

Acceso remoto

La gestión remota de los clientes Windows 10 es una tarea importante para cualquier administrador de empresa, ya que contribuye a la disponibilidad del sistema de información.

El puesto de trabajo se encuentra en el corazón del funcionamiento de la empresa; por tanto, el servicio de atención al usuario debe ser eficaz y reactivo. La evolución del parque informático se tiene en cuenta desde la dirección informática, que debe controlar los costes del entorno de trabajo del usuario.

Podemos resumir el ciclo de vida de un sistema operativo de la siguiente manera: planificación, despliegue, utilización, mantenimiento y transición.


Windows 10 presenta un amplio conjunto de funcionalidades para realizar estas tareas, por ejemplo a través de la virtualización de equipos, de la reparación remota o de las herramientas de centralización, como la consola de gestión **MMC** (*Microsoft Management Console*).

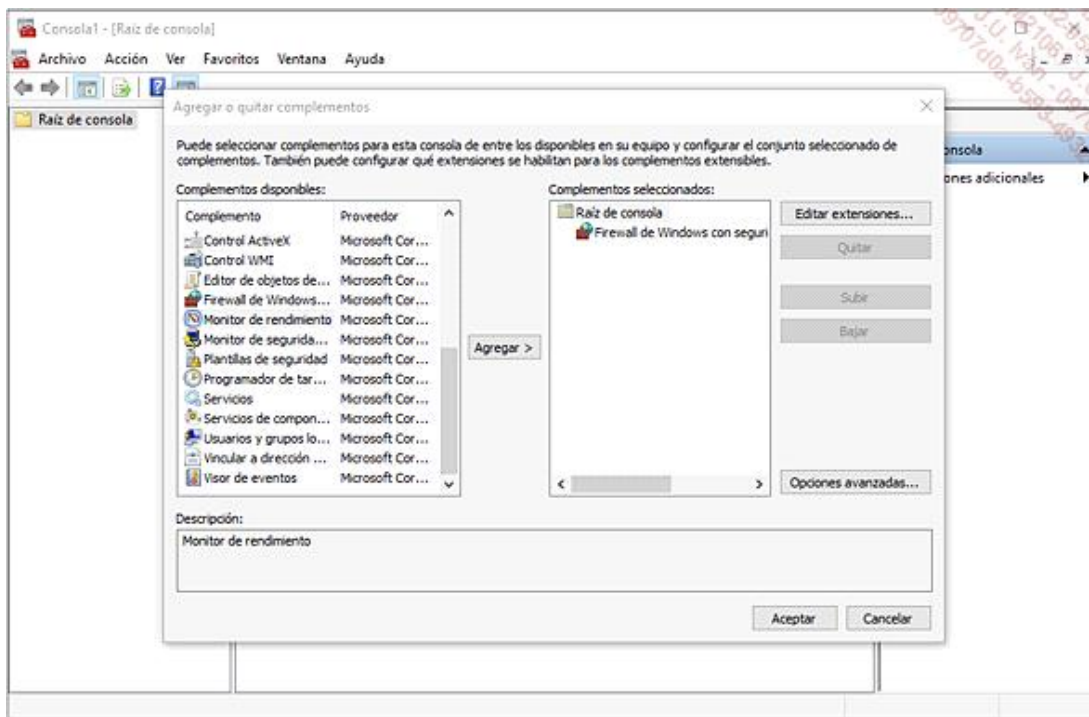
1. Microsoft Management Console

La consola **MMC** proporciona las herramientas de administración que permiten gestionar componentes de red (DHCP, DNS), equipos (cuentas, sesiones) o servicios (NAP, BITS) de manera local o remota.

Es posible acceder a la consola ejecutando el comando **mmc.exe** desde el escritorio. Cada componente que se haya de administrar debe agregarse manualmente a la consola, en la sección **Complementos**.

He aquí el procedimiento que permite agregar o eliminar un complemento:

- Pulse las teclas  + **R** e introduzca **mmc** en la ventana **Ejecutar**. Confirme haciendo clic en el botón **Sí** cuando aparezca la ventana de control de cuentas de usuario.
- Haga clic en el menú **Archivo** y, a continuación, en **Agregar o quitar complemento**. Seleccione el complemento o complementos disponibles (uno a continuación de otro) y haga clic en el botón **Agregar**. Por ejemplo, para configurar el firewall de un ordenador remoto, seleccione **Firewall de Windows con funcionalidad avanzada**. Cuando aparezca un cuadro de diálogo (como muestra la siguiente imagen) en el que se le invita a seleccionar qué ordenador, local o remoto, desea gestionar a través del complemento, seleccione la opción adecuada y confirme con el botón **Finalizar**.

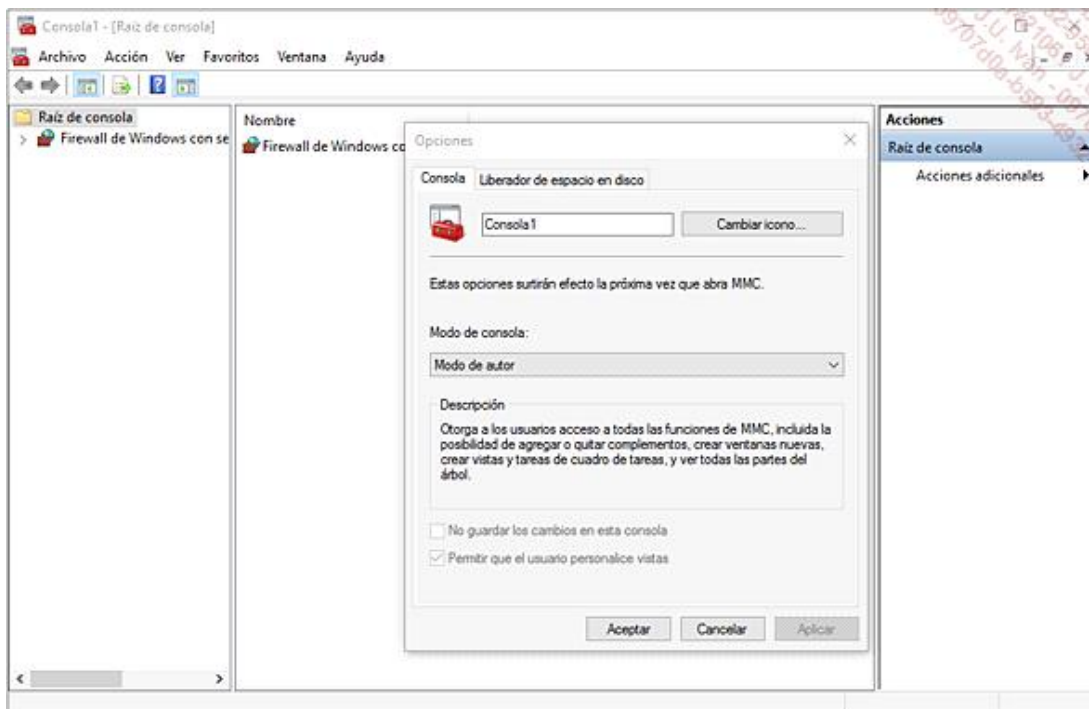


➤ No todos los complementos permiten administrar equipos remotos, como por ejemplo **Plantillas de seguridad**.

➔ Para eliminar un complemento, márkelo en **Complementos seleccionados** y haga clic en el botón **Quitar**.

Puede, después de haber constituido la lista de complementos, guardar en una carpeta compartida (o en un dispositivo extraíble) la consola, en un archivo con la extensión .msc, y de este modo reutilizarla para administrar otros clientes Windows 10 o servidores de su red corporativa.

En el menú **Archivo - Opciones**, el administrador puede restringir el acceso a los complementos seleccionando un **Modo de consola**:



Existen cuatro modos a su disposición:

- **Modo de autor:** acceso a todas las funcionalidades de la consola, incluida la adición y eliminación de complementos.
- **Modo usuario - acceso completo:** visualización completa del árbol sin posibilidad de agregar o eliminar complementos.
- **Modo usuario - acceso limitado, varias ventanas:** no estarán accesibles las zonas invisibles en la interfaz de complementos.
- **Modo usuario - acceso limitado - una ventana:** la consola se ejecuta en una única ventana, el usuario no puede acceder a las zonas ocultas mostradas en ella.

Como las consolas guardadas en el perfil del usuario utilizan espacio en disco, la pestaña **Liberador de espacio en disco** permite eliminar los archivos que contienen las modificaciones de visualización de un archivo de consola.

2. Herramientas de administración RSAT

Un administrador debe poder acceder a todas las funcionalidades y a todos los roles de los servidores de su empresa, tales como Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 y Windows Server 2012 R2, e independientemente del lugar donde se encuentre, ya que el objetivo es poder reparar o configurar los servicios críticos, tales como Active Directory y DNS. Hemos visto antes que la consola MMC permite añadir complementos para administrar, pero la herramienta es limitada: solo permite añadir los complementos para un puesto local, no para un servidor remoto. Para resolver esta carencia, Microsoft propone a los administradores que descarguen de forma gratuita los complementos para los roles y funcionalidades de un servidor Windows en la siguiente dirección: <https://www.microsoft.com/en-us/download/details.aspx?id=45520>

La herramienta está disponible para las dos arquitecturas, 32 y 64 bits, de Windows 10 Pro, Enterprise y Education, pero no para ARM. El archivo de instalación está empaquetado en forma de actualización, con la extensión .msu (*Microsoft Windows Update Stand-alone Installer*). No se requiere ninguna intervención por parte del usuario, pero es necesario un reinicio del puesto de trabajo.

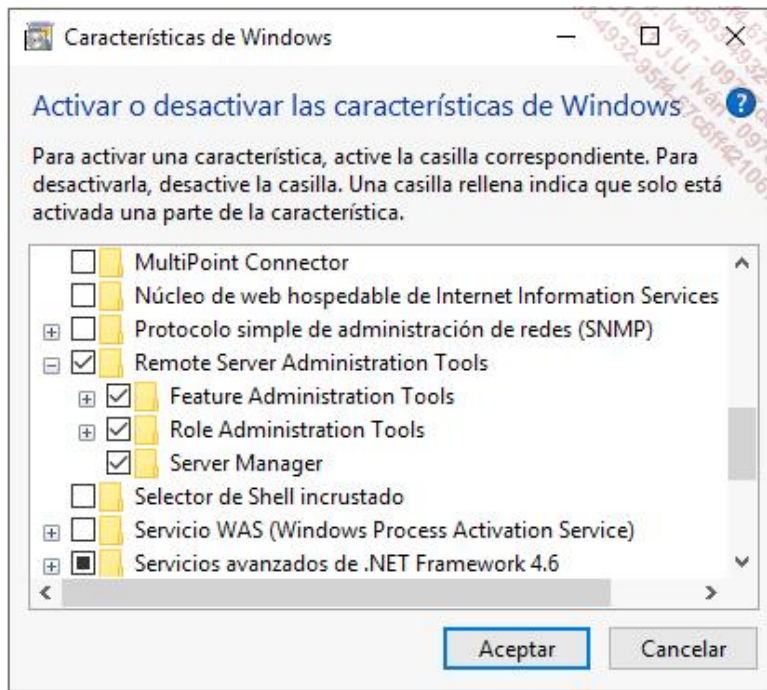
En términos de seguridad, es preferible evitar abrir una sesión remota en un servidor para su administración; es mejor dar prioridad al uso de un método seguro, a través de las herramientas RSAT.

En efecto, RSAT es por defecto seguro: solo los puertos y las excepciones de servicio requeridas para la gestión remota se definen en el firewall con las funcionalidades avanzadas de seguridad.

Puede administrar la versión Core (mínima) de Windows Server 2012 desde las herramientas RSAT. Después de haber instalado esas herramientas como administrador del puesto con Windows 10, todas las herramientas de administración están activadas, a diferencia de las anteriores versiones de RSAT.

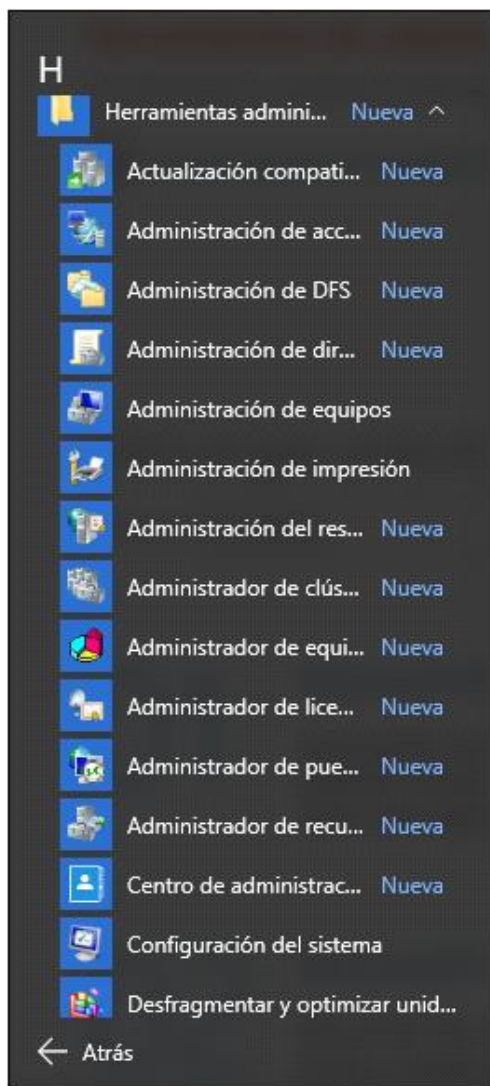
Para desactivar un componente RSAT, el administrador debe utilizar la interfaz **Programas y características**:

- Haga clic con el botón derecho del ratón en el menú **Inicio** y haga clic en **Programas y características** y en **Activar o desactivar las características de Windows**.
- Despliegue **Remote Server Administration Tools** y seleccione las herramientas de administración remota para eliminar.



→ Confirme pulsando **Aceptar**.

Para acceder a las herramientas de administración remota del servidor, podemos emplear diversos caminos; el más habitual es seleccionar **Todas las aplicaciones** en el menú **Inicio** y la opción **Herramientas administrativas**.



➤ Las herramientas RSAT solo pueden administrar recursos remotos, no locales.

Cuando las herramientas de administración RSAT instalan las consolas de gestión de los roles y características, se instalan también los comandos PowerShell que permiten administrarlas. El comando **Get-Command -Module NOMBREMODULO** (por ejemplo, **RDManagement** para Remote Desktop Services) permite enumerar estos nuevos comandos.

En adelante, la administración de roles y características, tales como DHCP, servicios Active Directory o incluso el equilibrio de carga, es mucho más sencilla desde un ordenador equipado con Windows 10 Enterprise o Windows 10 Pro.

3. PowerShell

PowerShell versión 5.0 combina un lenguaje de scripting y un intérprete por línea de comandos que permite gestionar y automatizar las acciones de administración de los sistemas Microsoft. El lenguaje está incluido en Windows 10 y es ejecutable en los ordenadores remotos en segundo plano. Los applets de comando permiten gestionar eficazmente el registro, los procesos, el registro de eventos, etc.

PowerShell, que necesita .NET Framework 5.0, proporciona un entorno gráfico (*PowerShell Integrated Scripting Environment* o *ISE*) que incluye un depurador. Permite la ejecución planificada de archivos de comando, la ejecución selectiva de código y la modificación multilingüe.

En particular, el administrador puede, de este modo, gestionar mediante comandos un dominio Active Directory, incluyendo las copias de seguridad, los servicios de acceso remoto, pero también ordenadores miembros de un grupo de trabajo (base de registro, sistema de archivos, etc.) y funcionalidades como Hyper-V o BitLocker.

La versión PowerShell suministrada con Windows 10 aporta nuevas mejoras, entre las que cabe destacar:

- **Gestión de métodos abreviados de teclado:** se soportan las funciones copiar ([Ctrl] + **C**), pegar ([Ctrl] + **V**) o seleccionar todo ([Ctrl] + **A**).
- **Gestión de vínculos simbólicos:** empleando el comando **New-Item** podemos crear o eliminar enlaces simbólicos.
- **Registro dedicado en el Visor de eventos:** el registro **Windows PowerShell** está disponible a partir del nodo **Registro de aplicaciones y servicios**.
- **Comando PSEDIT:** en adelante podremos editar archivos de forma remota empleando una sesión de PowerShell.
- **OneGet:** permite importar paquetes de terceros para gestionar mejor las aplicaciones y el sistema operativo.
- **PowerShellGet:** importación por Internet de nuevos módulos PowerShell.
- **Gestión de archivos:** gestión de archivos de tipo ZIP empleando los comandos **compress-archive** o **expand-archive**.

Con Windows 10, Microsoft soporta la funcionalidad en PowerShell llamada *Windows PowerShell Desired State Configuration* (DSC). El administrador puede, en adelante, gestionar el despliegue y la configuración de varios entornos de forma automatizada:

- Activación o desactivación de roles o servicios.
- Gestión de configuración básica del registro.
- Gestión de archivos y carpetas.
- Inicio y detención de servicios o procesos.
- Despliegue de software.
- Gestión de grupos y usuarios.

DSC proporciona nuevos comandos y recursos PowerShell.

Los applets de comando PowerShell tienen una sintaxis precisa: un verbo y un nombre separados por un guion (-).

El lenguaje permite conectar los applets entre sí para realizar una serie de acciones, separándolos con un pipe ("|"). Es posible crear, también, expresiones condicionales.

El administrador utiliza con frecuencia los verbos Get (obtener), Set (configurar) o Format durante la ejecución de los comandos.

PowerShell gestiona la definición de variables, que para declarar precedemos del carácter "\$" y a las que asignamos un valor después del símbolo "=".

Ejemplo: el comando **\$d=get-process | where-object {\$_.WorkingSet -gt 5000000}** almacena en la variable "d" los procesos locales cuyo umbral de trabajo sea superior a 5 MB. Para mostrar el valor de la variable y su resultado, bastará con teclear **echo \$d** o simplemente **\$d**.

```

Administrador: Windows PowerShell
Windows PowerShell
Copyright (C) 2012 Microsoft Corporation. Todos los derechos reservados.
PS C:\Windows\system32> $d=get-process | where-object {$_.WorkingSet -gt 5000000}
PS C:\Windows\system32> echo $d

Handles NPM(K) PM(K) VS(K) VM(K) CPU(s) Id ProcessName
-----
180 10 6032 9060 39 0.11 2904 audiodg
75 8 1972 7164 56 0.05 2964 conhost
166 19 1308 5524 44 6.43 684 csrss
331 10 3796 10988 72 0.20 1636 dashost
192 19 90432 33932 204 1.73 1064 dun
1435 82 54008 85756 586 11.86 300 explorer
137 11 2432 8464 102 0.03 3504 FlashUtil_ActiveX
617 47 12180 36888 197 4.02 192 iexplore
1015 129 149560 137572 386 160.46 2804 iexplorer
409 40 31308 44908 260 20.05 3324 iexplorer
651 45 14808 21672 1001 2.93 1540 LiveConn
877 22 5852 10536 36 10.00 776 lsass
416 74 69004 57248 212 185.60 1756 MsMpEng
510 75 40492 55272 203 8.70 3516 nspaint
401 31 104488 115576 624 2.12 3424 powershell
227 15 3308 15604 102 0.90 2968 RuntimeBroker
645 53 24204 23532 540 6.10 1580 SearchIndexer
240 12 3004 7000 31 2.06 760 services
453 25 5460 11272 82 5.05 1368 spoolsv
735 37 9716 16576 107 1.40 568 svchost
447 25 56548 54072 126 30.52 680 svchost
365 13 2900 8608 37 0.07 856 svchost
431 15 3576 7012 20 1.59 896 svchost
760 29 24664 26760 120 4.10 960 svchost
1543 62 17432 31200 541 14.07 1004 svchost
674 147 10408 26072 1434 7.50 1104 svchost
568 41 17044 17892 356 33.51 1416 svchost
143 11 1976 6596 43 0.05 1700 svchost
435 35 4672 11072 55 1.06 2100 svchost
249 16 2672 9804 94 4.10 1516 tabtip
316 21 5516 11812 62 0.41 1696 taskhost
279 27 5560 12124 492 0.62 1092 taskhostex
137 12 5400 10472 101 0.70 2500 IPAutoConnect
139 11 1068 4908 61 0.19 1000 IPAutoConnSvc
200 21 10512 10112 89 13.26 1720 vmtoolsd
259 24 10016 10340 130 13.31 2500 vmtoolsd
170 10 1672 12600 60 0.16 720 winlogon

```

Para acceder al archivo de ayuda de un applet, utilice el comando **get-help** seguido del nombre del applet. Para conocer la lista de applets, utilice el comando **get-command**.

El intérprete por línea de comando PowerShell es accesible en Windows 10 desde el escritorio:

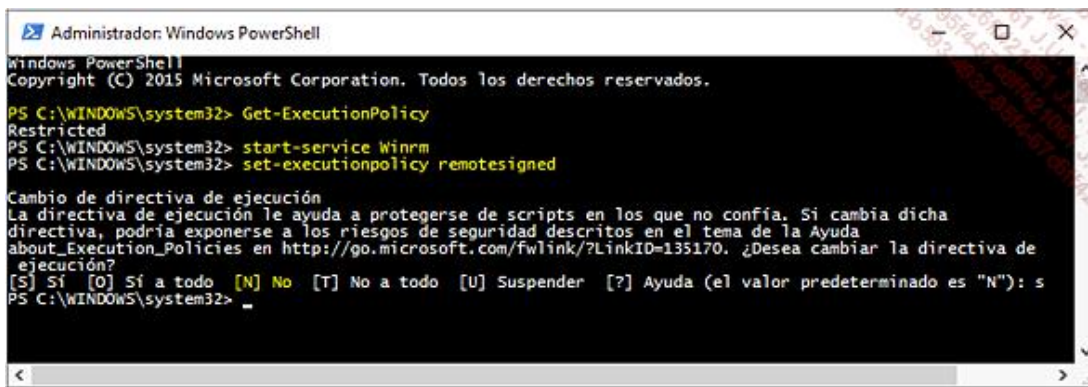
- ➔ Introduzca **powershell** en el campo de búsqueda situado en la barra de tareas y, a continuación, haga clic con el botón derecho en **Windows PowerShell** y seleccione **Ejecutar como administrador**. Acepte haciendo clic en el botón **Sí** cuando aparezca la ventana de control de cuentas de usuario.

La línea de comandos Windows PowerShell ejecuta por defecto los comandos, pero no los scripts (extensión .ps1): es el modo **Restricted**. Para conocer el modo actual, introduzca el comando **get-executionpolicy** en la línea de comandos PowerShell.

Existen otros tres modos de ejecución de scripts:

- **AllSigned**: se ejecutan los scripts firmados por un proveedor aprobado.
- **RemoteSigned**: es posible ejecutar un script creado por el administrador, pero no un script proveniente de Internet.
- **Bypass**: todos los scripts firmados y no firmados se ejecutarán, sea cual sea su procedencia.

Para definir el modo de ejecución de los scripts en **RemoteSigned**, introduzca el comando **set-executionpolicy remotesigned** desde una línea de comandos PowerShell ejecutada con privilegios de administrador.



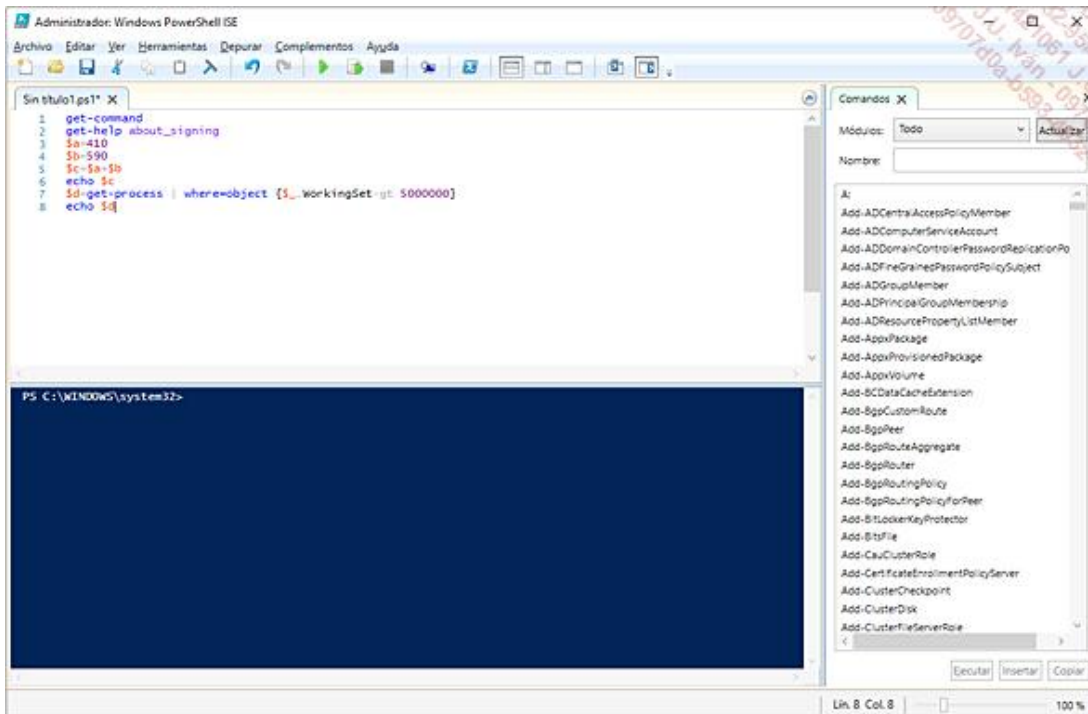
```
Administrador: Windows PowerShell
Windows PowerShell
Copyright (C) 2015 Microsoft Corporation. Todos los derechos reservados.

PS C:\WINDOWS\system32> Get-ExecutionPolicy
Restricted
PS C:\WINDOWS\system32> start-service WinRM
PS C:\WINDOWS\system32> set-executionpolicy remotesigned

Cambio de directiva de ejecución
La directiva de ejecución le ayuda a protegerse de scripts en los que no confía. Si cambia dicha
directiva, podría exponerse a los riesgos de seguridad descritos en el tema de la Ayuda
about_Execution_Policies en http://go.microsoft.com/fwlink/?LinkID=135170. ¿Desea cambiar la directiva de
ejecución?
[S] Sí [O] Sí a todo [N] No [T] No a todo [U] Suspender [?] Ayuda (el valor predeterminado es "N"): s
PS C:\WINDOWS\system32>
```

PowerShell presenta una interfaz gráfica llamada **Windows PowerShell ISE** disponible tecleando el comando **powershell_ise.exe** desde una ventana PowerShell o un símbolo del sistema.

También es posible ejecutar un script línea a línea, definir puntos de interrupción y visualizar el resultado en una ventana. El script generado puede guardarse con la extensión .ps1. La interfaz ISE tiene tres paneles y una pestaña que representa el script actual: el panel de comandos, situado arriba; el panel de salida, abajo, y el panel de ejecución de los módulos adicionales, a la derecha. Una herramienta de autocompletado asiste al administrador durante la introducción de comandos.



En cuanto a la ejecución de scripts en máquinas remotas, PowerShell necesita el protocolo WinRM (*Windows Remote Management*) y .NET Framework 5.0, ambos instalados en el ordenador de origen y en los de destino.

Windows 10 no activa de forma predeterminada la ejecución de scripts remotos, a diferencia de Windows Server 2012.

Para activarla, desde una ventana PowerShell ejecute el siguiente procedimiento como administrador del puesto con Windows 10:

- ➔ Inicie el servicio WinRM escribiendo **start-service WinRM**. Active la ejecución de scripts de forma remota: **enable-psremoting -force**. Observe que el comando **winrs** permite ejecutar un comando en un puesto

remoto, mostrando el resultado en el ordenador local.



Para que la activación de la ejecución de scripts esté operativa, solo hace falta que una tarjeta de red del ordenador esté definida en el perfil público.

Se presentan tres modos de comunicación:

- **Comunicación directa:** permite ejecutar un script en un ordenador específico.
- **Comunicación con distribución ramificada:** establece una comunicación con varios ordenadores y ejecuta los comandos cuyo resultado se mostrará en el ordenador de origen.
- **Comunicación de «varios a uno»:** varios administradores crean conexiones con diferentes privilegios en un único ordenador.

Al crear una conexión, esta puede ser temporal o permanente.

Una conexión temporal se cierra al terminar la ejecución del comando en el equipo remoto. El administrador utilizará el applet de comando **invoke-command** especificando el o los nombres DNS o NetBIOS de los equipos remotos.

Una conexión permanente se inicia mediante el applet **new-ssession** y se utiliza con el comando **enter-ssession**. La desconexión de una sesión activa se efectúa empleando **disconnect-ssession**. La lista de sesiones persistentes se muestra con el comando **get-ssession**.



Puede utilizar el parámetro **UseSSL** para cifrar la comunicación durante la utilización de los applets de comando **invoke-command**, **new-ssession** y **enter-ssession**.

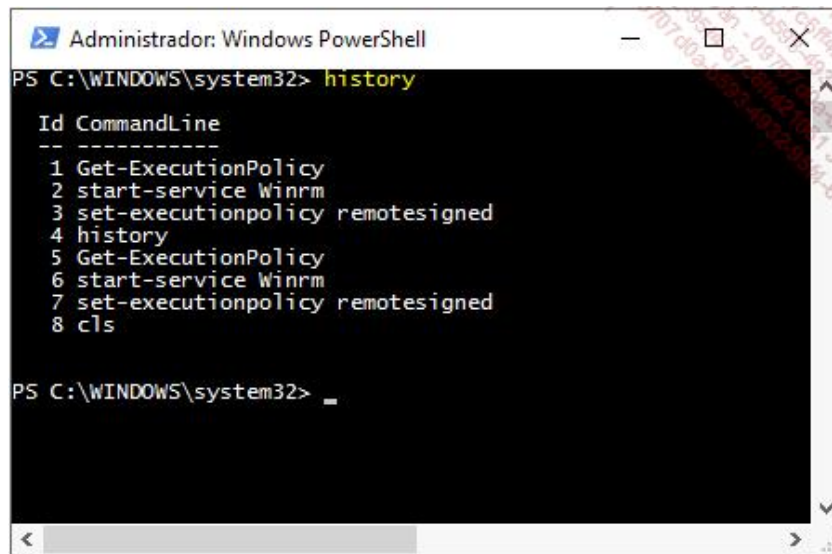
El comando se ejecuta en el equipo remoto, los resultados se muestran en el equipo local.

En un dominio Active Directory, los scripts PowerShell también pueden realizar un gran número de operaciones sobre los objetos de directiva de grupo, como unirlos a UO (Unidades Organizativas), modificarlos o eliminarlos, definir permisos, etc., mediante un módulo de importación llamado **import-module grouppolicy**.

Para conocer la lista de comandos PowerShell vinculados a las políticas de grupo, utilice el comando **get-help**.

Los comandos frecuentes de administración en un símbolo del sistema tienen su equivalente en lenguaje PowerShell, por ejemplo **Ipconfig** corresponde a **Get-NetIPConfiguration**, **Net Start** a **Start-Service** y finalmente **Shutdown** a **Restart-Computer**.

Visualizar el histórico de los últimos 30 comandos escritos es simple, basta con utilizar el commando **history** o pulsar la tecla [F7].

A screenshot of a Windows PowerShell window titled 'Administrador: Windows PowerShell'. The prompt is 'PS C:\WINDOWS\system32>'. The user has entered the command 'history', which has resulted in a list of commands numbered 1 through 8. The commands are: 1 Get-ExecutionPolicy, 2 start-service Winrm, 3 set-executionpolicy remotesigned, 4 history, 5 Get-ExecutionPolicy, 6 start-service Winrm, 7 set-executionpolicy remotesigned, and 8 cls. The prompt is now 'PS C:\WINDOWS\system32> _'.

Podemos invocar un comando con un **ID** específico mediante el comando **invoke-history ID**.

4. Reparación remota

Un administrador debe desplazarse a menudo hasta un servidor para poder configurarlo y garantizar su disponibilidad. El **Escritorio remoto** permite salvar esta distancia mediante una conexión de red. Pero un usuario puede también solicitar ayuda haciendo una llamada de **Asistencia remota**: en un caso, es el administrador quien se conecta por decisión propia a un recurso (Escritorio remoto); en el otro, es invitado (Asistencia remota).

a. Escritorio remoto

El Escritorio remoto conecta dos ordenadores, un cliente y un servidor, a una red, o desde Internet a través, por ejemplo, de una conexión VPN. Cuando el administrador está conectado, visualiza el escritorio del equipo remoto como si estuviera delante de él y tiene acceso a todos los programas y documentos almacenados, así como a los dispositivos conectados.

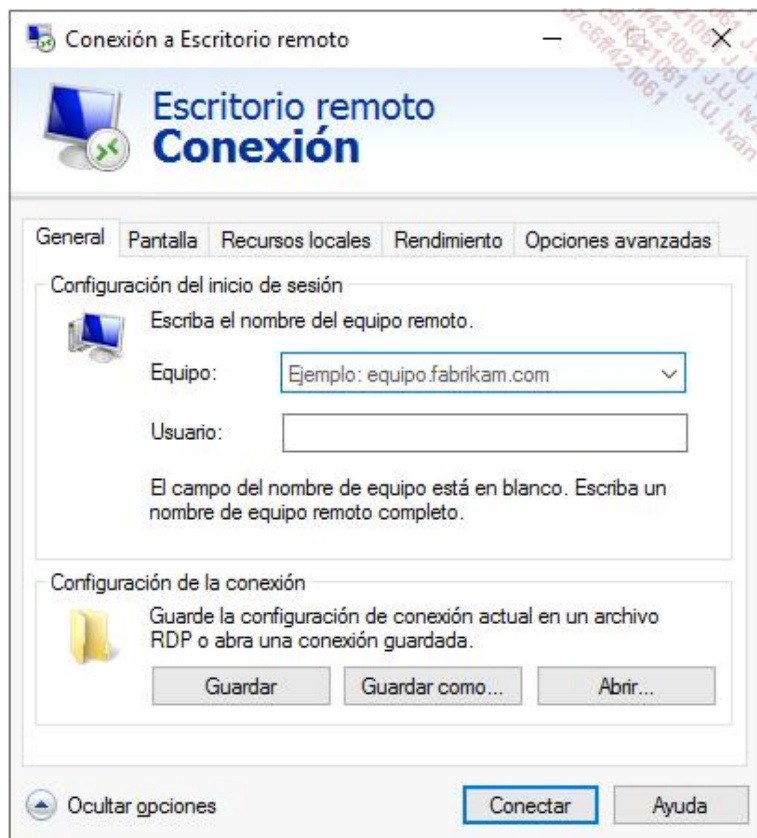
La característica Escritorio remoto está basada en una arquitectura cliente/servidor:

- **El servidor:** establecer una conexión a un equipo a través del método de Escritorio remoto implica la apertura del puerto TCP 3389 de entrada y, por tanto, la posibilidad de permitir que un atacante se conecte de manera remota a un puesto de la red corporativa. Conviene, pues, ser prudente durante la activación de esta característica y evaluar correctamente sus consecuencias.
- **El cliente:** es un software proporcionado con las cuatro ediciones de Windows 10 que permite conectarse a un servidor o a otro puesto de trabajo con Microsoft Windows desde una red (cableada, inalámbrica, 3G...). Las ediciones **Equipo de trabajo** siguientes soportan conexiones de Escritorio remoto: Windows 7 (Profesional, Enterprise y Ultimate), Windows Vista (Professional, Enterprise y Ultimate), Windows XP Profesional, Windows 8.1 Profesional y Enterprise y, por supuesto, Windows 10.

Para ejecutar el cliente de Escritorio remoto:

→ Desde el campo de búsqueda situado en la barra de tareas introduzca **Conexión a escritorio remoto**.

Otra forma de ejecutarlo desde el escritorio del usuario: señale con el ratón abajo a la izquierda de la pantalla, haga clic con el botón derecho en el menú **Inicio** y, a continuación, en **Ejecutar**. Introduzca **mstsc** y confirme con la tecla [Intro].

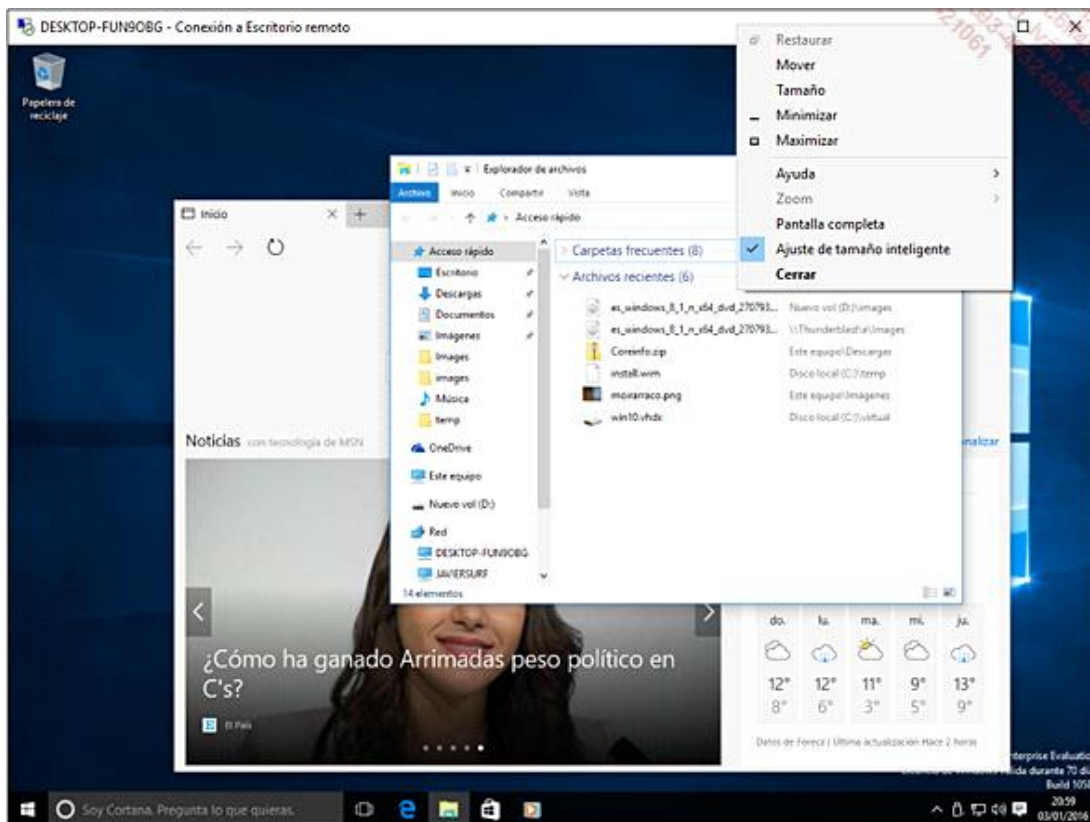


- Observe que el cliente de Escritorio remoto permite también establecer la conexión a la tecnología Microsoft RDS (*Remote Desktop Services*).

También es posible mostrar el escritorio remoto del ordenador al que estamos conectados de forma segura a través del protocolo RDP. Las opciones siguientes están disponibles mediante las diferentes pestañas del software cliente, haciendo clic en la flecha que apunta hacia abajo **Mostrar opciones**:

- La pestaña **General** gestiona la información de identificación de inicio de sesión (**Nombre de usuario** y contraseña), así como el nombre DNS o la dirección IP del **Equipo** remoto. El usuario puede guardar la **Configuración de la conexión** en un archivo con extensión **.rdp**.
- La pestaña **Pantalla** permite definir la resolución del escritorio remoto y la profundidad de los colores.
- La pestaña **Recursos locales** ofrece al administrador la configuración de la redirección de los recursos del puesto con Windows 10 al servidor (sonido, impresoras, teclado, etc.).
- Con esta nueva versión del cliente de Escritorio remoto, ahora es posible redirigir un dispositivo USB, como una memoria flash. En la pestaña **Recursos locales**, haga clic en el botón **Más**, despliegue el nodo **Unidades** y, si el dispositivo USB no está conectado, seleccione la opción **Unidades que conectaré más tarde**.
- La pestaña **Rendimiento** permite definir el ancho de banda utilizado durante la conexión al Escritorio remoto, para optimizar la visualización de las funcionalidades tales como el suavizado de fuentes, el estilo visual, etc.
- La pestaña **Opciones avanzadas** define el comportamiento del cliente en caso de fallo durante la autenticación con el servidor o los parámetros de conexión de la puerta de enlace del Escritorio remoto.

Una vez iniciada la conexión al equipo remoto, el usuario puede redimensionar automáticamente la ventana **Conexión a Escritorio remoto** haciendo clic con el botón derecho en la cabecera y seleccionando **Ajuste de tamaño inteligente**.

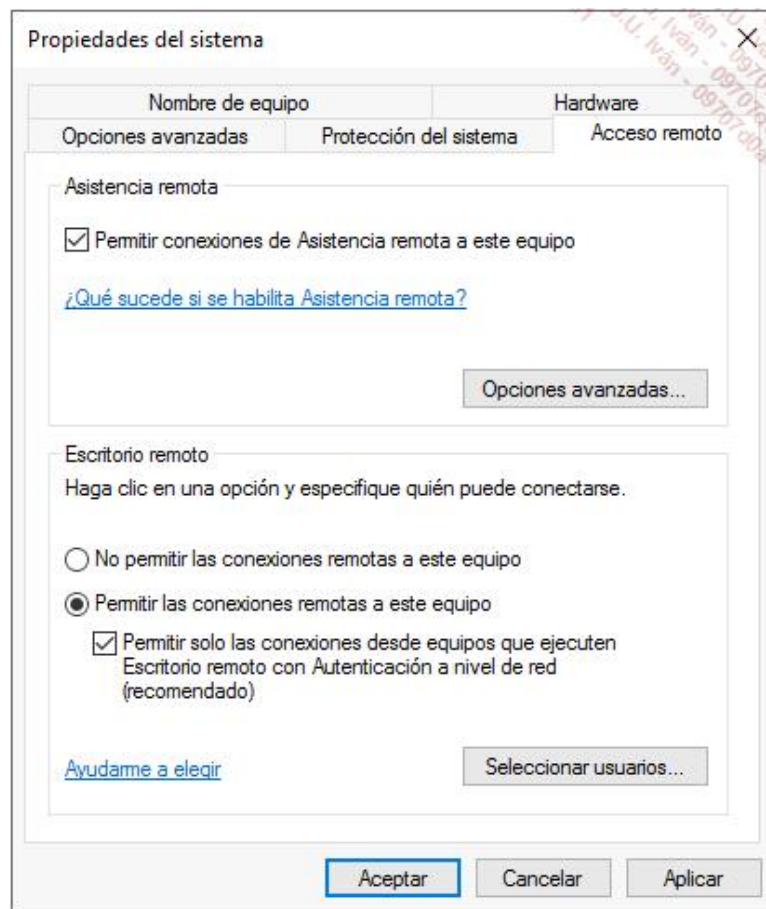


El Escritorio remoto bloquea el sistema objetivo impidiendo temporalmente un inicio de sesión interactivo.

Por último, el cliente se encarga del fraccionamiento en varias pantallas horizontales, con el objetivo de formar un único escritorio de mayor tamaño, empleando el comando **mstsc /span**.

Para activar el Escritorio remoto del lado servidor, en nuestro caso un puesto de trabajo con Windows 10, siga este procedimiento:

- ➔ Como administrador local, haga clic con el botón derecho en el menú **Inicio** y, a continuación, en **Sistema**. Haga clic en **Configuración de acceso remoto** y, a continuación, en la pestaña **Acceso remoto** marque la opción **Permitir las conexiones remotas a este equipo**.



Para mejorar la seguridad de la conexión, la opción **Permitir solo las conexiones desde equipos que ejecuten Escritorio remoto con Autenticación a nivel de red** está marcada por el sistema. El puerto TCP 3389 se abrirá de forma automática en sentido entrante en el firewall de Windows 10 para los perfiles **Privado** y **Público** de la tarjeta de red. Para cambiar el puerto de escucha predeterminado y así mejorar la seguridad del servidor, modifique el valor de la clave **PortNumber**, accesible en el nodo **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TerminalServer\WinStations\RDP-Tcp** del registro.

→ Haga clic en el botón **Seleccionar usuarios** para agregar al grupo local **Usuarios del Escritorio remoto** las cuentas o grupos con permisos de acceso remoto al servidor RDP de Windows 10.

Observe que solo las ediciones Profesional y Enterprise de Windows 10 soportan la activación del Escritorio remoto en modo servidor.

b. Aplicación Escritorio remoto de la Tienda (Windows Store)

Microsoft presenta en descarga desde la Tienda la aplicación gratuita **Escritorio remoto**. La principal ventaja es la posibilidad de agrupar en un emplazamiento centralizado las conexiones activas.

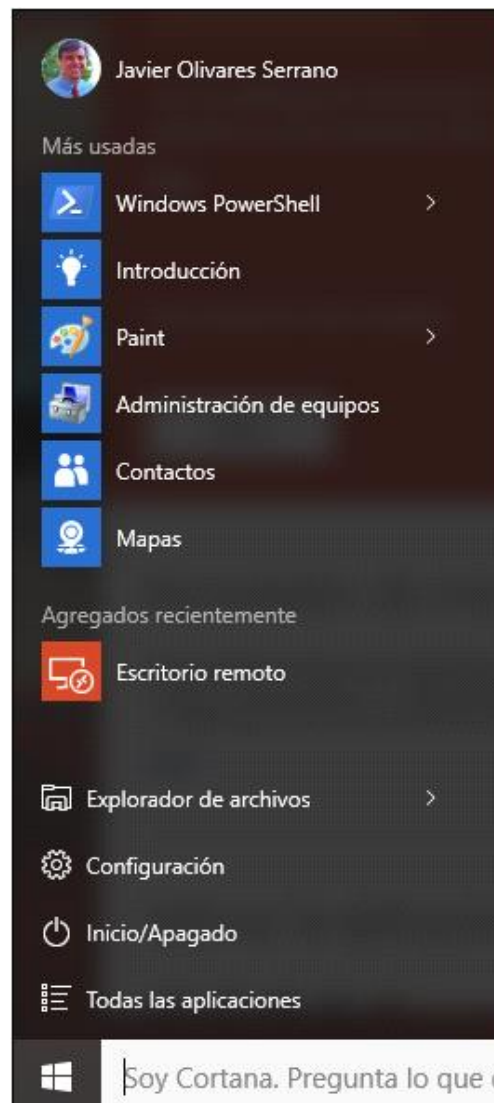
Mediante el uso compartido de la pantalla, el administrador puede en todo momento vigilar un ordenador remoto mientras continúa con sus tareas habituales. Orientado a tabletas táctiles, la aplicación gestiona el zoom al separar los dedos o el teclado en pantalla. Se incluyen nuevas funcionalidades, ofreciendo un uso más fluido en una sesión remota: **RemoteFX Multi-Touch Remoting** (gestión de los 10 dedos de las manos), **RemoteFX Multimedia and Sound** y **RemoteFX EasyPrint** (impresión simplificada en el equipo remoto).

Para descargar e instalar la aplicación **Escritorio remoto**:

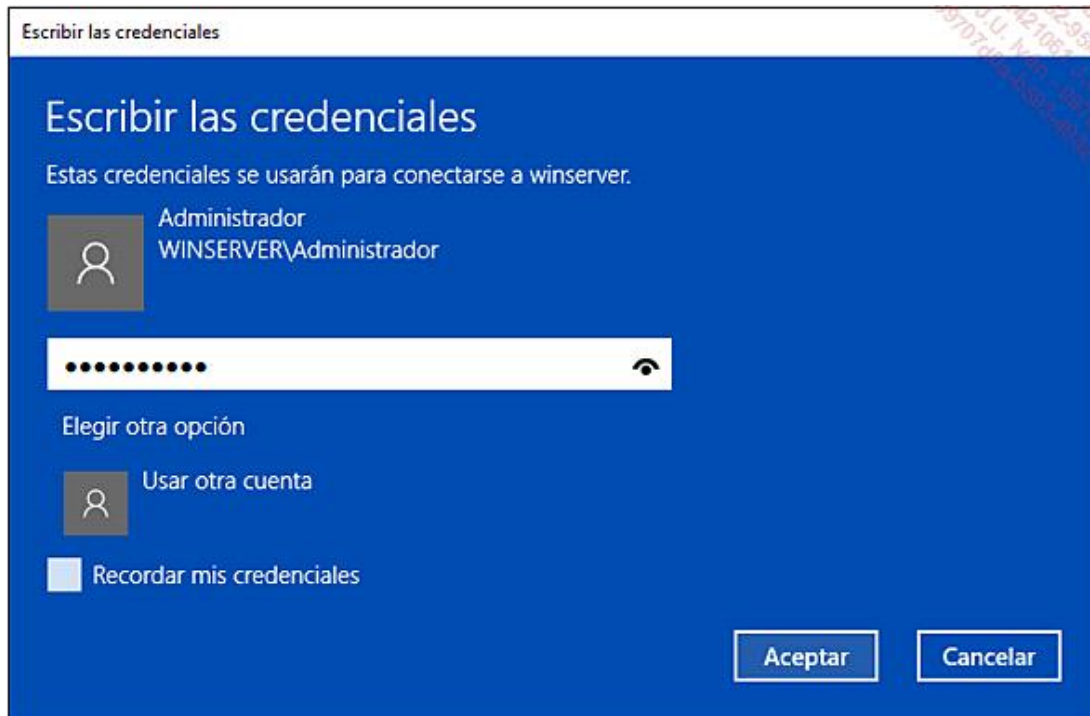
→ Desde el icono **Tienda** situado en la barra de tareas, introduzca **escritorio remoto** en la zona de búsqueda (arriba a la derecha) y acepte señalando a la lupa. Seleccione la aplicación **Escritorio remoto** en los resultados de la búsqueda y, a continuación, seleccione el botón **Instalar**.



Una vez instalada la aplicación, el icono **Escritorio remoto** está disponible en el menú **Inicio** en la sección **Agregados recientemente**.

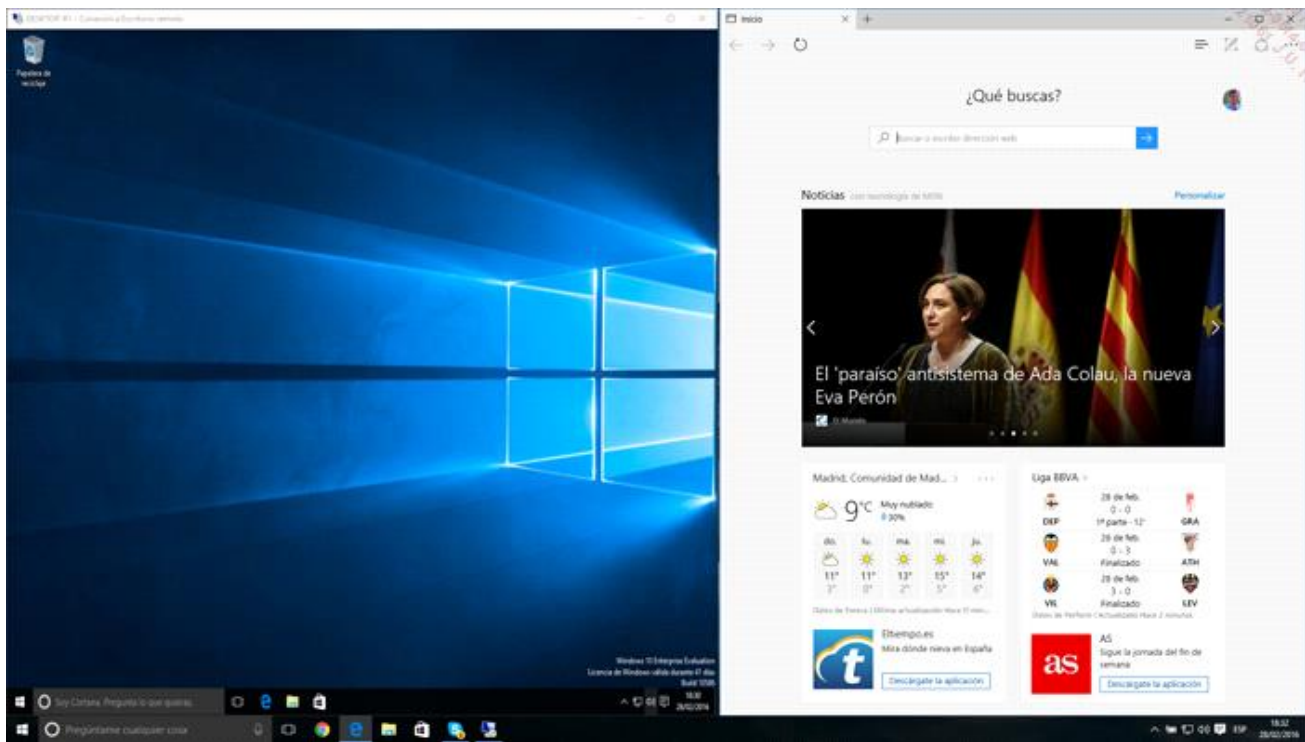


- Al ejecutar la aplicación, se solicita al administrador que teclee el nombre del equipo remoto o su dirección IP y, a continuación, haga clic en el botón **Conectar**. Se requiere obligatoriamente el nombre de usuario y una contraseña. El nombre del dominio es opcional y puede definirse respetando el método siguiente: **NOMBREDOMINIO\Nombre de usuario**. Si el equipo remoto forma parte de un grupo de trabajo, deberemos agregar **localhost\nombre de usuario**. La aplicación intenta, a continuación, autenticar el equipo remoto.



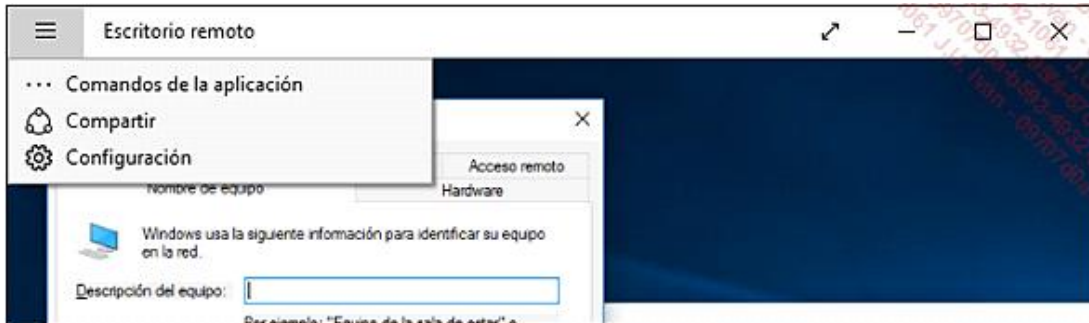
- Si la autenticación del equipo remoto no funciona, aparece un mensaje de aviso. Marque la opción **No volver a preguntarme sobre conexiones a este equipo** y, a continuación, haga clic en el botón **Conectarse de todas formas**. Se establece la conexión, el administrador tendrá, en adelante, acceso completo a los recursos (carpetas, archivos, impresoras, etc.) del equipo conectado.

Es posible poner la aplicación Escritorio remoto en una mitad de la pantalla. En nuestro ejemplo, la aplicación Escritorio remoto muestra un equipo remoto con Windows 10 a la izquierda de la pantalla y el navegador Edge se ubica a la derecha:





Los parámetros de conexión pueden definirse de la misma forma que el Escritorio remoto accesible desde el escritorio:

- Señale la esquina superior izquierda de la pantalla (tres barras horizontales) de la aplicación **Escritorio remoto**, y haga clic en **Configuración**.



- El administrador puede configurar los efectos visuales, definir qué dispositivos (impresora, micrófono, etc.) del ordenador local se utilizarán al conectar al ordenador remoto o informar la dirección de la puerta de enlace del Escritorio remoto.

 Configuración de la conexión

Apariencia

Elegir efectos visuales para mí (según las condiciones de la red)

Activado ☒

Dispositivos

Usar los dispositivos de este equipo cuando esté conectado a un equipo remoto

Impresora

Activado ☒

Portapapeles

Activado ☒

Tarjeta inteligente

Activado ☒

Micrófono

Desactivado ☐

Audio

Reproducir en este equipo ▼

Puerta de enlace de Escritorio remoto

Si el administrador de red ha configurado un servidor de puerta de enlace, se podrá conectar a los equipos de la red corporativa

Nombre del servidor

Opciones avanzadas

Mostrar miniaturas de escritorios recientes en la pantalla de inicio

Activado ☒

En **Configuración**, también es posible introducir la dirección de un servidor RemoteApp, tecnología diferente de una sesión RDS: la aplicación remota aparece como si se ejecutara en el equipo local. La única diferencia visible es el borde de la ventana, que mantendrá la apariencia de Windows Server 2008 y no la de Windows 10.

Un programa RemoteApp puede ejecutarse de tres maneras:

- A partir de un archivo con la extensión RDP distribuido por el administrador.
- Mediante un archivo Windows Installer (.msi) implementado mediante un objeto de directiva de grupo.
- Con un vínculo al programa RemoteApp disponible desde un sitio de Internet gestionado por los servicios RDS.

© Éditions ENI – Todos los derechos reservados – Copia personal de Iván J.U.

- 17 -

c. RemoteFX

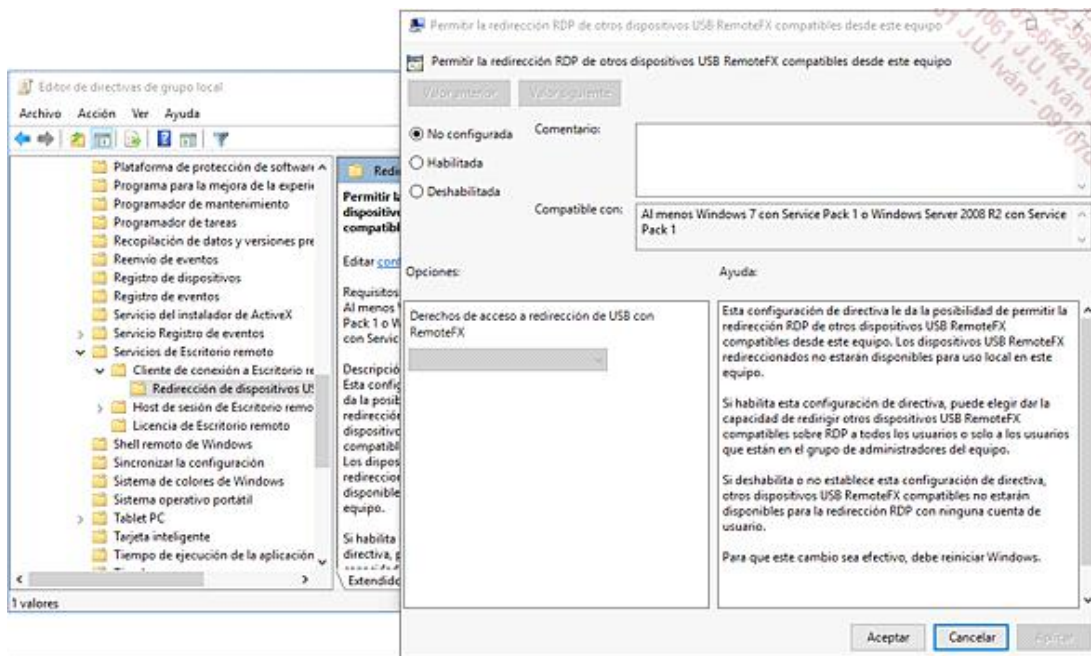
Aparecido con Windows Server 2008 R2 Service Pack 1, RemoteFX se basa en el protocolo RDP (*Remote Desktop Protocol*) para ofrecer una experiencia de usuario mejorada en el caso de una conexión remota: es capaz de tener en cuenta la visualización de vídeos, la redirección de dispositivos (impresora, cámara) o la audición de música.

Mediante la virtualización del puesto de trabajo VDI (*Virtual Desktop Infrastructure*) hospedada en un servidor Hyper-V o RDS, los recursos de hardware de aceleración gráfica de este serán compartidos entre los usuarios.

Disponible con Windows 10 Enterprise, esta tecnología puede utilizar también el hardware cliente para proporcionar contenido multimedia, en vez de los recursos del servidor remoto, reduciendo de esta manera el uso del ancho de banda.

RemoteFX USB Redirection permite que un dispositivo USB (escáner, impresora multifunción...) conectado a un servidor sea redirigido a un puesto con Windows 10 sin necesidad de instalar el controlador correspondiente. Para configurar la actualización de esta tecnología, es necesario utilizar el **Editor de directivas de grupo local**:

- Pulse las teclas **Win** + **R** del teclado e introduzca **gpedit.msc** y confirme con el botón **Aceptar**. En la ventana **Editor de directivas de grupo local**, despliegue el nodo **Configuración del equipo - Plantillas administrativas - Componentes de Windows - Servicios de Escritorio remoto - Cliente de Conexión a Escritorio remoto y Redirección de dispositivos USB RemoteFX**. Haga doble clic, por ejemplo, en el parámetro **Permitir la redirección RDP de otros dispositivos USB RemoteFX compatibles desde este equipo**. Seleccione la opción **Habilitada**.



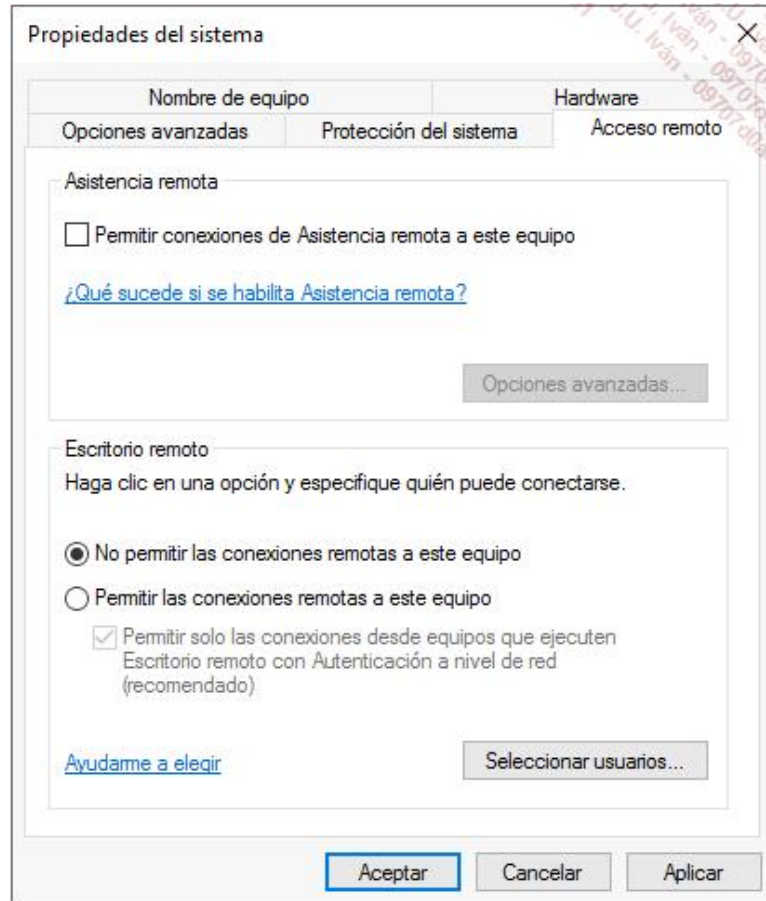
- Confirme haciendo clic en **Aceptar**.

d. Asistencia remota

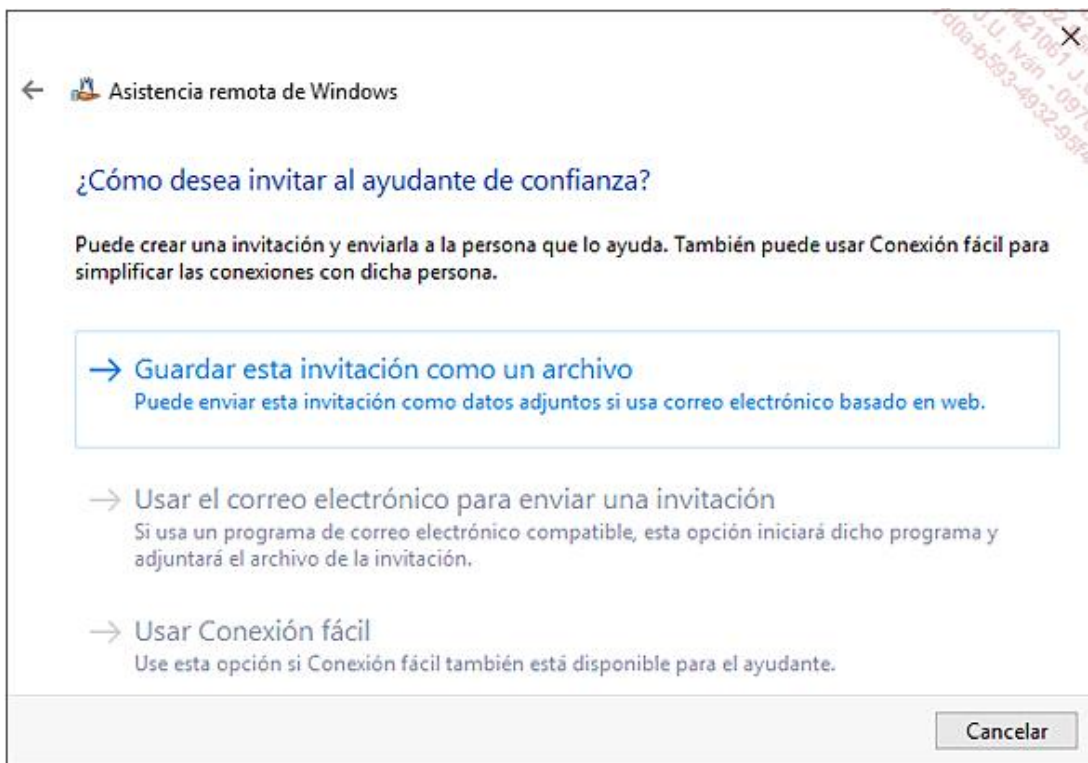
La característica **Asistencia remota** ofrece al usuario la posibilidad de solicitar ayuda a un administrador sin desconectarse de su sesión actual, viendo lo que hace el técnico, a diferencia del Escritorio remoto. También es posible conversar por escrito con el usuario remoto o enviarle archivos, como **Microsoft Fix it** (consulte el capítulo Protección y recuperación del sistema) para resolver problemas.

La asistencia remota está activada por defecto en Windows 10. Para desactivar esta característica:

- Desde el escritorio del usuario, haga clic con el botón derecho del ratón en el menú **Inicio** y, a continuación, seleccione **Sistema**. Haga clic en **Configuración de acceso remoto** y, a continuación, en la pestaña **Acceso remoto**, marque la opción **Permitir conexiones de Asistencia remota a este equipo**. Observe que, haciendo clic en el botón **Opciones avanzadas**, el usuario puede definir la duración de las invitaciones en la opción **Establezca por cuánto tiempo pueden permanecer abiertas las invitaciones**, así como la versión mínima de sistema operativo que puede conectarse a su equipo.



Con Windows 10, existen tres métodos que permiten solicitar ayuda desde el ordenador objetivo, como muestra la siguiente imagen:



- **Guardar esta invitación como un archivo:** crea un archivo con extensión .msrcIncident. Este archivo debe enviarse al técnico a través de un recurso compartido de red, de un almacenamiento extraíble o bien por correo electrónico.
- **Usar el correo electrónico para enviar una invitación:** el proceso es el mismo que en el caso anterior, aunque el archivo de invitación se integra directamente en el programa de mensajería predeterminado.
- **Usar Conexión fácil:** esta característica permite solicitar ayuda haciendo que su equipo esté disponible desde Internet, sin enviar un archivo de invitación. La solicitud puede iniciarse directamente desde la lista de contactos del usuario con problemas.

Al usar Conexión fácil, el Asistente remoto genera una contraseña aleatoria para proporcionarle acceso a la persona que presta la asistencia. Una vez establecida la conexión, se intercambia la información de contacto entre los dos equipos. En lo sucesivo, no será obligatorio el uso de contraseña.

➤ Conexión fácil utiliza el protocolo PNRP (*Peer Name Resolution Protocol*) para enviar una invitación del Asistente remoto vía Internet: su router debe tener esto en cuenta.

Para arrancar la Asistencia remota y, por ejemplo, solicitar ayuda usando Conexión fácil, siga este procedimiento:

- ➔ Desde la barra de búsqueda ubicada en la barra de tareas, introduzca **msra** y seleccione **msra**.
- ➔ A continuación, haga clic en **Invitar a una persona de confianza para ayudarle**.
- ➔ Seleccione **Usar Conexión fácil** y, a continuación, siga las instrucciones en pantalla.

La Asistencia remota puede configurarse con precisión por línea de comandos utilizando el comando **msra.exe**:

- **/novice:** la Asistencia remota se ejecuta para solicitar ayuda.
- **/openfile:** abre un archivo de invitación específico.
- **/offereasyhelp:** utiliza la característica Conexión fácil ejecutando la Asistencia remota.
- **/expert:** el administrador presenta la ayuda mediante un archivo de invitación o Conexión fácil.

5. Enlaces remotos seguros

El acceso remoto de un puesto con Windows 10 designa el hecho de acceder a los datos almacenados en ordenadores conectados a una red, como Internet o una extranet.

Un usuario móvil, como un comercial, necesita acceder a los recursos de la empresa (carpetas, correos electrónicos...) desde fuera de la red.

Windows 10 presenta funcionalidades útiles para hacer que el sistema de información esté disponible y sea seguro para los usuarios itinerantes.

Por ejemplo, con **DirectAccess**, el administrador podrá acceder fácilmente a los servidores críticos de la empresa aun cuando esté lejos de ellos, sin ninguna intervención por su parte.

a. Cliente VPN

Windows 10 ofrece a los usuarios móviles la instalación de plug-ins VPN compatibles con las principales soluciones del mercado: Check Point, F5, Juniper Networks y SonicWall. Además, existen dos maneras de crear una conexión VPN: una mediante el Centro de redes y recursos compartidos, y la otra por medio de la nueva interfaz.

Vamos a detallar esta última:

- Desde la zona de búsqueda situada en la barra de tareas, introduzca **VPN** y haga clic en **Cambiar redes privadas virtuales (VPN)**. A continuación, haga clic en **Agregar una conexión VPN**. En el campo **Proveedor de VPN**, seleccione **Windows (integrado)**. Proporcione un nombre a la conexión en el campo **Nombre de conexión**. A continuación, indique la dirección del servidor remoto, un nombre de usuario y una contraseña. Asegúrese de que la opción **Recordar información de inicio de sesión** se encuentra marcada.

← Configuración

Agregar una conexión VPN

Proveedor de VPN

Windows (integrado)

Nombre de conexión

VPN JO

Nombre de servidor o dirección

139.54.23.18

Tipo de VPN

Automático

Tipo de información de inicio de sesión


- Nombre de usuario y contraseña
- Tarjeta inteligente
- Contraseña de un solo uso

Guardar Cancelar


La conexión a una red privada virtual estará disponible en adelante:

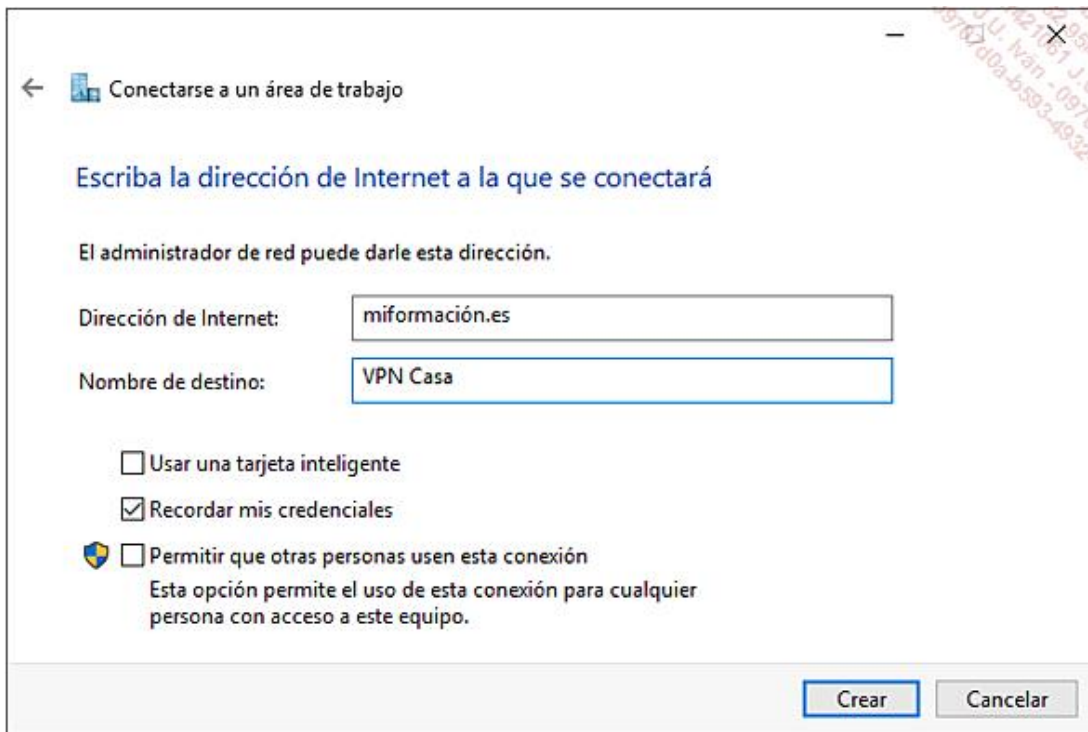


Observe que Windows 10 soporta también la autenticación mediante tarjeta o una OTP (*One Time Password*).

Para ejecutar la conexión VPN creada previamente, desde el escritorio, haga clic con el botón izquierdo en el icono de red  ubicado abajo a la derecha de su pantalla, en la barra de tareas, y, a continuación, seleccione su conexión VPN.

Si desea solamente utilizar el cliente VPN para conectarse a un servidor de acceso remoto de Microsoft, puede seguir este procedimiento:

- Haga clic con el botón derecho del ratón en el icono  y seleccione **Abrir el Centro de redes y recursos compartidos**. Haga clic en **Configurar una nueva conexión o red**. Introduzca la dirección de Internet del servidor VPN (en nuestro ejemplo, miformación.es) y llame a la conexión **VPN Casa**. Asegúrese de que la opción **Recordar mis credenciales** se encuentra marcada. Haga clic en **Crear**.



Su conexión VPN con el cliente Microsoft ha sido creada.

b. VPN Connect

El BYOD (*Bring Your Own Device*) es una práctica consistente en que un usuario utilice su propio ordenador personal en un contexto profesional. Esta tendencia, cada vez más extendida en las empresas, conlleva problemas sociales, como el hecho de que un trabajador puede trabajar en cualquier lugar, pero también a cualquier hora. Adicionalmente, los datos de la empresa están almacenados, en adelante, en equipos personales que no están gestionados por la política de la empresa. La seguridad se convierte en un gran problema con este tipo de prácticas.

La funcionalidad VPN Connect permite crear una conexión VPN de forma automática cuando se ejecuta una aplicación de Windows 10 o cuando el puesto de trabajo utiliza un sufijo DNS definido.

VPN Connect no funciona en un cliente miembro de un dominio, pero puede desplegarse con el nuevo cliente VPN Windows 10. El tipo de VPN soportado es obligatoriamente *Split Tunneling*, con el fin de no interrumpir la conectividad de otras aplicaciones cuando se establece la conexión VPN Connect.

Por ejemplo, para crear una conexión VPN automática cuando se ejecuta la aplicación Skype, debemos encontrar en primer lugar su identificador.

Partamos de la premisa de que el usuario ya ha creado una conexión VPN llamada VPNConnect:

- Desde la zona de búsqueda, introduzca **powershell** y, a continuación, haga clic con el botón derecho en **Windows PowerShell** y seleccione **Ejecutar como administrador**. Acepte haciendo clic en el botón **Sí** cuando la ventana de control de cuenta de usuario aparezca.
- Defina el tipo de VPN como *Split Tunneling* introduciendo el comando **Set-VpnConnection -name VPNConnect -SplitTunneling \$true** y, a continuación, acepte pulsando la tecla [Intro].

Busque ahora el identificador de la aplicación Skype:

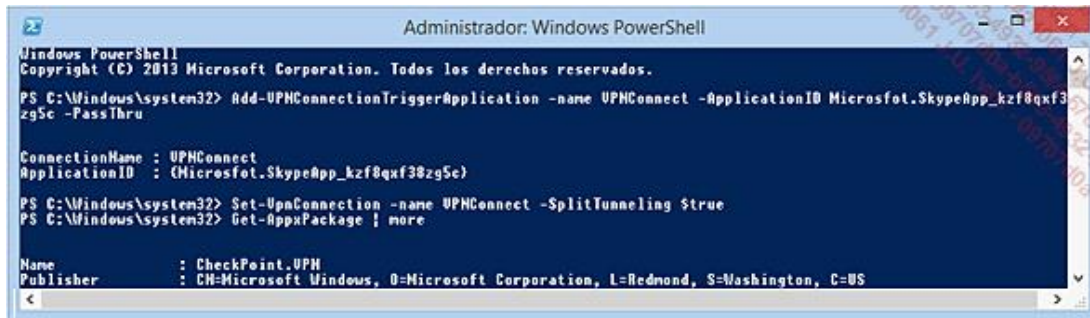
- Introduzca el comando **Get-AppxPackage | more** y acepte pulsando la tecla [Intro]. En nuestro ejemplo,

crearemos la conexión VPN cuando se ejecute la App Skype. Anote el valor del campo PackageFamilyName: **Microsoft.SkypeApp_kzf8qxf38zg5c**.

Ejecute la conexión VPNConnect al iniciar la aplicación Skype introduciendo el comando siguiente:

Add-VPNConnectionTriggerApplication -name VPNConnect -ApplicationID

Microsoft.SkypeApp_kzf8qxf38zg5c -PassThru y, a continuación, acepte con la tecla [Intro].



```
Administrador: Windows PowerShell
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. Todos los derechos reservados.
PS C:\Windows\system32> Add-VPNConnectionTriggerApplication -name VPNConnect -ApplicationID Microsoft.SkypeApp_kzf8qxf38zg5c -PassThru

ConnectionName : VPNConnect
ApplicationID    : (Microsoft.SkypeApp_kzf8qxf38zg5c)

PS C:\Windows\system32> Set-VPNConnection -name VPNConnect -SplitTunneling $true
PS C:\Windows\system32> Get-AppxPackage | more

Name           : CheckPoint.VPN
Publisher      : CN=Microsoft Windows, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
```

En adelante, cuando se ejecute la App Skype, se iniciará una conexión VPN automáticamente.



Cuando se cierre la App Skype, la conexión VPN también lo hará.

c. Reconexión automática VPN

Windows 10 ofrece a los usuarios itinerantes la capacidad de restablecer automáticamente una conexión VPN (*Virtual Private Network*) a la red corporativa en caso de corte temporal de Internet, sin intervención por parte del usuario.

Un túnel VPN proporciona a un usuario remoto una conexión a la red local de la empresa manteniendo la seguridad de los datos enviados.

Internet se usa generalmente como soporte de transmisión utilizando un protocolo de tunelización, encargado de encapsular los datos. Una conexión VPN vincula dos redes físicas mediante un enlace privado.

Existen dos tipos de conexiones VPN:

- **Acceso remoto VPN** (o VPN punto a sitio): permite a un usuario iniciar una conexión VPN desde su puesto de trabajo con Windows 10 hacia la red corporativa, generalmente a través de la red Internet.

- **VPN de sitio a sitio:** dos routers conectan dos sitios remotos a través de un enlace WAN seguro mediante una conexión permanente VPN, por ejemplo, la sede de una empresa situada en Madrid y su sucursal en Zaragoza. Así, los usuarios de Madrid pueden acceder a los recursos de Zaragoza (carpetas compartidas, impresoras...) y viceversa.

Windows 10 soporta cuatro protocolos de tunelización:

- PPP (*Point-to-Point Tunneling Protocol*).
- L2TP/IPsec (*Layer 2 Tunneling Protocol with Internet Protocol Security*).
- SSTP (*Secure Socket Tunneling Protocol*).
- IKEv2 (*Internet Key Exchange*).

La característica **Reconexión automática VPN** resulta especialmente práctica para los usuarios itinerantes. Así, un usuario remoto con una conexión a Internet activa podrá reconectarse automáticamente a los recursos de su empresa en caso de desconexión.

Esta funcionalidad utiliza el modo túnel de IPsec con IKEv2 y la extensión **MOBIKE** (Movilidad y Multihoming de IKEv2).

La infraestructura del lado del servidor que gestiona la instalación de la reconexión automática VPN es menos exigente que la de DirectAccess. Es necesario tener:


- Una infraestructura de clave pública (PKI) que proporcione un certificado para el equipo cliente.
- Un servidor VPN (Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 o Windows Server 2012 R2) con dos tarjetas de red, una conectada a Internet y la otra a la red local de la empresa. Los puertos UDP 500 para IKE y 4500 para IPsec deben estar autorizados en sentido entrante en el firewall.
- Un equipo con Windows 10 con la conectividad necesaria para acceder a la red remota.





Los sistemas operativos Windows Server 2008 R2, Windows Server 2012 y Windows 7/Windows 8.1 soportan también la reconexión automática VPN.

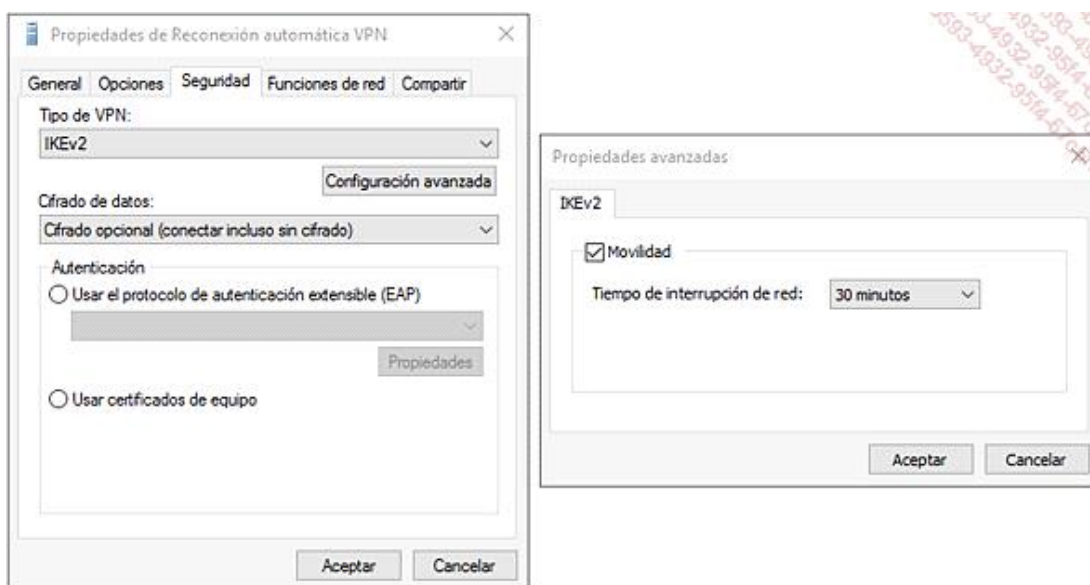
Para que el cliente Windows 10 pueda conectarse al servidor VPN, es necesario importar el certificado raíz emitido por este servidor.

He aquí el procedimiento, automatizable empleando un objeto de directiva de grupo:

- ➔ Pulse las teclas  + **R** e introduzca **mmc** y acepte con la tecla [Intro]. Confirme haciendo clic en el botón **Sí** cuando aparezca la ventana de control de cuentas de usuario. Haga clic en el menú **Archivo** y, a continuación, en **Agregar o quitar complemento**.
- ➔ En la lista de la izquierda, **Complementos disponibles**, seleccione **Certificados** y, a continuación, haga clic en el botón **Agregar**. En la ventana **Complemento Certificados**, seleccione la opción **Cuenta de equipo** y, a continuación, haga clic en **Siguiente** y **Finalizar**. Confirme con **Aceptar**.
- ➔ Despliegue en la zona de la izquierda **Certificados (equipo local)** y, a continuación, el nodo **Entidades de certificación raíz de confianza**. Haga clic con el botón derecho en **Certificados** y, a continuación, seleccione **Todas las tareas** e **Importar**. Haga clic en el botón **Siguiente** y, a continuación, seleccione el certificado raíz emitido usando el botón **Examinar**.

Una vez importado el certificado, podrá crear una conexión VPN:

- Haga clic con el botón derecho del ratón en el icono  y seleccione **Abrir el Centro de redes y recursos compartidos**. Haga clic en **Configurar una nueva conexión o red**. Introduzca la dirección de Internet del servidor VPN (en nuestro ejemplo, el servidor remoto que contiene el certificado importado) y llame a la conexión **Reconexión automática VPN**. Verifique que la opción **Recordar mis credenciales** se encuentra marcada. Haga clic en **Crear**.
- Haga clic en el botón **Guardar**.
- Para configurar los parámetros de seguridad que permitan la reconexión VPN, señale el icono Escritorio, haga clic con el botón derecho en el icono  situado abajo a la derecha de su pantalla y, a continuación, en **Abrir el centro de recursos compartidos**. Haga clic en **Cambiar configuración del adaptador**. A continuación, haga clic con el botón derecho en **Reconexión automática VPN** y seleccione **Propiedades**.
- Haga clic en la pestaña **Seguridad** y seleccione **IKEv2** en el campo **Tipo de VPN**. Haciendo clic en el botón **Configuración avanzada** podrá configurar el tiempo de interrupción de red antes de la desconexión definitiva del cliente Windows 10. Confirme con el botón **Aceptar**.



La reconexión VPN es efectiva ahora del lado cliente.

- Si el ordenador portátil que ejecuta Windows 10 entra en modo de suspensión, la conexión se perderá y el usuario deberá introducir manualmente sus credenciales al salir de la suspensión.

d. DirectAccess

Windows Server 2008 R2 introdujo la funcionalidad DirectAccess, similar a la reconexión automática VPN, ya que ofrece conectar automáticamente al usuario itinerante a la red empresarial, pero esta vez... sin conexión VPN.

Así, los administradores pueden implementar a distancia los objetos de directiva de grupo, las actualizaciones de seguridad y el software en los equipos con Windows 10; la conexión bidireccional es transparente mientras haya disponible un acceso a Internet, aunque ningún usuario haya abierto una sesión en el equipo.

La seguridad está garantizada por una autenticación del usuario y del equipo miembro del dominio, por un cifrado de los datos intercambiados entre las partes y un control del acceso a los recursos de la empresa (opcional).

DirectAccess se integra ahora en el servicio RRAS (*Routing and Remote Access Server*) en un único rol llamado **Remote Access** (acceso remoto), disponible con Windows Server 2012 R2.

El despliegue de DirectAccess ya no necesita una PKI (*Public Key Infrastructure*), protocolo complejo de implementar, y aporta funcionalidades del lado del servidor:

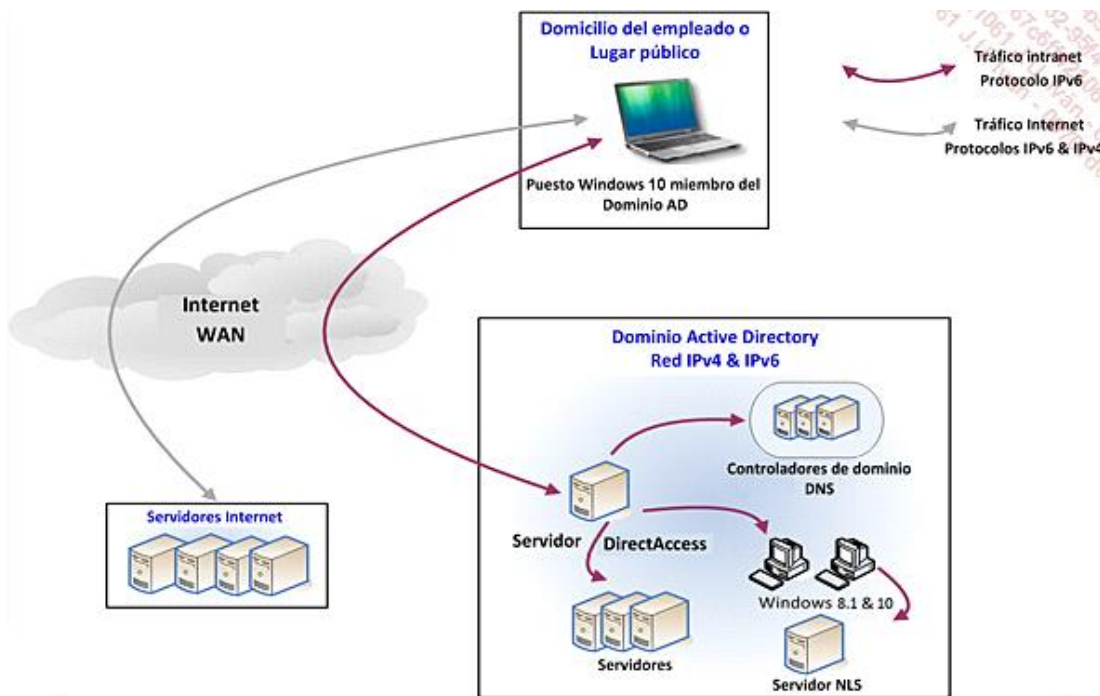
- Soporte de protocolo de intercambio de ruta llamado BGP (*Border Gateway Protocol*).
- Soporte de funciones de reverse proxy para las aplicaciones web hospedadas en la red interna.
- Gestión de pasarela VPN de sitio a sitio.
- Distribución de tareas entre los diferentes servidores de un grupo mediante el reparto de carga. Se soportan ocho nodos, pero, en caso de fallo de uno de ellos, las conexiones activas no se transferirán a los demás nodos.
- Gestión de autenticación por OTP (*One Time Password*) utilizando, por ejemplo, un módulo TPM (*Trusted Platform Module*) integrado en un cliente.
- Soporte de PowerShell y de las versiones Core de Windows Server 2012.
- Soporte para varios dominios.
- Disponibilidad de un asistente para la configuración simplificada de DirectAccess.

A nivel de cliente, Windows 10 permite a las aplicaciones preconfiguradas conectarse automáticamente a la red empresarial al abrir una conexión VPN cuando se arranquen.

Del lado del servidor, DirectAccess requiere un dominio AD DS (*Active Directory Domain Services*) con DNS, así como un servidor Windows 2008 R2 o Windows Server 2012 que disponga de dos tarjetas de red físicas, una conectada a Internet y la otra a la red local de la empresa. A partir de ahora, no es necesario poseer dos direcciones públicas IPv4 consecutivas para hacer funcionar DirectAccess porque el servidor puede ubicarse detrás de un router que soporte la función NAT (*Network Address Translation*).

Un puesto compatible con DirectAccess posee una versión cliente (Windows 7 Ultimate, Windows 7 Enterprise, Windows 8 Enterprise, Windows 8.1 Enterprise, Windows 10 Enterprise y Windows 10 Education) o una versión servidor (Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2) de un sistema operativo de Microsoft, y debe ser miembro del mismo dominio que el servidor DirectAccess.

Aquí tenemos un esquema que representa la solución y los diferentes flujos de información:



La funcionalidad se basa en el protocolo IPv6 para transferir los datos. Sin embargo, un cliente DirectAccess puede acceder a los recursos de la red interna que posean una dirección IPv4 mediante los protocolos NAT64 y DNS64, pero la conexión se realizará de manera unidireccional, del cliente DirectAccess hacia el recurso seleccionado.

El servicio se integra con NAP (*Network Access Protection*) para asegurarse de que el cliente DirectAccess que quiere conectarse a la red empresarial supera las pruebas de integridad predefinidas.

Los parámetros y certificados que se han de aplicar en los clientes Windows 10 se implementan mediante un objeto de directiva de grupo, generado desde el asistente de instalación de DirectAccess.

Un servidor web IIS (*Internet Information Services*), llamado NLS (*Network Location Server*), se ubica en la red local de la empresa, accesible solo para los clientes Windows 10 conectados a la intranet. De esta forma, si el puesto de trabajo no puede acceder al servidor NLS empleando el protocolo HTTPS, entonces se considera que el cliente está conectado a una red remota, como Internet.

Windows 10 aporta un conjunto de novedades conjuntamente con la tecnología DirectAccess:

- Gestión de redundancia geográfica: los servidores DirectAccess permiten al cliente comprobar el acceso a la red empresarial pudiendo ubicarse en diferentes zonas geográficas.
- Visualización del estado de una conexión DirectAccess en el centro de actividades.
- Integración de comandos DirectAccess en PowerShell para poder verificar y configurar la solución.

Empleando la consola DirectAccess, instalada con el rol Acceso remoto, es posible definir uno de los dos métodos de conexión del cliente Windows 10:

- Servidor seleccionado: se establece una sesión segura entre el cliente y el servidor DirectAccess, pero IPsec no se usa para las comunicaciones en la red local de la empresa.
- Red empresarial: se requiere un cifrado de extremo a extremo para acceder a los recursos internos, así como una conectividad IPv6 y el acceso a servidores de aplicaciones Windows Server 2012.

Para establecer una conexión con el servidor DirectAccess, el cliente Windows 10 efectúa previamente una serie de etapas:

1. Detección de una conexión a una red. Si está conectado a la intranet, DirectAccess está deshabilitado. Si está conectado a Internet, DirectAccess está habilitado.
2. Conexión al servidor DirectAccess con autenticación de las dos partes empleando certificados de equipo.
3. Autenticación en un controlador de dominio cuya dirección IP se ha obtenido previamente del servidor DNS de referencia.
4. Acceso a los recursos de la empresa que el usuario puede ver en función de su nivel de acceso. El servidor DirectAccess transfiere el tráfico.

Todo este proceso es transparente para el usuario.

El lenguaje PowerShell permite administrar un cliente Windows 10 Direct-Access empleando comandos como:

- **Reset-DAClientExperienceConfiguration**: restaura los parámetros de configuración DirectAccess a sus valores predeterminados.
- **New-DAEntryPointTableItem**: crea un punto de entrada para un nuevo sitio.
- **Get-DAClientExperienceConfiguration**: muestra la configuración del cliente DirectAccess.

```

Administrador: Windows PowerShell
PS C:\WINDOWS\system32> get-command -module -DAClientComponents
PS C:\WINDOWS\system32> get-daclientexperienceconfiguration

Description                : DA Client Settings
CorporateResources          :
IPsecTunnelEndpoints        :
CustomCommands              :
PreferLocalNamesAllowed     : False
UserInterface               : False
PassiveMode                  : False
SupportEmail                :
FriendlyName                 :
ManualEntryPointSelectionAllowed : True
GslbFqdn                    :
ForceTunneling               : Default

PS C:\WINDOWS\system32>

```

e. VPN SSTP

SSTP (*Secure Socket Tunneling Protocol*) es un tipo de túnel VPN disponible desde Windows Server 2008. Permite la encapsulación de paquetes PPP (*Point-to-Point Protocol*) sobre el protocolo HTTPS. Esta tecnología permite, por ejemplo, utilizar métodos de autenticación físicos, como EAP-TLS (tarjeta inteligente).

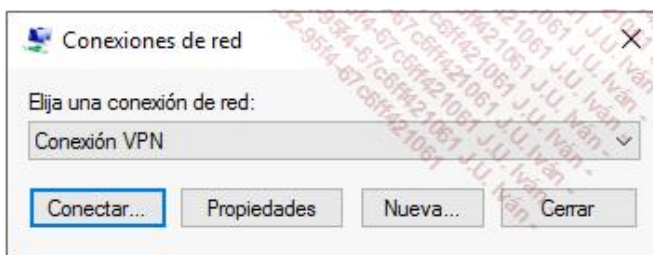
Como la inmensa mayoría de los firewalls empresariales permiten el paso del protocolo HTTPS (puerto 443) de tráfico de salida, el establecimiento de la conexión es sencillo.

El protocolo SSTP es compatible con los ordenadores cliente que ejecutan Windows Vista SP1, Windows 7, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows 8, Windows 8.1 y Windows 10. Estos últimos deben aprobar obligatoriamente la autoridad que ha emitido el certificado de servidor SSTP.

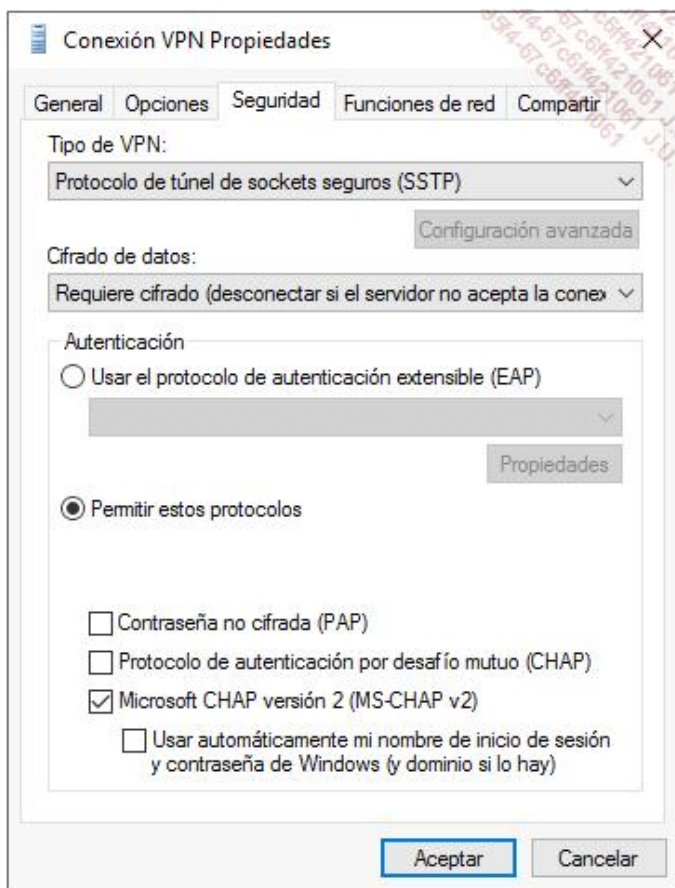
Para crear un túnel SSTP desde un cliente Windows 10, primero hay que importar el certificado del servidor VPN

SSTP (consulte el procedimiento de importación en la sección Reconexión automática VPN) y, a continuación, crear la conexión VPN:

- Pulse las teclas **Windows** y **R** e introduzca **rasphone** en la ventana **Ejecutar** y confirme pulsando [Intro]. Si no ha creado la conexión remota, haga clic en el botón **Aceptar** para crear una lista de entrada en la carpeta de **Conexiones de red**.



- Haga clic en el botón **Nueva**.
- Haga clic en **Red del área de trabajo** en la ventana **Set up a new connection**. Introduzca la dirección de Internet del servidor VPN y llame a la conexión **Conexión SSTP**; a continuación, haga clic en el botón **Crear**.
- Haga clic en el botón **Propiedades** de la ventana **Conexiones de red** y, a continuación, en la ventana **Seguridad**. Seleccione **Protocolo de túnel de sockets seguros (SSTP)** en el campo **Tipo de VPN**. Configure a continuación el método de autenticación: **EAP** (*Extensible Authentication Protocol*), **PAP** (poco seguro), **CHAP** (*Challenge Handshake Authentication Protocol*) o **MS-CHAP V2**.



Impresoras

El desarrollo de la informática, y el ahorro conseguido gracias a las campañas "sin papel", no han podido eliminar la impresión de documentos como soporte de información.

Un administrador debe poder gestionar eficazmente varias impresoras y servidores de impresión en la red a su cargo para, de este modo, dedicarse a tareas que consuman menos tiempo.

Según Microsoft, Windows 10 integra varios cientos de controladores de impresoras en el sistema; los antiguos controladores de dispositivos de impresión están disponibles en el sitio <https://www.microsoft.com/es-es/windows> o en el del fabricante del hardware.

Windows 10 detecta automáticamente las impresoras USB, pero no aquellas que utilizan puertos serie o paralelo. En ese caso, será necesario configurar manualmente el puerto en la interfaz **Dispositivos e impresoras**.

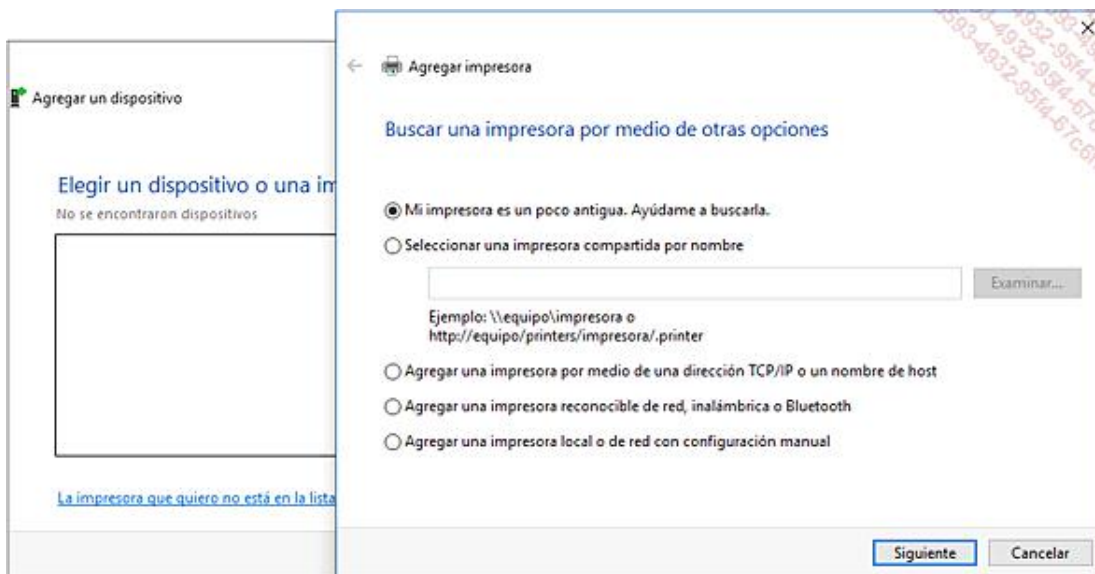
El soporte XPS (*XML Paper Specifications*), lenguaje de descripción de documento, se implementa de forma estándar, siempre que el dispositivo de impresión gestione los lenguajes PDL (*Page Description Language*) y XPS. En la inmensa mayoría de los casos, Windows 10 proporciona el controlador de impresión necesario para el funcionamiento adecuado de la impresora. En caso contrario, puede hacer falta utilizar el disco suministrado por el fabricante o descargar el controlador de su sitio de Internet.

Cuando el usuario conecta una impresora a un ordenador provisto de Windows 10, este le atribuye un puerto y busca el controlador adecuado. Un ordenador con una impresora que emplee un controlador de 64 bits no podrá gestionar la impresión de documentos si los equipos remotos desean utilizar una versión de 32 bits del controlador. En este caso, bastará con que el administrador instale manualmente el controlador de 32 bits desde las **Propiedades de la impresora** en la pestaña **Avanzadas**.

Conectamos una impresora desde **Dispositivos e impresoras** siguiendo el procedimiento que describimos a continuación:

- Desde el campo de búsqueda de la barra de tareas, introduzca **dispositivos e impresoras** y seleccione **Dispositivos e impresoras**. El botón **Agregar una impresora** ejecuta el asistente de instalación de impresoras plug-and-play conectadas localmente o por la red.

Haciendo clic en **La impresora que quiero no está en la lista**, se solicita al usuario que defina manualmente los parámetros de la impresora:

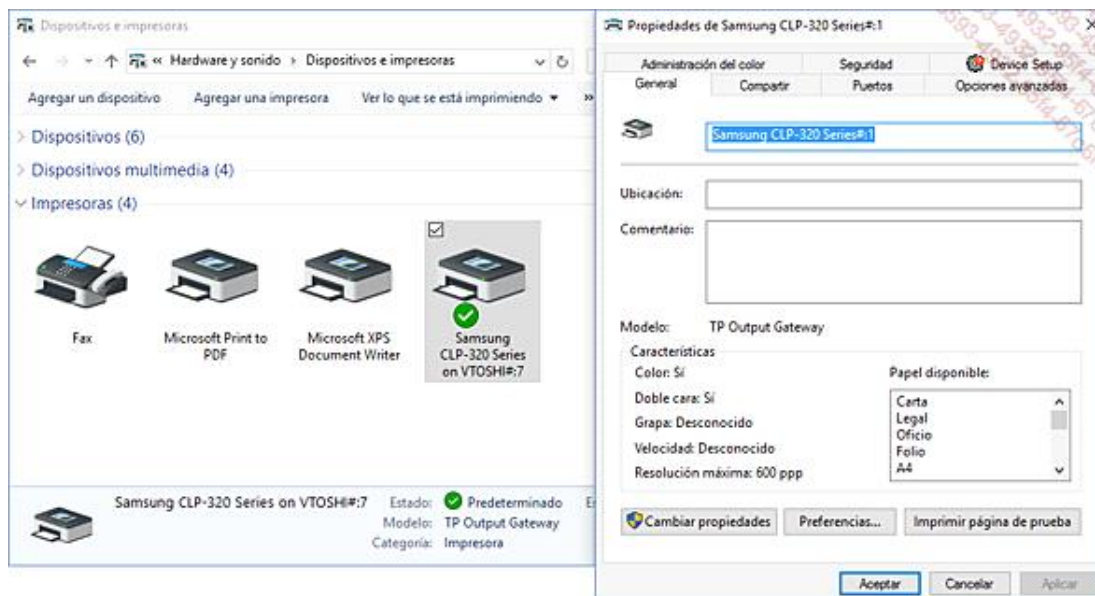


De este modo, es posible buscar la impresora por nombre de recurso compartido (\Servidor\Nombreimpresora), dirección IP, conectividad (Bluetooth, inalámbrica...) o por tipo de conexión (serie, paralelo). La opción para marcar **Mi impresora es un poco antigua. Ayúdame a buscarla** ejecuta un asistente.

Una vez definido el mecanismo para añadir la impresora, Windows 10 busca un controlador apropiado en el almacén de controladores (comando **pnputil.exe**) y, a continuación, si este no está localizable, presenta al usuario la opción de insertar un medio provisto por el fabricante o efectuar una búsqueda en el sitio Windows Update.

En **Dispositivos e impresoras**, seleccionando una impresora instalada, el usuario puede **Ver lo que se está imprimiendo**, configurar las **Propiedades del servidor de impresión** o **Quitar dispositivo**.

Haciendo clic con el botón derecho en el icono de la impresora, esta puede definirse como impresora predeterminada y es posible mostrar sus propiedades:

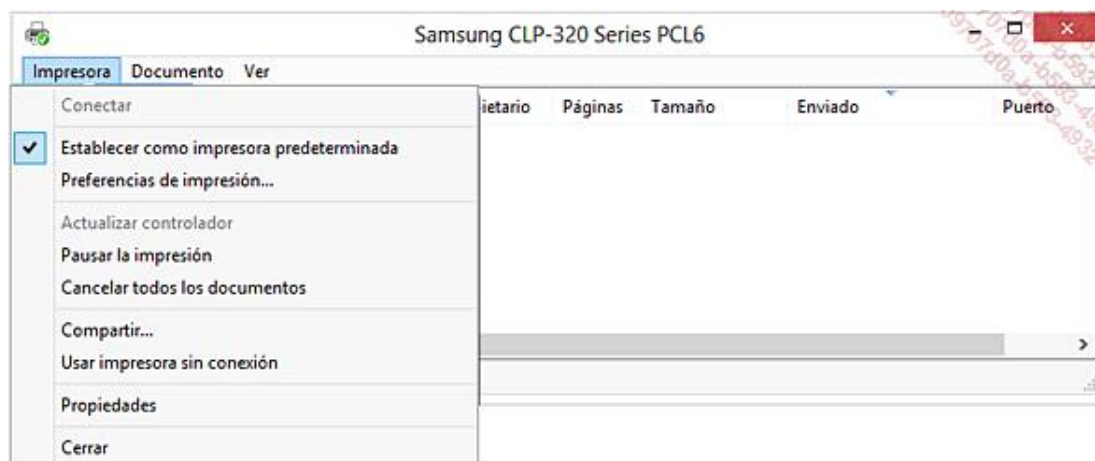


La pestaña **Compartir** de las propiedades de la impresora permite gestionar la compartición de la impresora con los demás usuarios de la red, así como agregar controladores suplementarios para los ordenadores que tengan un sistema operativo anterior de Microsoft.

La pestaña **Seguridad** permite definir específicamente las cuentas que deben tener acceso a la impresora, utilizando los permisos **Imprimir** un documento (gestión de sus propios trabajos de impresión solamente), **Administrar esta impresora**, **Administrar documentos** (modificación del orden de la cola de impresión) y **Permisos especiales** (**Lectura**, **Cambiar permisos** y **Tomar posesión**).

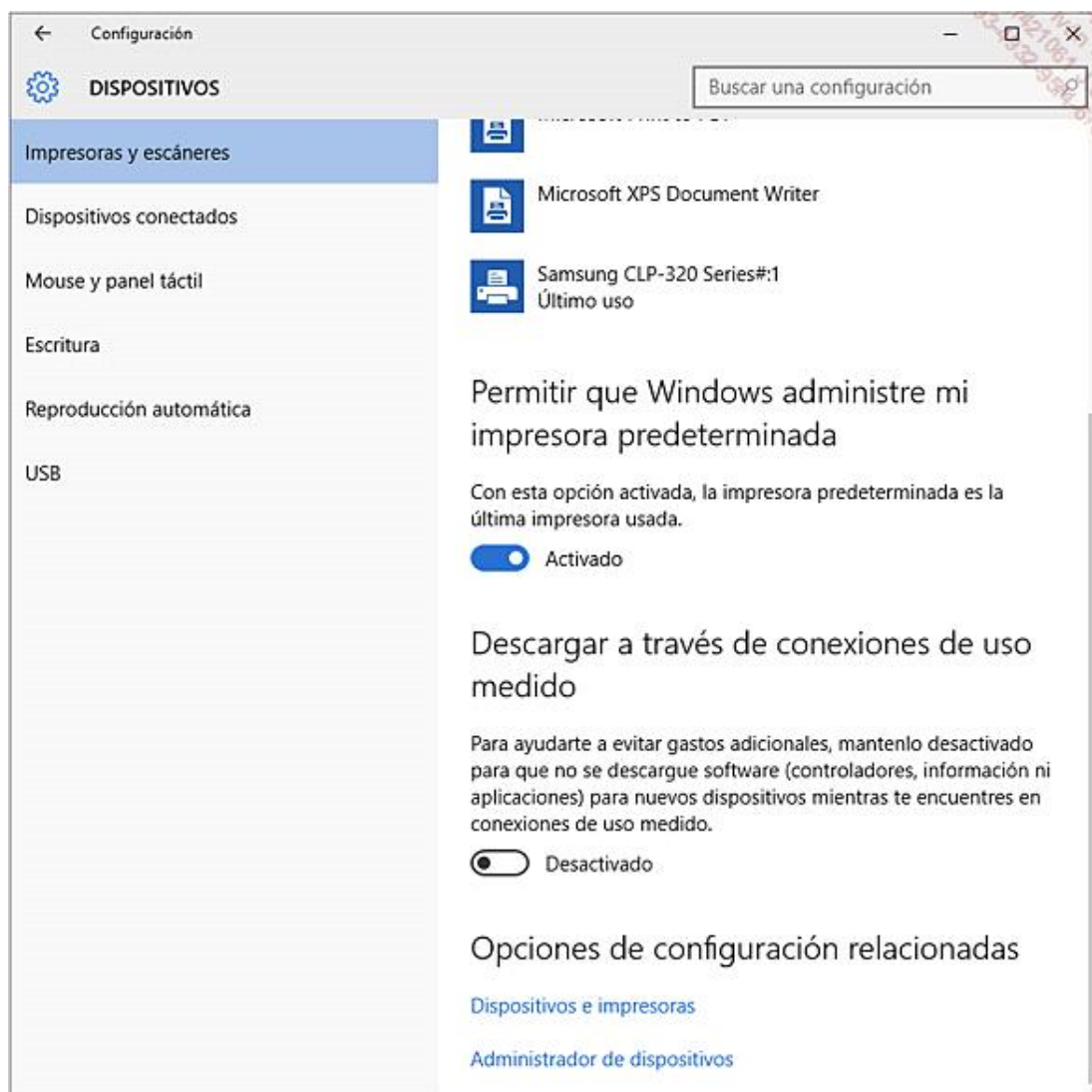
➡ Por defecto, el grupo Todos tiene autorización de impresión en una impresora seleccionada.

Haciendo doble clic en una impresora, se muestran los documentos en curso de impresión.



Es posible pausar, cancelar o reiniciar la impresión de todos o parte de los documentos y definir el dispositivo como impresora predeterminada.

Desde la nueva interfaz de Windows, el usuario puede gestionar sus impresoras y dispositivos conectados haciendo clic en el menú **Inicio, Configuración y Dispositivos**. Nuevas opciones están disponibles, como la posibilidad de no descargar controladores mientras el equipo se encuentre conectado a una red de uso medido.



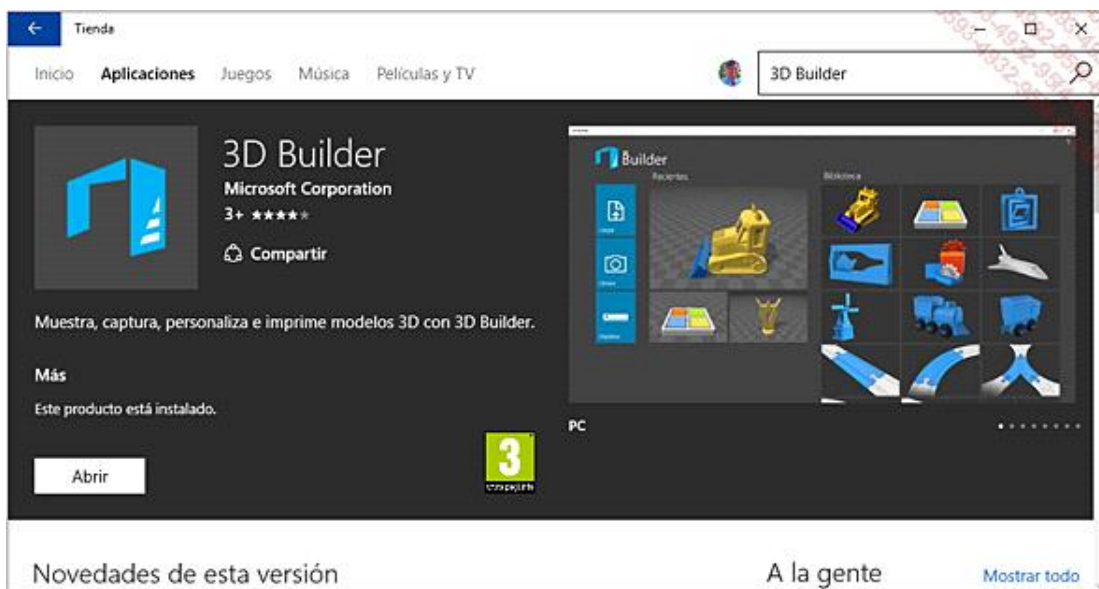
1. Impresora 3D

La impresión 3D (tridimensional) permite crear un objeto real concebido a partir de un software DAC (diseño asistido por computadora). El archivo 3D obtenido se transfiere a una impresora 3D que deposita el material capa a capa para obtener la pieza previamente creada. De esta forma, un particular o una empresa pueden crear sus propios objetos personalizados.

Windows 10 reconoce automáticamente las principales impresoras 3D del mercado gracias a un acuerdo establecido con fabricantes como 3D Systems o Makerbot. Se incluyen los controladores. Microsoft ofrece en descarga gratuita desde la Tienda de Windows la app 3D Builder para que el usuario pueda visualizar, concebir e imprimir sus propios objetos 3D. La aplicación se suministra con una biblioteca de objetos de ejemplo.

Adicionalmente, Windows 10 soporta los formatos STL (*STereoLithography*), OBJ o 3MF, necesarios para la impresión de objetos 3D.

Una simple búsqueda en la Tienda de Windows con la palabra clave « 3D Builder » permite instalar la app:



Los principales fabricantes de impresoras 3D ofrecen también sus propias apps en la Tienda de Windows. Pero los desarrolladores también pueden utilizar las API (*Application Programming Interface*) nativas suministradas con Windows 10 para ofrecer funcionalidades de impresión 3D integradas en sus apps.

2. WI-FI Direct Printing

La funcionalidad Wi-Fi Direct Printing es una tecnología que permite imprimir directamente desde un dispositivo (smartphone, tableta u ordenador) a una impresora y sin ningún punto de acceso intermedio o router inalámbrico.

No se requiere la instalación de un controlador de impresora o software dedicado y todas las funciones de la impresora están disponibles mediante este procedimiento.

Cada vez más fabricantes de impresoras soportan la conexión inalámbrica directa asegurando la conexión mediante una clave WPA/WPA2 (*Wi-Fi Protected Access*).

Wi-Fi Direct Printing requiere una tarjeta Wi-Fi que soporte Wi-Fi Direct, al igual que una impresora de red que soporte Wi-Fi Direct Printing.

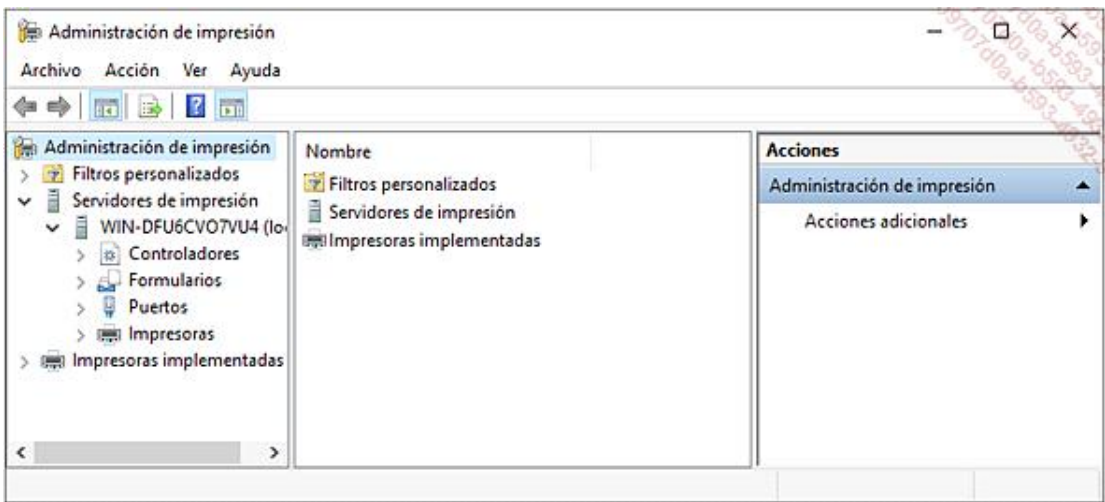
Para imprimir un documento en una impresora que soporte esta funcionalidad, bastará con seleccionar la red inalámbrica que lleve el nombre de la impresora desde la barra de tareas del icono Escritorio y conectarse empleando la clave requerida.

3. Consola Administración de impresión

Windows 10 simplifica la implementación de impresoras en los clientes miembros de un dominio Active Directory. Mediante el complemento **Administración de impresión**, el administrador puede configurar las impresoras de red de la empresa. Además, esta consola permite gestionar de forma centralizada las colas de impresión y recibir notificaciones por correo electrónico cuando aparece un problema.

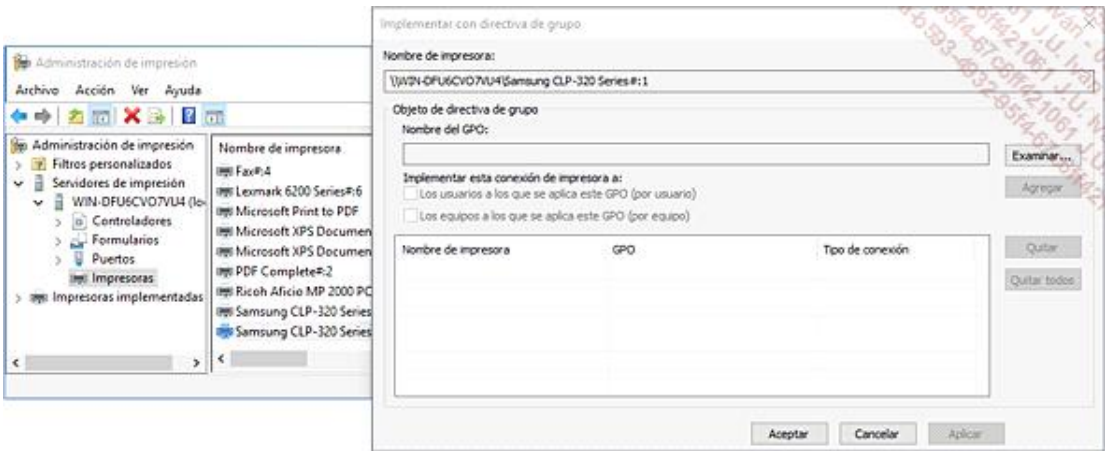
Para acceder a la consola Administración de impresión, siga este procedimiento, asegurándose previamente de que el puesto con Windows 10 es miembro de un dominio Active Directory:

- En el campo de búsqueda situado en la barra de tareas, introduzca **herramientas** y seleccione **Herramientas administrativas**. En la ventana **Herramientas administrativas** haga doble clic en **Administración de impresión**.



Para implementar una impresora en los equipos cliente:

- Despliegue el nodo **Servidores de impresión - NombreDeSuOrdenador** y, a continuación, **Impresoras** de la consola **Administración de impresión**. Haga clic con el botón derecho en el nombre de la impresora que se ha de implementar y, a continuación, seleccione **Implementar con directiva de grupo**.



- En la ventana **Implementar con directiva de grupo**, haga clic en el botón **Examinar** y seleccione la directiva de grupo utilizada para implementar la impresora; a continuación confirme pulsando **Aceptar**. Conviene ahora seleccionar el tipo de implementación, bien sea por **Usuarios**, por **Equipos** o ambos, marcando las opciones correspondientes. No olvide confirmar la implementación haciendo clic en el botón **Agregar** y, a continuación, en **Aceptar**.

Para crear una notificación (correo o ejecución de un script) vinculado a los trabajos de impresión:

- Haga clic con el botón derecho en el nodo **NombreDeSuOrdenador** y, a continuación, en **Establecer notificaciones**. Marque la opción **Enviar notificación por correo electrónico** e introduzca las **Direcciones de correo electrónico de los destinatarios**, del **remitente**, del **Servidor SMTP** y el **Mensaje** que desea transmitir. La opción **Ejecutar script** permite definir la **Ruta de acceso** y los **Argumentos adicionales** de un script creado al efecto.

Seleccionando el nodo **Impresoras implementadas** de la consola Administración de impresión, el administrador podrá visualizar el conjunto de impresoras implementadas usando un objeto de directiva de grupo desde el equipo con Windows 10.

La vista de los trabajos de impresión en curso se efectúa haciendo clic con el botón derecho en el nodo **Impresoras** y, a continuación, en **Vista extendida**.

Las impresoras se implementarán automáticamente en los puestos seleccionados en el plazo de actualización de 90 minutos del objeto de directiva de grupo. Observe que los ordenadores cliente que ejecutan Windows 2000, Windows XP o Windows Server 2003 deberán ejecutar el archivo **PushPrinterConnections.exe** mediante un script de arranque (para implementaciones por equipo) o de inicio de sesión (para implementaciones por usuario).

4. Impresión directa en sucursales

La **impresión directa en sucursales** reduce el uso de ancho de banda cuando un usuario desea imprimir un documento en un dispositivo de impresión ubicado en una sucursal y gestionado por un servidor Windows Server 2012 o Windows Server 2012 R2 situado en una oficina principal. Los datos de impresión ya no viajan del servidor

de impresión central a la impresora ubicada en la sucursal, sino que se transmiten directamente a la impresora desde el equipo con Windows 10 y, a continuación, se ponen en caché en la sucursal. De esta forma, en caso de fallo en el enlace WAN (*Wide Area Network*) entre la sucursal y el servidor de impresión, la impresora estará siempre disponible.

En resumen, el cliente Windows 10 no envía nunca el documento a imprimir al servidor de impresión.

La característica de impresión directa en sucursales necesita una impresora de red, un servidor Windows Server 2012 o Windows Server 2012 R2 y clientes Windows 8, Windows 8.1, Windows 10 Enterprise y Windows 10 Education. Las funcionalidades de cuota, de auditoría y de grupo de impresión no estarán accesibles durante el uso de la impresión directa en sucursales.

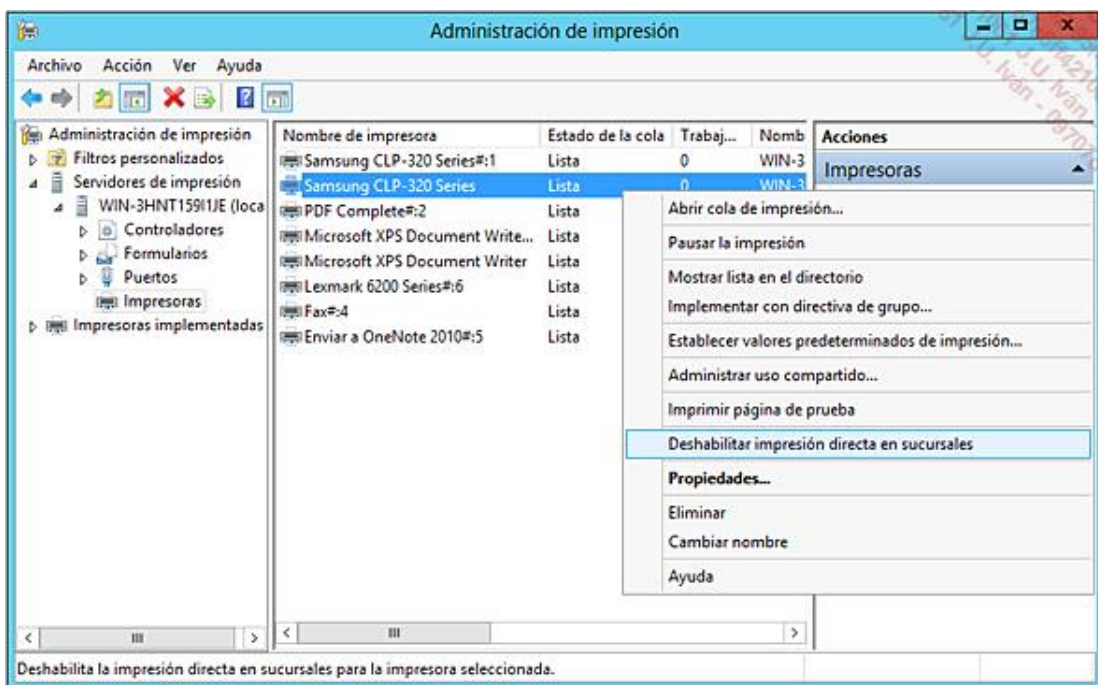
Las versiones anteriores del sistema operativo cliente (Windows XP, Windows Vista, etc.) no podrán utilizar la característica e imprimirán directamente en el servidor ubicado en la oficina principal.

Para configurar la Impresión directa en sucursales, utilice la consola **Administración de impresión** suministrada con Windows Server 2012, o bien el comando PowerShell **Set-Printer**:

- Abra una sesión como administrador en un servidor Windows Server 2012 y, a continuación, introduzca el comando PowerShell siguiente: **Set-Printer -name NombreImpresora -ComputerName NombreOrdenador -RenderingMode BranchOffice**.



El comando que se mostrado arriba permite activar la impresión directa en sucursales, visible con la consola Administración de impresión de un servidor Windows Server 2012:

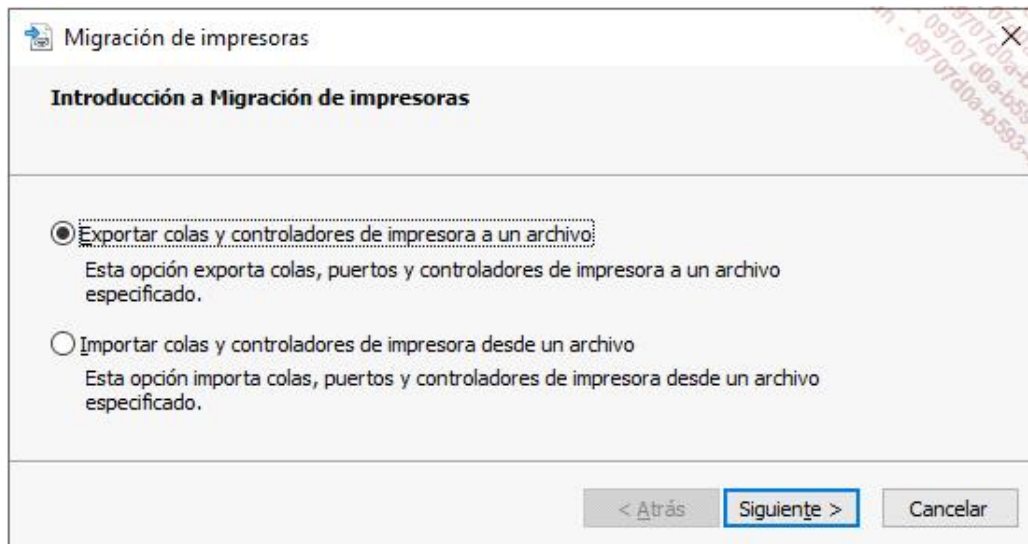


5. Migración de una impresora

Windows 10 proporciona el asistente **Migración de impresoras**, que permite importar (o exportar) las colas de impresión, los puertos y los controladores de una impresora a otro sistema operativo de Microsoft más reciente.

El asistente de Migración de impresoras se encuentra en el archivo **Printbrmui.exe**, almacenado en la carpeta **c:\windows\system32**. Ejecute este archivo desde un **Símbolo del sistema** para exportar los parámetros de una impresora:

- Desde el asistente Migración de impresoras, marque la opción **Exportar colas y controladores de impresora a un archivo**.



- Confirme haciendo clic en **Siguiete**. Marque la opción **Este servidor de impresión** y, a continuación, haga clic en el botón **Siguiete**, verifique la lista de elementos que se han de exportar y haga clic en **Siguiete**. Introduzca una carpeta de destino para el archivo con extensión **printerExport**. Confirme haciendo clic en los botones **Siguiete** y **Finalizar**.

➤ Es posible acceder también al asistente Migración de impresoras desde la consola Administración de impresión, haciendo clic en el nodo **Nombre de servidor de impresión** y, a continuación, seleccionando **Exportar impresoras a un archivo** o **Importar impresoras desde un archivo**.

6. Impresión con reconocimiento de ubicación de red

Windows 10 permite definir automáticamente la impresora por defecto cuando detecte que el usuario ha cambiado de red inalámbrica o física.

Esta funcionalidad está disponible con las ediciones Profesional, Enterprise y Education del sistema y solamente para ordenadores portátiles (se verifica la presencia de una batería).

Para el usuario, bastará con definir una impresora por defecto, la cual se asignará automáticamente a la red actual. Y así sucesivamente con las demás impresoras.

Para gestionar los parámetros de impresión con reconocimiento de ubicación de red, siga este procedimiento:

- Haga clic con el botón derecho del ratón en el menú **Inicio** y seleccione **Panel de control**. Haga doble clic en **Dispositivos e impresoras**.

- Seleccione una impresora y, a continuación, haga clic en **Administrar impresoras predeterminadas** en la barra de herramientas.
- Marque la opción **Cambiar mi impresora predeterminada cuando cambio de red**. En la lista **Seleccionar red**, haga clic en la red y, a continuación, en la impresora predeterminada correspondiente. Por último, confirme con el botón **Agregar**.

A continuación se muestra la interfaz de impresión con reconocimiento de ubicación de red:

Red	Impresora predeterminada
Ninguna red	Microsoft Print to PDF
Orange-d6b2 (conectada)	Samsung CLP-320 Series (3 redireccionado)

Si no desea utilizar esta característica, bastará con marcar la opción **Usar siempre la misma impresora como impresora predeterminada** en el cuadro de diálogo **Administrar impresoras predeterminadas**. Sin embargo, esta funcionalidad es interesante porque los usuarios que carecen de conocimientos técnicos no tendrán que contactar con el departamento de soporte técnico para configurar su impresora al cambiar de red.

Gestión de contenido con BranchCache

El despliegue del sistema de información de una empresa a sus usuarios es un proceso que necesita tener en cuenta limitaciones de seguridad y disponibilidad. La gestión de contenidos tiene como objetivo la cobertura del ciclo de vida de la información: la recolección, optimización, puesta a disposición y el archivado de los datos.

Muy a menudo, el ancho de banda se ve sometido a una fuerte demanda al hacer disponibles los archivos compartidos. Windows 10 ofrece la posibilidad de poner en caché la información para economizar el uso del ancho de banda.

1. Presentación de BranchCache

¿Sus enlaces entre oficinas están sobrecargados? **BranchCache** es una tecnología de almacenamiento en caché disponible desde Windows 7 (ediciones Enterprise y Ultimate) y Windows 2008 R2 (64 bits). Windows 10 soporta esta funcionalidad.

Particularmente útil en las redes separadas por enlaces WAN (sucursales), BranchCache permite a un cliente Windows 10 poner en caché los datos a los que accede desde una sucursal (páginas de Internet o carpetas compartidas), con objeto de mejorar su disponibilidad para los ordenadores de su propia red.

Ofrece múltiples ventajas: optimización del ancho de banda y mayor disponibilidad de los datos en caché.

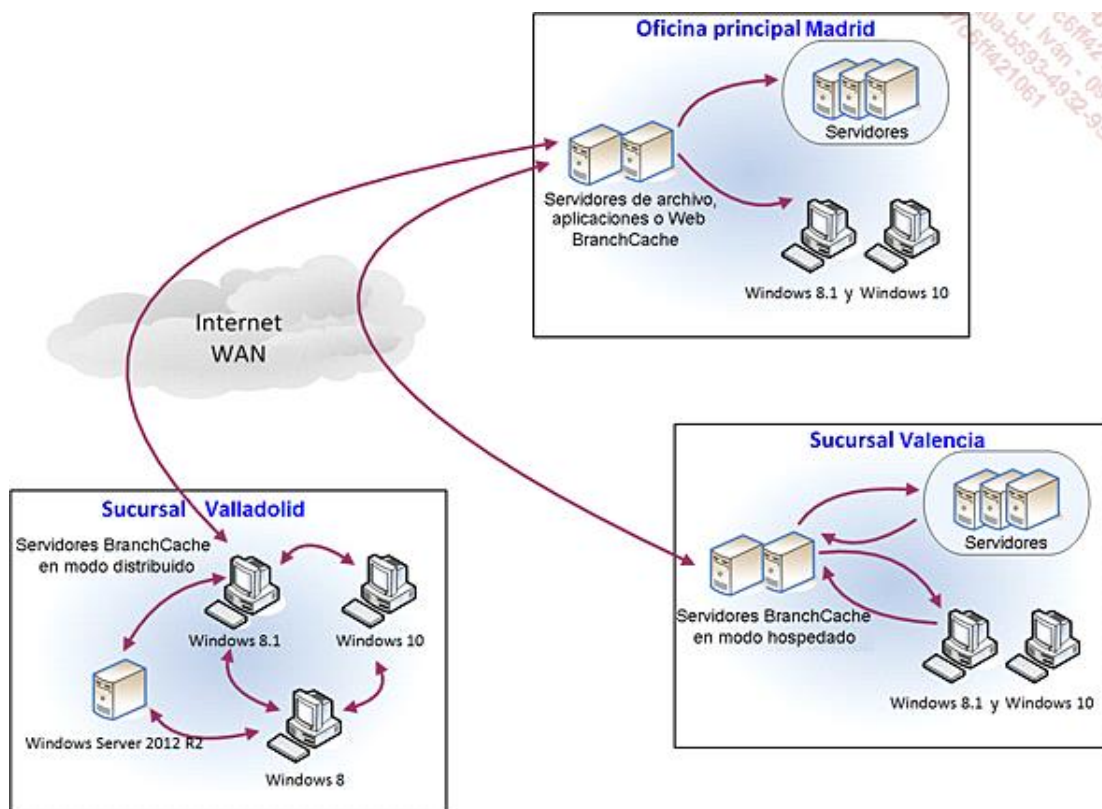
La caché puede ser **hospedada** en un servidor Windows Server 2008 R2, Windows Server 2012 o Windows Server 2012 R2, ubicado en la sucursal, o **distribuida** en los ordenadores con Windows 10 de los usuarios de la red. Una sucursal puede contener servidores BranchCache configurados en modo hospedado, mientras que otra sucursal puede contener los clientes en modo distribuido. La oficina principal, por su parte, gestiona el servidor BranchCache de **contenido**, replicado en las sucursales de acuerdo con uno de los dos modos citados previamente.

Un servidor BranchCache puede hospedar contenido accesible desde los siguientes protocolos:

- HTTP y HTTPS (rol del servidor web IIS), permitiendo el acceso a sitios intranet.
- SMB (*Server Message Block*) para la compartición de carpetas.
- BITS (*Background Intelligent Transfer Service*) para el acceso a aplicaciones hospedadas en servidores.

Para activar BranchCache en modo hospedado en un servidor Windows Server 2012 R2, será necesario agregar la funcionalidad del mismo nombre para gestionar los protocolos HTTP/HTTPS y BITS y el rol de Servicios de archivo para gestionar el protocolo SMB.

He aquí un esquema de implementación de BranchCache:



El modo distribuido tiene unos costes muy bajos, ya que no necesita servidores Windows Server 2008 R2, Windows Server 2012 o Windows Server 2012 R2.

- Los recursos disponibles desde Internet, como las actualizaciones de seguridad o los sitios visitados, se alojarán en caché. Solo se incluirán los datos almacenados en los servidores de red de área local de la empresa.

2. Modo de caché distribuida

El modo de caché distribuida se basa en una arquitectura punto a punto (*peer to peer*): el contenido se pone en caché automáticamente en los clientes Windows 10 una vez que ha sido descargado desde un servidor Windows Server 2012 o Windows Server 2012 R2 ubicado en una sucursal.

En lo referente a seguridad, los protocolos de red HTTP(S), SMB y BITS están soportados y la gestión de acceso a la caché del recurso se realiza en función de los permisos del usuario. Además, las transferencias entre clientes en modo caché distribuida utilizan un esquema de cifrado basado en AES 128.

El procedimiento de acceso a un recurso BranchCache en modo distribuido es sencillo:

1. El cliente Windows 10 accede a un recurso ubicado en un servidor de archivos Windows Server 2012 R2. Este, antes de verificar su acceso, le envía un conjunto de identificadores con aquello que quiere descargar.
2. El cliente verifica en su propia red local si otro cliente tiene ya los datos buscados empleando un protocolo de multidifusión en UDP. En caso negativo, vuelve a contactar con el servidor para solicitarle el recurso y lo almacena en su caché local.
3. Si otro equipo desea acceder a un recurso previamente almacenado en un cliente de su red, contactará con el servidor de archivo y, a continuación, buscará al cliente.

Observe que el servicio BranchCache no está activado por defecto en Windows 10, pero es posible automatizar su despliegue gracias a un objeto de directiva de grupo.

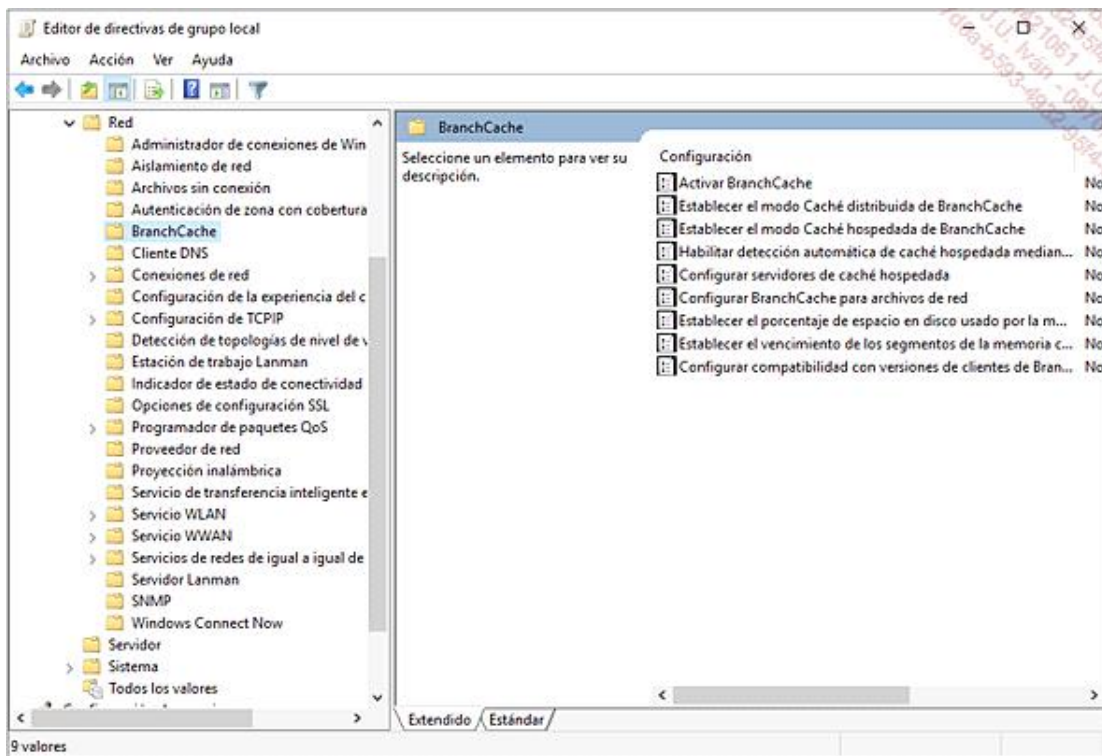
Es necesario respetar tres etapas para configurar BranchCache en un cliente Windows 10:

1. Activar la característica.
2. Seleccionar el modo de caché (distribuido u hospedado).
3. Crear reglas en el firewall para los protocolos BranchCache.

Proceda en ese orden, ya que la selección del modo de caché no activará BranchCache.

Para activar BranchCache en un puesto con Windows 10 empleando una directiva de grupo local, utilice este procedimiento.

- Desde el escritorio, pulse las teclas **Win** y **R**, introduzca **gpedit.msc** en la ventana **Ejecutar** y confirme con la tecla [Intro]. Desde el árbol de la consola Editor de directiva de grupo local, despliegue los nodos **Configuración del equipo - Plantillas administrativas - Red** y, a continuación, haga clic en **BranchCache**.



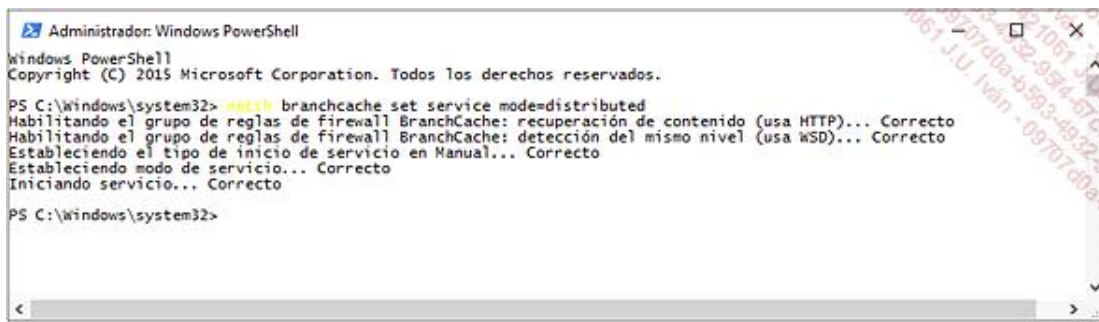
- Haga doble clic en **Activar BranchCache**, haga clic en la opción **Habilitada** y confirme pulsando **Aceptar**.

Para activar el modo de Caché distribuida:

- Haga doble clic en el parámetro **Establecer el modo caché distribuida de BranchCache**, seleccione la opción **Habilitada** y, a continuación, haga clic en **Aceptar**.

También puede activar BranchCache en modo caché distribuida empleando el comando **netsh.exe** ejecutado como administrador local:

Netsh branchcache set service mode=distributed



```
Administrador: Windows PowerShell
Windows PowerShell
Copyright (C) 2015 Microsoft Corporation. Todos los derechos reservados.

PS C:\windows\system32> branchcache set service mode=distributed
Habilitando el grupo de reglas de firewall BranchCache: recuperación de contenido (usa HTTP)... Correcto
Habilitando el grupo de reglas de firewall BranchCache: detección del mismo nivel (usa WSD)... Correcto
Estableciendo el tipo de inicio de servicio en Manual... Correcto
Estableciendo modo de servicio... Correcto
Iniciando servicio... Correcto

PS C:\windows\system32>
```

PowerShell ofrece los mismos comandos, con nuevas mejoras, para configurar BranchCache. Para visualizar estos comandos, escriba **Get-Command -Module BranchCache** en una ventana PowerShell.

A continuación, se crea una regla de firewall que abre el tráfico necesario para el funcionamiento de BranchCache.

Para resolver los problemas vinculados al uso de BranchCache, existe un registro de las operaciones, disponible desde el **Visor de eventos**:

- En la zona de búsqueda situada en la barra de tareas, introduzca **Visor** y seleccione **Visor de eventos**.
Despliegue **Registros de aplicaciones y servicios\Microsoft\Windows\BranchCache\Operativo**.

➤ Observe que un cliente puede utilizar el modo de caché hospedado o distribuido, pero no los dos a la vez.

Bien implementado, BranchCache es transparente para el usuario y optimiza eficazmente el ancho de banda.

Gestión de periféricos BYOD

Windows 10 aporta varias soluciones para gestionar los periféricos personales de los empleados de la empresa. La seguridad de acceso a los recursos es un gran problema con esta nueva tendencia. La proliferación de dispositivos como las tabletas con Android o los smartphones de Apple genera problemáticas de gestión.

Los usuarios tienen necesidad de acceder a la intranet, a su mensajería electrónica, a los datos compartidos o a las bases de datos de la empresa.

El principal obstáculo para la implantación de BYOD es la cantidad de diferentes sistemas operativos móviles. Windows 10, gracias al soporte de Open MDM (*Mobile Device Management*), garantiza la gestión de los dispositivos móviles.

De esta forma, los administradores podrán controlar e inventariar el parque BYOD, gestionando de forma remota los terminales móviles y forzando el despliegue de herramientas de seguridad.

Windows 10 soporta el protocolo OMA Device Management para la gestión de los dispositivos móviles; de esta forma, los productos de terceros como Mobile Iron o Air Watch pueden gestionar los periféricos Windows 10.

1. Acceso al trabajo

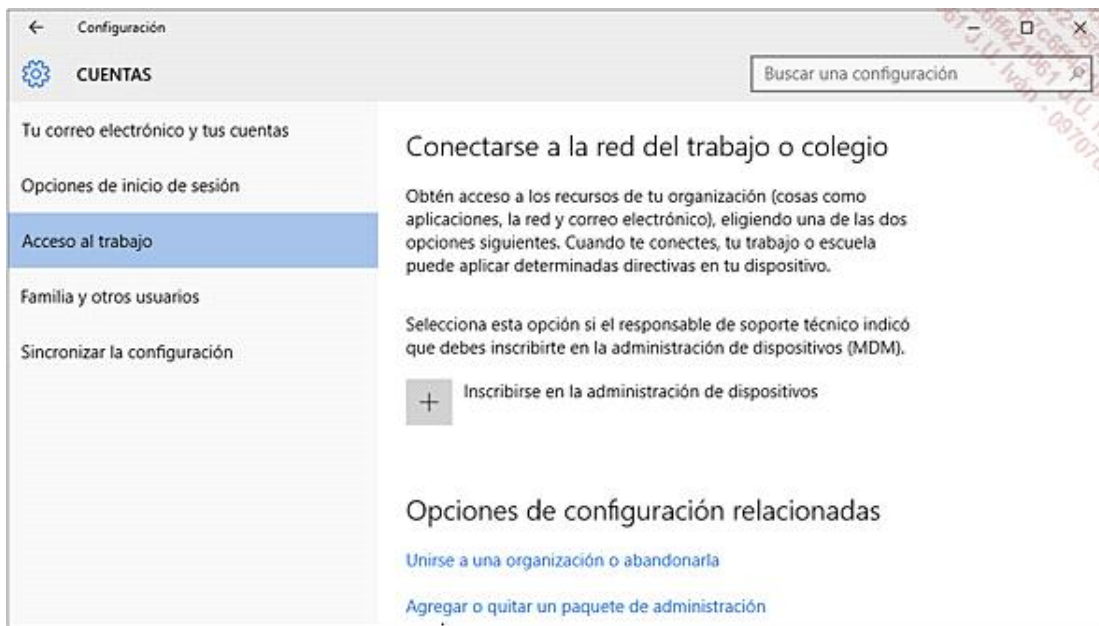
Hasta ahora, un equipo era miembro de un dominio o no. Si este no era el caso, resultaba difícil que una persona ajena a la empresa pudiera acceder a sus recursos. Acceso al trabajo es una funcionalidad que derriba esta frontera ofreciendo a un usuario que aporta su propio equipo el acceso a los recursos del dominio, con su equipo parcialmente gestionado por un administrador.

El registro del equipo no puede forzarse y es obligatoriamente iniciativa de su propietario.

Gracias a una infraestructura gestionada por un servidor Windows Server 2012 R2 provista del rol ADFS (*Active Directory Federation Services*), un puesto con Windows 10 puede unirse parcialmente a un dominio Active Directory. Es necesario, por supuesto, que el usuario cuente con un identificador en este último.

A continuación se describe el procedimiento:

- ➔ Haga clic en el menú **Inicio** y en **Configuración**. Luego seleccione **Cuentas**. Haga clic en la sección **Acceso al trabajo**. Seleccione **Acceso al trabajo** y luego haga clic en el botón **Conectar**. Introduzca el e-mail registrado por el administrador de la empresa y haga clic en el botón **Siguiente**.



2. Carpetas de trabajo

La funcionalidad Carpetas de trabajo (o Work Folders) permite a un usuario que dispone de su equipo personal sincronizar los archivos entre varios PC o dispositivos, que pueden o no estar unidos a un dominio Microsoft.

A diferencia de la app OneDrive, donde los datos se almacenan en la *cloud*, aquellos gestionados por Carpetas de trabajo lo están en un servidor Windows Server 2012 R2. La empresa mantiene de esta forma el control de la ubicación y la confidencialidad de los documentos.

Windows 10 Pro, Enterprise y Education soportan esta funcionalidad.

En caso de fallo de conectividad a la intranet de la empresa o la red Internet, el usuario trabajará sobre los datos almacenados de manera local. Al restablecer la conexión, estos se sincronizarán automáticamente. Mediante el sistema de archivo NTFS, el administrador puede asignar cuotas para impedir que el espacio de disco en los servidores se desborde rápidamente. El ancho de banda también se preserva. Los usuarios pueden cifrar sus documentos y beneficiarse de las capacidades de alta disponibilidad proporcionadas por Windows Server 2012 para acceder en todo momento a sus datos.

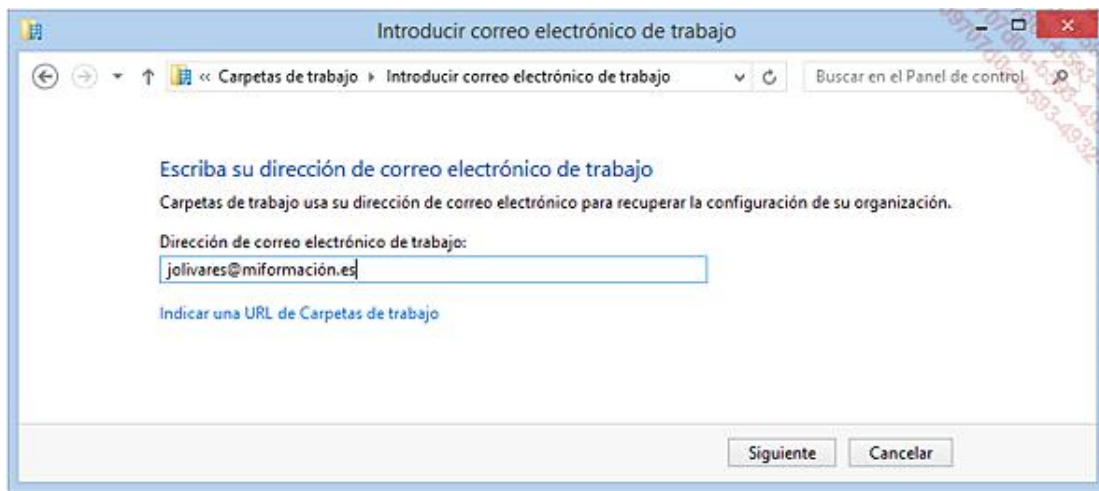
Del lado del servidor, Windows Server 2012 requiere la instalación de los roles AD DS (*Active Directory Domain Services*), DNS y Servicios de archivo y almacenamiento.

Del lado del cliente Windows 10, los datos sincronizados de los usuarios se almacenan por defecto en la carpeta **%USERPROFILE%\Work Folders**. Debemos contar con espacio libre en disco suficiente para albergar los documentos, así como un espacio adicional de 6 GB si el directorio de carpetas de trabajo se almacena en la partición del sistema. Puede utilizarse un dispositivo USB formateado con el sistema de archivos NTFS.

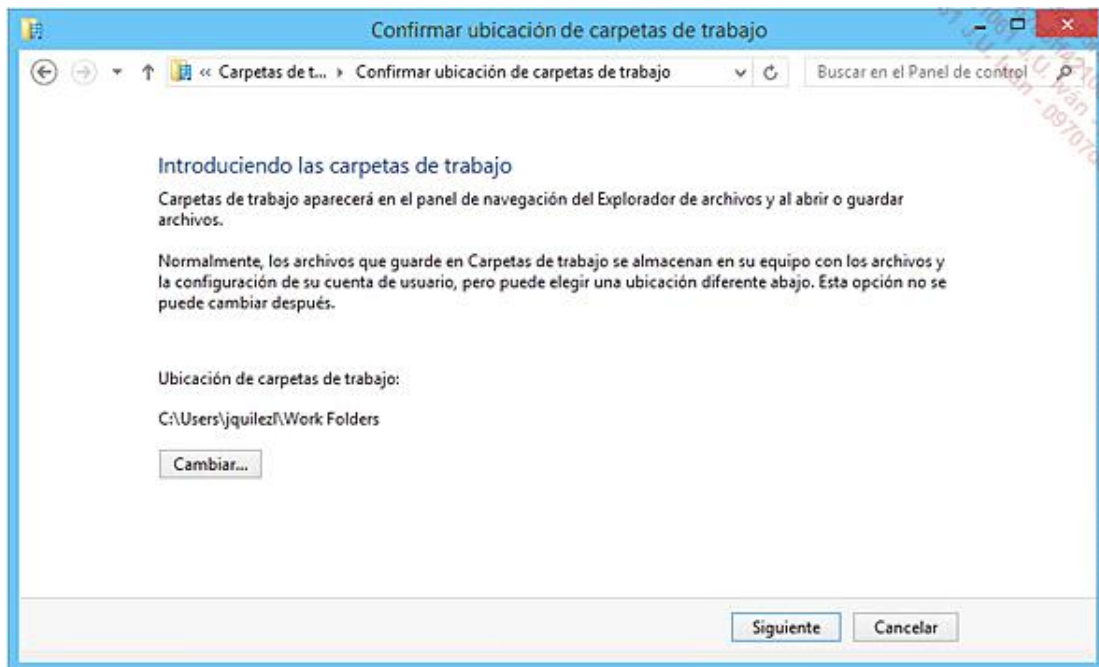
Por último, el tamaño máximo por defecto de un archivo individual no puede exceder los 10 GB.

Para configurar la funcionalidad Work Folders en Windows 10, siga este procedimiento:

- Haga clic con el botón derecho del ratón en el menú **Inicio** y en **Panel de configuración**. Haga doble clic en **Carpetas de trabajo** y, a continuación, en **Configurar carpetas de trabajo**. Introduzca su dirección de correo electrónico profesional y, a continuación, su identificador y contraseña de Active Directory.

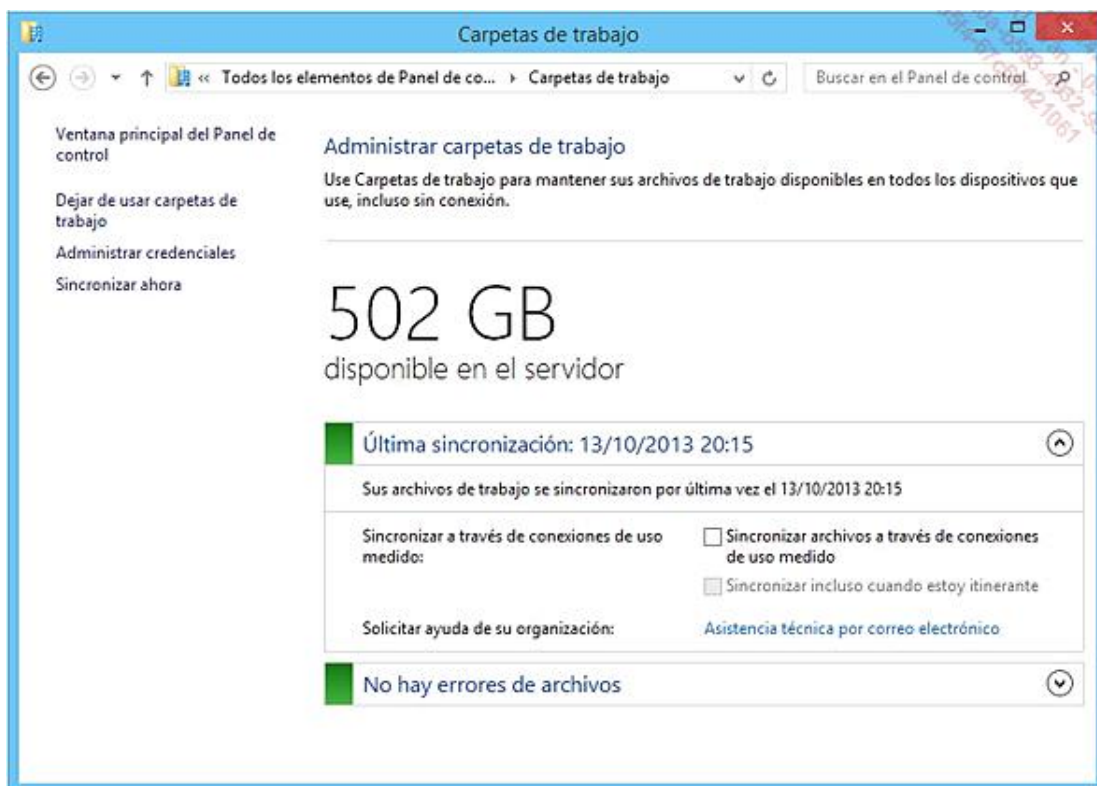


→ Defina la ruta de acceso a sus carpetas de trabajo y, a continuación, haga clic en el botón **Siguiente**.



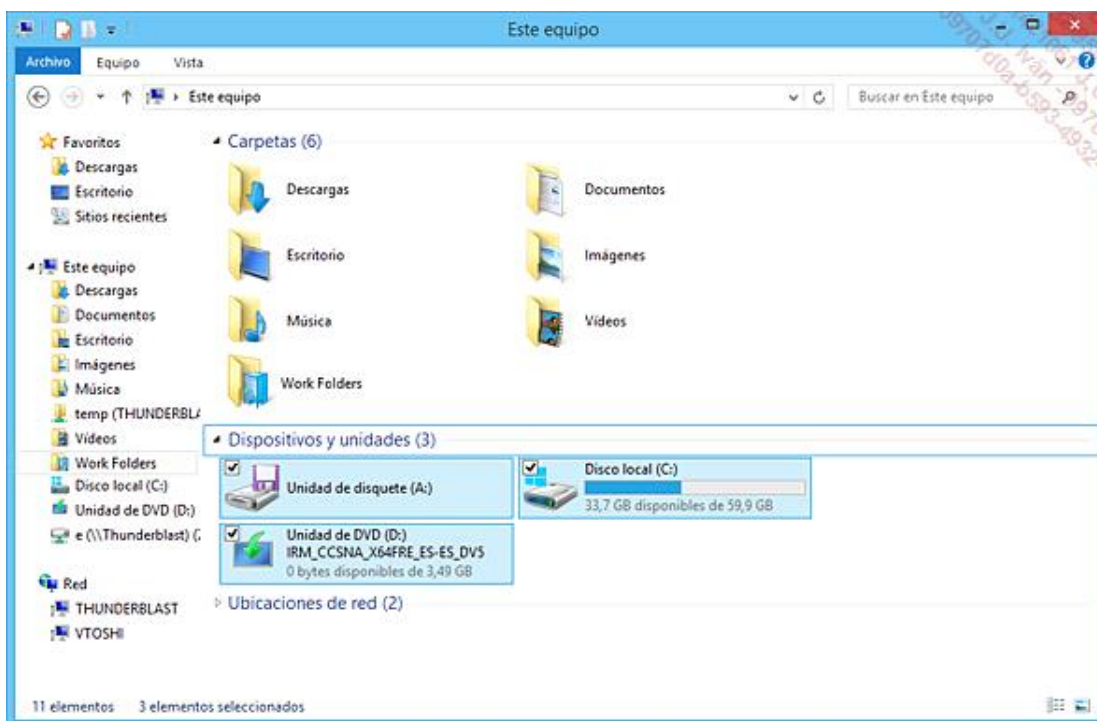
→ Marcando la opción **Acepto estas directivas en mi equipo**, el administrador de la empresa puede forzar la autenticación por contraseña durante el inicio de sesión, cifrar los datos almacenados en la carpeta Work Folders y, por último, borrarlos de forma remota en caso de robo de su equipo. Haga clic en los botones **Configurar carpetas de trabajo** y, a continuación, en **Cerrar** para terminar la configuración.

Desde el panel de control, haciendo clic en el icono **Carpetas de trabajo**, el usuario podrá visualizar la fecha de la última sincronización, sincronizar los archivos en conexiones limitadas, comunicarse con soporte técnico de la empresa o visualizar el espacio en disco disponible en el servidor:



El menú situado a la izquierda de la interfaz permite detener la sincronización Work Folders, gestionar la información de identificación en caso de cambio de contraseña del usuario y, por último, efectuar una sincronización manual de los datos.

Para acceder a la carpeta sincronizada Work Folders desde el **Explorador de archivos**, haga clic en **Este equipo**; la carpeta **Work Folders** aparece entre las carpetas Documentos, Imágenes, Descargas, etc.



En combinación con la funcionalidad de Acceso al trabajo, Work Folders ofrece una gestión precisa de los usuarios que no pertenecen al dominio y sus dispositivos.