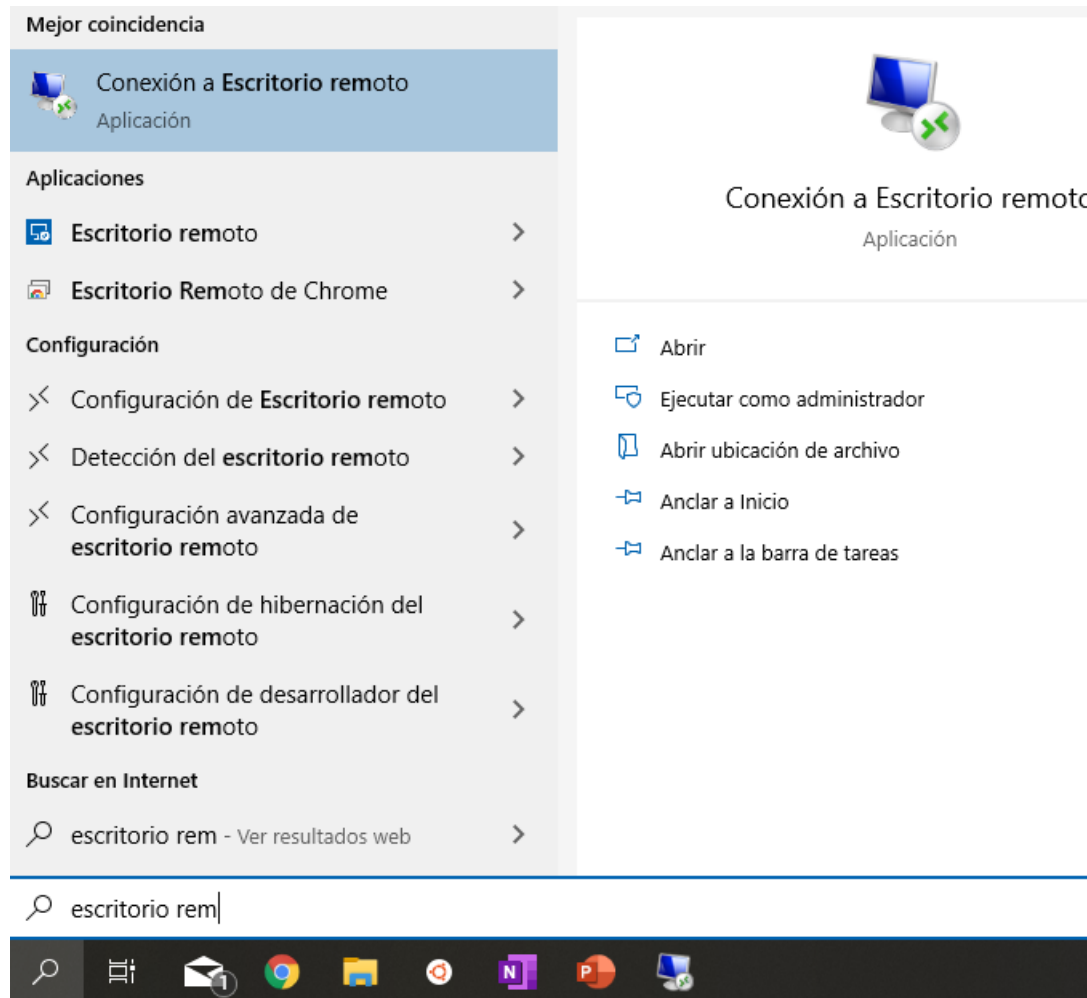
- Es un protocolo propietario desarrollado por Microsoft que nos permite comunicarnos con la ejecución de una aplicación (cliente) y un servidor Windows (aunque también puede ser tu computadora personal)
- Emplea el puerto TCP 3389 en el lado servidor
- Permite interaccionar con la maquina como si estuviéramos accediendo a ella de forma directa (debería ser “transparente al usuario”)
- Permite la compresión de la información intercambiada (para mejorar el rendimiento en las redes menos veloces)

9.W Servidor Remote Desktop

- Características :
 - Soporta colores de hasta 32 bits.
 - Cifrado de 128 bits utilizando el algoritmo RC4
 - Redireccionamiento de audio (permite escuchar lo que emite la maquina)
 - Permite portapapeles compartido
- Versiones más modernas (>6.0)
 - Soporte para TLS en ambos lados (Seguridad a nivel de transporte)
 - Mejora del ancho de banda
 - Otras mejoras (Soporte de varios monitores)

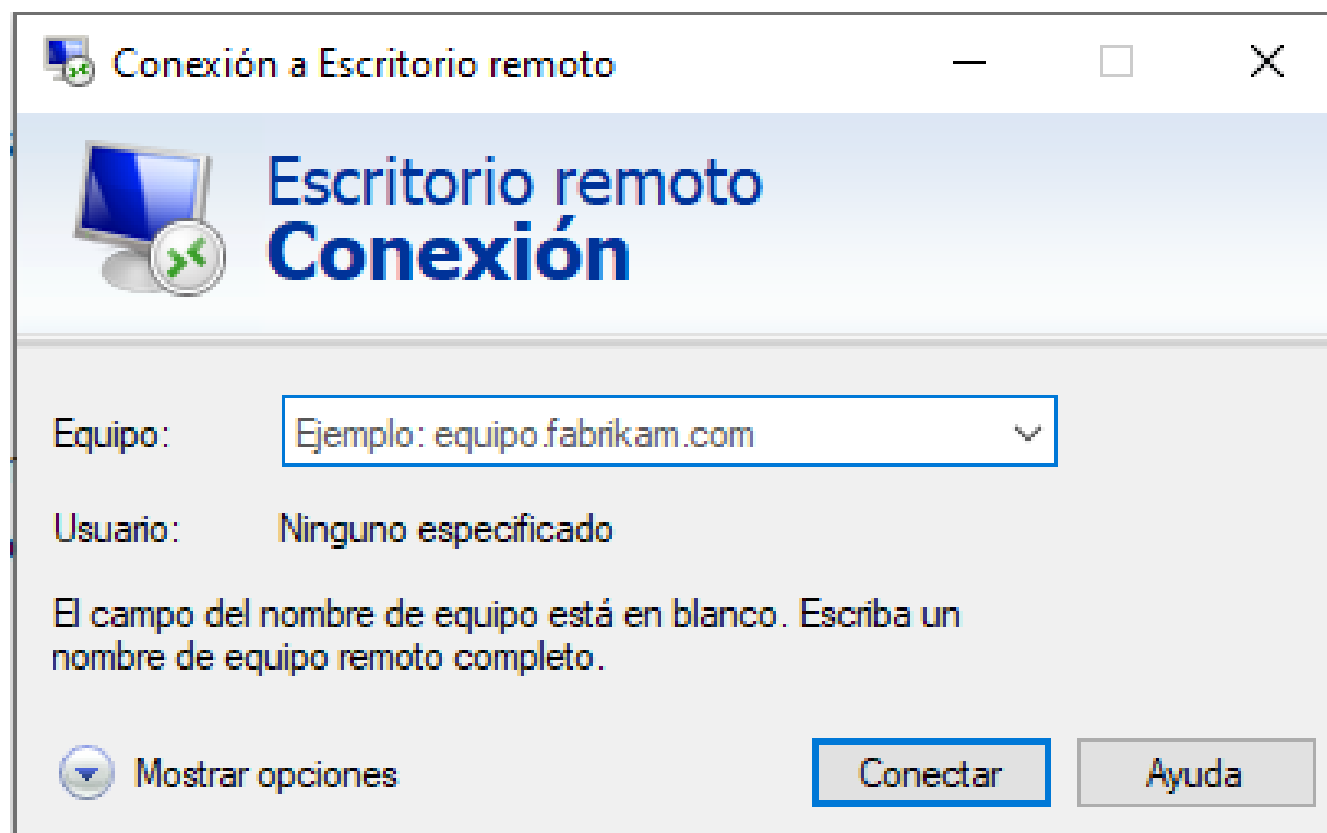
9.W Cliente Remote Desktop

- ¿Cómo accedo en Windows al cliente de escritorio remoto?



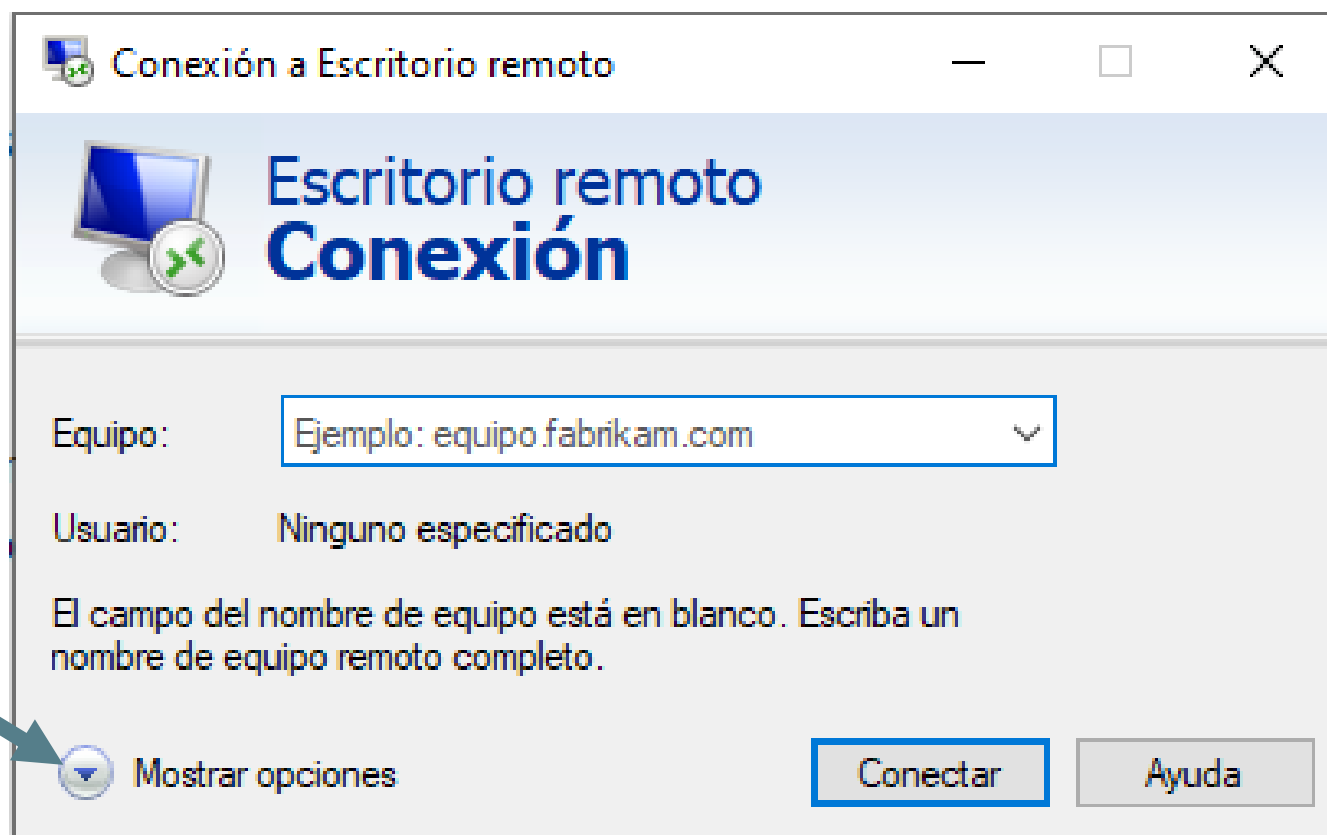
9.W Cliente Remote Desktop

- Versión clásica



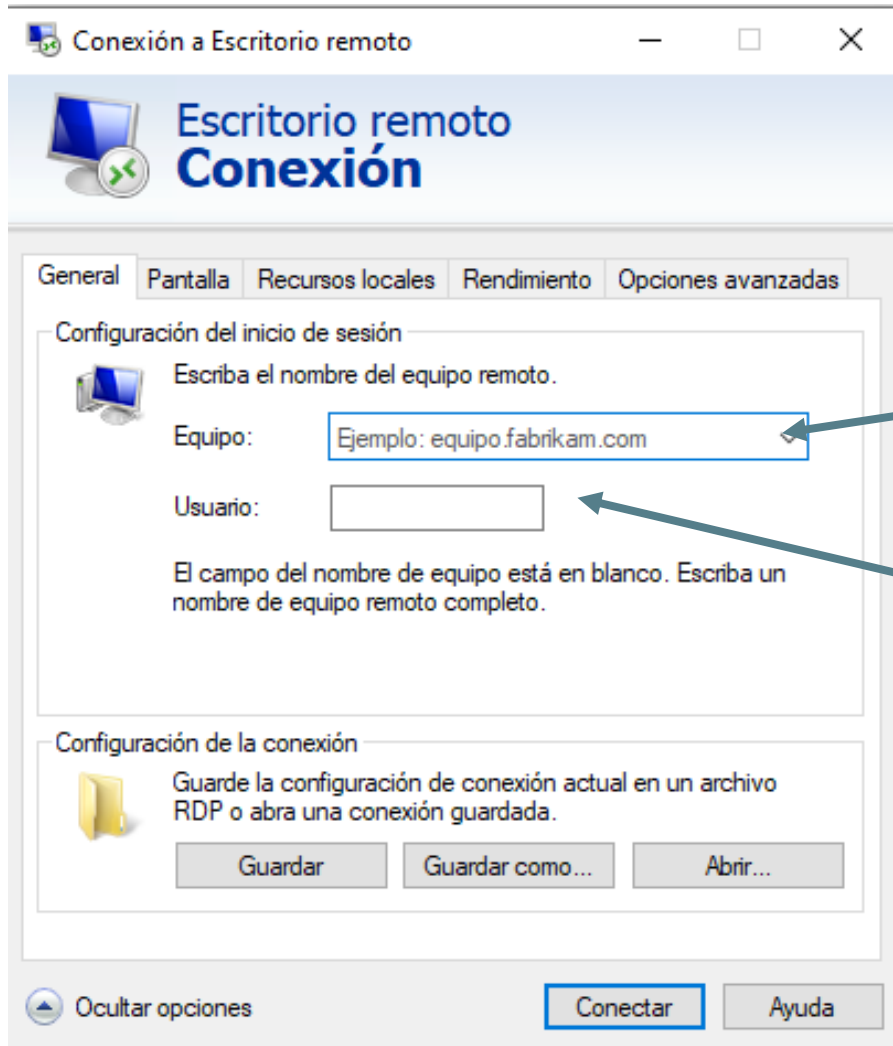
9.W Cliente Remote Desktop

- Versión clásica



9.W Cliente Remote Desktop

- Versión clásica



Conexión a Escritorio remoto

Escritorio remoto
Conexión

General | Pantalla | Recursos locales | Rendimiento | Opciones avanzadas

Configuración del inicio de sesión

Escriba el nombre del equipo remoto.

Equipo:

Usuario:

El campo del nombre de equipo está en blanco. Escriba un nombre de equipo remoto completo.

Configuración de la conexión

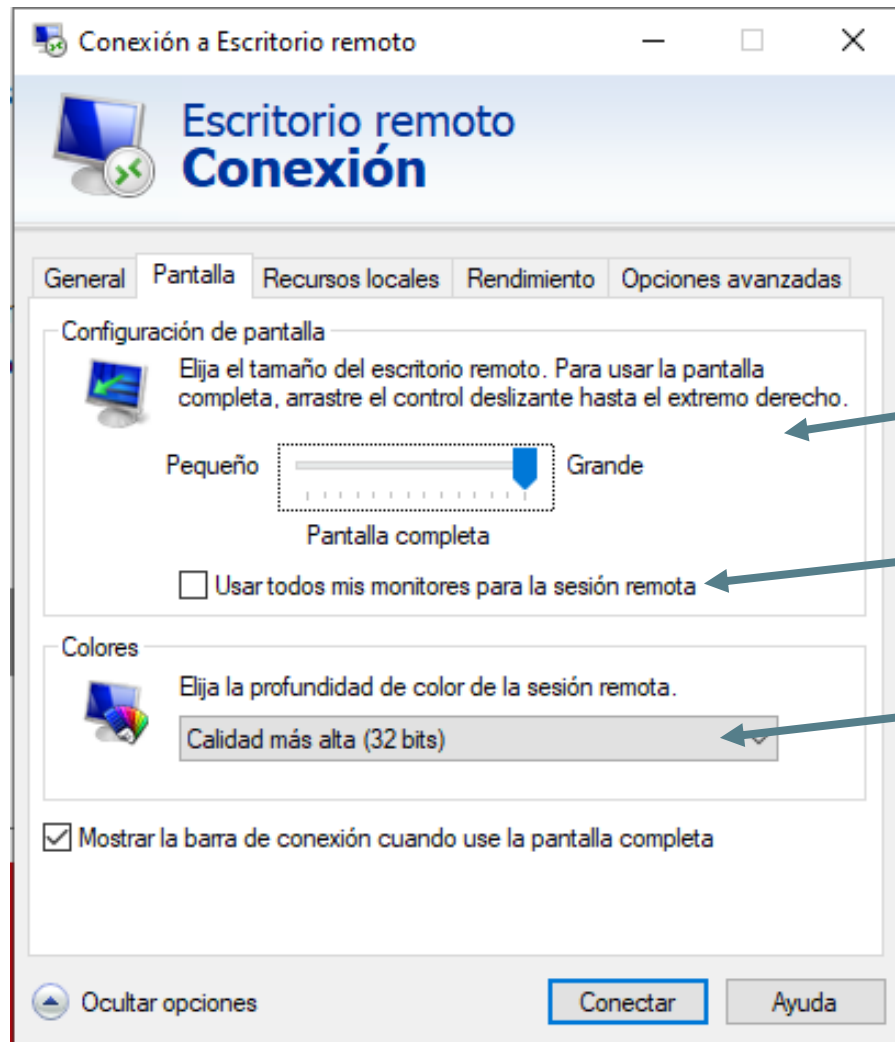
Guarde la configuración de conexión actual en un archivo RDP o abra una conexión guardada.

Introducimos aquí
la IP de la maquina
a la que queremos
conectarnos :
Ej: 156.35.119.33

Introducimos el
usuario que
queremos utilizar

9.W Cliente Remote Desktop

- Versión clásica



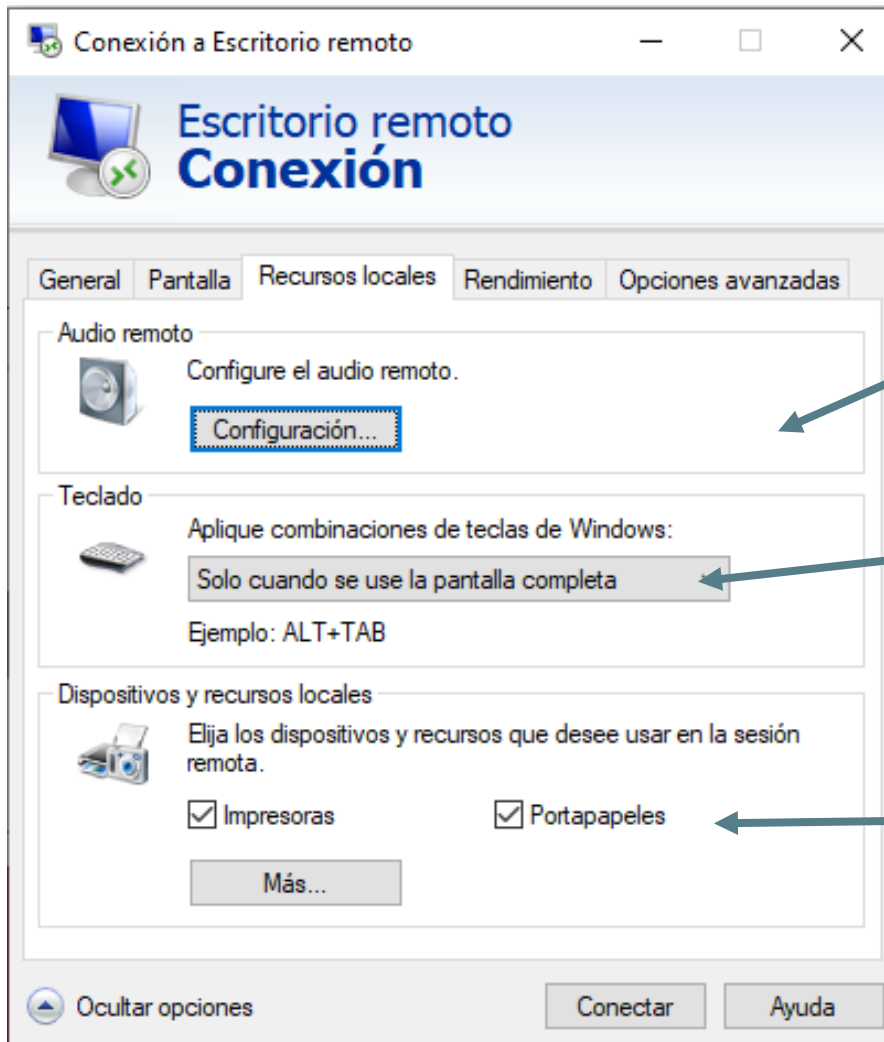
También podemos
cambiar la resolución
de la pantalla

Soporte para varios
monitores

Podemos cambiar la
profundidad de color
(a menos peor se verá)

9.W Cliente Remote Desktop

- Versión clásica



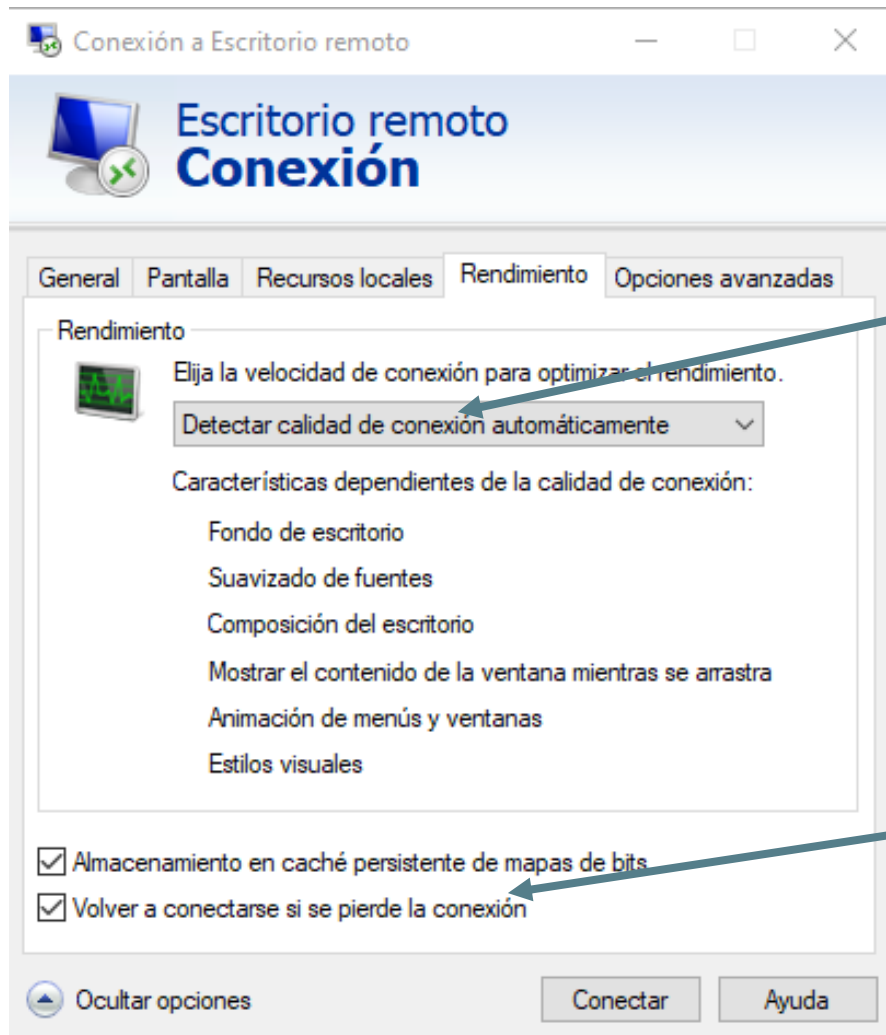
Podemos elegir si se reproducirá el audio en nuestro equipo (o si se grabará) (Defecto SI Y NO)

Habilitar / deshabilitar atajos de teclado y combinaciones de teclas

Recursos que se emplearan en la sesión remota

9.W Cliente Remote Desktop

- Versión clásica

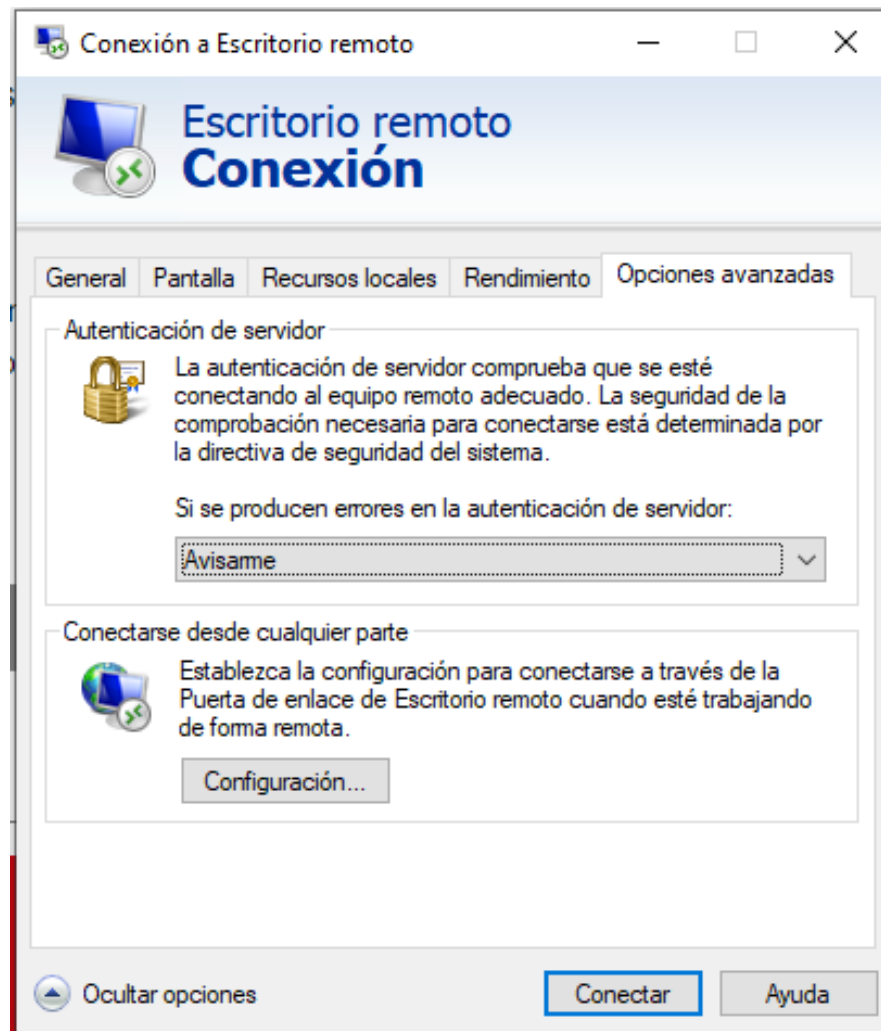


Características adaptativas (depende del ancho de red/carga las habilita/deshabilita)

Cacheado y reconexión (carga más rápida y más fluida)

9.W Cliente Remote Desktop

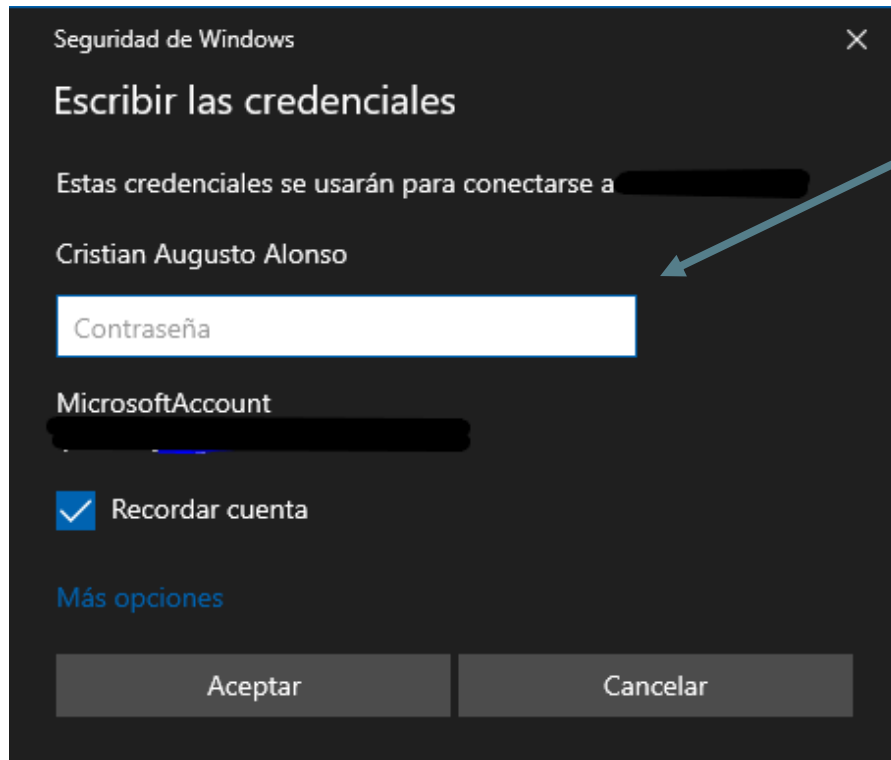
- Versión clásica



Configuraciones avanzadas como la puerta de enlace y comprobaciones de la autenticación del servidor

9.W Cliente Remote Desktop

- Versión clásica

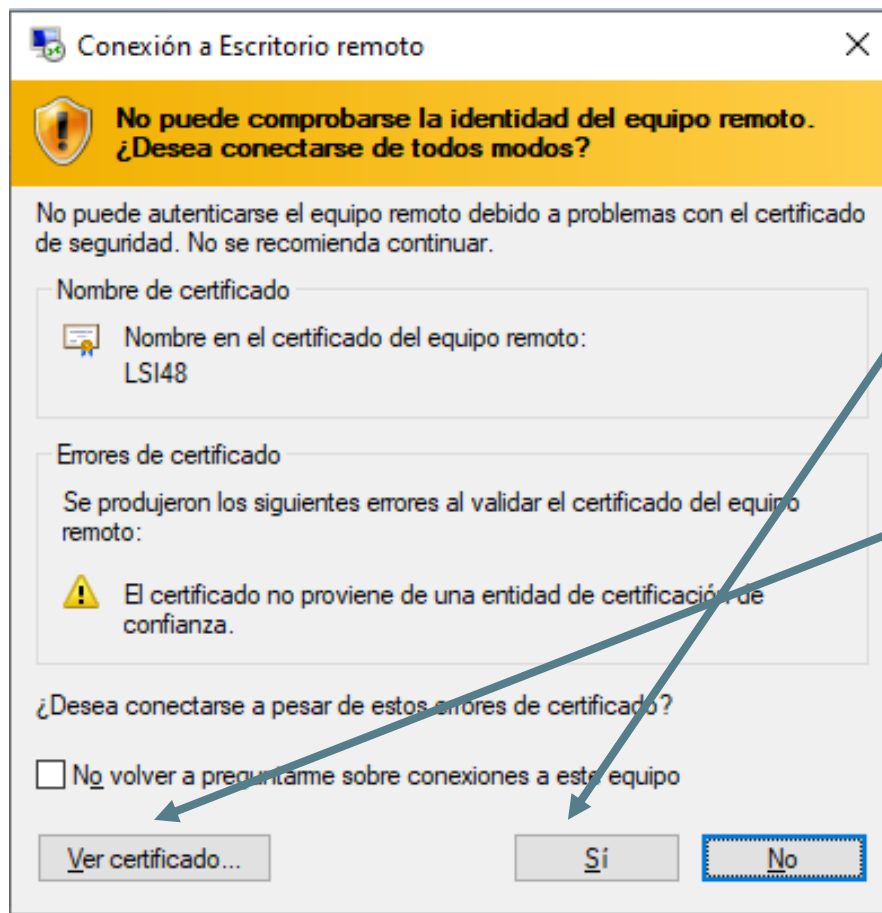


The image shows a Windows Security dialog box titled 'Seguridad de Windows' with a close button (X) in the top right corner. The main heading is 'Escribir las credenciales'. Below this, it says 'Estas credenciales se usarán para conectarse a' followed by a redacted name. The username 'Cristian Augusto Alonso' is displayed. There is a text input field labeled 'Contraseña' (Password). Below the password field, it says 'MicrosoftAccount' followed by a redacted email address. There is a checked checkbox labeled 'Recordar cuenta' (Remember account). At the bottom left, there is a link 'Más opciones' (More options). At the bottom, there are two buttons: 'Aceptar' (Accept) and 'Cancelar' (Cancel).

Debemos introducir la contraseña para acceder

9.W Cliente Remote Desktop

- Versión clásica

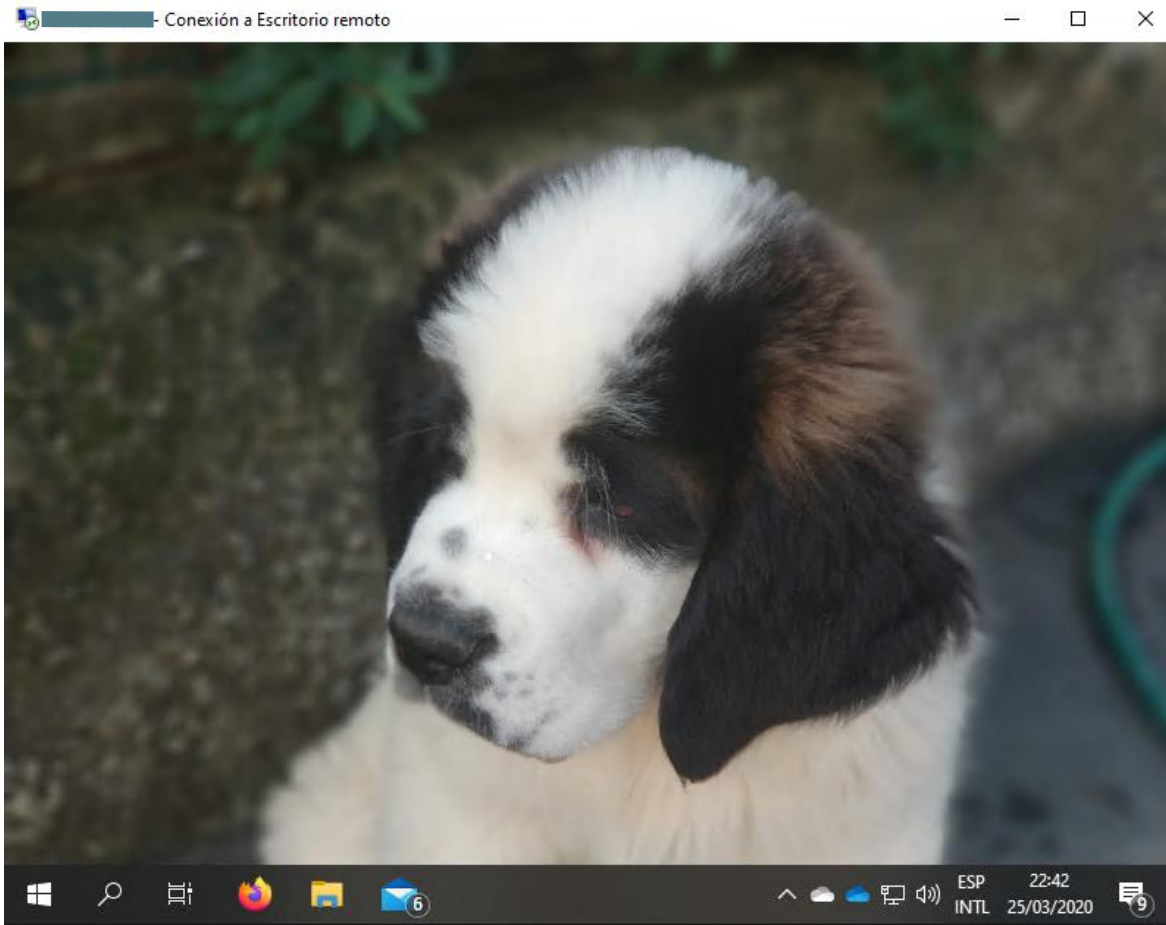


Deberemos de instalar el certificado (para en futuras conexiones tener el equipo ya declarado como "de confianza")

Se podría ver el certificado y por ende comprobar ante alguna entidad la validez del mismo

9.W Cliente Remote Desktop

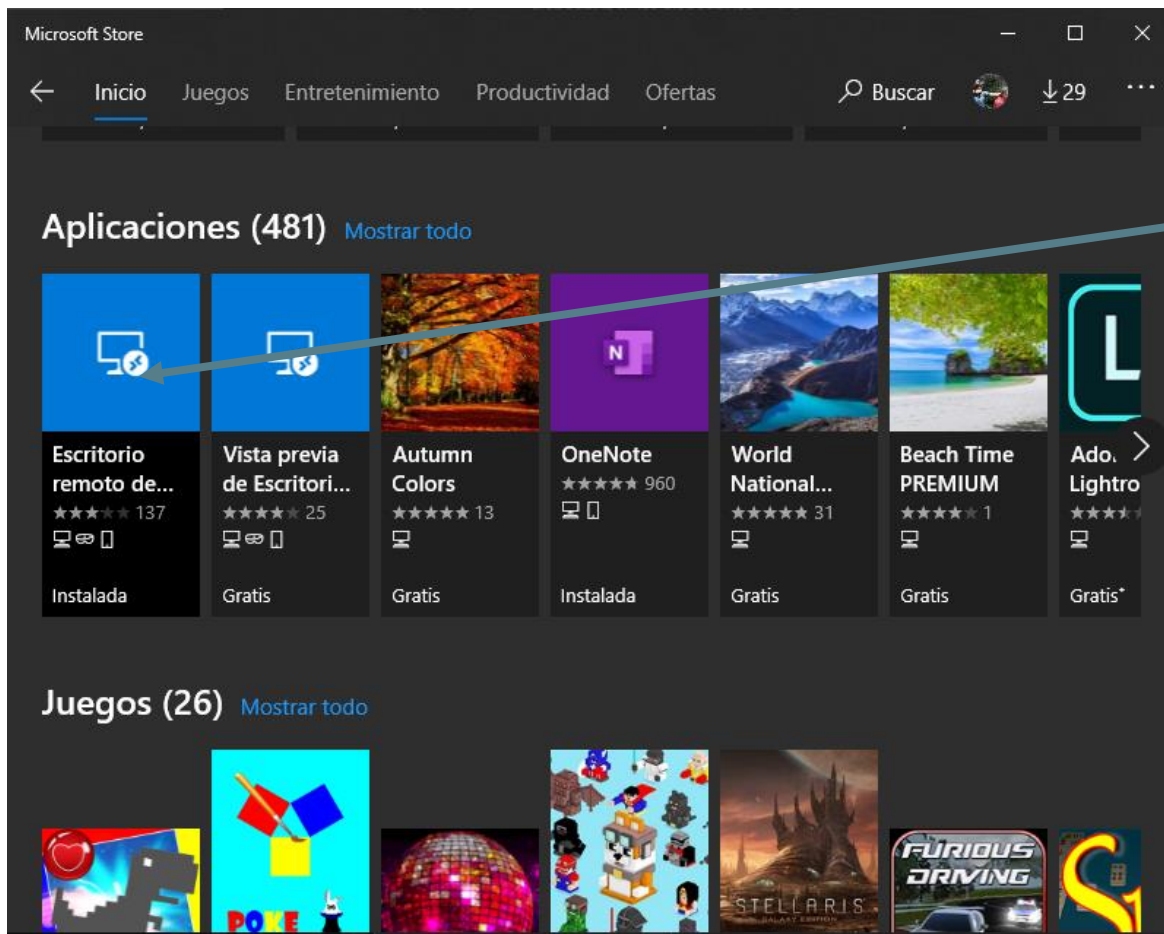
- Versión clásica



Ya podríamos interactuar con el mismo sin ningún problema

9.W Cliente Remote Desktop

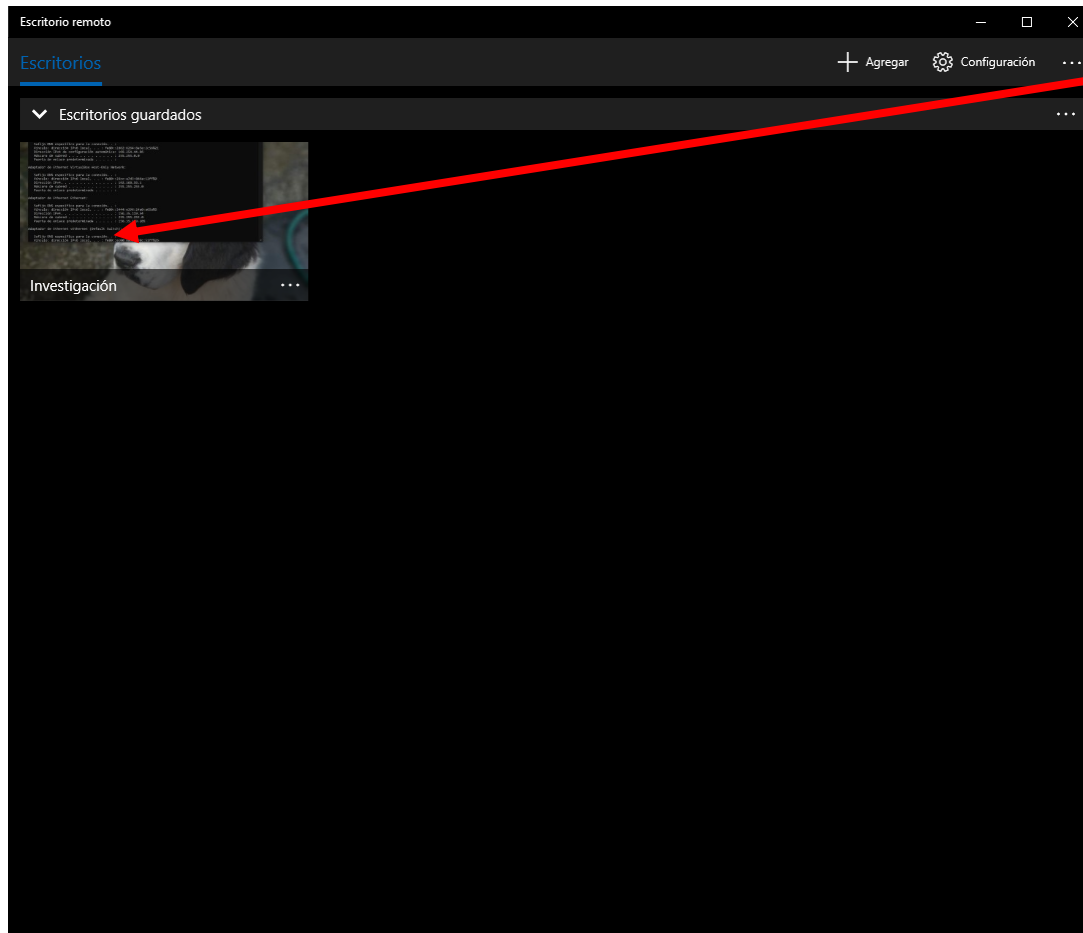
- VERSION “MODERNA”



Se obtiene en la Store de Microsoft, es una aplicación gratuita y no tiene grandes diferencias en cuanto a funcionalidad.

9.W Cliente Remote Desktop

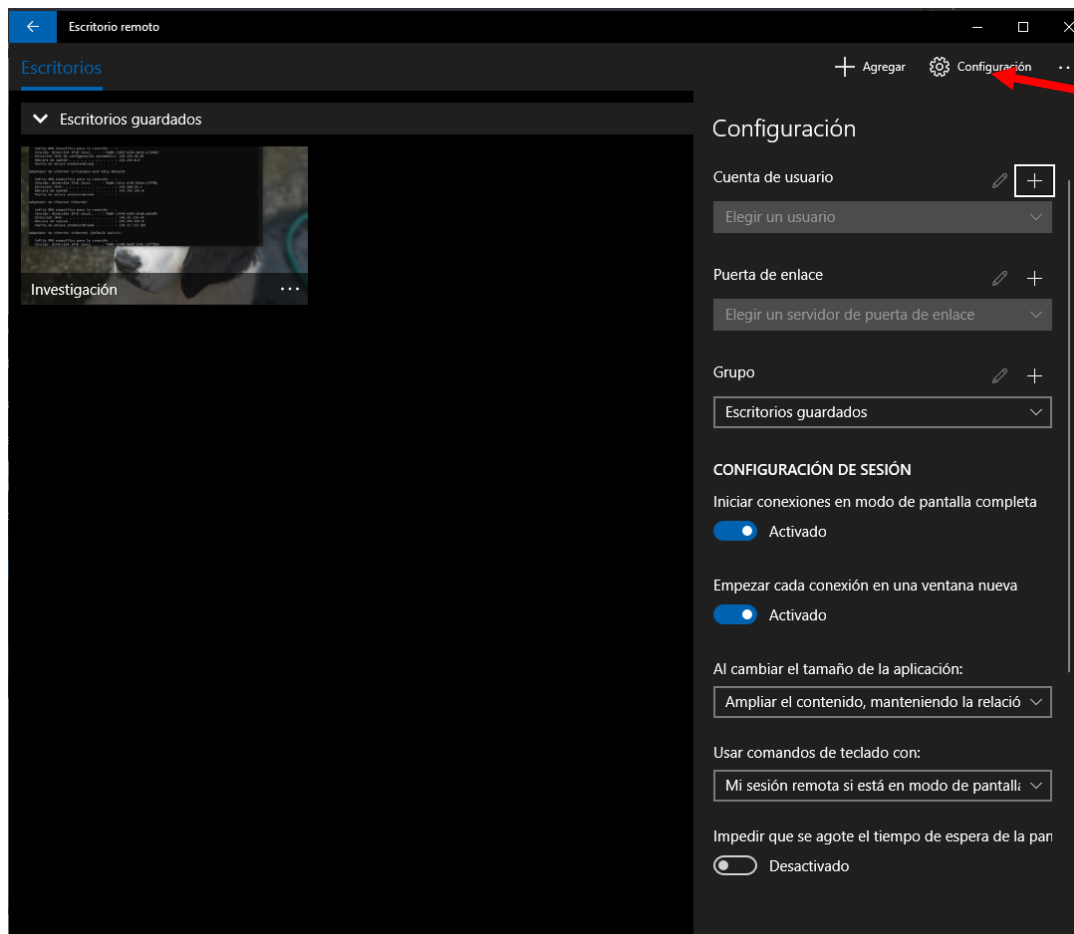
- VERSION "MODERNA"



Diferentes sesiones guardadas,
mucho mas intuitiva y facil

9.W Cliente Remote Desktop

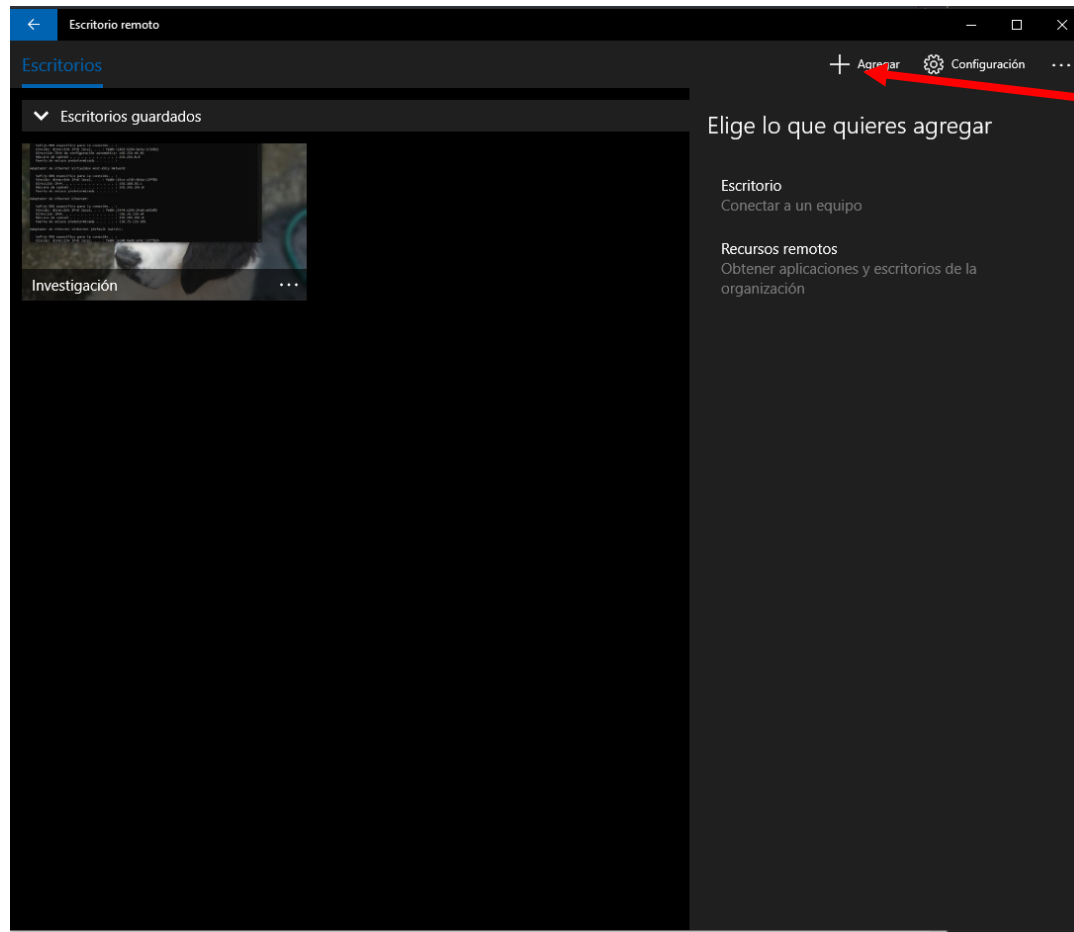
- VERSION “MODERNA”



Si pulsamos en configuración, se nos abren opciones similares a la anterior aplicación

9.W Cliente Remote Desktop

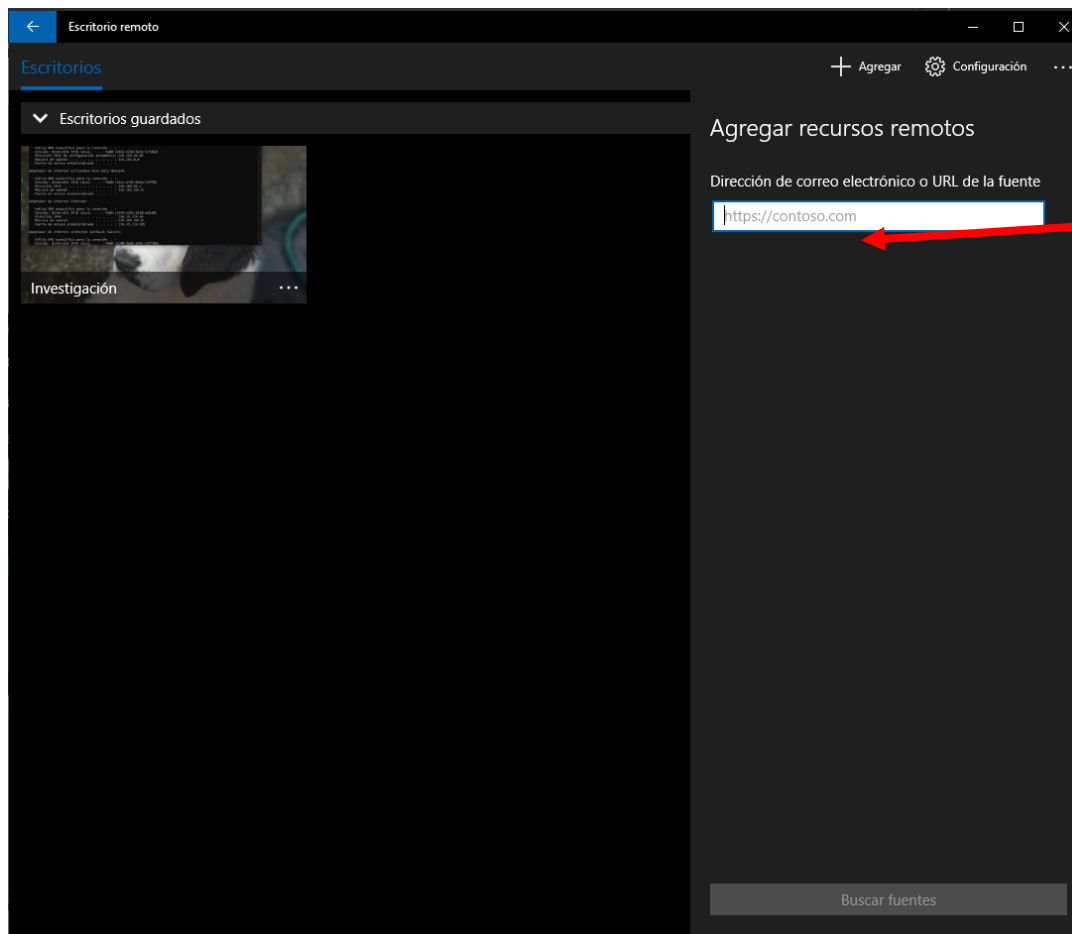
- VERSION “MODERNA”



Si pulsamos agregar, nos permite además acceder a recursos remotos de tu empresa/ organización

9.W Cliente Remote Desktop

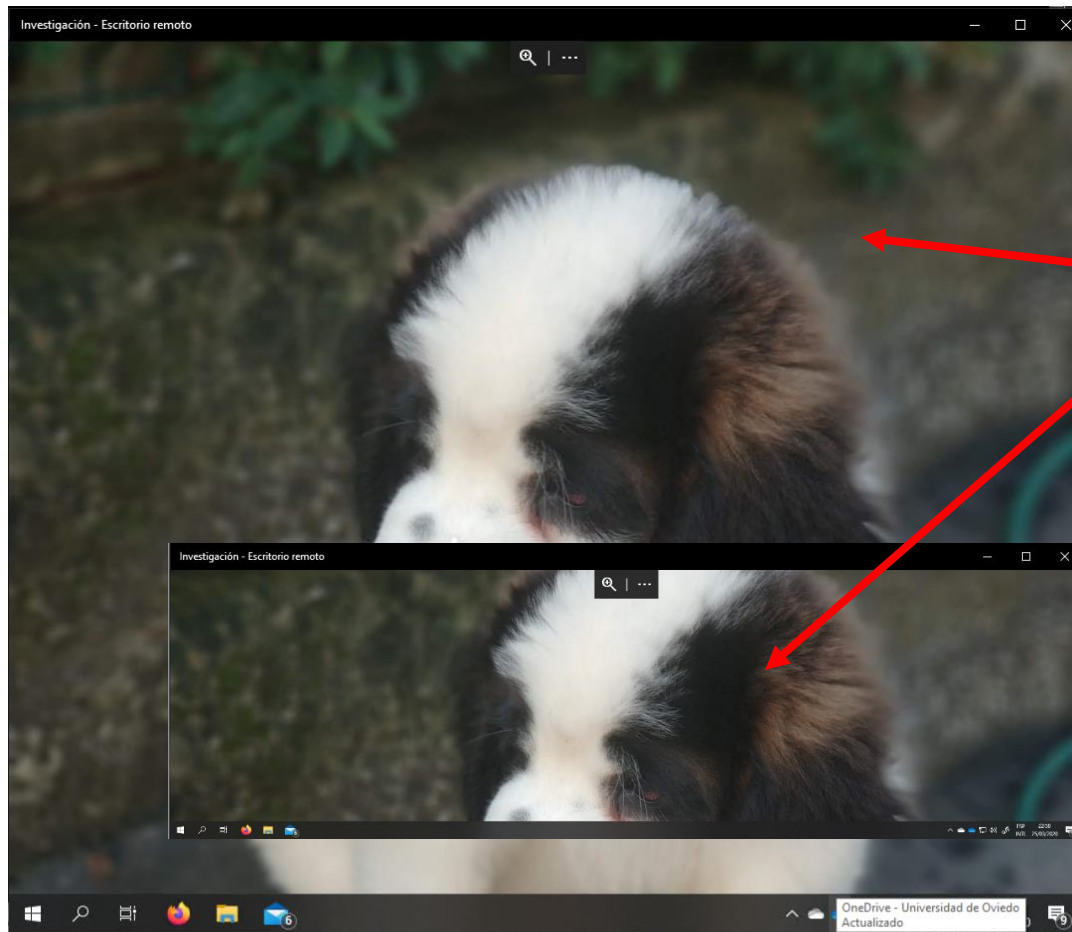
- VERSION "MODERNA"



Para acceder a los mismos
bastaría con especificar la URL

9.W Cliente Remote Desktop

- VERSION “MODERNA”



Nos conectaríamos de forma análoga, alguna ventaja : resolución adaptativa al tamaño de la ventana

9.W Servidor Remote Desktop

- COMO ACTIVARLO



¡IMPORTANTE! No todas las versiones de Windows vienen con esa características

Versiones Soportadas

W10 Pro

W10 Education (cuenta Uniovi)

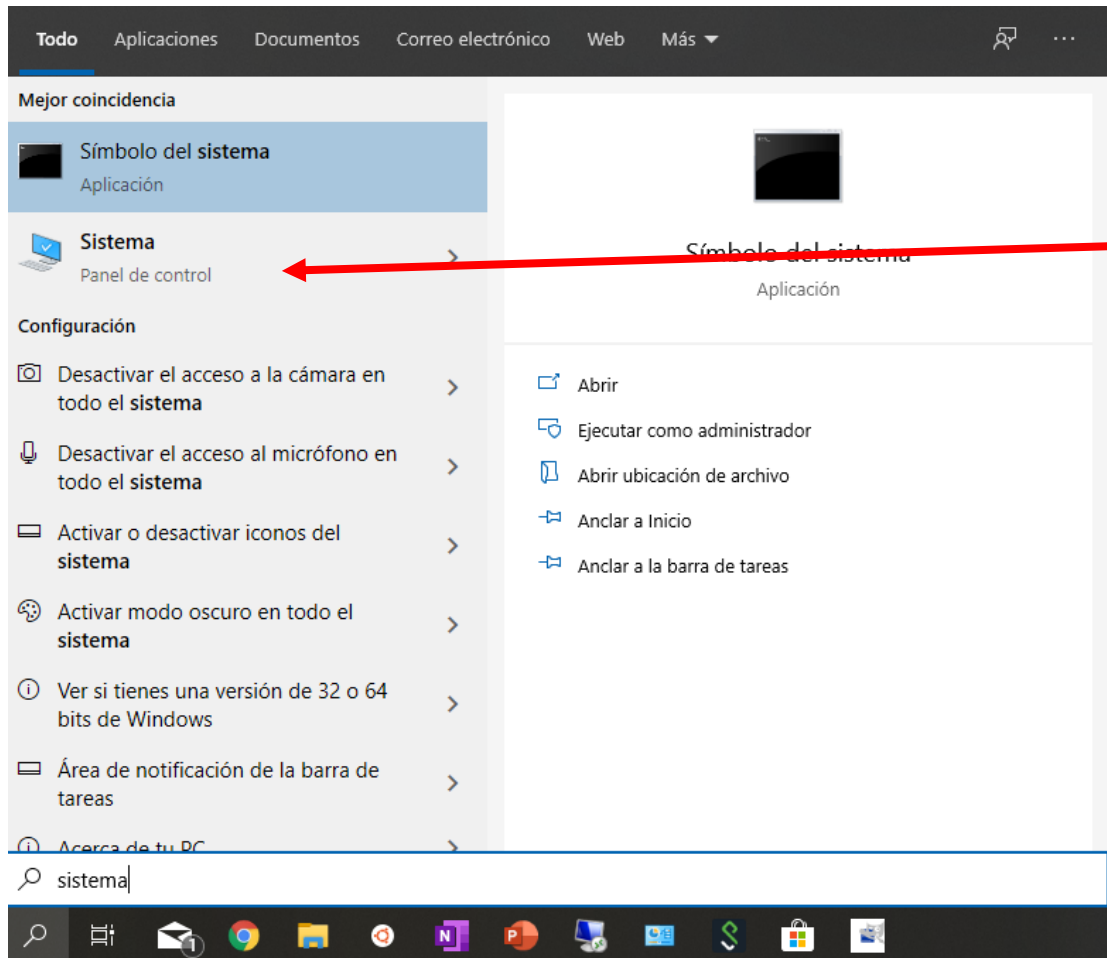
WS2019 2016...

Versiones no soportadas:

W10 Home (la habitual en los ordenadores domesticos)

9.W Servidor Remote Desktop

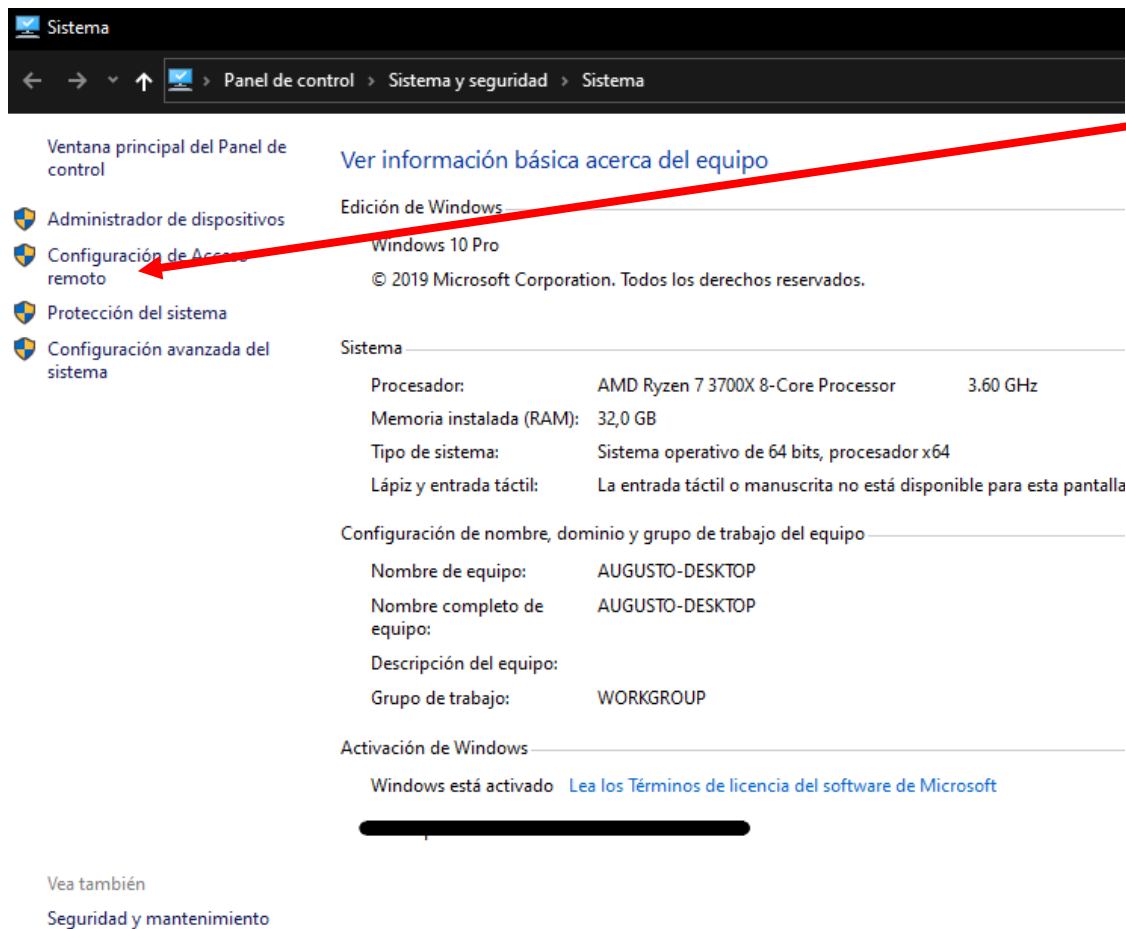
- COMO ACTIVARLO



Vamos a Panel de Control /Sistema

9.W Servidor Remote Desktop

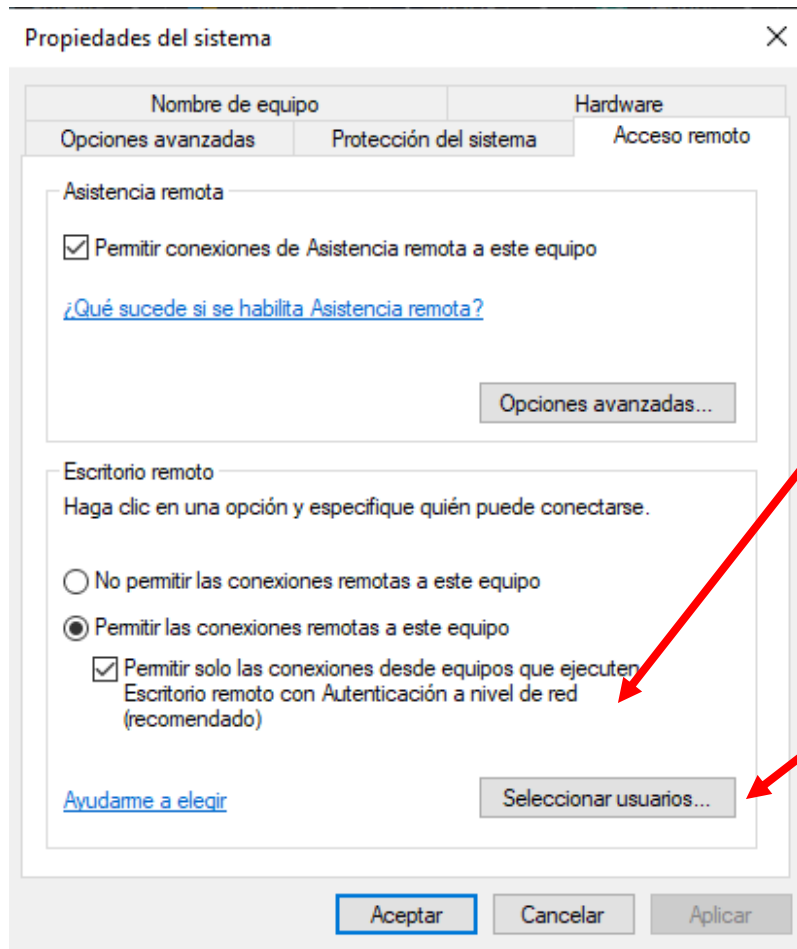
- COMO ACTIVARLO



Configuración de Acceso Remoto

9.W Servidor Remote Desktop

- COMO ACTIVARLO



Habilitamos las conexiones remotas utilizando RDP al sistema (importante marcar la segunda opción)

Podemos personalizar que usuarios podrán hacer conexiones remotas

9. Hacia donde querríamos ir:

- Thin-Clients que se conecten a nuestras computadoras del despacho/casa para ganar en potencia de computo sin drenar la batería



Fuente revistaGQ all rights reserved



Fuente Microsoft.com all rights reserved

9. Situación actual

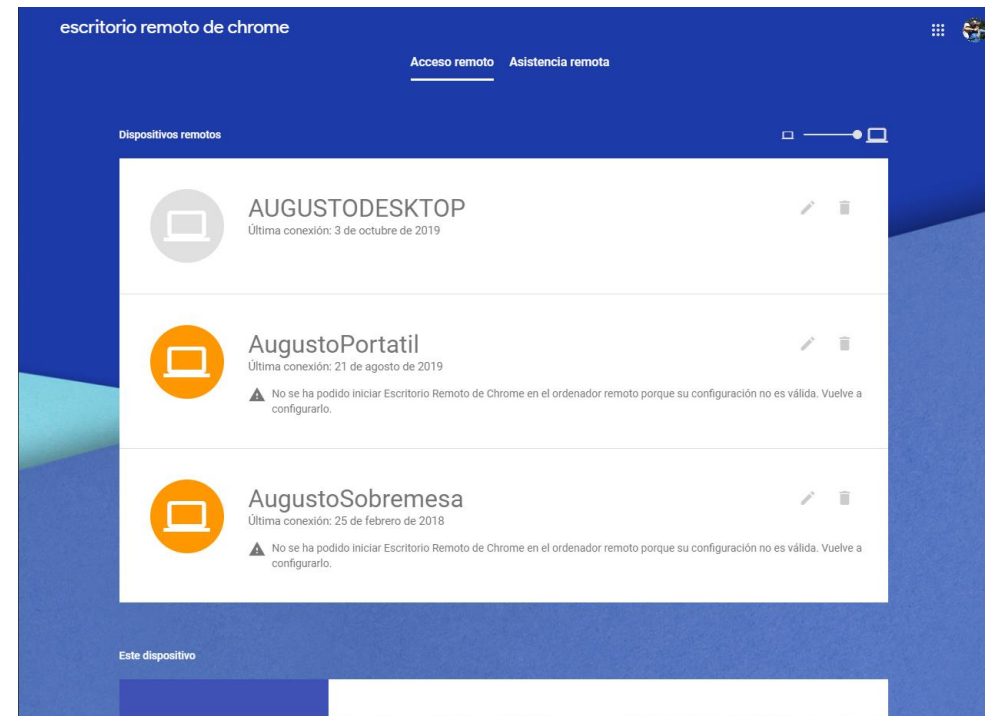
- Actualmente la infraestructura no esta totalmente preparada para esto:

1. Red poco fiable e inestable

2. Maquinas tras NAT

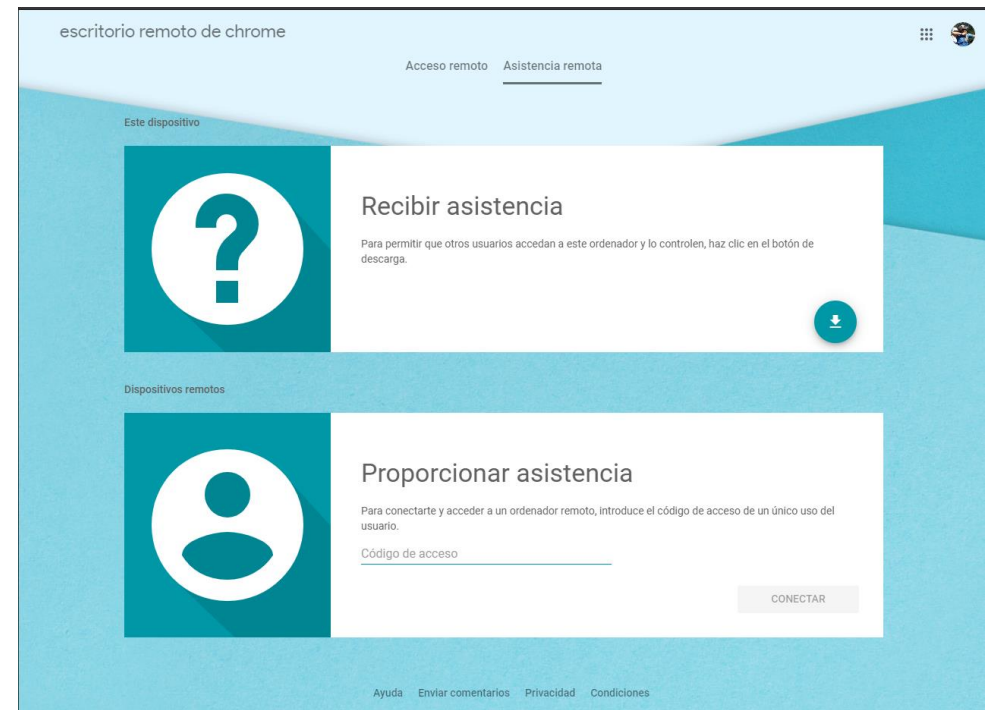
9. Maquinas tras NAT (SOLUCIONES)

- Soluciones propietarias: Google Remote Desktop
- Es una aplicación que permite tanto asistencia como conexión a equipos remotos tras NAT
- Actualmente tiene un cliente web, requiere de la instalación de un “servidor” en las maquinas a controlar de forma remota.
- Te permite gestionar los escritorios remotos de varias maquinas.
- El Wifi de la universidad la tiene “capada”



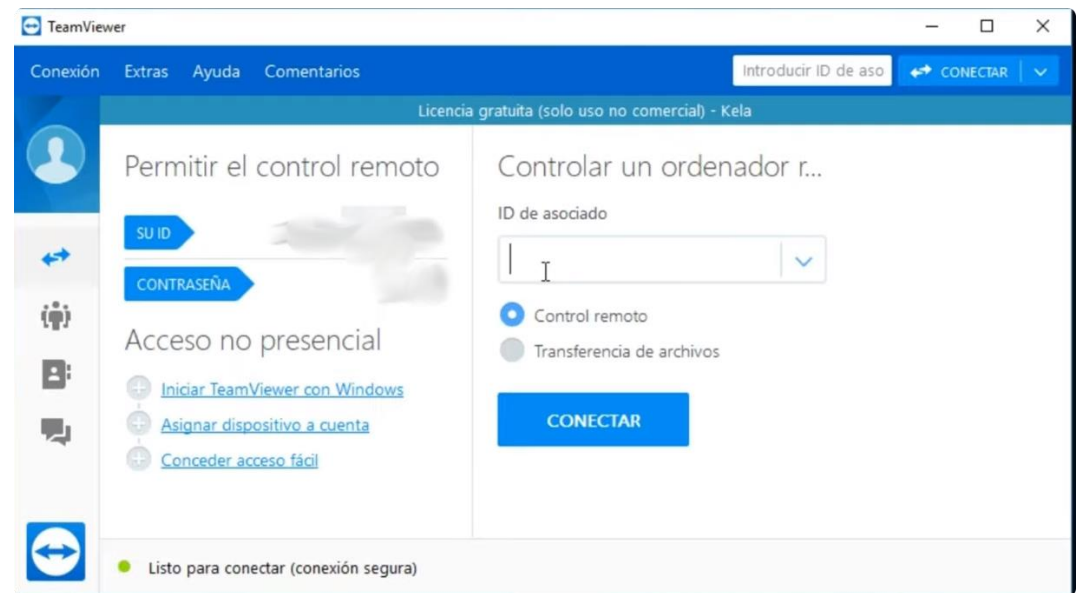
9. Maquinas tras NAT (SOLUCIONES)

- Soluciones propietarias: Google Remote Desktop
- Es una aplicación que permite tanto asistencia como conexión a equipos remotos tras NAT
- Actualmente tiene un cliente web, requiere de la instalación de un “servidor” en las maquinas a controlar de forma remota.
- Te permite gestionar los escritorios remotos de varias maquinas.
- El Wifi de la universidad la tiene “capada”



9. Maquinas tras NAT (SOLUCIONES)

- Soluciones propietarias:
TeamViewer
- Permite de igual forma acceder a una maquina tras NAT
- Hay que instalarse la aplicación, la hay tanto para Linux como para Windows.
- De forma análoga permite teleasistencia o acceder a tus equipos de forma remota.
- Tiene una cuenta gratuita, de la cual es muy sencillo que te “echen” si observan patrones de actividad sospechosa.



9. Maquinas tras NAT (SOLUCIONES)

- Soluciones mas caseras (IDEAS):
- Túneles/Servicios DNS/Scripts
- Túneles : serveo.net , instancia en el cloud...
- Servicios DNS: DuckDNS, NO-IP...
- Scripts : hago pooling comprobando la IP y cuando cambie la envié a mi correo electrónico, twitter...
- Todos ellos acompañados de algún mecanismo que redireccione del router hacia nuestra computadora

