(EN) REMOTE DESKTOP - Safe connection

Connection to remote desk (mstsc) of sure way (Universitat of València)

Characteristics that has to have the squad to access (to the that will connect us):

1. Have updated the Operating system (important updates and of security).
2. Have installed the antivirus corporate and that was updated.
3. Have enabled the remote desk for an user of the system.
4. We will not enable the remote user for the user “administrator” neither “invited” (or similar).
5. The key of the user enabled to access by means of remote desk has to be robust (me- nimo 8 characters, mayus/minus, numbers, etc..).
6. Enable the blockade of screen (user/password) after a time of inactivity.
7. Enable the cortafuegos local so that only they allow for the connections entrantes the port 3389 to the net 147.156.0.0/16.
8. Maintain enabled the remote desk during the periods of time (dias) strictly necessary, in case of not needing connect us through remote desk during a prolonged time, deshabilitarlo.

Characteristics that has to have the squad from which will connect us:

1. Have updated the Operating system (important updates and of security).
2. Have installed an antivirus and that was updated.
3. Have actuated the cortafuegos local of the squad.
4. Have configured the client of VPN of the Universitat of València (OpenVPN):


5. Have of a client of remote desk (mstsc).
6. Know the public IP of the squad of the Universitat of València to the that want to connect us.
7. When we finalise the connection by means of remote desk, is advisable desconectar also the connection VPN.