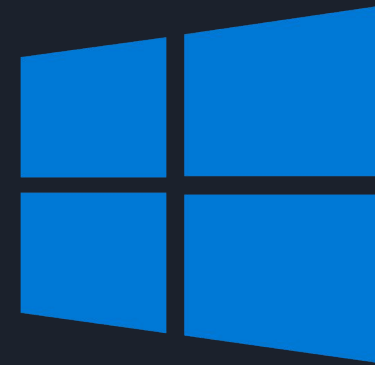


Manual para VPN en Windows



Configuración de la VPN

Link de la lista de VPNs a configurar:

[VPN's QC](#)



Introducción

Existen dos métodos para crear las VPN's

-> Por línea de comando en PowerShell.

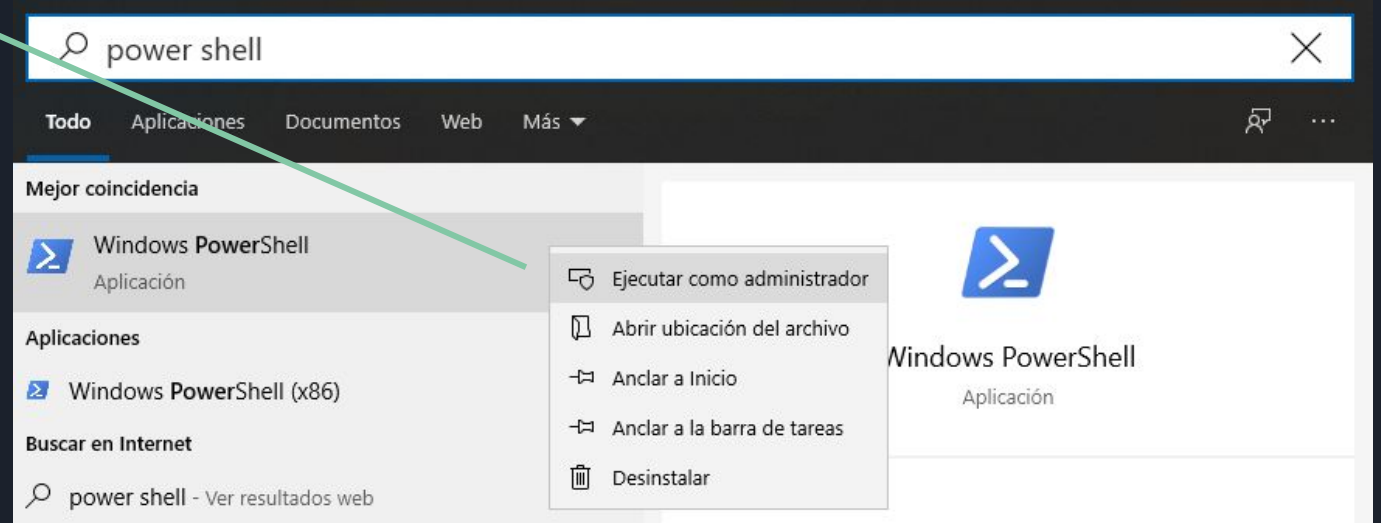
-> Paso a paso y gráficamente.



Se pueden seguir ambas,
pero PowerShell es la más
rápida y cómoda.

Configuración de la VPN (Método 1)

Buscar en Windows PowerShell.
-> Ejecutar como Administrador.



Configuración de la VPN

Copiar y ejecutar el siguiente comando:

```
Add-VpnConnection -Name 'UAT-GLOBAL-MEX' -ServerAddress  
'uat-global-mex.dlatv.net' -L2tpPsk 'amco2020' -TunnelType  
L2tp -EncryptionLevel Required -AuthenticationMethod  
Chap,MSChapv2 -Force -RememberCredential -PassThru
```


Nombre de la VPN



IP de la VPN



Preshared Key



Configuración de la VPN

Para cada comando de VPN se debe mostrar un resultado similar al siguiente:

```
Administrador: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Prueba la nueva tecnología PowerShell multiplataforma https://aka.ms/pscore6

PS C:\Windows\system32> Add-VpnConnection -Name 'UAT-ANDINA-PER' -ServerAddress 'uat-andina-per.dlatv.net' -L2tpPsk 'amc
o2020' -TunnelType L2tp -EncryptionLevel Required -AuthenticationMethod Chap,MSChapv2 -Force -RememberCredential -PassTh
ru
ADVERTENCIA: The currently selected encryption level requires EAP or MS-CHAPv2 logon security methods. Data encryption
will not occur for Pap or Chap.

Name                : UAT-ANDINA-PER
ServerAddress        : uat-andina-per.dlatv.net
AllUserConnection    : False
Guid                 : {E6838D35-70BF-42F8-BFDE-FE6AE3A95298}
TunnelType           : L2tp
AuthenticationMethod : {Chap, MsChapv2}
EncryptionLevel       : Required
L2tpIPsecAuth        : Psk
UseWinlogonCredential : False
EapConfigXmlStream   :
ConnectionStatus      : Disconnected
RememberCredential    : True
SplitTunneling        : False
DnsSuffix            :
IdleDisconnectSeconds : 0
```

Agregar Clave al Registro

Copiar y ejecutar el siguiente comando:

```
REG ADD HKLM\SYSTEM\CurrentControlSet\Services\PolicyAgent /v  
AssumeUDPEncapsulationContextOnSendRule /t REG_DWORD /d 0x2 /f
```

```
PS C:\Windows\system32> REG ADD HKLM\SYSTEM\CurrentControlSet\Services\PolicyAgent /v AssumeUDPEncapsulationContextOnSen  
dRule /t REG_DWORD /d 0x2 /f  
La operación se completó correctamente.  
PS C:\Windows\system32>
```

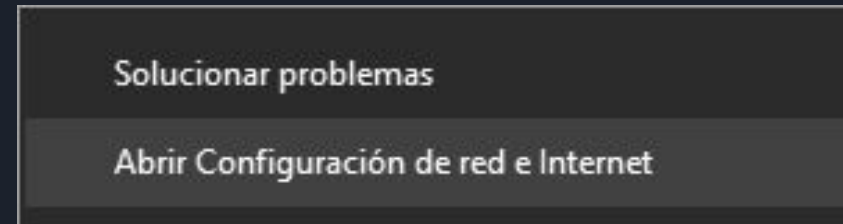
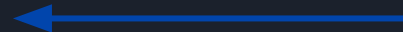
-> Es indispensable reiniciar el Equipo
para que se efectúen los cambios.

Configuración de la VPN (Método 2)

1.- Hacer clic derecho en el ícono de **Wi-Fi**.



2.- Seleccionar **Abrir Configuración de red e internet**.



-> Dentro de la ventana que se abra, buscar y hacer clic en **Centro de redes y recursos compartidos**.



Configuración de la VPN

Cambiar la configuración de red



Configurar una nueva conexión o red

Configurar una conexión de banda ancha, de acceso telefónico o VPN; o bien configurar un enrutador o punto de acceso.

1.- Cambiar la configuración de red:
-> Seleccionar **Configurar una nueva conexión o red**.

2.- Seleccionar **Conectarse a un área de trabajo**.



Conectarse a un área de trabajo

Configurar una conexión de acceso telefónico o VPN a su área de trabajo.

¿Desea usar una conexión de la que ya dispone?

☒ No, crear una nueva conexión

NOTA: Puede salir el siguiente mensaje:
-> Seleccionar **No, Crear una nueva conexión** y dar clic en **Siguiente**.

Configuración de la VPN

¿Cómo deseas conectarte?:

-> Seleccionar **Usar mi conexión a internet (VPN)**.



Configuración de la VPN

1.- Dirección de Internet:

-> Ingresar la IP de la VPN.

2.- Nombre de destino:

-> Escribir el nombre que le asignaremos a nuestra VPN.

-> Ejemplo: "México_UAT"

El administrador de red puede darle esta dirección.

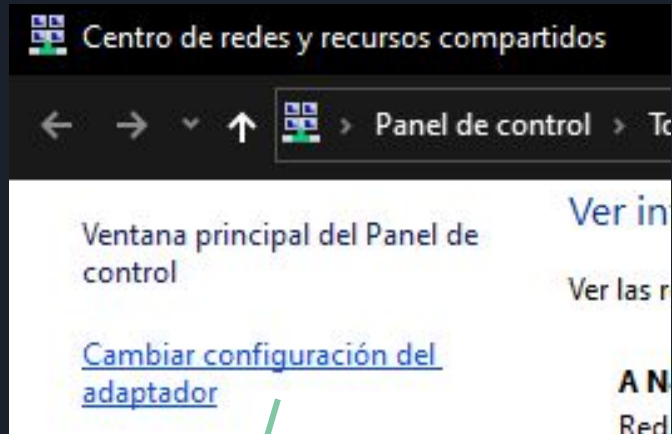
Dirección de Internet:

uat-aup-arg.dlatv.net

Nombre de destino:

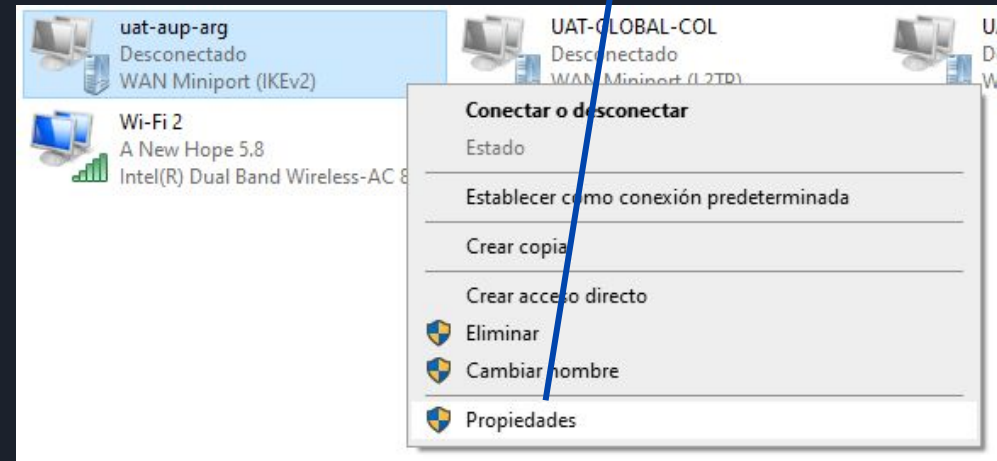
uat-aup-arg

Configuración de la VPN

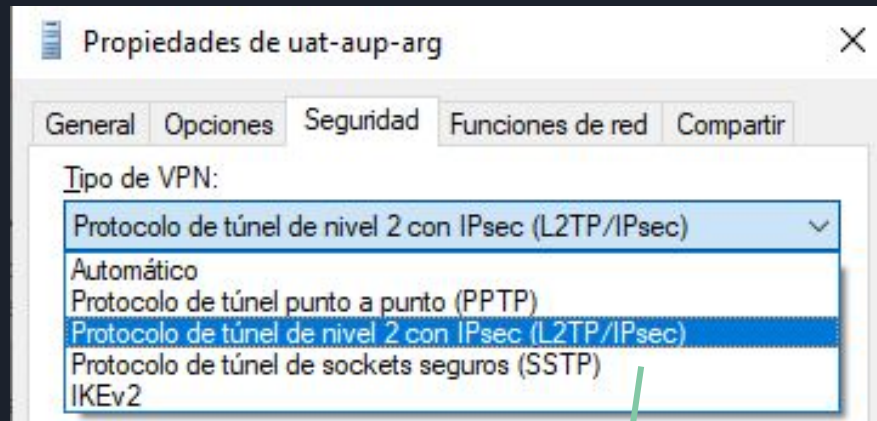


1.- En la ventana de **Centro de redes y recursos compartidos**, en el panel de la izquierda:
-> Seleccionar **Cambiar configuración del adaptador**.

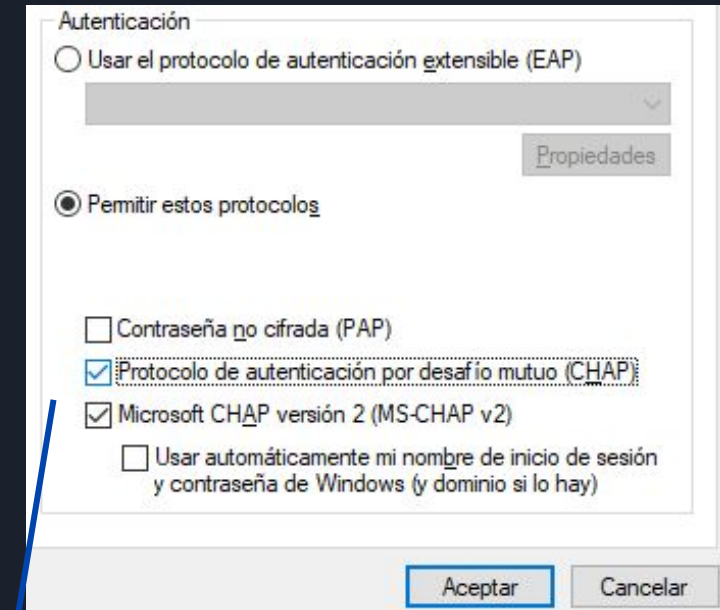
2.- En la VPN recién creada dar clic derecho:
-> Seleccionar **Propiedades**.



Configuración de la VPN

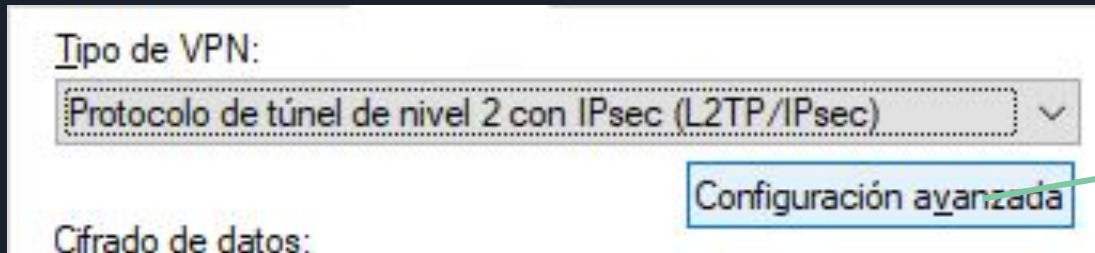


Ir a la pestaña **Seguridad**
Tipo de VPN:
-> Seleccionar **Protocolo de túnel de nivel 2 con IPsec (L2TP/IPsec)**.



Marcar **Permitir estos protocolos**:
-> Marcar **Protocolo de autenticación por desafío mutuo (CHAP)**.
-> Marcar **Microsoft CHAP versión 2 (MS-CHAP v2)**.

Configuración de la VPN



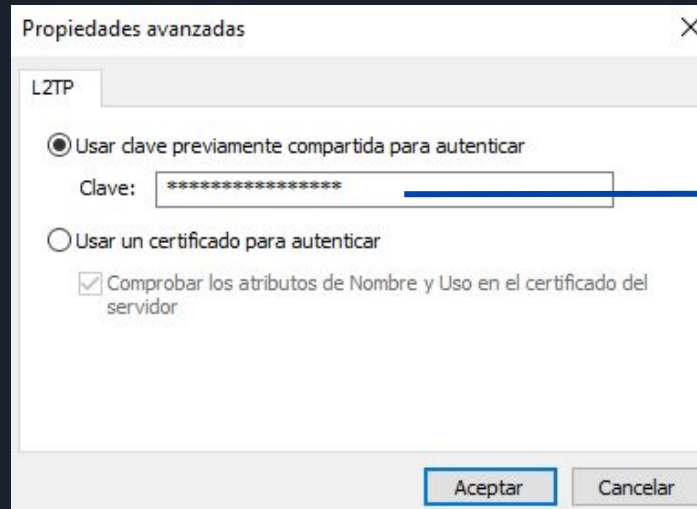
Tipo de VPN:

Protocolo de túnel de nivel 2 con IPsec (L2TP/IPsec) ▼

Cifrado de datos:

Configuración avanzada

1.- Tipo de VPN:
-> Dar clic en **Configuración Avanzada**.



Propiedades avanzadas

L2TP

☒ Usar clave previamente compartida para autenticar

Clave: *****

☐ Usar un certificado para autenticar

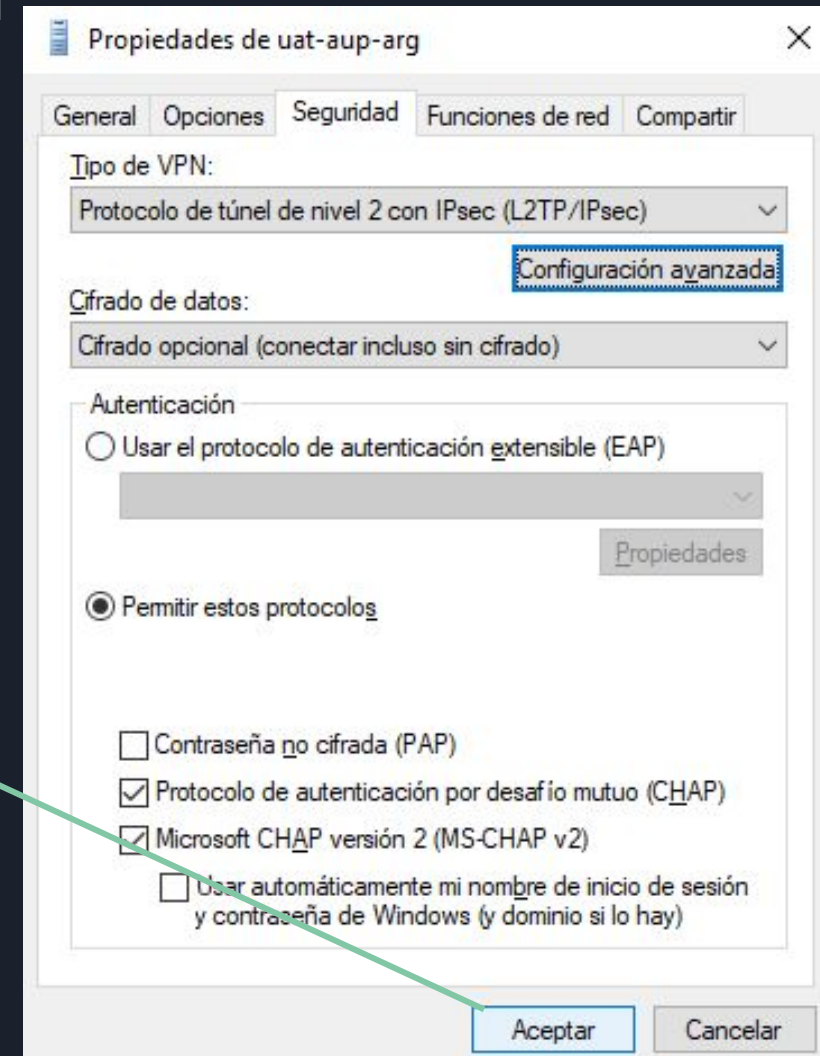
☒ Comprobar los atributos de Nombre y Uso en el certificado del servidor

Aceptar Cancelar

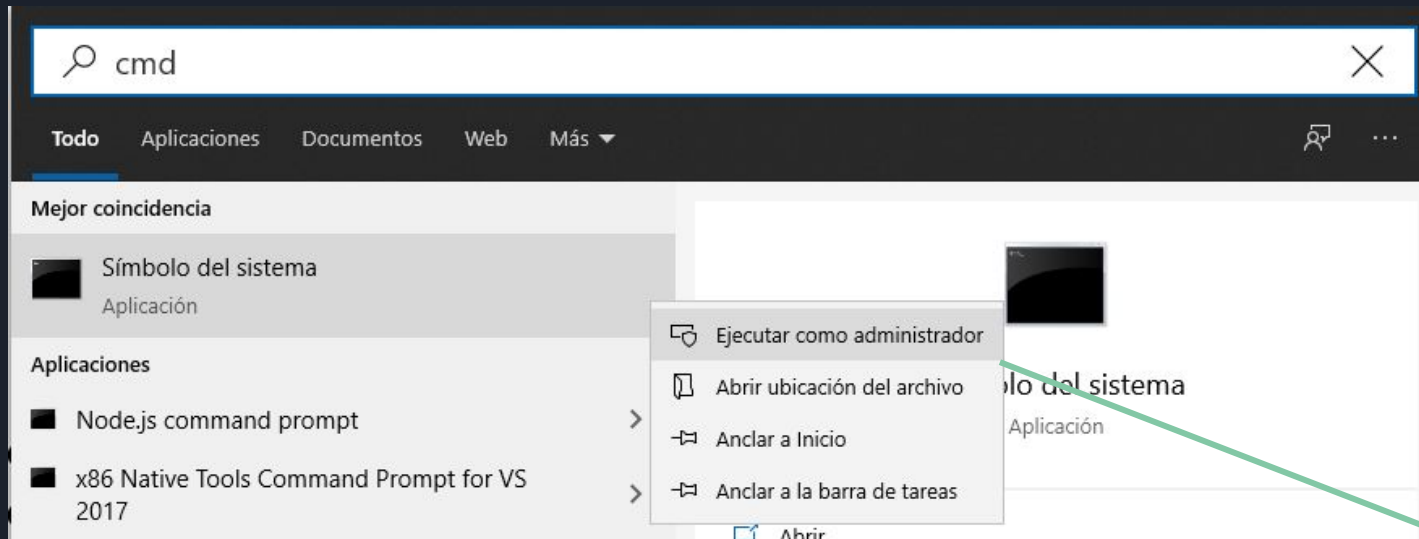
2.- Usar clave previamente compartida para autenticar:
-> Ingresar la **Pre Shared Key**.
-> Dar clic en **Aceptar**.

Configuración de la VPN

Dar clic en **Aceptar** para guardar todos los cambios realizados a la VPN.



Agregar Clave al Registro

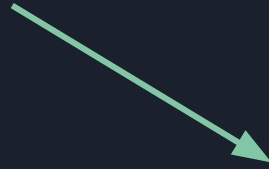


Buscar en Windows **CMD**:
-> Ejecutar como Administrador.

Agregar Clave al Registro

Copiar y ejecutar el siguiente comando:

```
REG ADD HKLM\SYSTEM\CurrentControlSet\Services\PolicyAgent /v  
AssumeUDPEncapsulationContextOnSendRule /t REG_DWORD /d 0x2 /f
```



```
Administrador: Símbolo del sistema
Microsoft Windows [Versión 10.0.18363.657]
(c) 2019 Microsoft Corporation. Todos los derechos reservados.

C:\Windows\system32>REG ADD HKLM\SYSTEM\CurrentControlSet\Services\PolicyAgent
/v AssumeUDPEncapsulationContextOnSendRule /t REG_DWORD /d 0x2 /f_
```

Presionar **Enter**.

-> Se debe de visualizar: **La operación se completó correctamente.**



-> Es indispensable reiniciar el Equipo para que se efectúen los cambios.

```
Administrador: Símbolo del sistema
Microsoft Windows [Versión 10.0.18363.657]
(c) 2019 Microsoft Corporation. Todos los derechos reservados.

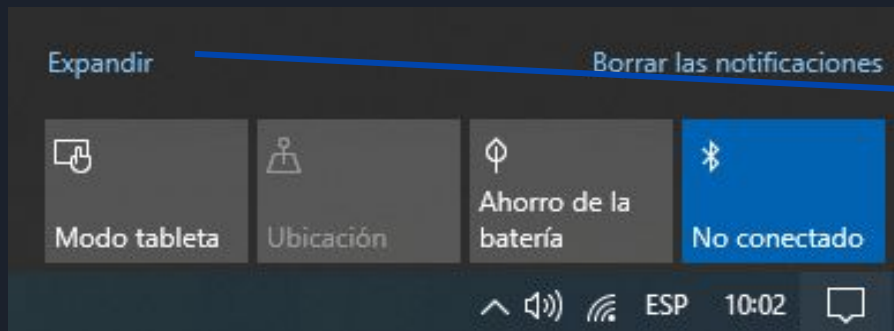
C:\Windows\system32>REG ADD HKLM\SYSTEM\CurrentControlSet\Services\PolicyAgent
/v AssumeUDPEncapsulationContextOnSendRule /t REG_DWORD /d 0x2 /f
La operación se completó correctamente.

C:\Windows\system32>
```

Activar la VPN



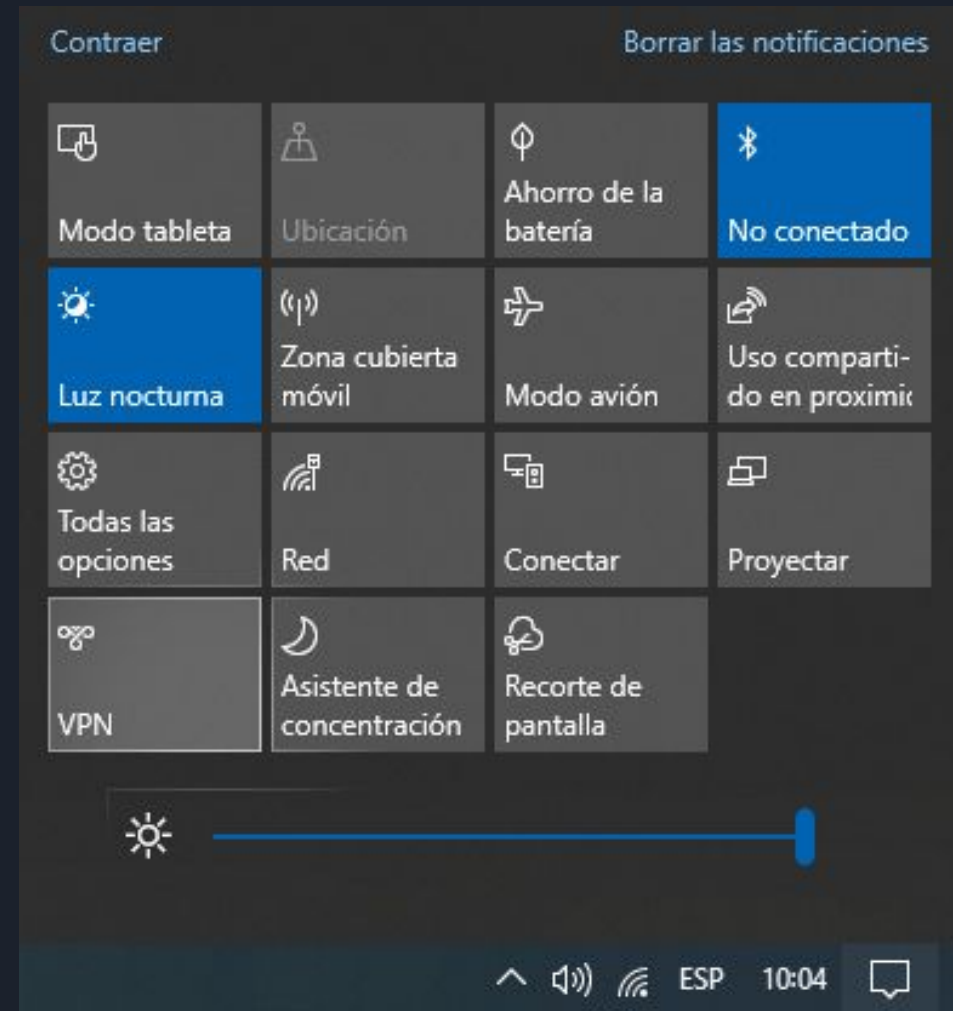
1.- Hacer clic en el icono de **Notificaciones**



2.- Hacer clic en **Expandir** para mostrar todos los accesos directos de Windows

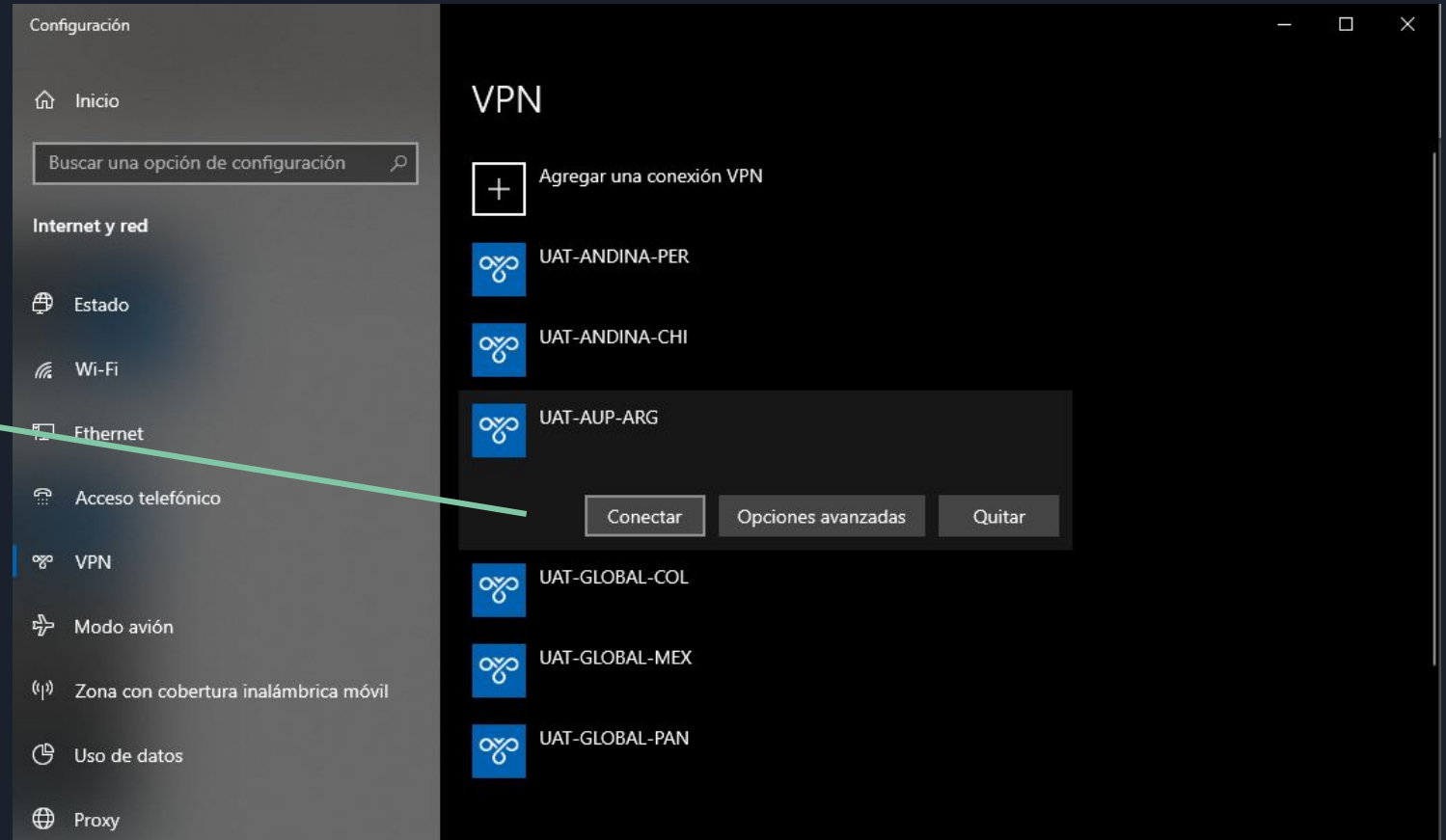
Activar la VPN

Dar clic en el
icono de VPN.

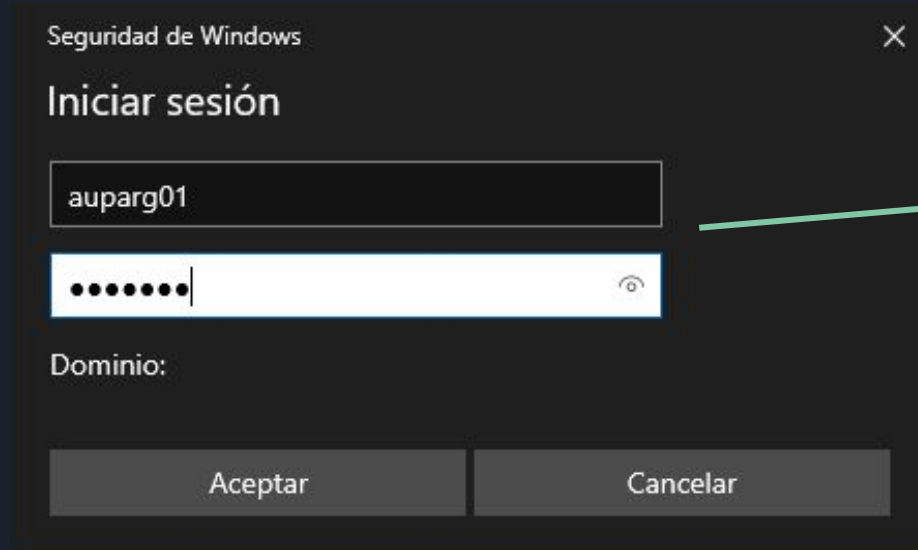


Activar la VPN

Seleccionar la VPN deseada.
-> Dar clic en **Conectar**.



Activar la VPN



Seguridad de Windows

Iniciar sesión

auparg01

.....

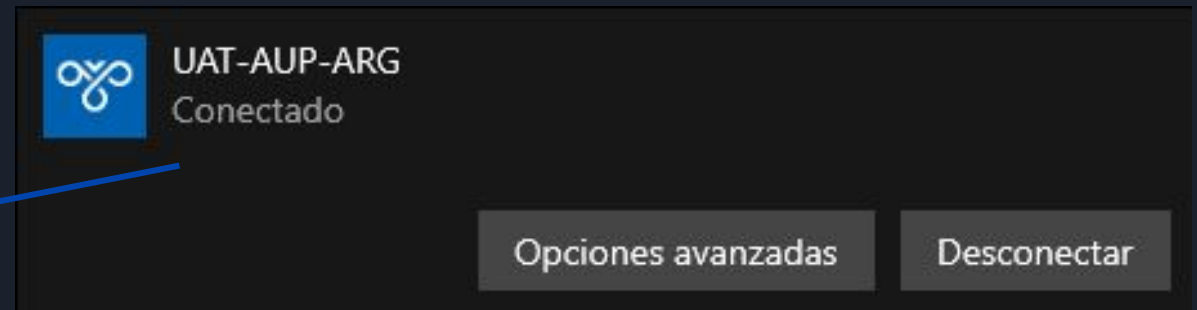
Dominio:

Aceptar Cancelar

1.- Iniciar sesión:

- > Ingresar el nombre de usuario de la VPN.
- > Ingresar contraseña de la VPN.

2.- Asegurarse que se conecte correctamente a la VPN.



Alerta de conexión con VPN's

En el caso de intentar realizar la conexión de nuestro equipo con las VPN's y se muestre la siguiente alerta:

No se puede conectar a... Error en el intento de conexión L2TP porque el nivel de seguridad encontró un error de proceso durante las negociaciones iniciales con el equipo remoto.

Causa del fallo:

-> Tras instalar la actualización de Enero conocida como KB5009543 en **Windows 10** y KB5009566 en **Windows 11**, los equipos son incapaces de conectarse a ningún tipo de VPN L2TP dando un código de error al intentarlo.

Alerta de conexión con VPN's

1. Damos clic derecho en el botón de inicio, y damos clic en Terminal Windows (Administrador) o Windows Powershell (Administrador) dependiendo de la versión de Windows en la que te encuentres.
2. Una vez estemos dentro, copiamos el siguiente comando dependiendo de tu sistema operativo:

Windows 10: `wusa /uninstall /kb:5009543`

Windows 11: `wusa /uninstall /kb:5009566`

3. Cuando termine el proceso de desinstalación, reiniciamos el equipo.
4. Nos dirigimos a Configuración > Windows Update o Configuración > Actualización y seguridad > Windows Update, y pulsamos en Pausar actualizaciones. Recomendamos pausar las mismas en el periodo maximo que permita (35 días) hasta que Microsoft pueda solucionar la falla.