



6 Gestión de recursos en rede




Sumario

6	Xestión de recursos en rede.....	1
6.1	Convencións empregadas.....	4
6.2	Introdución á administración de sistemas operativos de servidor.....	5
6.2.1	Configuración do sistema operativo Windows Server 2019: A súa contorna de traballo.....	5
6.2.1.1	Xanela inicial de configuración en Windows Server 2019.....	5
6.2.1.2	A barra de Inicio no escritorio de Windows Server 2019.....	8
6.2.1.3	O Panel de control.....	13
6.2.1.4	Configuración desde a consola de comandos.....	14
6.2.1.5	Aplicacións útiles de administración de Windows Server 2019.....	15
6.2.2	Introdución á administración de usuarios e grupos locais en Windows Server 2019.....	16
6.2.2.1	Configuración de usuarios e grupos locais en Windows Server 2019.....	18
6.2.2.2	Xestión de usuarios e grupos desde o Panel de control en Windows Server 2019.....	21
6.3	Administración de dominios.....	22
6.3.1	Estrutura de traballo en grupo.....	22
6.3.1.1	Configurar un grupo de traballo por rede nun terminal Windows.....	24
6.3.1.2	Acceso a recursos compartidos grupo traballo desde Windows e Linux.....	27
6.3.2	Protocolo LDAP.....	29
6.3.3	Os dominios.....	31
6.3.3.1	Planificación e requisitos necesarios para montar unha estrutura de dominio.....	33
6.3.4	Servizo de directorio: Active Directory (AD) en Windows.....	34
6.3.5	A contorna de traballo de administración de Active Directory.....	36
6.3.5.1	Administración de unidades organizativas de Active Directory de Windows.....	39
6.3.5.2	Administración de contas de usuario de dominio de Windows.....	41
6.3.5.3	Administración de grupos de usuarios en Active Directory de Windows.....	43
6.3.5.4	Administración de contas de equipos de Active Directory de Windows.....	44
6.3.6	Introdución á configuración do sistema operativo Windows Server.....	45
6.3.6.1	Empregando cmdlets.....	45
6.3.6.1.1	Variables en PowerShell.....	45
6.3.6.1.2	Cambiar o nome de equipo.....	46
6.3.6.2	Utilizando utilidades específicas.....	46
6.3.6.2.1	Crear recurso compartido.....	46
6.3.6.2.2	Permisos de acceso NTFS a carpetas.....	46
6.3.6.2.3	Crear Unidades Organizativas (OU).....	46
6.3.6.2.4	Crear grupos globais de seguridade.....	46
6.3.6.2.5	Engadir usuario.....	46
6.3.6.2.6	Engadir usuario a grupo.....	47
6.3.6.2.7	Borrar elementos.....	47

Material docente elaborado a partir da base dos materiais formativos de FP Online
propiedade do Ministerio de Educación e Formación Profesional.

[Aviso Legal](#)

6.1 Convencións empregadas

	Esta icona fai referencia a notas de introdución
	Esta icona indica aclaración
	Esta icona fai referencia a arquivos de configuración, de rexistro...
	Esta icona indica casos de uso
	Esta icona fai referencia a avisos o advertencias
	Esta icona indica incidentes
	Esta icona fai referencia a sección que inclúen instrucións paso a paso
	Esta icona fai referencia a sección que inclúen capturas de pantalla
	Esta icona fai referencia a actividades
	Esta icona fai referencia a documento esencial (licenza: http://www.ohmyicons.com)
	Referencia a ligazón recomendada (licenza: http://iconleak.com)

6.2 Introducción á administración de sistemas operativos de servidor

6.2.1 Configuración do sistema operativo Windows Server 2019: A súa contorna de traballo

Windows Server 2019 é o sistema operativo para servidores de rede da casa Microsoft. Baséase no núcleo ou kernel Windows NT 10.0. Foi construído sobre a base de Windows Server 2016. Intégrase moi ben na nube, usando a plataforma Azure de Microsoft, pero tamén están dispoñibles outras plataformas de Cloud Aloxamento como AWS entre outras. Esta preparado para ser un sistema convidado na nube pero tamén para ser un sistema anfitrión aloxando VM e contedores de forma robusta e segura.

Ten suficientes melloras que motivan á actualización do seu antecesor Windows Server 2016, como poden ser a ampliación do soporte de Azure, Hybrid Cloud, Soporte de Linux, Kubernetes, Shielder VMs (tamén para Linux), Storage Replica para todas as versións. Engadíronse novas prestacións como: System Insight, Windows image, Windows Defender ATP, cifrado entre máquinas virtuais e Storage migration service.

6.2.1.1 *Xanela inicial de configuración en Windows Server 2019*

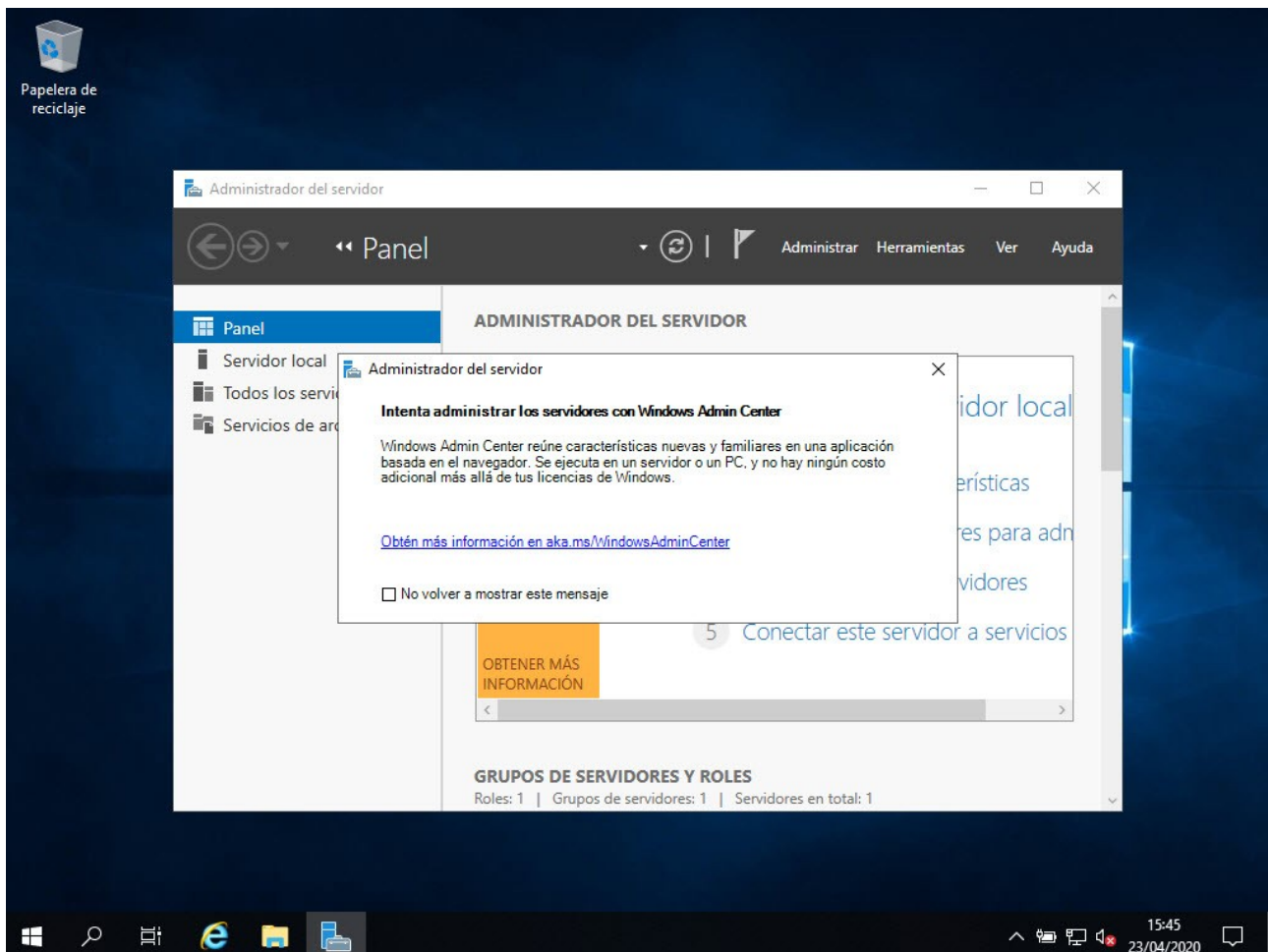
Despois da instalación o escritorio gráfico de Windows Server 2019 móstrase soamente coa icona da Papeleira de reciclaxe. Cando iniciamos por primeira vez o propio sistema aparécenos a xanela do Administrador do servidor coa cal podemos empezar a realizar tarefas de configuración básica. Ao momento, aparécenos outra xanela onde nos informa que tamén podemos realizar tarefas de administración con Windows Admin Center. Nesta última xanela temos unha ligazón que nos leva a unha páxina de Microsoft con mais información sobre Windows Admin Center.

Dentro da ferramenta do Administrador do servidor temos varias opcións:

- Servidor local: aquí podemos realizar algunhas opcións de configuración inicial, como:
 - Establecer zona horaria: aparece unha xanela para configurar a data e hora do sistema operativo
 - Configuración de rede: permitíranos especificar os parámetros de configuración como TCP/IP, DNS, porta de ligazón, etc., para conectarnos á rede.
 - Proporcionar nome do equipo e dominio: aparece a xanela de Configuración do Sistema, na que dispón dunha pestana con entradas para cambiar o nome do equipo, grupo de traballo ou dominio para a conexión
 - Habilitar comentarios e actualizacións automáticas.
 - Descargar e instalar actualizacións: permite abrir a ferramenta de Windows Update que nos permitirá configurar a forma de que o sistema se actualice.

- Habilitar escritorio remoto: aparece a xanela de Configuración do Sistema coa pestana activa Acceso remoto onde podemos habilitar a posibilidade de acceder ao escritorio do servidor remotamente (por defecto estará deshabilitado por cuestión de seguridade).
- Configurar Firewall de Windows: aparece a xanela de entrada para configurar a devasa de Windows, permitiéndonos habilitar ou deshabilitar e crear regras de acceso a aplicacións, servizos e portos.

Ilustración que mostra a pantalla do Administrador do servidor e un aviso



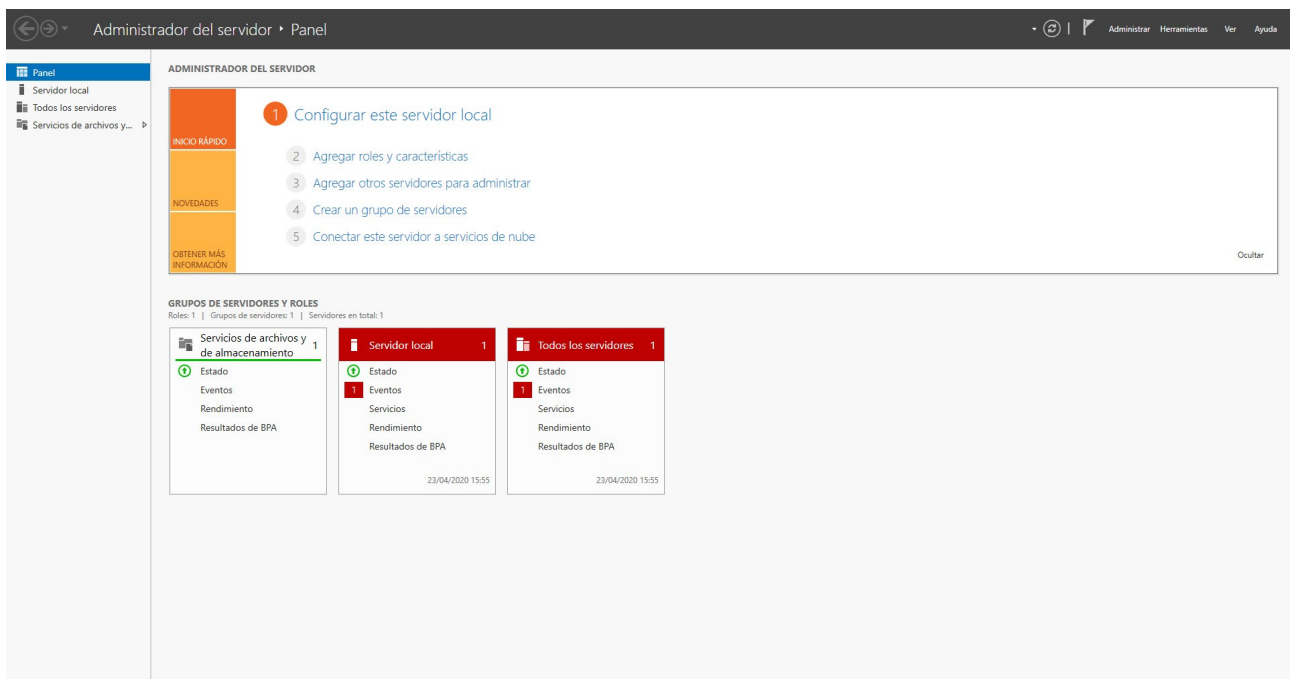
Windows Server 2019 (Elaboración propia)

- En Panel podemos realizar as seguintes accións:
 - Agregar roles e características: son funcións adicionais do noso Windows Server, aínda que non forman parte directamente das funcións, poden complementar ou aumentar a súa funcionalidade, ou mellorar a funcionalidade de todo o servidor, independentemente das funcións que estean instaladas. Cando pulsamos na opción Agregar roles e características aparece unha xanela

onde nos informa de que antes de engadir novos roles temos que configurar os seguintes elementos: conta de administrador cunha conta segura, IP estática e actualizacións de seguridade. Despois debemos seguir co asistente para instalar un rol ou características. Ver como agregar un rol e característica.

- Agregar outros servidores para administrar: podemos agregar novos servidores situados na rede local ou remotamente para a súa xestión e control.
- Crear un grupo de servidores: permite crear un novo grupo de servidores, dependendo dos requirimentos e funcionalidades de cada un, para ter unha administración centralizada.
- Conectar este servidor a servizos de nube.

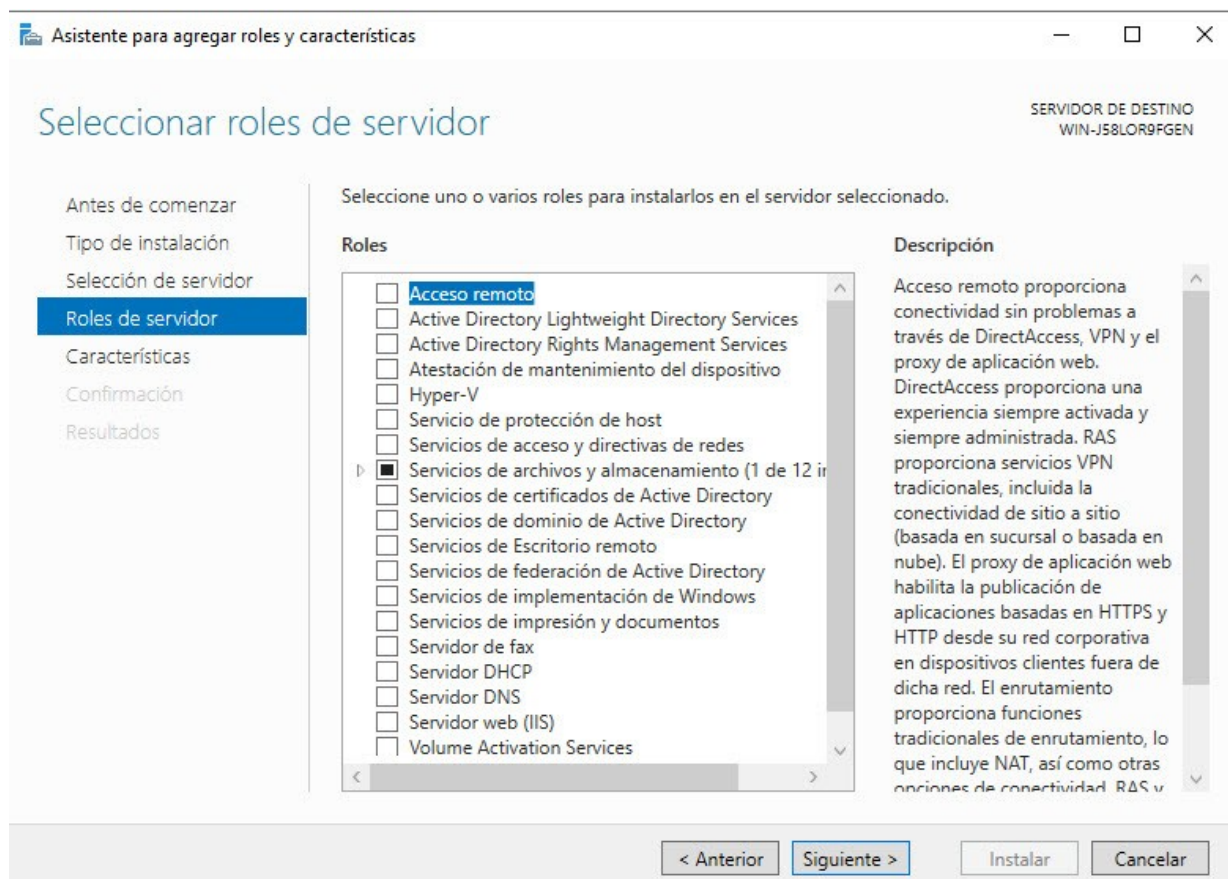
Ilustración que mostra o Administrador do servidor



Windows Server 2019 (Elaboración propia)

- Todos os servidores: mostra a listaxe completa dos servidores que están a ser administrados.
- Servizos de arquivos e de almacenamento: aquí vannos a aparecer todos os servizos que instalemos, para que podamos acceder rapidamente á súa configuración.

Ilustración que mostra os roles para instalar



Windows Server 2019 (Elaboración propia)

6.2.1.2 A barra de Inicio no escritorio de Windows Server 2019

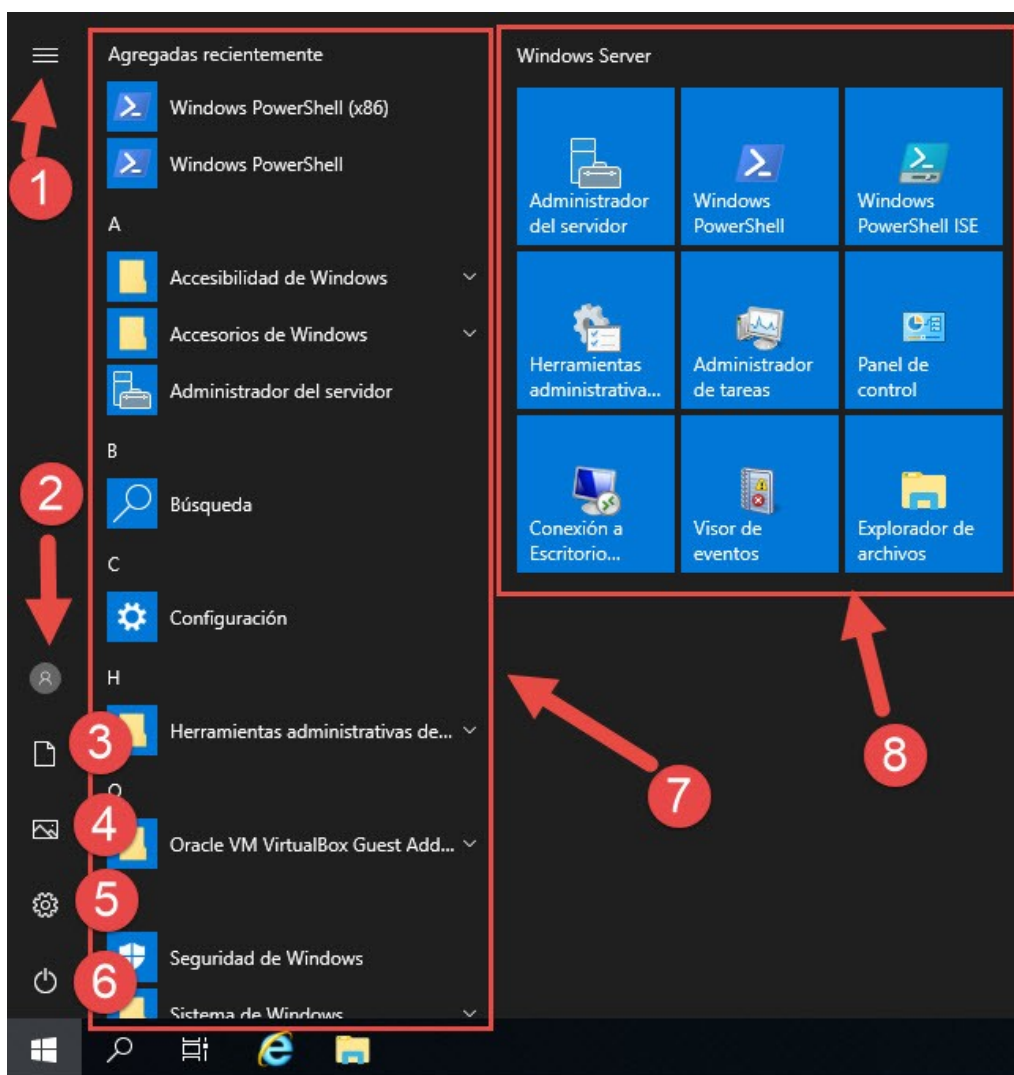
O menú de Inicio divídese en dous partes. A parte esquerda móstranos iconas de aplicacións e configuracións. Na parte dereita atopas baldosas de aplicacións de administración de Windows Server que funcionan como accesos directos a esas aplicacións.

O menú de Inicio ten as seguintes partes:

1. Menú (expándese para mostrar os nomes de todos os elementos do menú).
2. Conta. Do usuario co que iniciaches sesión. Ao picar sobre a icona da conta móstranos outra información como: outros usuarios creados, outras opcións como: pechar sesión, bloquear e cambiar a configuración da conta.
3. Documentos. Ábrese o explorador de arquivos, coa cartafol documentos aberta.
4. Imaxes. Ábrese o explorador de arquivos, coa cartafol imaxes aberta.
5. Configuración. Permite realizar diferentes configuración sobre o sistema, como: contas de usuario, rede, etc.

6. Inicio/Apagado. Ten tres opcións: apagar e reiniciar.
7. Listaxe de todas as aplicacións instaladas no sistema. Ao picar sobre elas co botón esquerdo ábreñse. Se facemos clic co botón dereito pódense facer diferentes opcións sobre elas, como: ancorar ao comezo, ancorar á barra de tarefa e configuración da aplicación.
8. Acceso directo a aplicacións que nos permiten administrar o sistema, como: administrador do servidor, PowerShell, Conexión a escritorio remoto, etc.

Ilustración que nos mostra o menú de Inicio

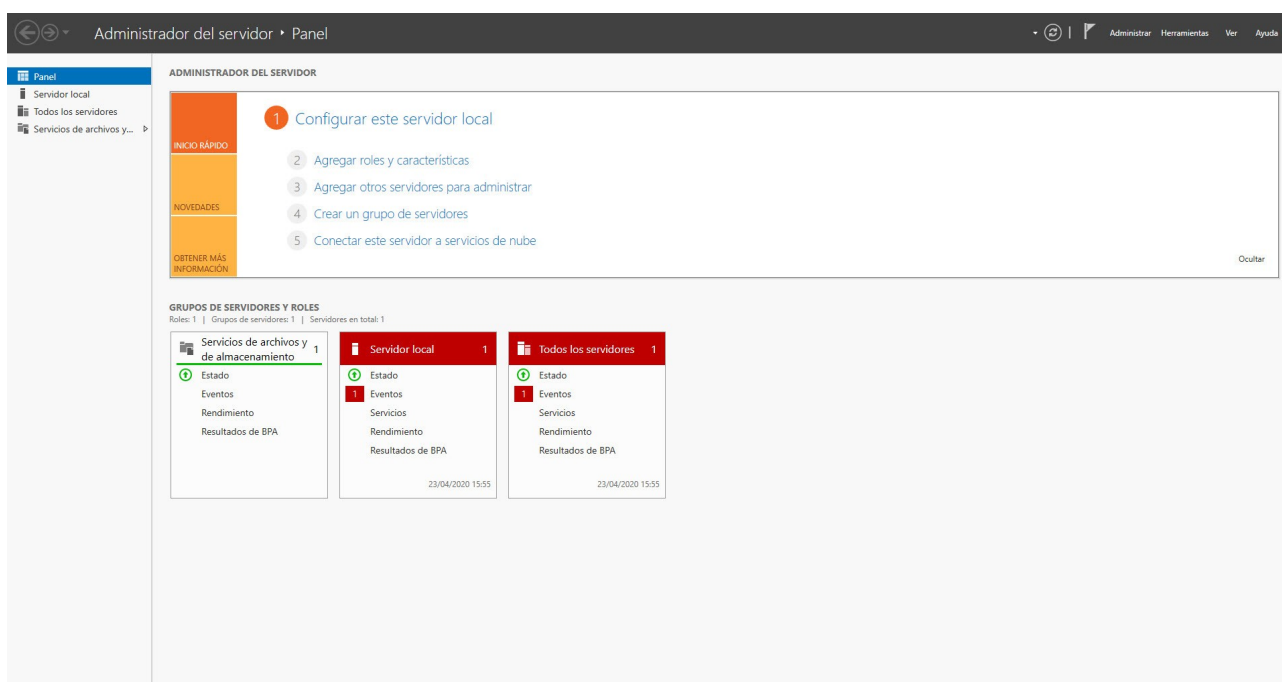


Windows Server 2019 (Elaboración propia)

O menú de Inicio permítenos o acceso rápido aos módulos operativos do sistema como son:

- **Administrador do servidor:** Simplifica a tarefa de administración e protección das distintas funcións de servidor. Permite aos administradores:
 - Permite agregar e fornecer roles.
 - Administrar equipos remotos.
 - Configurar un conxunto de servidores para administralos mediante consola.
 - Iniciar ou deter servizos e administrar contas de usuario locais.
 - Determinar o estado do servidor, identificar eventos críticos, e analizar e solucionar problemas ou erros de configuración.
 - Modificar información moi rapidamente como: nome do equipo, grupo de traballo ou o dominio ao que pertence a máquina. O escritorio remoto ou a xestión remotas pódense configurar.

Ilustración que mostra a pantalla do Administrador do servidor

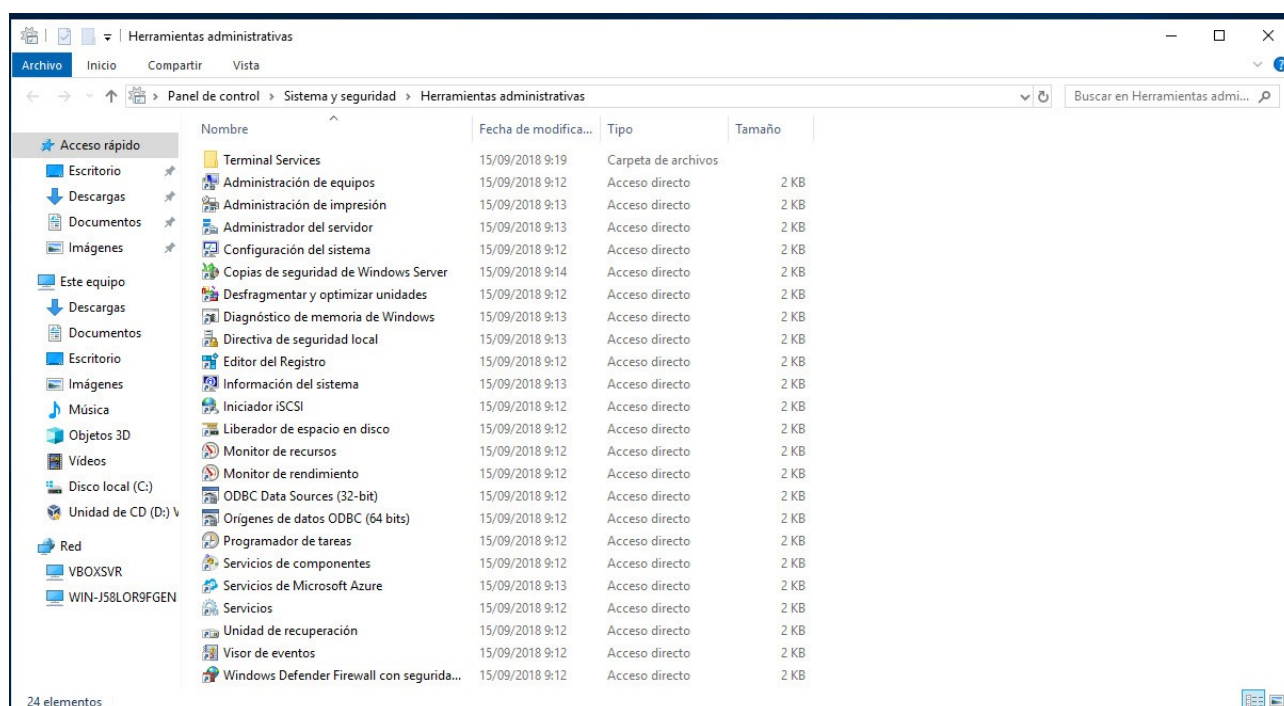


Windows Server 2019 (Elaboración propia)

- **Windows PowerShell:** aparece un interface de consola onde executar os cmdlets.
- **Windows PowerShell ISE:** é unha ferramenta que nos pode axudar a coñecer os cmdlets, a executalos e a descubrir o que podemos facer con estes.
- **Panel de control:** permite aos usuarios ver e manipular axustes e controis básicos do sistema.

- Explorador de archivos: aplicación que nos permite administrar archivos, cartafolios, etc.
- Conexión de escritorio remoto: accede á aplicación do escritorio remoto.
- Ferramentas administrativas: permite acceder a diferentes utilidades necesarias para facilitar a administración do sistema.
- Visor de eventos: permite consultar e administrar dunha forma potente e centralizada a información contida nos múltiples rexistros de eventos (logs) das aplicacións e servizos de Windows.

Ilustración que mostra as Ferramentas administrativas



Windows Server 2019 (Elaboración propia)

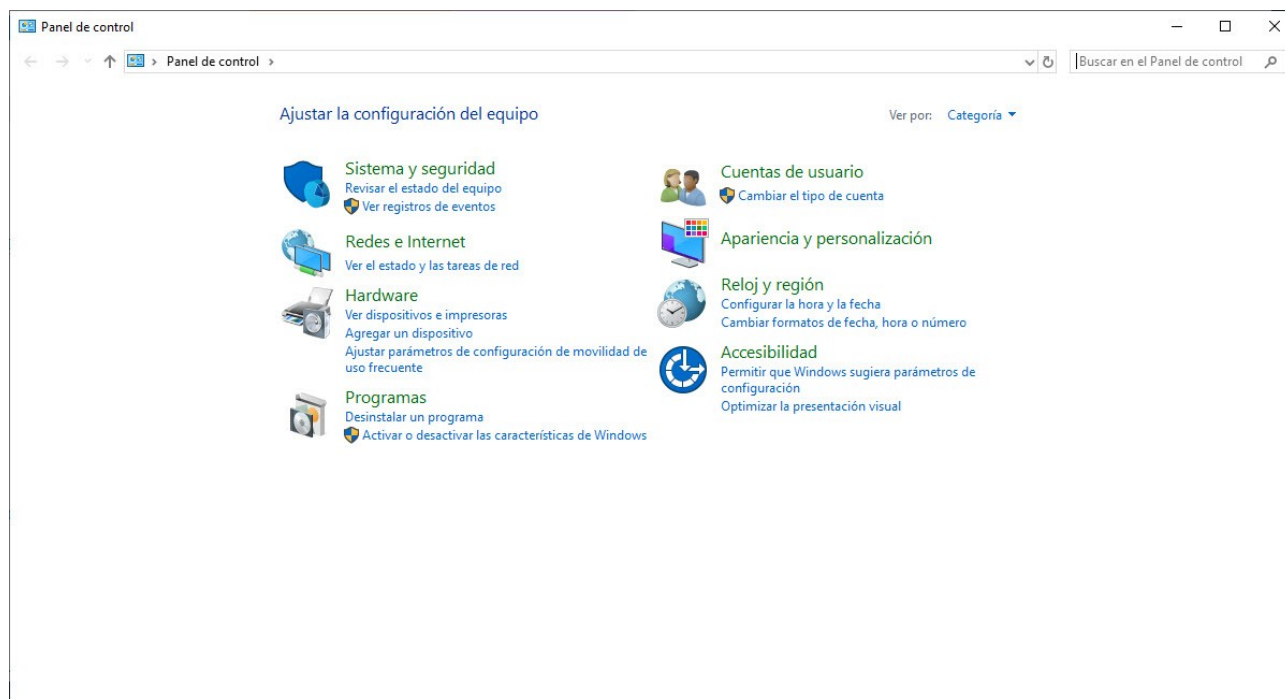
Descripción das Ferramentas administrativas de Windows Server:

- **Administración de equipos:** permitiranos acceso a xanelas de Microsoft Management Console (MMC) na que podemos realizar tarefas como:
 - Administración de discos: é unha utilidade do sistema para administrar os discos ríxidos e os volumes ou as particións que conteñen.
 - O visor de eventos: é un complemento de MMC que permite examinar e administrar rexistros de eventos. É unha ferramenta indispensable para supervisar o mantemento dos sistemas e solucionar os problemas que xurdan.

- O complemento de MMC Programador de tarefas axúdalle a programar tarefas automatizadas que realizan accións a unha hora concreta ou cando se produce un determinado evento. Mantén unha biblioteca de todas as tarefas programadas, proporcionando unha vista organizada das tarefas e un punto de acceso cómodo para administralas. Desde a biblioteca, pode executar, deshabilitar, modificar e eliminar tarefas.
- **Administrador do servidor:** Simplifica a tarefa de administración e protección das distintas funcións de servidor. Permite aos administradores:
 - Permite agregar e fornecer roles.
 - Administrar equipos remotos.
 - Configurar un conxunto de servidores para administralos mediante consola.
 - Iniciar ou deter servizos e administrar contas de usuario locais.
 - Determinar o estado do servidor, identificar eventos críticos, e analizar e solucionar problemas ou erros de configuración.
 - Modificar información moi rapidamente como: nome do equipo, grupo de traballo ou o dominio ao que pertence a máquina. O escritorio remoto ou a xestión remotas pódense configurar.
- **Configuración do sistema:** realizar accións avanzadas para solucionar problemas e configurar o sistema.
- **Copias de seguridade de Windows:** permite realizar unha copia de seguridade e recuperación do servidor.
- **Directiva de seguridade local do sistema:** permite ver e modificar a directiva de seguridade local, como dereitos de usuario e directivas de auditoria.
- **Iniciador iSCSI:** permite conectarnos a destinos iSCSI remotos e configurar os valores de conexión.
- **Monitor de rendemento:** realizar diagnóstico de problemas de confiabilidade e rendemento e recompilar datos de rendemento.
- **Orixes de datos ODBC:** manter as orixes dos datos ODBC e os controladores
- **Programador de tarefas:** programar as tarefas do equipo para que se executen.
- **Servizos:** inicia, detén e configura servizos de Windows.
- **Servizos de compoñentes:** aplicación de administración dos Servizos de compoñentes (COM+).
- **Visor de eventos:** para mostrar mensaxes de supervisión e solucionar problemas desde Windows e outro programas.

6.2.1.3 O Panel de control

Para abrir o Panel de control facemos clic na lupa e escribimos Panel de control. Seleccionamos panel de control e abríralenos unha xanela cun conxunto de ferramentas e utilidades presentadas mediante iconas. Cada icona representa o acceso a unha categoría de utilidades agrupadas por afinidade funcional. Podemos realizar as seguintes tarefas:



Windows Server 2019 (Elaboración propia)

- Sistema e seguridade: presenta o acceso rápido a Seguridade e mantemento, Firewall de Windows Defender, Sistema que nos presenta a información xeral do sistema, Opcións de enerxía, Ferramentas administrativas e Flash Player.
- Contas de usuario: permite crear, modificar e eliminar contas de usuarios cos seus contrasinais correspondentes. Tamén nos permite administrar as credenciais para ver e eliminar as credenciais gardadas para iniciar sesión en sitios web, aplicacións conectadas e redes.
- Redes e Internet: accedemos ao centro de redes e recursos compartidos. Podemos ver o estado da rede, configurar a conexión do dispositivo de rede, conectarnos a unha rede e configurar o uso compartido de arquivos. Tamén accedemos a Arquivos sen conexión que permite o almacenamento local de arquivos remotos. Ilustración que mostra o Panel de control de Windows Server
- Hardware: aparecen unha serie de funcións de configuración, das que destacamos a configuración de dispositivos e impresoras, configuración de son, opcións de

enerxía, centro de mobilidade e reprodución automática de CD ou outros dispositivos.

- Programas: comprobamos os programas instalados, permitindo a desinstalación dun programa, activar ou desactivar as características de Windows, ver as actualizacións instaladas, verificar que programa abre, por defecto, un tipo de arquivo determinado.
- Contas de usuario: permite crear, modificar e eliminar contas de usuarios cos seus contrasinais correspondentes.
- Aparencia e personalización: podemos configurar os parámetros relacionados co aspecto de Windows, como fondo de pantalla, personalizar a barra de tarefas, menú de inicio, instalar ou quitar fontes, cetro de accesibilidade, etc.
- Reloxo, idioma e rexión: podemos configurar a data e hora, o idioma (instalar ou desinstalar idiomas) formato de rexións en moeda, etc., e engadir reloxos para diferentes zonas horarias.
- Accesibilidade: aparece a xanela de Centro de accesibilidade para poder configurar a pantalla, teclado, rato, sons de alerta.

6.2.1.4 Configuración desde a consola de comandos

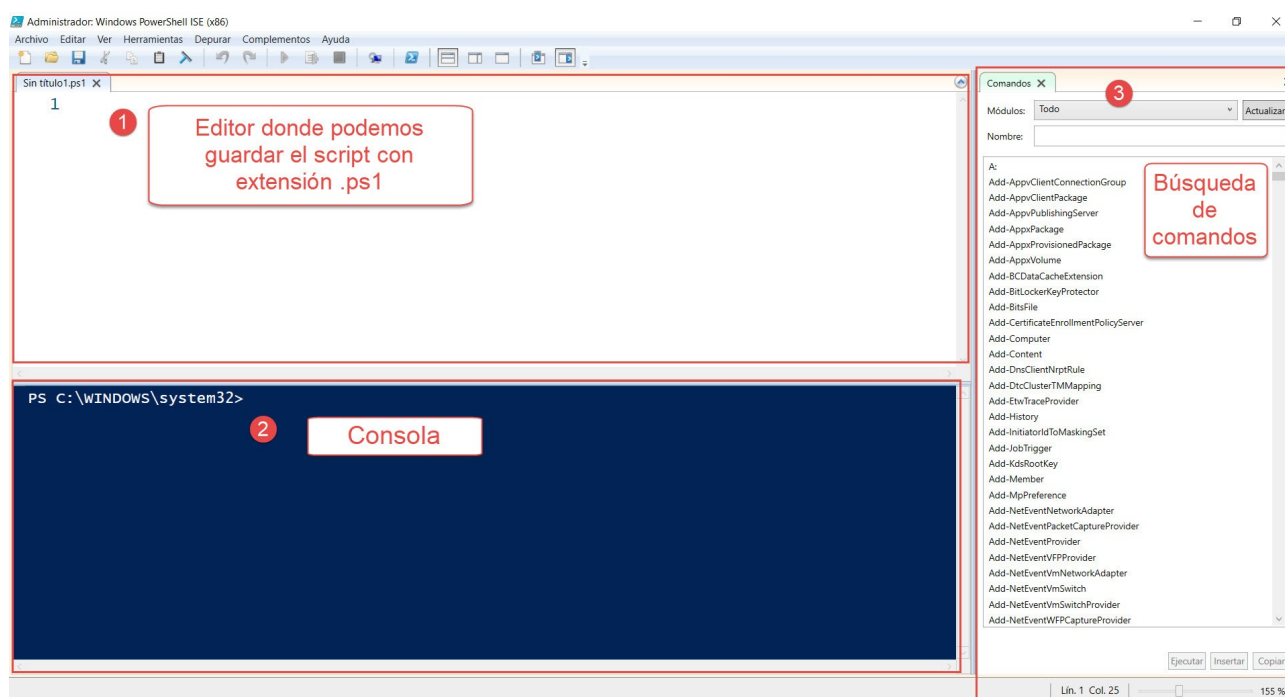
Aínda que non se dispoña da versión Core instalada, desde calquera Windows Server podemos traballar desde modo consola coa aplicación cmd.exe. Ademais, Windows Server 2019 ten a ferramenta PowerShell que é unha contorna de liña de comandos orientado para o traballo dos administradores de sistemas. O seu principal característica é que é unha contorna de comandos que acepta e devolve obxectos .NET, xa que está creado sobre Common Language Runtime de .NET e de Framework .NET.

Os comandos de PowerShell ou cmdlets teñen o seguinte formato de escritura:

```
C:\Users\Administrador> Acción_a_realizar para_que_objet_ou_elemento
```

Exemplo: Get-Help dá a axuda en forma de obxectos. Os comandos están deseñados para utilizarse en combinación con outros comandos.

Ilustración que muestra a pantalla principal de PowerShell



Windows Server 2019 (Elaboración propia)

As acciões máis usadas con comandos son:

ACCIÓN	DESCRIPCIÓN
Add-	Agregar un elemento a un objeto
Get-	Consultar un objeto o un subconjunto de tipo objeto
Set-	Modificar el contenido de u objeto
Enable-	Habilitar un objeto
Disable-	Deshabilitar un objeto
New-	Crear un nuevo ejemplar de objeto
Remove-	Eliminar un ejemplar de objeto

6.2.1.5 Aplicacións útiles de administración de Windows Server 2019

Microsoft Management Console (MMC) tamén hospeda e mostra ferramentas ou aplicacións administrativas creadas por Microsoft e por outros provedores de software que nos permiten configurar redes, o hardware dos equipos, servizos, usuarios, etc. Ademais de acceder pola contorna de escritorio a MMC, tamén podemos executar as partes ou ferramentas de MMC mediante comandos. Para acceder a estas opcións,

podemos entrar na consola do sistema desde Inicio-Executar e escribir a orde cmd.exe, tamén podemos introducilos directamente desde Inicio->Executar e escribimos o nome da ferramenta ou aplicación que desexamos abrir, e por último tamén podemos acceder desde a consola de PowerShell.

Algunhas das aplicacións que conforman as consolas MMC por orde alfabética son:

Aplicacións que conforman as consolas MMC

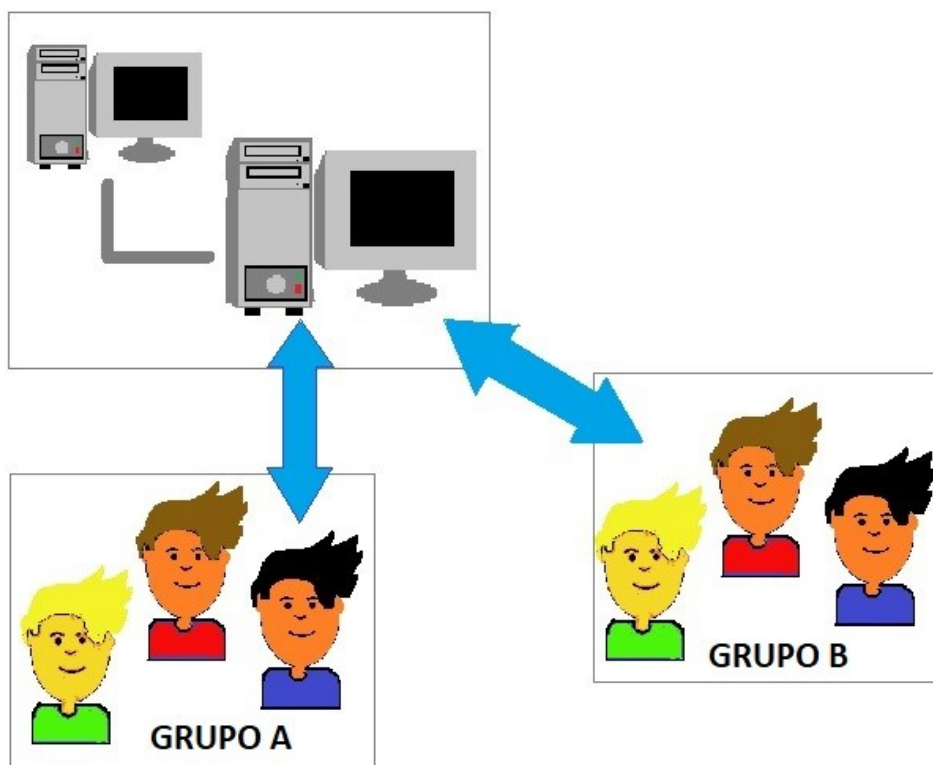
APLICACIÓN	DESCRIPCIÓN
<i>compmgmt.msc</i>	Permitir acceder a la Administración de equipos.
<i>dfrg.msc</i>	Permitir desfragmentar el disco duro.
<i>eventvwr.msc</i>	Se abre el visor de eventos que muestra eventos del sistema operativo, software y de hardware.
<i>firewall.cpl</i>	Configuración del Firewall de Windows.
<i>perfmon.msc</i>	Comprobar el rendimiento del sistema.
<i>powercfg.cpl</i>	Configuraciones y opciones de energía.
<i>printmanagement.msc</i>	Administrador impresoras.
<i>secpol.msc</i>	Configurar la política de seguridad local.
<i>services.msc</i>	Gestionar los servicios locales que aporta el sistema.
<i>taskschd.msc</i>	Programador de tareas.

6.2.2 Introducción á administración de usuarios e grupos locais en Windows Server 2019

Windows Server é un sistema multiusuario onde varios usuarios poden iniciar sesión simultaneamente no computador desde unha contorna de traballo en rede, desde outros terminais ou estacións de traballo. Debemos estar como usuario administrador para poder configurar o servidor. Un servidor dispón de contas de acceso local para acceder pola rede desde o propio servidor ou global a unha ordenador estación de traballo ou terminal.

É dicir, unha conta de usuario é unha identificación asignada de maneira única ao usuario para permitirlle:

Ampliar a imaxe que mostra os grupos e usuarios en Windows Server



Antonio López (Elaboración propia)

- Iniciar sesión nun dominio para acceder aos recursos de toda a rede.
- Iniciar sesión nun equipo local para acceder aos recursos locais ou a un grupo de traballo.

Cando varios usuarios van ter os mesmos dereitos e privilexios no servidor, é conveniente crear un grupo co devandito perfil de acceso, permitíndonos crear usuarios que se poidan engadir a un grupo definido, deste xeito automaticamente adquieren os privilexios de acceso ao grupo. Hai dous tipos diferentes de grupos:

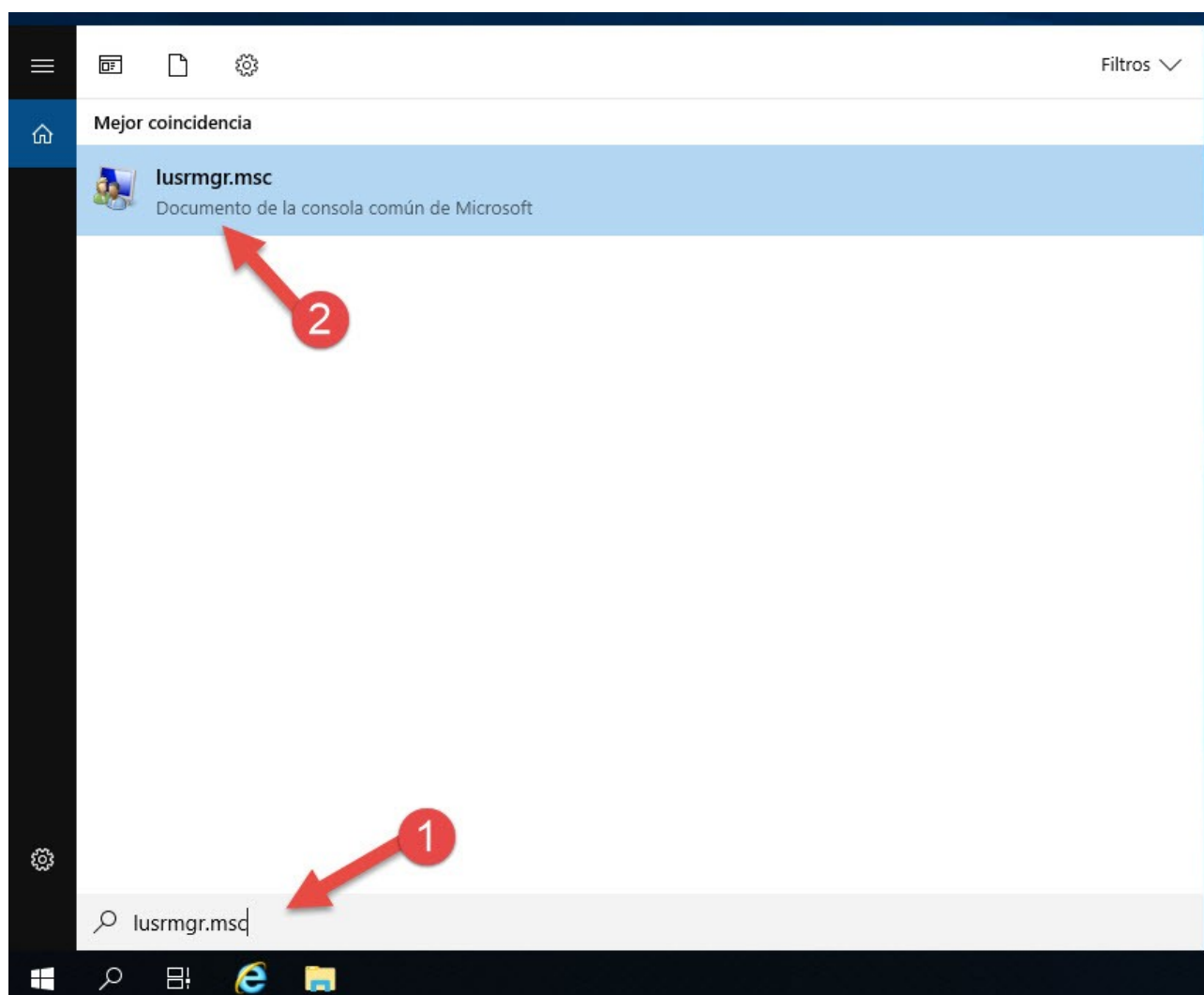
- Grupos locais: Outorgan aos usuarios permisos para que accedan a un recurso de rede. Tamén serven para conceder aos usuarios privilexios para xestionar tarefas de sistema (como cambiar a hora, facer copias de seguridade, recuperar arquivos, etc.). Existen grupos locais predeterminados. Mentres non se defina un dominio todas as contas xunto coa de Administrador considéranse locais. Podemos crear novas contas locais e asignarlles diferentes permisos de acceso ao sistema.

- Grupos globais: Úsanse para organizar as contas de usuario de dominio. Tamén se usan en redes de varios dominios, cando os usuarios dun dominio necesitan ter acceso a recursos doutro dominio.

6.2.2.1 Configuración de usuarios e grupos locais en Windows Server 2019

Operacións que podemos realizar con usuarios locais (para consultar a descrición dos campos dos diferentes formularios acceder á propia axuda na xanela mostrada por Windows):

Ilustración que mostra como abrir a aplicación de Usuarios e grupos locais.

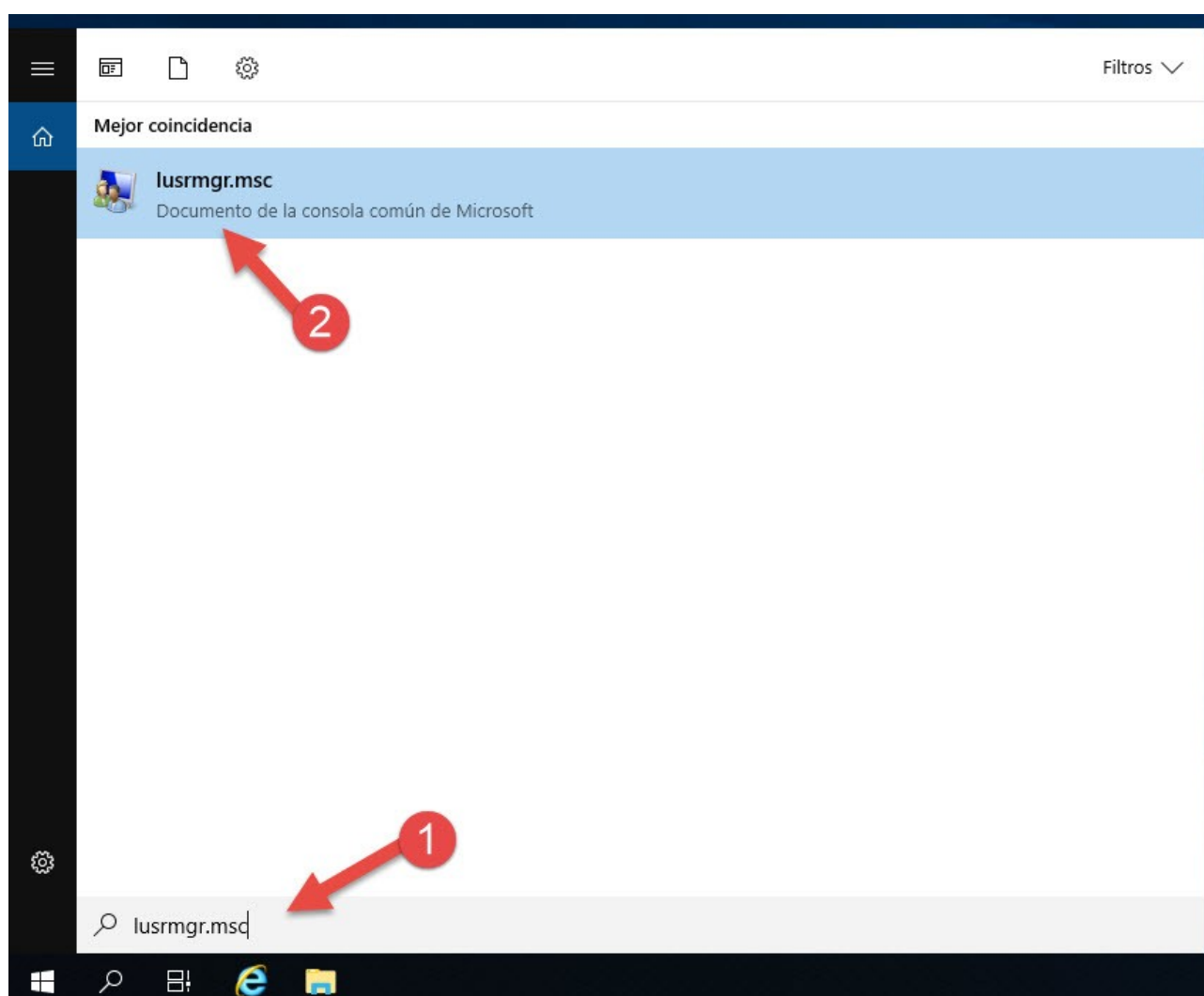


Windows Server 2019 (Elaboración propia)

Facemos clic na lupa e escribimos lusrmgr.msc que é a aplicación de Usuarios e grupos locais. Picamos sobre ela, xa temos aberta esta aplicación.

- Para crear contas de usuario local seguir os seguintes pasos:
 - Abrimos a aplicación Usuarios e grupos locais. No panel da esquerda pulsamos en Usuarios, no panel central aparécennos os usuarios creados.
 - Se non creamos ningún usuario, aparécennos os usuarios predeterminados o Administrador, Convidado, DefaultAccount e WDAGUtilityAccount (se ten unha frecha cara abaixo indica que por seguridade está deshabilitado).
 - Pulsamos o botón dereito do rato desde zona branca do panel central, do menú seleccionar Usuario novo. Do formulario completar os campos e dar ao botón Crear.

Ilustración que mostra as propiedades do usuario administrador.



Windows Server 2019 (Elaboración propia)

- Para dar de baixa de usuario local do servidor seguir os pasos seguintes:

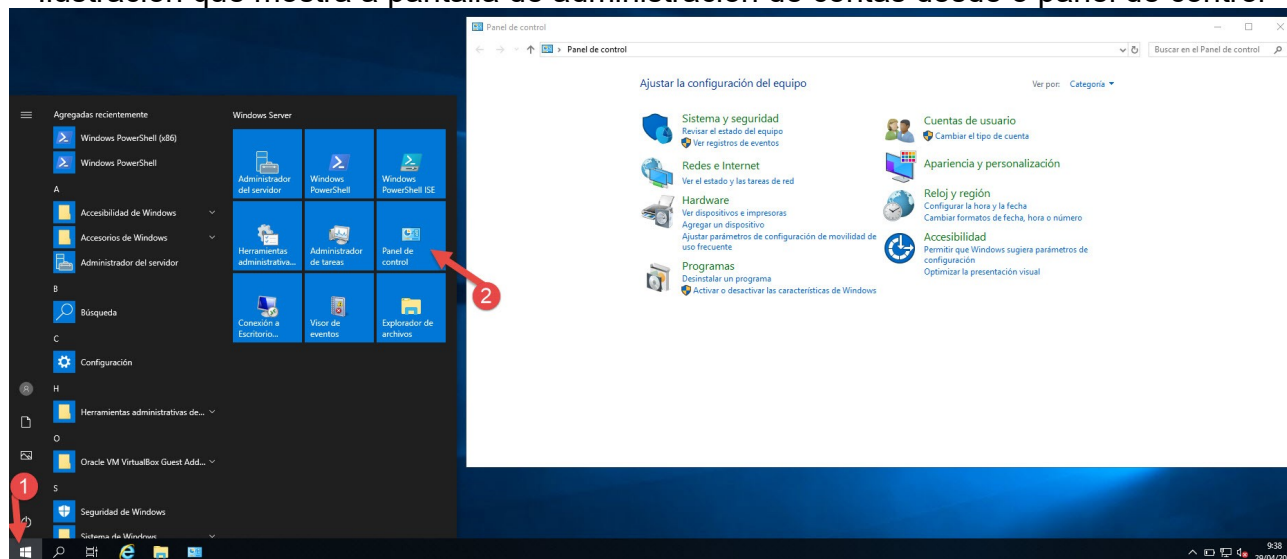
- Abrimos a aplicación Usuarios e grupos locais. No panel da esquerda pulsamos en Usuarios.
- Co botón dereito seleccionamos o usuario para dar de baixa. Seleccionamos a opción Eliminar. Da xanela de confirmación pulsar Se. Non se pode recuperar unha conta de usuario eliminada. Non é posible eliminar as contas Administrador e Convidado.
- Se necesitamos modificar os datos dun usuario debemos seguir as seguintes indicacións:
 - Abrimos a aplicación Usuarios e grupos locais. No panel da esquerda pulsamos en Usuarios
 - Co botón dereito seleccionamos o usuario para modificar e seleccionamos a opción Propiedades.
 - Aparece unha xanela coas seguintes pestanas ou formularios:
 - Xeneral: onde se poden modificar os datos que identifican o usuario dentro do sistema como o seu nome e directivas de seguridade da conta.
 - Membro de: permite ver ou cambiar os grupos aos que pertence o usuario. Un usuario pode pertencer a varios grupos, con privilexios adquiridos da suma de todos eles. Para engadir o usuario a un grupo pulsamos no botón Agregar, clic en Opcións avanzadas, clic en Localización para indicar da lista que aparece, o computador onde debe buscar os grupos aos que queremos pertencer e seguidamente dar ao botón Buscar agora. Para que no panel inferior aparezan todos os grupos seleccionamos ao que queremos pertencer e pulsamos Aceptar. Para quitar o usuario dun grupo, da xanela inicial, seleccionamos o grupo e damos ao botón Quitar.
 - Perfil: Define o roteiro de acceso ao perfil do usuario e o script de inicio de sesión.
 - Contorna: permite configurar a contorna de servizos de escritorio remoto (permite que os usuarios poden conectarse de forma remota usando o servizo de escritorio remoto para executar programas e usar os recursos de rede do devandito servidor) e o modo de conexión de dispositivos ao comezo de sesión. Indicamos o programa que se executará ao iniciar a sesión e as impresoras das que poderá dispoñer o cliente.
 - Sesións: podemos configurar o tempo de espera e a reconexión aos servizos de servizos de escritorio remoto. Permite indicar, por seguridade, en que tempo se forza a desconectar unha sesión sen actividade ou activa.
 - Control remoto: configura o control remoto dos Servizos de escritorio remoto.

- Perfil de Servicios servicios de escritorio remoto: permite configurar o roteiro de acceso ao perfil de usuario dos servicios de escritorio remoto ou para denegar o inicio de sesión aos servicios de escritorio remoto.
- Marcado: para permitir ou denegar o acceso a redes, as opcións de devolución de chamadas e para asignar direccións IP estáticas.

6.2.2.2 Xestión de usuarios e grupos desde o Panel de control en Windows Server 2019

Windows Server 2019 está deseñado para poder acceder ás ferramentas e recursos por diferentes camiños ou accesos, dunha forma moi parecida a Windows 10 desde Inicio-Configuración-Contas-Outros usuarios, podemos xestionar as contas de usuario dun modo fácil e rápido desde Panel de control. Para realizar esta tarefa debemos ser usuario do grupo de administradores.

Ilustración que mostra a pantalla de administración de contas desde o panel de control

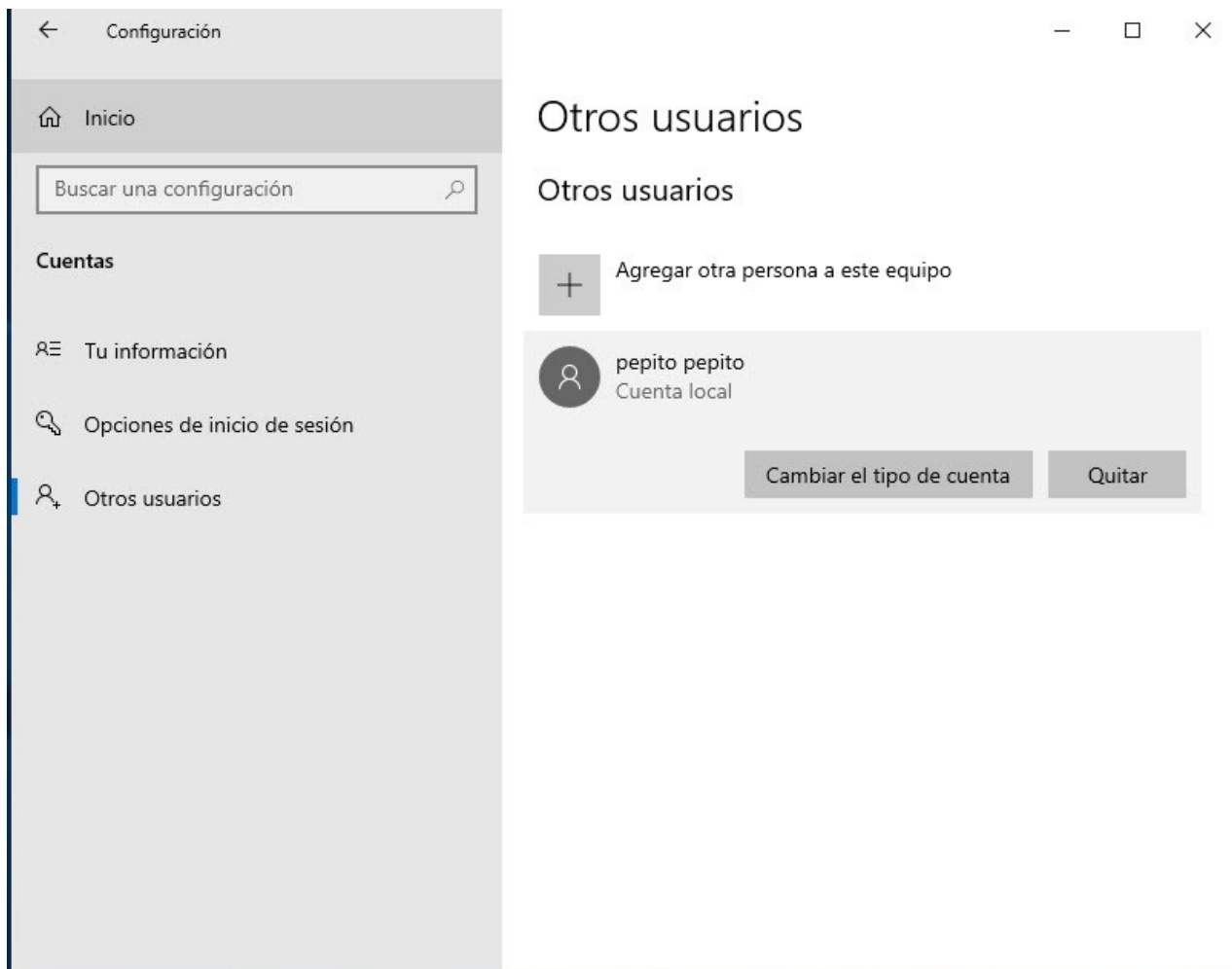


Windows (Elaboración propia)

Desde este lugar podemos:

- **Crear conta de usuario:** desde Inicio-Configuración-Contas-Outros usuarios-Agregar outra persoa a este equipo. Aparecéenos a xanela onde podemos xestionar os usuarios e grupos locais. Isto tédelo explicado no apartado 1.2.1 Configuración de usuarios e grupos locais en Windows Server 2019.
- **Cambiar o tipo de conta ou eliminar unha conta de usuario:** Inicio-Configuración-Contas-Outros usuarios. Aquí picamos sobre o usuario e aparécenos dúas opcións: cambiar o tipo de conta, onde podemos elixir: usuario estándar ou usuario administrador. Tamén podemos eliminar a conta pulsando no botón Quitar.

Ilustración que muestra a administración de usuarios desde o panel de configuración



Windows Server (Elaboración propia)

6.3 Administración de dominios

6.3.1 Estrutura de traballo en grupo

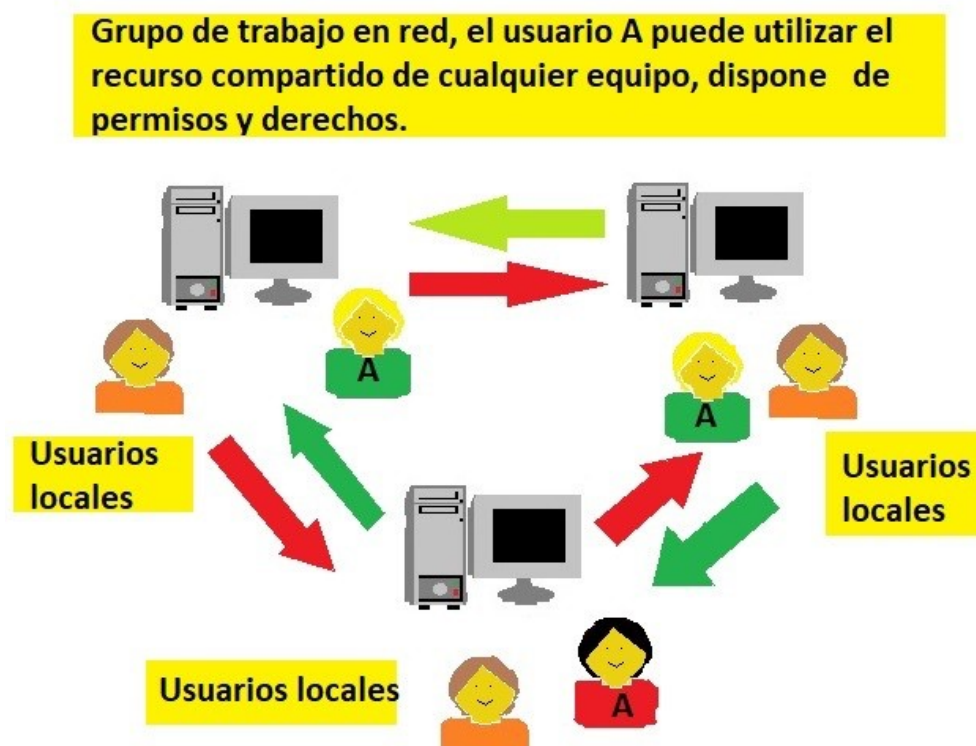
Os usuarios poden acceder localmente ao sistema operativo dun computador, que actúa como terminal dunha rede na que existen equipos servidores, todo dependerá do modo en que o usuario se identifique, ou realice o login á hora de entrar no sistema. Os computadores mediante os sistemas operativos en rede permiten o acceso aos seus recursos compartidos mediante dous métodos:

- Como membro dun Grupo de Traballo.
- Como membro dun Dominio.

Un grupo de traballo defínese como un conxunto de computadores en rede que comparten recursos de software e hardware. No modelo de grupo de traballo non existe

un servidor central e ordenadores clientes, senón que son redes de igual a igual ou punto a punto peer to peer. Para acceder ao recurso basta con estar na rede, coñecer a localización do recurso e o seu contrasinal. Dentro de una mesma subrede poden existir diferentes grupos de traballo.

Nun grupo de traballo cada equipo conserva unha lista dos usuarios autorizados e os recursos dispoñibles. Como son listas descentralizadas hai que dar de alta a cada novo usuario en cada computador.



Windows, de forma predeterminada, ten configurada a compartición de recursos nunha estrutura de grupo de traballo, (chamado WORKGROUP). Entre computadores con sistema operativo Linux, podemos compartir recursos mediante o servizo NFS que permite o acceso a recursos desde ordenadores clientes a outros que actúan de servidor, sempre que existan os permisos adecuados. Para compartir recursos entre redes mixtas, é dicir, que dispoñan de computadores con SO Windows e Linux será necesario utilizar o protocolo SMB.

Para integrar o equipo nun grupo de traballo en rede, debemos ter configurada a tarxeta rede de forma correcta dando valores aos protocolos TCP/IP, DNS, porta de ligazón, etc., estudado xa en unidades anteriores.

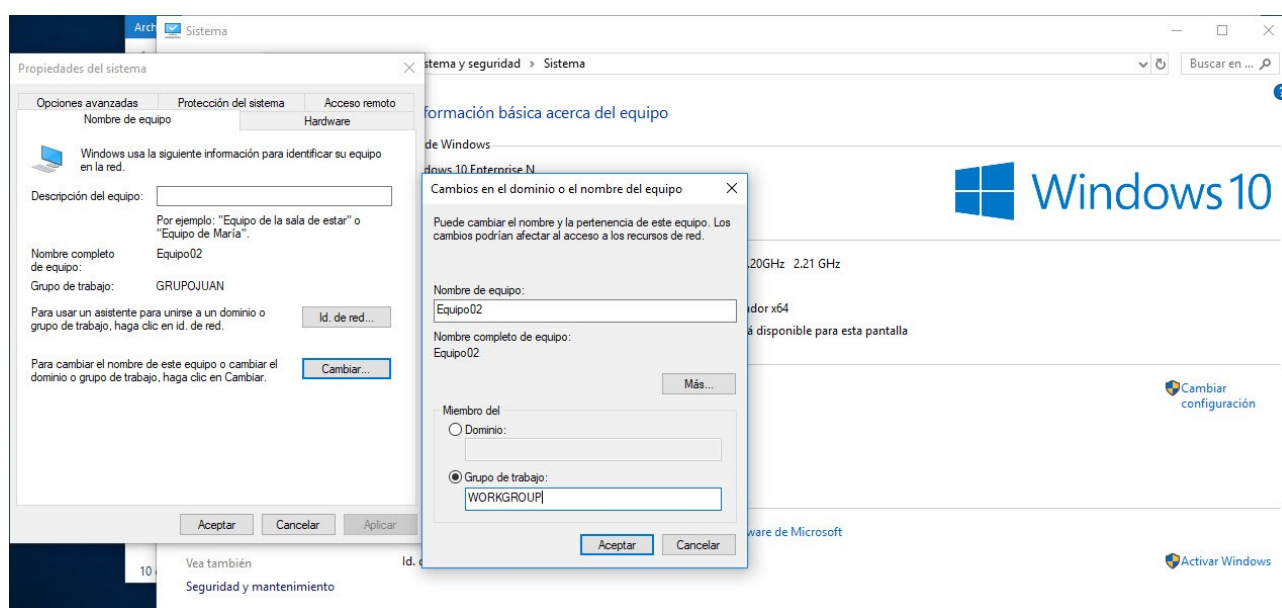
En Windows 10 xa non está dispoñible o Grupo Hogar, que permitía a creación automática, por parte do sistema, do grupo co fin de facilitar ao usuario a compartición de recursos dentro dunha rede, o único inconveniente é que soamente permite esta configuración a equipos que dispoñen do sistema operativo Windows 7 ou Vista.

Tampouco está dispoñible en Windows 10 a función denominada Mapa de rede, que permite usar o protocolo LLTD que detecta a topoloxía de rede co fin de mostrarnos un gráfico para axudarnos a buscar outros equipos e dispositivos que nese instante están conectados na nosa rede local. Para mostrar o mapa, damos a Inicio-Panel de control-Rede e Internet-Centro de redes e recursos compartidos, na parte superior dereita da xanela, pulsamos en Ver o mapa completo. (Con configuración de rede como pública non funcionará). Desde Windows 8 esta opción xa non está dispoñible.

6.3.1.1 Configurar un grupo de traballo por rede nun terminal Windows

Un computador ao iniciar o arranque dentro dunha contorna de rede poida que incorpórese a un grupo de traballo. En Windows para engadir un equipo a un grupo de traballo debemos seguir

Ilustración que mostra onde se configura o grupo de traballo en Windows



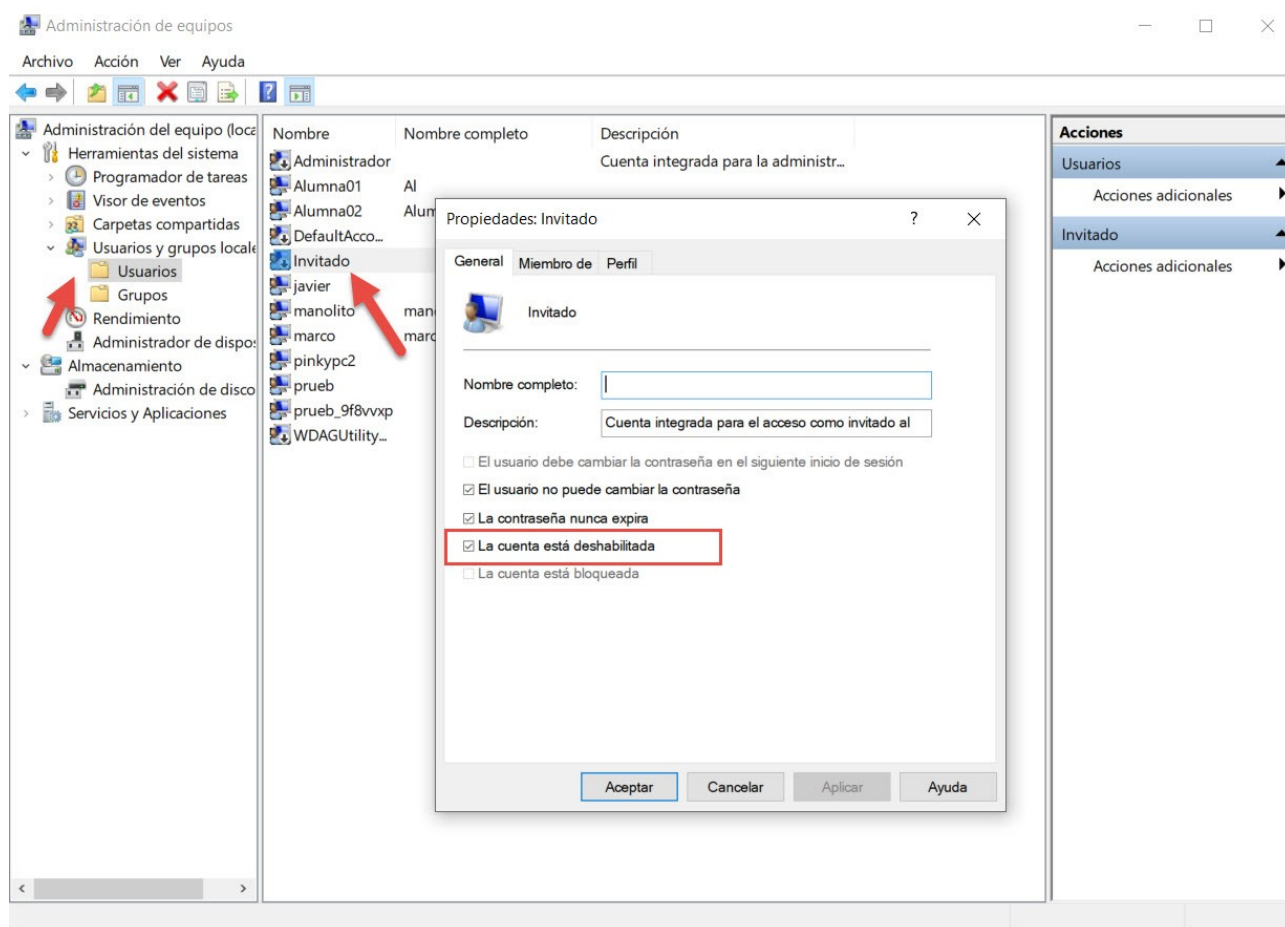
Windows (Elaboración propia)

os seguintes pasos: Na barra de procura escribimos Grupo de traballo, picamos no resultado Cambiar grupo de traballo. Ábrese unha xanela onde nos aparece información do nome do equipo e do grupo de traballo. Para cambiar o grupo de traballo, picamos en ele botón Cambiar, aparece a xanela onde temos os campos que identificarán o computador (nome de equipo) dentro dun grupo de traballo (de forma predeterminada

será WORKGROUP), desde este lugar podemos cambiar o nome do mesmo para que se incorpore ao grupo de traballo que desexemos.

O login de inicio de sesión en Windows, para un usuario nun equipo que pertence a un grupo de traballo, presenta a forma de petición de acceso de nome de usuario local e clave. Cando se inicia sesión localmente ou remotamente, soamente tense acceso aos recursos do equipo que a conta ou grupo permitan. Para que un usuario poida acceder localmente aos recursos dun computador dun grupo de traballo, terá que estar dado de alta e iniciar a sesión no propio computador.

Ilustración que mostra as propiedades do usuario Invitados



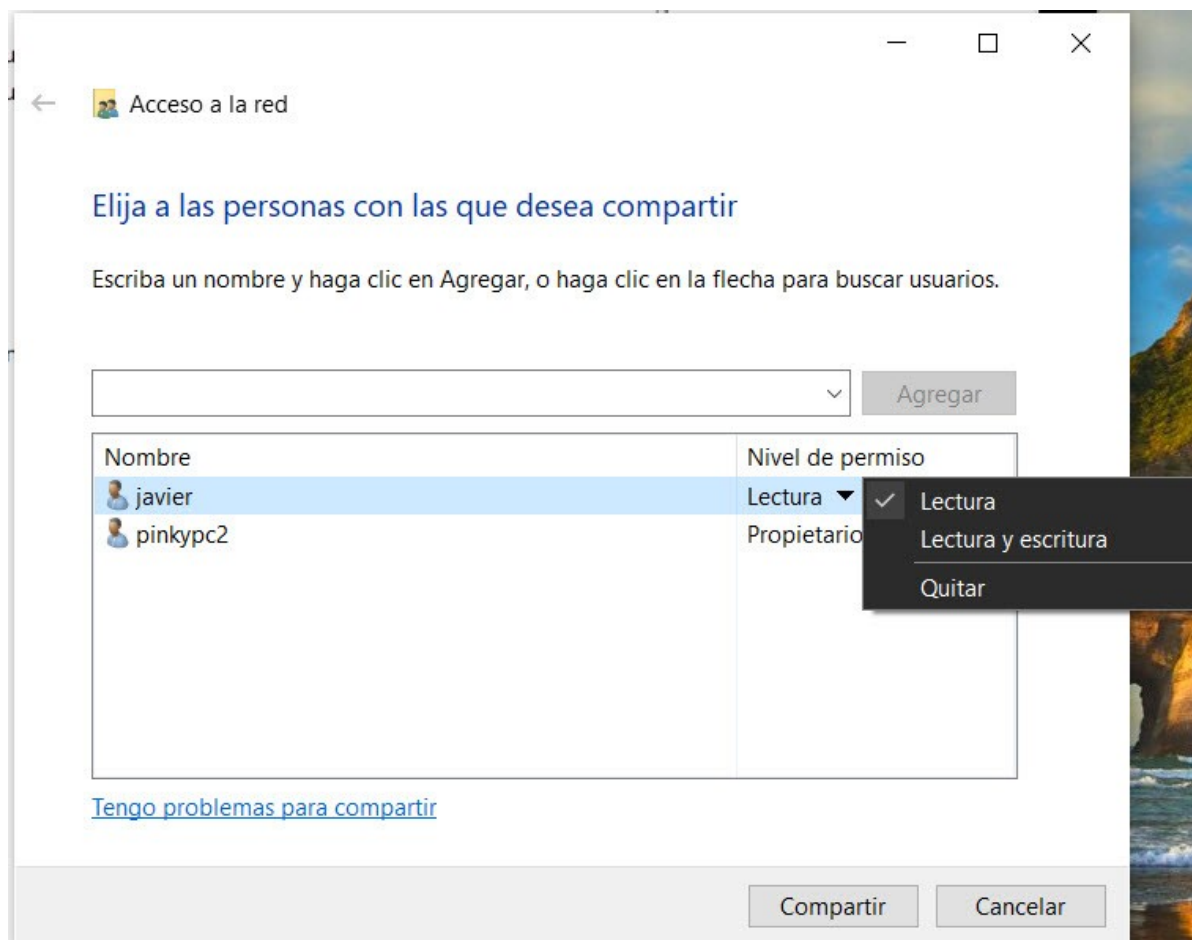
Windows (Elaboración propia)

Hai que lembrar que existe unha conta predeterminada común en todos, coa que se podería acceder se temos permisos adecuados ao recurso que é a de Invitado, pero por seguridade no sistema atópase desactivada, podemos comprobalo escribindo no panel de procura Ferramentas administrativas-Administración de equipos- Usuarios e grupos locais-Usuarios, seleccionar a conta de Invitado e pulsar co botón dereito do rato e facer clic en Propiedades, veremos unha xanela cos valores da conta de Invitado. Se desexamos acceder a un recurso compartido por outro ordenador membro do grupo de

traballo, o usuario deberá estar dado de alta no computador que serve o recurso, para que cando lle solicite o login de acceso poida identificarse (se accede coa mesma conta que o equipo co que iniciou sesión non lle solicitará identificación).

En Windows para comprobar os equipos e os grupos de traballo pertencentes a unha mesma rede séguense os seguintes pasos: no panel de procura escribimos Panel de control, picamos no resultado panel de control, facemos clic en Redes e internet->Ver os equipos e dispositivos de rede. Aparécenos a xanela de Rede, onde se mostras todos os equipos que están no noso grupo de traballo.

Ilustración que mostra como agregar usuarios e permisos a un recurso compartido

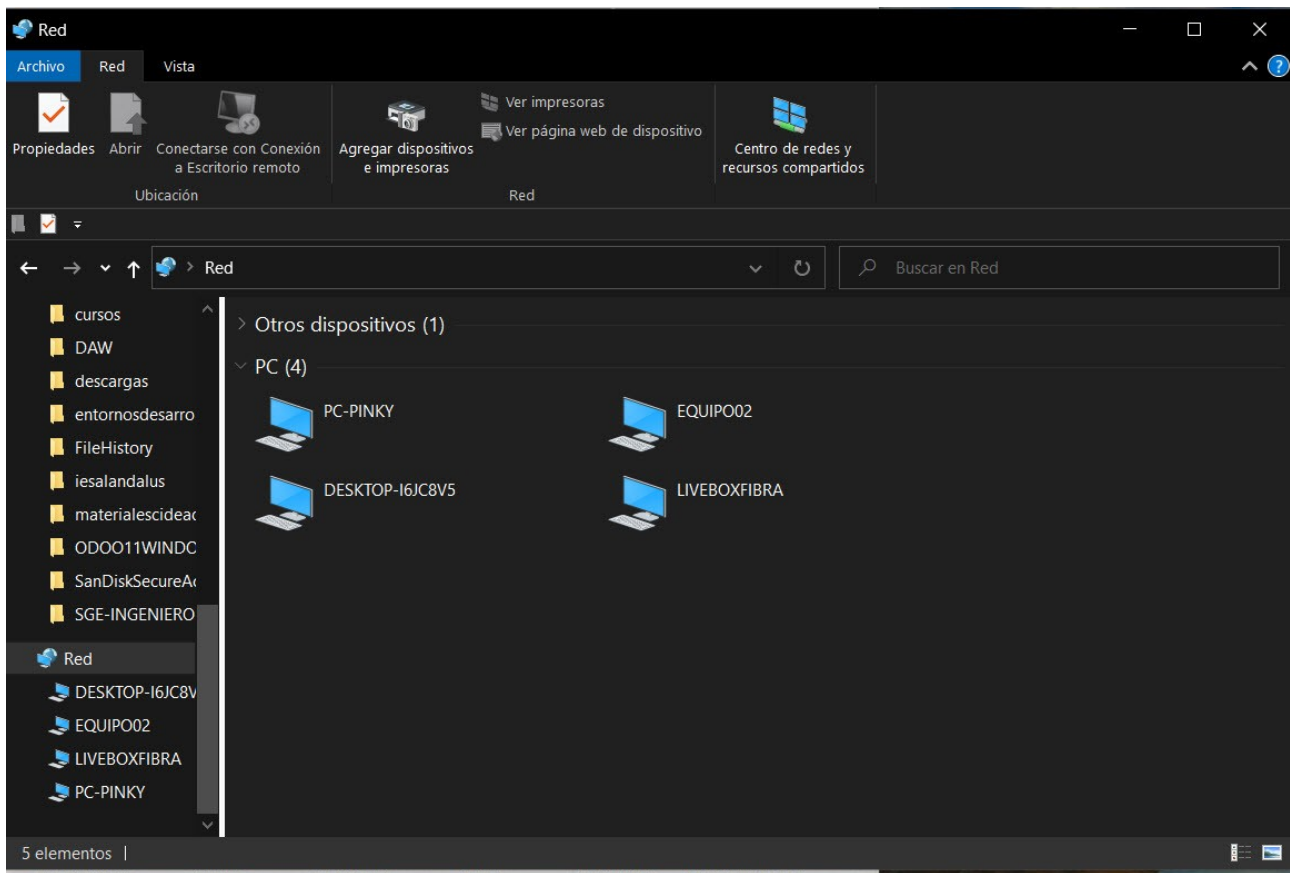


Windows (Elaboración propia)

Tamén podemos acceder abrindo o explorador de arquivos con Tecla Windows + E, no panel da esquerda, pulsamos na icona de Rede.

Se desexamos compartir un recurso para os computadores do grupo debemos acceder ao recurso co explorador, seleccionar co rato e pulsar o botón dereito, facemos clic na opción do menú Conceder acceso a e seguidamente en Usuarios específicos para elixir cales poden utilizar o recurso e que permisos.

Ilustración que mostra os equipos que hai no mesmo grupo de traballo



Windows (Elaboración propia)

6.3.1.2 Acceso a recursos compartidos grupo traballo desde Windows e Linux

Para localizar un recurso compartido desde calquera Windows seguimos os seguintes pasos:

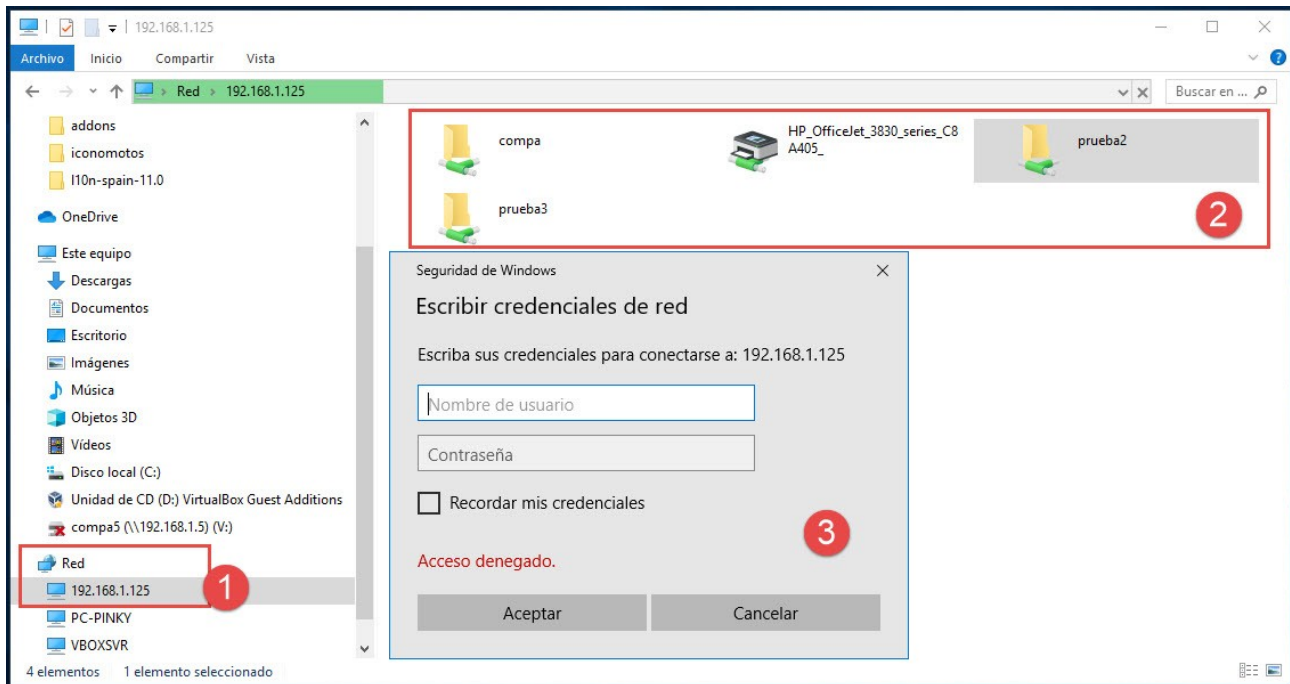
Desde Panel de control seleccionamos a opción Redes e Internet ->Centro de redes e recursos compartidos, e pulsamos na opción Ver equipos e dispositivos. Outro camiño é abrir o Explorador de arquivos desde a barra de tarefas e pulsar en Rede, e seleccionamos o equipo. Se o usuario que accede non é o mesmo que o usuario que ten dereitos sobre o recurso compartido, poida que pregúntenos Nome de usuario do recurso compartido e contrasinal (se o usuario que iniciou sesión en Windows é o mesmo que o usuario Samba de Linux non pedirá usuario e clave ao acceder ao recurso compartido), seguidamente aparecerán os recursos compartidos polo equipo.

Ilustración que mostra como acceder a un recurso compartido



Windows (Elaboración propia)

Ilustración que mostra como acceder a un recurso compartido



Windows (Elaboración propia)

Outra forma de acceder é escribindo na barra de direccións do explorador de arquivos, a dirección IP do equipo ao que desexamos acceder ou o seu nome NetBIOS, con formato:

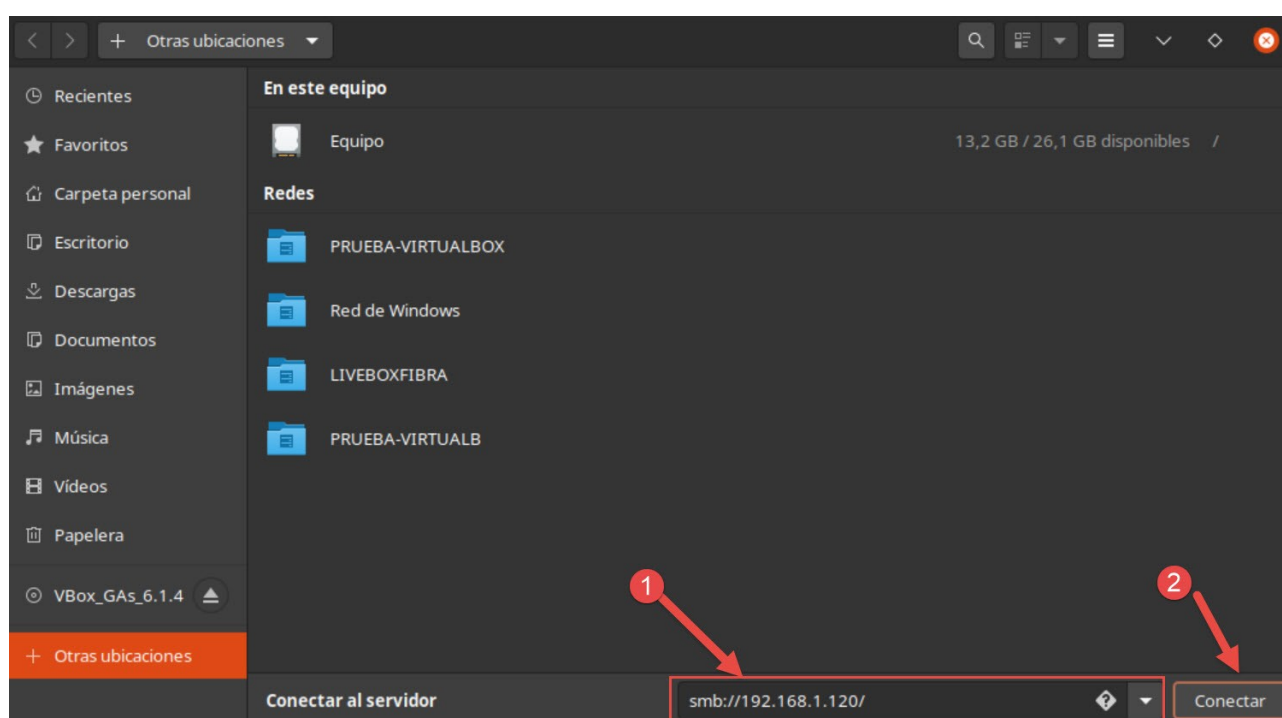
\\ip_equipo\ ó \\ip_equipo\recurso_compartido.

Lembremos que sendo un usuario Administrador, desde o panel de procura escribimos Panel de control picamos sobre Panel de control- Redes e Internet, podemos xestionar todos os aspectos referido á configuración da rede, como poden ser:

- Cambiar a configuración da tarxeta de rede.
- Cambiar as opcións de uso compartido para distintos perfís da rede, activando e desactivando opcións como Detección de redes, Permitir o uso compartido da impresora.

- Compartir recursos e acceder aos recursos compartidos por outros equipos.
- Ver o estado actual da rede.
- Conectarse a unha unidade de rede, é dicir, visualizar na contorna de traballo un recurso compartido por outro equipo coma se fose unha unidade ou dispositivo conectado no propio equipo, de maneira que facilita o seu acceso en todas as sesións cun simple clic coma se fose unha unidade de disco. Para a súa realización seleccionamos Inicio-Equipo, damos na icona de Rede do panel esquerdo e do menú pulsamos en Conectar a unha unidade de rede, seguimos o asistente que nos pedirá un nome de unidade para o recurso compartido que posteriormente debemos buscar na contorna de rede dando no botón Examinar.

Ilustración que mostra como conectarse a un equipo Windows desde Linux



Ubuntu (Elaboración propia)

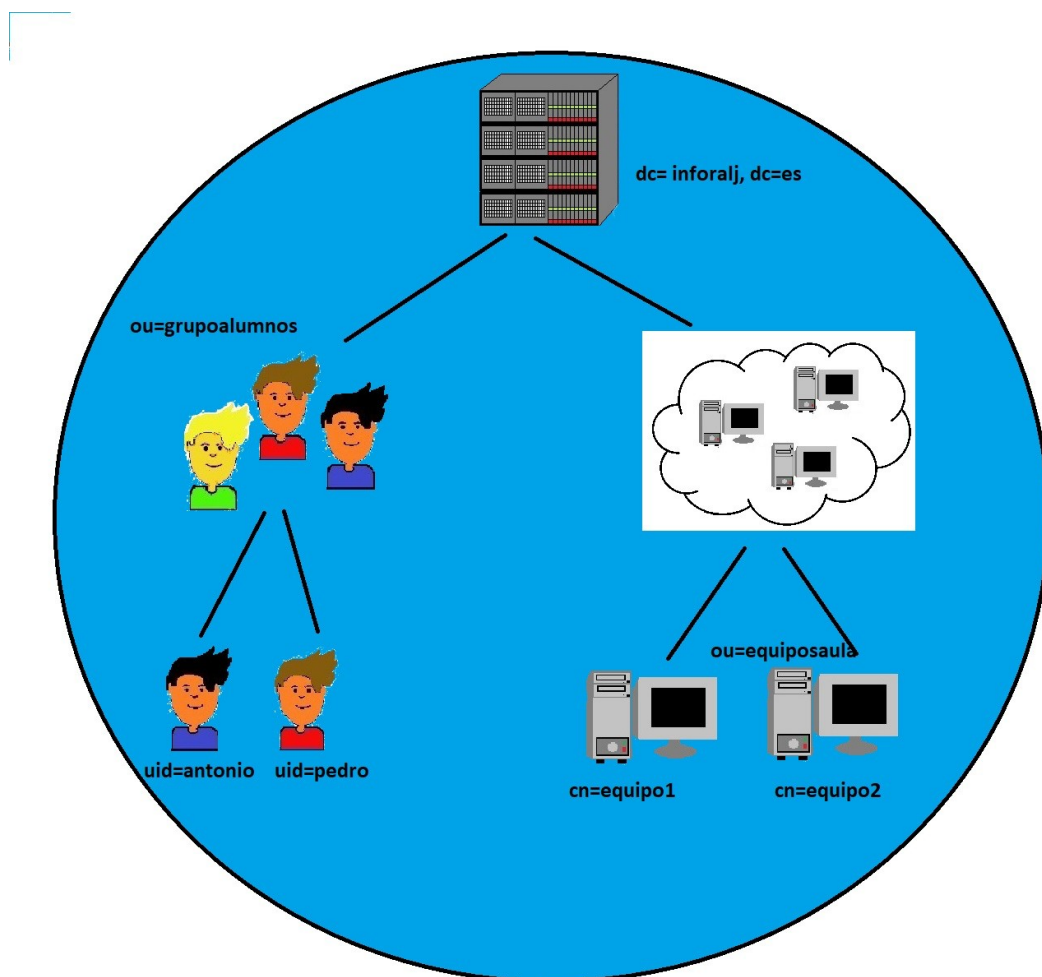
É importante considerar que as conexións múltiples para un servidor ou recurso compartido compatible polo mesmo usuario, usando máis dun nome de usuario, non están permitidas. Para poder acceder a outro recurso debemos pechar todas as conexións ao servidor ou recurso compartido e volver tentar conectar nunha nova sesión.

6.3.2 Protocolo LDAP

Mediante a activación do chamado servizo de directorio de rede conséguese dispoñer de información ordenada xerarquicamente dos obxectos como son os usuarios, equipos, recursos, impresoras, etc. O protocolo LDAP é o que se encarga de xestionar o acceso ao servizo para permitir aos usuarios almacenar datos, realizar consultas, operacións de

administración, etc., dentro do directorio de rede. A propia función AD ou directorio activo de Windows utiliza unha tecnoloxía parecida a LDAP xunto co servizo DNS para xestionar e coordinar os recursos da rede dunha forma centralizada.

Ilustración que mostra unha estrutura dun dominio, con unidades organizativas, usuarios e equipos



Antonio López (Elaboración propia)

En Linux non existe o concepto de directorio activo pero pódese habilitar a mesma función instalando o servizo LDAP (Protocolo Lixeiro de Acceso a Directorios) combinando as aplicacións Samba coa aplicación OpenLDAP permitindo xestionar un servizo de directorio mediante unha base de datos, que manterá a información relacionada das contas de usuarios e obxectos existentes na rede.

O servizo LDAP permite o acceso á devandita información mediante un esquema de directorio que contén as definicións dos obxectos que poden darse de alta no directorio. O directorio está baseado nunha estrutura xerárquica de árbore de obxectos, na que cada obxecto está identificado por propiedades denominadas atributos. Cada atributo identifícase mediante un nome distinguido ou DN, tipo ou clase de obxecto (ObjectClass)

e valores asociados. A cantidade de atributos dependerán do obxecto, poden ter atributos como cn (describe o nome común), sn (para o apelido).

Cada entrada do directorio é unha cadea de caracteres formada por pares "tipo_atributo"="valor" separados por comas, que representa o roteiro investido que leva desde a posición lóxica da entrada na árbore ata a raíz do mesmo. O nome raíz do directorio LDAP utiliza a identificación de obxectos da mesma forma que os dominios DNS. Por exemplo, a raíz ou base da empresa Inforalj S.A sería: "dc=inforalj, dc=é".

A partir desa base, a árbore se subdivide nos nodos ou ramas, subnodos e obxectos ou follas da árbore. Seguindo co exemplo do debuxo, a continuación móstrase un subconxunto dos atributos do usuario "antonio":

```
dn: uid=antonio, ou=grupoalumnos, dc=inforalj, dc=com
objectClass: person
cn: antonio lopez
sn: lopez
description: alumno clase
mail: antonio@inforalj.es
```

6.3.3 Os dominios

Windows utiliza o concepto de dominio como unha agrupación de computadores nunha contorna de rede, (servidores e estacións de traballo), controlados por un computador que actúa de servidor principal, o cal garda a lista de usuarios e nivel de acceso de cada un, así como a xestión centralizada de recursos, equipos, servizos, etc. Estes servidores son Controladores de Dominio (Windows Server 2019 e Linux) e axudan á administración da seguridade do grupo. Os computadores integrados no dominio non necesitan fisicamente estar na mesma rede, ademais, a diferenza dos grupos de traballo presentan maior seguridade e organización.

O AD de Windows é unha implementación de LDAP xa que trata os recursos da rede como obxectos que teñen propiedades e atributos. Por exemplo, cada obxecto identifícase por un atributo de nome relativo ou nome común (CN), ademais tamén teñen un atributo chamado nome distintivo (DN) que describe a localización do obxecto no directorio.

Cando un computador está configurado para pertencer a un dominio, utilízanse contas usuario de dominio creadas no servidor para iniciar sesión desde un ordenador cliente. Calquera usuario cunha conta de dominio, pode iniciar sesión desde calquera equipo que estea incluído no dominio, sempre que non estea restrinxido o seu acceso desde a

configuración do Active Directory do servidor no caso de Windows, ou servizo de directorio en Linux.

Cando nunha rede xérase un controlador de dominio, podemos dicir que nese momento creouse un dominio. No caso de Windows Server, realizarase no momento de instalar os Servizos de dominio de Active Directory. Se varios dominios forman parte dun sistema de comunicación, poderanse establecer relacións de confianza entre eles para compartir os recursos. Mediante a organización das redes en dominios, podemos dividir redes grandes en máis pequenas, permitindo crear dominios principais cos seus correspondentes subdominios e estruturas xerárquicas independentes.



isoalisal (Elaboración propia)

A estrutura xerárquica dun dominio nunha rede Windows, ten forma de árbore composta por un dominio principal ou raíz que será o pai de todos os dominios fillos ou subdominios da árbore. Un conxunto xerárquico de árbores formarán un bosque de dominios. As árbores de dominio e os dominios dunha árbore, poderanse comunicar establecendo relacións de confianza, que permiten ao usuario iniciar sesión nun dominio, e utilizar os recursos xestionados por outro dominio desta forma podemos compartir recursos entre os dominios.

Nunha rede que teña unha infraestrutura grande necesitarase máis dun controlador de dominio, todos dispoñerán dunha copia do Directorio Activo, así o usuario poderase validar no que estea máis dispoñible mellorando a actividade de validación de usuarios. Os controladores dispoñen do chamado catálogo global, que ten a función de manter unha información esquematizada e actualizada dos usuarios, grupos, equipos e recursos de todos os dominios dun bosque.

6.3.3.1 Planificación e requisitos necesarios para montar unha estrutura de dominio

Para evitar posibles problemas no futuro, antes de comezar a instalación dos servizos de dominio nun directorio activo, debemos pensar nunha serie de consideracións relacionadas con ampliacións das estruturas dos sistemas e as súas configuracións, como son:

Ilustración que mostra un servidor



[bocian \(CC0\)](#)

- Saber cantos servidores con funcións de controlador de dominio necesítanse. Debemos ter en conta que un só dominio pode dar servizo dos seus recursos, a gran cantidade de usuarios.
- Coñecer que funcións deben xestionar os dominios e subdominios. Pensando sempre que as relacións de confianza que se xeren, poidan permitir que os administradores outorguen permisos para que os recursos de calquera dos dominios dun bosque ou árbore estean dispoñibles para todos os usuarios dos dominios.
- Pensar cantas unidades organizativas necesítanse e quen xestionase a súa administración.
- Definir as directivas de grupo e de seguridade local.
- Planificar cantas contas de usuarios, grupos e equipos xestionará cada dominio.
- Definir un plan de seguridade baseado na replicación dos servizos de directorios.
- Mellorar as necesidades de hardware para os controladores de dominio, como nos compoñentes de:

- Procesador rápido ou a posibilidade de multiprocesadores. Melloraranse os procesos de replicación sen que afecte a outros procesos do servidor.
- Ampliar a memoria RAM, como mínimo deberá ser de 2GB.
- Dispoñer de suficiente disco, para almacenar a información da base de datos do directorio activo.
- Dispoñer dun sistema de seguridade, que xestione a tolerancia a fallos, baseado en RAID- 1 ou RAID-5.
- Ter acceso a un servidor que forneza servizos de nomes de dominio (DNS), que pode estar instalado no propio servidor de dominio sempre que a súa dirección IP de rede sexa estática.
- Ter instalado un servidor que actúe de controlador de dominio principal, (Windows Server ou Linux Server).
- Configurar o protocolo de rede TCP/IP.
- Ter espazo suficiente no disco para montar o servizo de directorio, no caso de Windows formatada a NTFS.
- Deseñar un diagrama ou esquema, que identifique a cantidade de servidores e clientes, así como a función e os recursos que prestará cada un dos servidores.
- Avaliar a posibilidade de instalar servidores virtuais. Podemos pensar no concepto de servidor virtual, que presta as mesmas funcións que un servidor real, de maneira que nun servidor físico podemos instalar varios servidores virtuais, permitíndonos un gran aforro económico en equipos.

6.3.4 Servizo de directorio: Active Directory (AD) en Windows

En Windows, cando se instala o AD o equipo convértese en servidor de dominio ou controlador de dominio dentro da rede, proporcionando unha fonte centralizada de información, co fin de facilitar a procura e utilización dos obxectos do directorio por parte de usuarios e dispositivos da rede. Lembremos que un directorio activo, dispón da seguinte estrutura lóxica en forma de árbore xerárquica:

- Un conxunto de árbores de dominio agrupados e relacionados lóxicamente forman un bosque de dominios. Cada árbore do bosque xestiónase polo seu propio espazo de nomes, pero comparten o mesmo catálogo global permitindo localizar e acceder aos recursos de todo o bosque de dominios, desde calquera equipo do propio bosque, axilizando a procura dos recursos. Raíz do directorio ou dominio raíz.
- Clases de obxectos que serán cada un dos elementos que controla o servizo de Directorio Activo. Serán usuarios, equipos, agrupacións de usuarios, agrupacións de equipos, unidades organizativas dos propios obxectos. Cada elemento controlado polo servizo de AD denomínase obxecto e dispón dunhas propiedades dependendo da clase de obxecto á que pertence.

- Os Subdominios son dominios fillos que se engaden ao dominio principal ou raíz, formando a árbore de dominios. Todos os dominios están relacionados polas chamadas relacións de confianza, compartindo o mesmo catálogo global ou repositorio de todos os obxectos da árbore de dominios, permitindo desta maneira o acceso a todos os recursos da árbore. O catálogo global contén información resumida dos recursos (usuarios, grupos, equipos, etc.) de todos os dominios. Os subdominios comparten o mesmo espazo de nome que o dominio raíz, formado polo seu propio nome máis o nome do dominio raíz.

Ilustración que mostra un dominio cun bosque e árbores



isoalisal (Elaboración propia)

En dominios Windows, os servidores que pertencen a unha árbore de dominio, poden ser controladores de dominio secundarios, encargados de ter unha copia da información do directorio activo, ou servidores membros encargados de almacenar os arquivos e recursos da rede. A base de datos que se mantén no controlador de dominio, cópiase ou duplica mediante o proceso de replicación en todos os controladores de dominio da rede, de maneira que cando se produza calquera modificación no Directorio Activo, se replicará a todos os controladores de dominio.

O AD necesita o servizo DNS, que organiza grupos de equipos nunha xerarquía de dominios usada na internet e baseada en diferentes niveis que identifican equipos, dominios de nivel superior asignando nomes de servidor a direccións TCP/IP. Será necesario configurar o servizo DNS para instalar o AD de Windows. Os arquivos que xestionan a información da base de datos do Active Directory son:

Ficheiros da base de datos do Active Directory

Fichero de AD	Funcionalidad
Ntds.dit	Contiene el almacén de datos formado por tres tablas indexadas: tabla de datos, de enlace y de seguridad.
Edb.chk	Mantiene la confirmación de las transacciones realizadas en la base de datos y en los archivos log.
Temp.edb	Utilizado como soporte temporal para la realización de las transacciones.
Edb.log	Contiene registro de las operaciones que no han sido realizadas en la base de datos.
Edbxxx.log	Contiene registro de las operaciones realizadas en la base de datos del Active Directory.

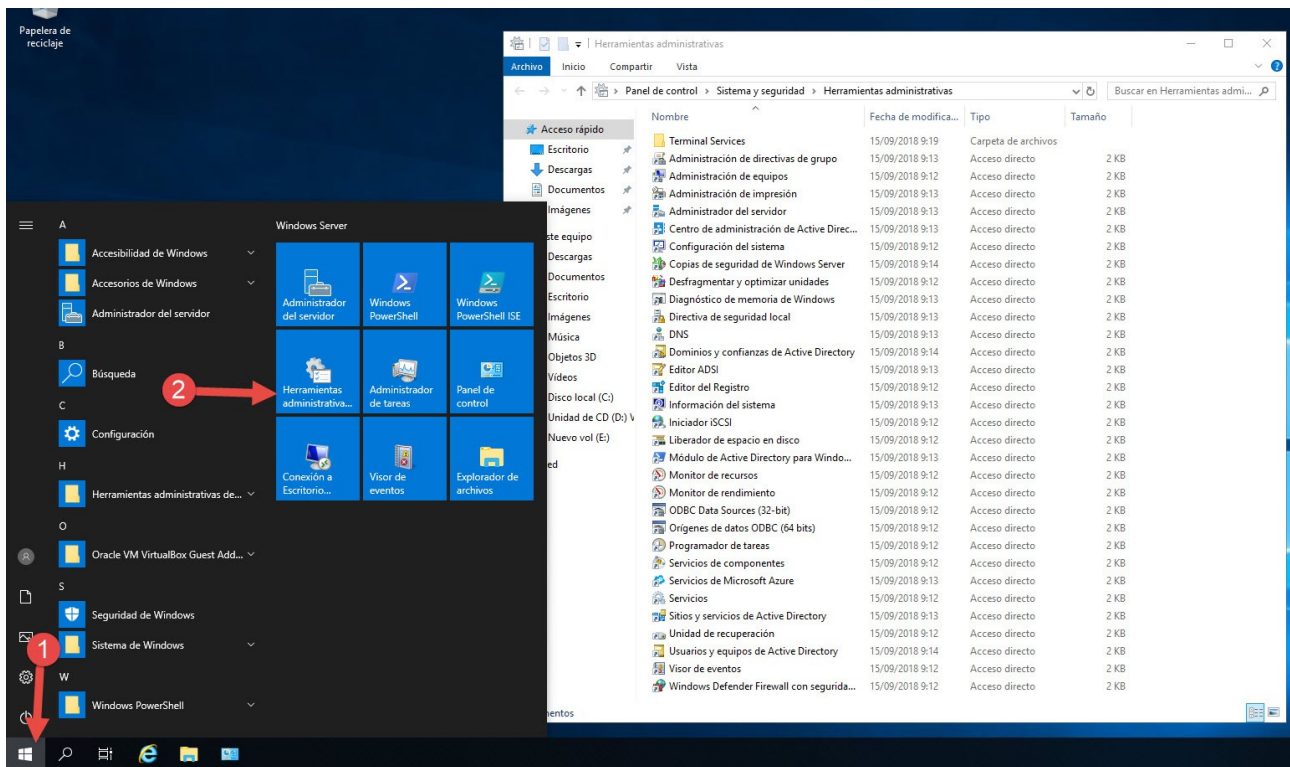
6.3.5 A contorna de traballo de administración de Active Directory

O usuario administrador do servidor deberá realizar tarefas como crear e modificar contas de usuario, engadir terminais ao dominio, organizar e agrupar obxectos, etc. O sistema operativo Windows Server, dispón de ferramentas na contorna gráfica e en liña de comandos para facilitar a administración de AD.

Podemos acceder ás aplicacións de administración de Active Directory desde o menú Inicio-Ferramentas administrativas, onde podemos seleccionar opcións que abrirán consolas de administración MMC para a realización de tarefas como:

- Servizos de dominio de Active Directory, para xestionar os servizos.
- Usuarios e equipos de Active Directory, onde podemos realizar tarefas relacionadas con usuarios, grupos, equipos e unidades organizativas.
- Sitios e servizos de Active Directory, para administrar os obxectos específicos do sitio que implementan a topoloxía de replicación entre sitios. Estes obxectos almacénanse no contedor de sitios dos Servizos de dominio de AD.
- Dominios e confianza de Active Directory, permite traballar cos obxectos de dominio, árbores e bosques creando relacións de confianza.
- Administración de directivas de grupo, podemos realizar as tarefas relacionadas coa seguridade de obxectos do AD mediante a configuración das directivas de grupo.
- Editor ADSI, realiza diagnósticos do AD para poder resolver problemas creando atributos e propiedades personalizadas para os usuarios e grupos.

Ilustración que mostra as ferramentas que ten Active directory nas Ferramentas administrativas



Windows (Elaboración propia)

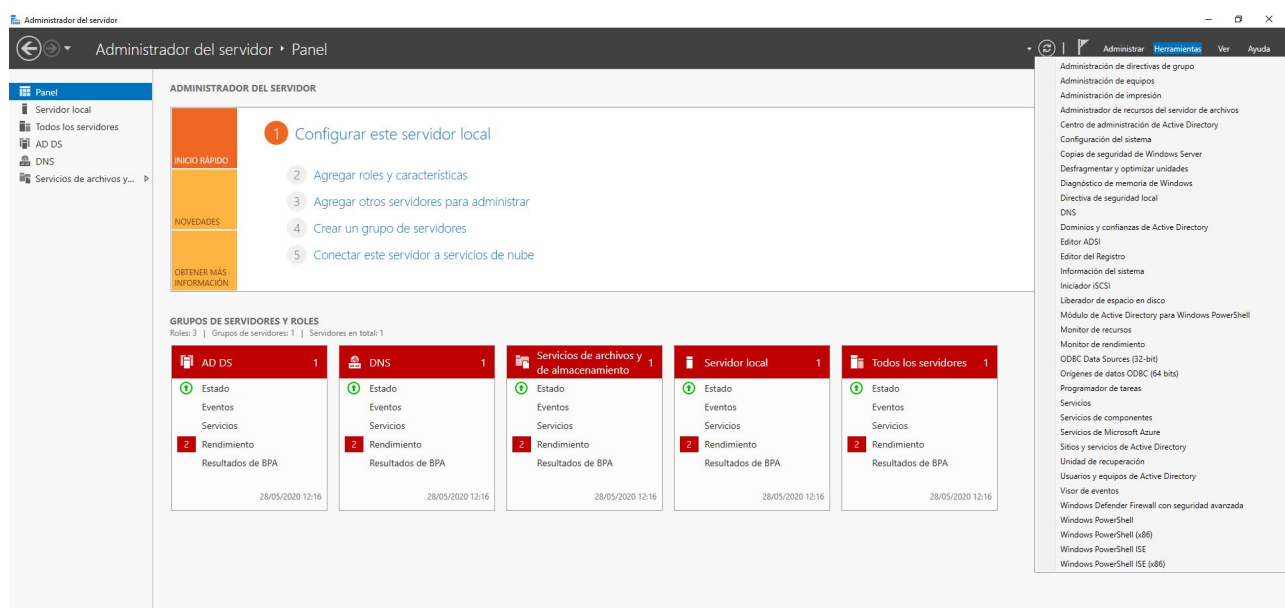
Para poder administrar o AD, temos o Administrador do Servidor. O Administrador do servidor é unha ferramenta onde temos o control centralizado de todas as tarefas que se executan no servidor tales como roles e características.

Co Administrador do servidor podemos:

Analizar e xestionar os roles e características instaladas en Windows Server.

- Executar tarefas de administración asociadas aos servizos implementados no servidor tales como iniciar, parar, deter ou eliminar servizos.
- Analizar o comportamento dos roles e características de Windows Server.
- Verificar o estado operativo do servidor en tempo real.

Ilustración que muestra a pantalla principal do Administrador do Servidor en Windows Server



Windows (Elaboración propia)

Para abrir o Administrador do servidor facemos clic en Inicio-Administración do servidor. Para ver como usar en Administrador do servidor, pica aquí. Desde o podemos acceder a diferentes ferramentas que nos permiten administrar o servidor e un dominio. Para acceder a elas, abrimos o administrador do servidor e pulsamos no menú Ferramentas que se atopa na parte superior dereita. Algunhas destas ferramentas son:

- **Ferramentas de administración do dominio:** permítennos administrar diferentes aspectos do dominio. Algunhas delas son:
 - **Dominios e confianza de Active Directory:** permite aumentar o nivel de funcionalidade do noso dominio, engadindo novas características ao Directorio Activo e crear relacións de confianza entre dominios.
 - **Usuarios e equipos de Active Directory:** permítenos definir o modo no que se usará a nosa infraestrutura de rede. Permítenos crear e administrar as contas de usuario que poderán usar os recursos de AD e as contas para os computadores desde os que devanditos usuarios poderán conectarse. Ademais facilitáanos a súa organización en grupos, unidades organizativas, etc.
 - **Sítios e servizos de Active Directory:** esta ferramenta permite definir a topoloxía do noso directorio activo, creando e administrando os sitios que forman a estrutura xeográfica da rede e creando vínculos entre eles.
- **Ferramentas de administrador do servidor:** permítennos administrar diferentes aspectos do servidor. Algunhas delas son:

- **Programador de tarefas:** con ela podemos programar tarefas repetitivas para que se realicen automaticamente, sen que o usuario teña que estar pendentes delas.
- **Windows PowerShell:** é unha ferramenta coa que podemos realizar múltiples tarefas administrativas.
- **Monitor de recursos:** permítenos monitorar o tráfico e recursos no noso servidor.
- **Copias de seguridade de Windows Server:** permítenos crear unha política de copias de seguridade no noso servidor.

6.3.5.1 Administración de unidades organizativas de Active Directory de Windows

As unidades organizativas (UO) son obxectos do directorio que nos permiten agrupar de forma organizada os obxectos, (usuarios, grupos, equipos, recursos compartidos e mesmo unidades organizativas), do dominio no que se definen. Algunhas das súas funcións e características son:

- **Facilitan a seguridade do dominio**, aplicando directivas de seguridade ás propias unidades organizativas.
- Permiten **repartir a administración** do AD, entre distintos administradores do dominio co fin de xestionar os recursos de maneira máis eficaz e segura.
- **Non se poden crear UO dentro dos contedores predeterminados do Directorio Activo, menos no contedor Domain Controllers.**
- As unidades organizativas **non poden conter obxectos doutros dominios.**
- Na estrutura xerárquica do dominio **sitúase nun nivel inferior ao dominio.**
- Pódense utilizar as unidades organizativas para crear unha estrutura funcional da organización interna departamental, (almacén, vendas, contabilidade, etc.) dunha empresa, no uso dos recursos e servizos informáticos, ofrecidos polo servidor de dominio, agrupando en conxuntos significativos os usuarios, grupos e recursos segundo as súas necesidades.
- En conclusión, podemos considerar ás UO, como cartafoles especiais ou contedores do directorio activo, con directivas de seguridade que servirán **para almacenar ou agrupar os usuarios, grupos, equipos, recursos compartidos**, co fin de ter ordenados os obxectos do dominio.

Ilustración que mostra os elementos dun dominio

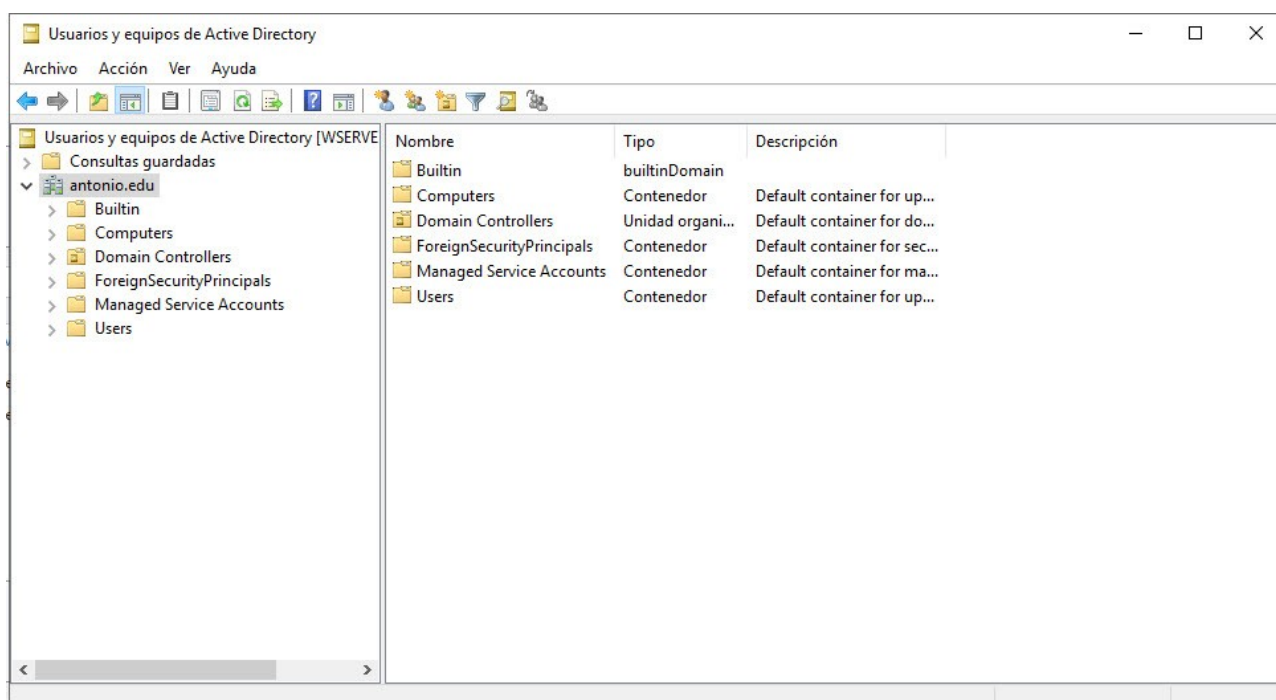


isoalisl (Elaboración propia)

Ademais das unidades organizativas, en calquera dominio o sistema xera de forma predeterminada unha serie de cartafoles para xestionar os obxectos do dominio, e atópanse na consola MMC de Usuarios e equipos de AD, tendo activada a propiedade de Características avanzadas do menú Ver e algunhas son:

- **Builtin:** Visualiza as contas de usuarios.
- **Computers:** Lista as contas de equipo.
- **Domain Controllers:** É a única unidade organizativa creada de forma predeterminada polo sistema e contén os controladores de dominio.
- **ForeignSecurityPrincipals:** Describe os obxectos dun dominio externo no que haxa unha relación de confianza co dominio actual.
- **NTDS Quotas:** Ten os datos de cota de AD.
- **Program Data:** Contén información das aplicacións do Directorio.
- **System:** Visualiza a información da configuración do sistema.
- **Users:** Lista os usuarios.

Ilustración que mostra os elementos dun dominio desde a ferramenta Usuarios e equipos de Active Directory

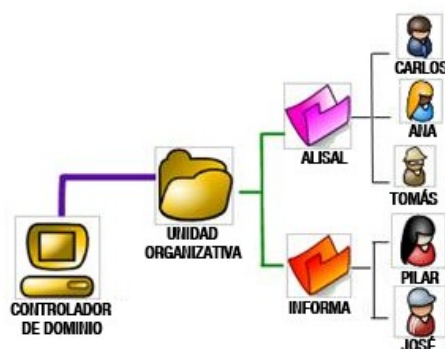


Windows (Elaboración propia)

6.3.5.2 Administración de contas de usuario de dominio de Windows

As contas de usuario de dominio, tamén chamadas globais, permiten acceder aos recursos de todo o dominio da rede desde calquera terminal que se atope asociado ao servidor de dominio, e débense administrar nos servizos do AD onde se poderán conceder permisos e dereitos dos recursos do dominio.

Ilustración que mostra como se organizan os usuarios



isoalisl (Elaboración propia)

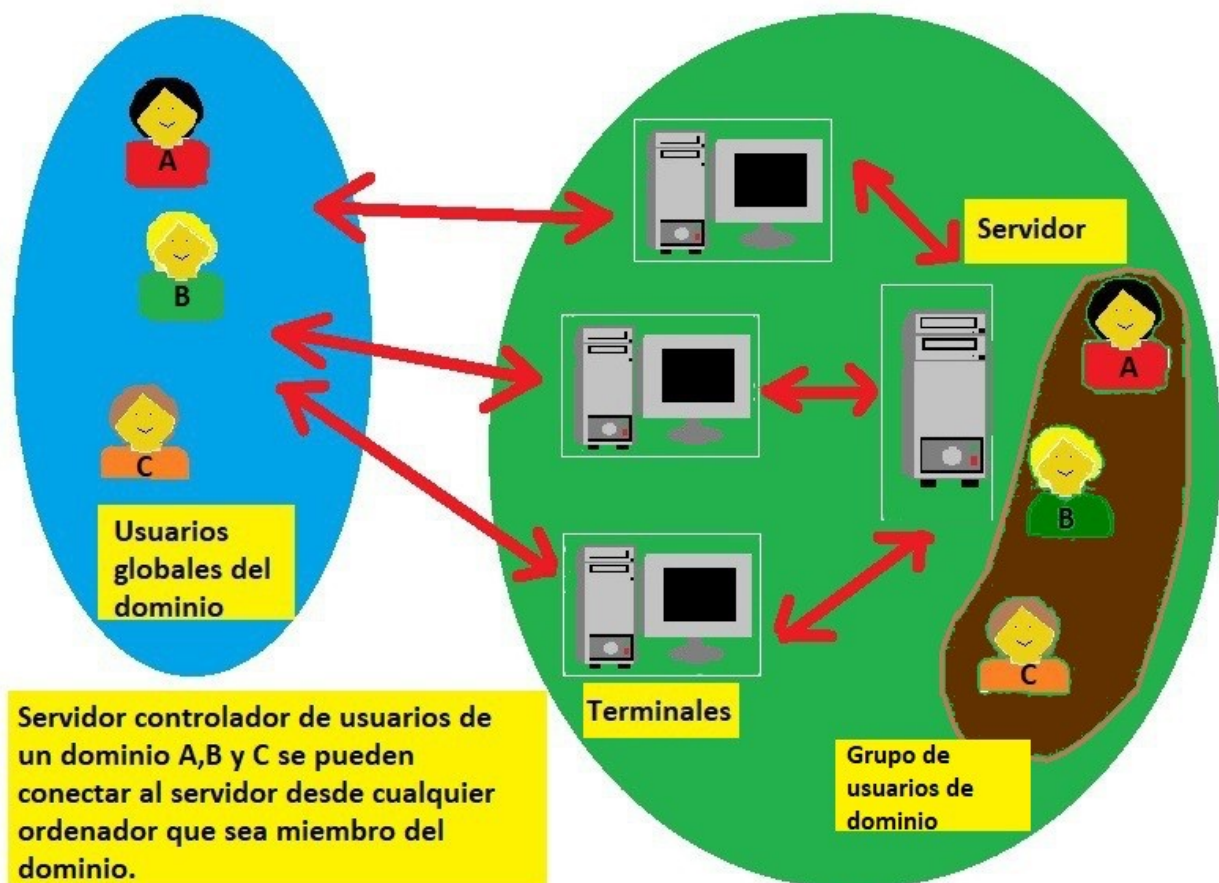
As contas de usuario teñen as seguintes características:

- Están definidas por un **nome e un contrasinal** que non se pode repetir, é dicir non pode haber dúas contas de usuarios iguais.
- Os **nomes da conta** están representados por non máis de 20 caracteres en maiúsculas, minúsculas, números e caracteres especiais menos: /, |, :, ;, =, <, > e *.
- Os **contrasinais** non conteñen menos 7 caracteres, e algún debe ser en minúsculas, maiúsculas e numérico. O servidor, por seguridade, lembrará as últimas 24 contrasinais dun usuario, (durante 1 ou 42 días, dependendo da configuración).
- Os **nomes de conta principais de seguridade dentro do servidor**, están representados polo nome de usuario e o sufixo @ seguido do nome do dominio ou nome principal, por exemplo “antonio@informatica.alisal.local”. Segundo isto podemos referenciar o nome dun usuario de dúas formas: polo seu nome (por exemplo “antonio”) ou pola súa definición DNS (como “antonio@informatica.sur.local”).
- Windows define **tipos de contas** como:
 - **Administrador**: Xerada no proceso de instalación. Ten o dereito e os permisos necesarios para a configuración total do dominio, por iso é membro de varios grupos relacionados coa administración do sistema. A conta Administrador non se pode eliminar nin quitar do grupo Administradores á que pertence, pero pódese cambiar o nome ou deshabilitar. Non se pode borrar pero pódese deshabilitar. Por seguridade é conveniente ter máis dunha conta de administrador.
 - **Convidado**: Xerada no proceso de instalación. É a que utilizan os usuarios que non dispoñen de conta no dominio para poder acceder aos seus recursos. Por seguridade de forma predeterminada está deshabilitada e pódese borrar. É membro do grupo de Invitados.
 - **Usuarios**: No momento que se crea o controlador de dominio no servidor os usuarios locais pasan a ser usuarios do dominio.
 - **De contacto**: Son contas de correo electrónico.
- As contas de usuario xestiónanse dentro do cartafol Users ou dun contedor creado como unidade organizativa da xanela de xestión do domino do Directorio Activo.
- Cada conta de usuario dispón de identificador de seguridade SID, que se crea no momento de dar de alta ao usuario, este número representa ao usuario dentro dos procesos do sistema.

6.3.5.3 Administración de grupos de usuarios en Active Directory de Windows

As contas de grupo utilizámolos para xestionar a administración dos recursos de varios usuarios á vez dentro do directorio activo. Cos grupos podemos formar conxuntos de usuarios que van ter unha administración común, en permisos e recursos compartidos co fin de facilitar a administración de usuarios, e así evitar facelo de forma individual (usuario por usuario).

Ilustración que mostra grupos de usuarios de dominio



Antonio López (Elaboración propia)

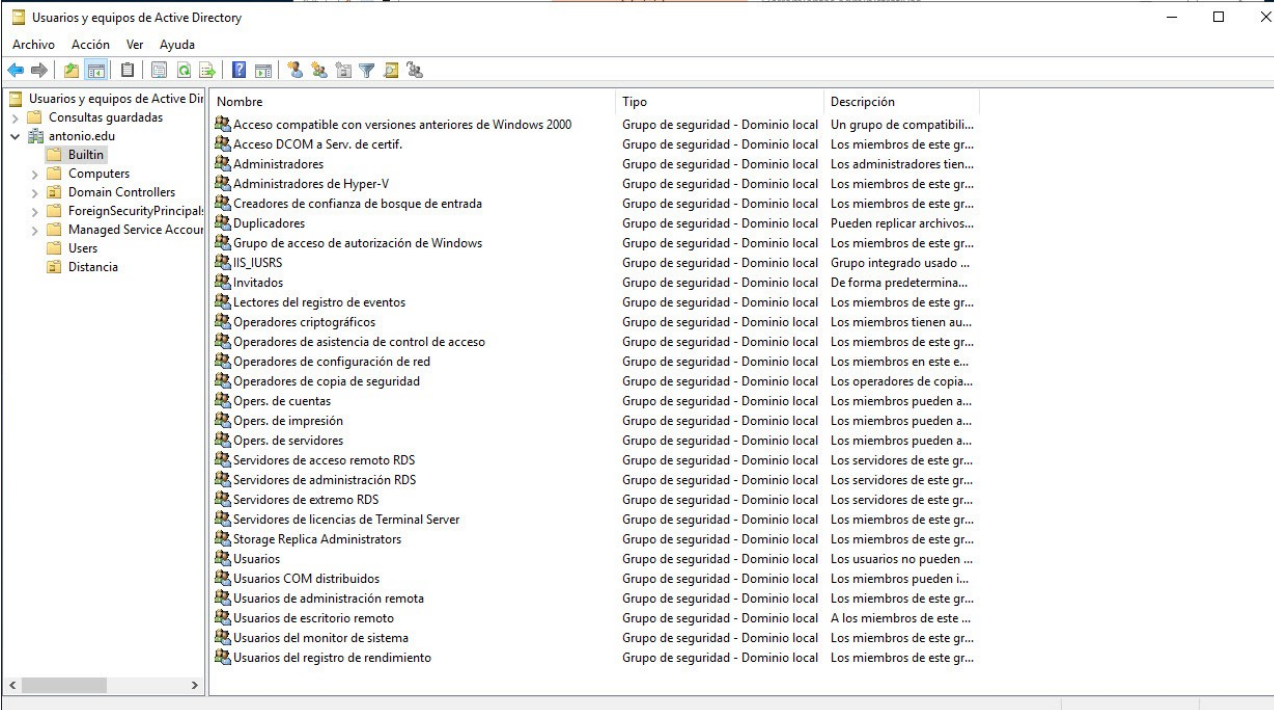
Os grupos de usuarios poden conter a outros grupos producindo unha estrutura xerárquica de anidamento de grupos dentro do directorio. Cando creamos un grupo no AD debemos definirlle dúas características:

Características dos Grupos de usuarios de Active Directory

Tipo de grupo	De seguridad	Se utilizan para asignar usuarios con permisos y derechos sobre los recursos.
	De distribución	Son usuarios sin seguridad con los que se tiene comunicación por correo electrónico.
Ámbito del grupo	Universal	Usuarios, grupos Globales y Universales que incluso pueden pertenecer a otros dominios. Se almacenan en el catálogo global y se replican por toda la red.
	Global	Los usuarios podrán acceder a cualquiera de los dominios del árbol, sus usuarios y grupos Globales deben pertenecer al mismo dominio. No se replica fuera del dominio.
	Local de dominio	Sus miembros acceden a los recursos locales del dominio. Son miembros usuarios, grupos Globales de cualquier dominio, grupos locales del mismo dominio o grupo Universal. Los grupos locales no se pueden procesar en otros dominios.

Desde Inicio-Ferramentas administrativas-Usuarios e equipos de AD, ao seleccionar o cartafol Users ou Builtin temos no panel dereito a lista de usuarios e grupos predefinidos, na columna de Descrición podemos ver a súa funcionalidade e na de Tipo vemos as calidades ámbito e tipo de grupo. Cando se crea o AD, o sistema xera grupos predeterminados con permisos e dereitos predefinidos.

Estes atópanse na consola MMC de Usuarios e grupos do AD dentro do cartafol Users (como grupos globais e universais) e do cartafol Builtin (como grupos de dominio local).



	Nombre	Tipo	Descripción
	Acceso compatible con versiones anteriores de Windows 2000	Grupo de seguridad - Dominio local	Un grupo de compabili...
	Acceso DCOM a Serv. de certif.	Grupo de seguridad - Dominio local	Los miembros de este gr...
	Administradores	Grupo de seguridad - Dominio local	Los administradores tien...
	Administradores de Hyper-V	Grupo de seguridad - Dominio local	Los miembros de este gr...
	Creadores de confianza de bosque de entrada	Grupo de seguridad - Dominio local	Los miembros de este gr...
	Duplicadores	Grupo de seguridad - Dominio local	Pueden replicar archivos...
	Grupo de acceso de autorización de Windows	Grupo de seguridad - Dominio local	Los miembros de este gr...
	IIS_IUSRS	Grupo de seguridad - Dominio local	Grupo integrado usado ...
	Invitados	Grupo de seguridad - Dominio local	De forma predetermina...
	Lectores del registro de eventos	Grupo de seguridad - Dominio local	Los miembros de este gr...
	Operadores criptográficos	Grupo de seguridad - Dominio local	Los miembros tienen au...
	Operadores de asistencia de control de acceso	Grupo de seguridad - Dominio local	Los miembros de este gr...
	Operadores de configuración de red	Grupo de seguridad - Dominio local	Los miembros en este e...
	Operadores de copia de seguridad	Grupo de seguridad - Dominio local	Los operadores de copia...
	Opers. de cuentas	Grupo de seguridad - Dominio local	Los miembros pueden a...
	Opers. de impresión	Grupo de seguridad - Dominio local	Los miembros pueden a...
	Opers. de servidores	Grupo de seguridad - Dominio local	Los miembros pueden a...
	Servidores de acceso remoto RDS	Grupo de seguridad - Dominio local	Los servidores de este gr...
	Servidores de administración RDS	Grupo de seguridad - Dominio local	Los servidores de este gr...
	Servidores de extremo RDS	Grupo de seguridad - Dominio local	Los servidores de este gr...
	Servidores de licencias de Terminal Server	Grupo de seguridad - Dominio local	Los miembros de este gr...
	Storage Replica Administrators	Grupo de seguridad - Dominio local	Los miembros de este gr...
	Usuarios	Grupo de seguridad - Dominio local	Los usuarios no pueden ...
	Usuarios COM distribuidos	Grupo de seguridad - Dominio local	Los miembros pueden i...
	Usuarios de administración remota	Grupo de seguridad - Dominio local	Los miembros de este gr...
	Usuarios de escritorio remoto	Grupo de seguridad - Dominio local	A los miembros de este ...
	Usuarios del monitor de sistema	Grupo de seguridad - Dominio local	Los miembros de este gr...
	Usuarios del registro de rendimiento	Grupo de seguridad - Dominio local	Los miembros de este gr...

6.3.5.4 Administración de contas de equipos de Active Directory de Windows

Ilustración que mostra unha estrutura dun dominio e unha serie de terminais



isoalial (Elaboración propia)

Pódense xestionar contas dos equipos da rede que pertencen ao dominio, co fin de controlar o acceso e os recursos da rede. Poden estar almacenadas en calquera unidade organizativa como pode ser Computers, (creada polo sistema de forma predeterminada) onde se almacenan todas as contas dos equipos, menos as dos equipos que son controladores de dominio, que se gardan no contedor Domain Controllers.

Cando unha conta dun equipo esta creada no Directorio Activo, desde o propio servidor que actúa de controlador de dominio, podemos administrar remotamente o equipo. O controlador de dominio almacena o nome do equipo e un identificador único dentro do sistema.

É recomendable tentar que a maioría dos equipos clientes dispoñan dun sistema operativo e de hardware homoxéneo, para facilitar a administración dos mesmos, por exemplo mediante a creación de imaxes do sistema.

É importante lembrar, que para realizar calquera operación de administración o usuario debe dispoñer dos permisos e dereitos necesarios, é dicir, debe pertencer a algún grupo de administradores.

6.3.6 Introducción á configuración do sistema operativo Windows Server

6.3.6.1 Empregando cmdlets

Un cmdlet é un comando lixeiro que se usa na contorna PowerShell.

Os cmdlets realizan unha acción e adoitan devolver un obxecto de Microsoft .NET ao comando seguinte na canalización. Un cmdlet é un único comando que participa na semántica de canalización de PowerShell.

6.3.6.1.1 Variables en PowerShell

```
$NomeVariable=valor
```

```
$NomeEquipo="DAM Server"
```

6.3.6.1.2 Cambiar o nome de equipo

```
Rename-Computer -NewName $NomeEquipo -Restart -Force
```

6.3.6.2 Utilizando utilidades específicas

6.3.6.2.1 Crear recurso compartido

Perfiles\$

```
net share perfiles$=W:\perfiles /grant:"Todos,Full" /Cache:None
```

6.3.6.2.2 Permisos de acceso NTFS a carpetas

W:\usuarios

(directorios onde se gardarán as carpetas persoais dos usuarios, só terán que ter permisos de Administrador — Control Total.)

W:\usuarios\alumnos

(Neste directorio, e todos os subdirectorios, os usuarios do grupo G-Profesores terán permisos de Lectura e Execución)

```
icacls W:\usuarios /inheritance:r /grant "Administrador:(OI)(CI)F" /T
icacls W:\usuarios\alumnos /inheritance:d /grant "G-Profesores:(OI)(CI)RX"
icacls W:\usuarios /T
```

6.3.6.2.3 Crear Unidades Organizativas (OU)

```
dsadd ou "ou=IESLOSADA,dc=ies,dc=local"
dsadd ou "ou=usuarios,ou=IESLOSADA,dc=ies,dc=local"
dsadd ou "ou=profesores,ou=usuarios,ou=IESLOSADA,dc=ies,dc=local"
```

6.3.6.2.4 Crear grupos globais de seguridade

```
dsadd group "cn=G-Usuarios,ou=usuarios,ou=IESLOSADA,dc=IES,dc=local" -scope g
dsadd group "cn=G-Profesores,ou=profesores,ou=usuarios,ou=IESLOSADA,dc=IES,dc=local"
        -memberof "cn=G-Usuarios,ou=usuarios,ou=IESLOSADA,dc=IES,dc=local" -
scope g
```

6.3.6.2.5 Engadir usuario

```
dsadd user "cn=profel,ou=profesores,ou=usuarios,ou=ieslosada,dc=ies,dc=local" `
        -samid profel -upn profel@ies.local -display Profel -desc "Profesor de
IES" `
        -pwd abc123.. -mustchpwd yes `
        -hmdrv W: -hmdir \\Server\usuarios$\profesores\profel `
        -profile \\Server\perfiles$\profel
```


- samid: Specifies the Security Accounts Manager (SAM) name as the unique SAM account name for this user, for example, Linda. If you do not specify the SAM name, dsadd attempts to create the SAM account name by using up to the first 20 characters from the common name (CN) value of UserDN.
- upn: Specifies the user principal name of the user that you want to add, for example, Linda@widgets.contoso.com.
- display: Specifies the display name of the user that you want to add.
- desc: Specifies the description of the user that you want to add.
- pwd: Specifies that the password for the user be set to Password or an asterisk (*). If you set the password to *, dsadd prompts you for a user password.
- mustchpwd: Specifies whether users must change their passwords when they next log on. The available values are yes and no. By default, users do not have to change their passwords (no).
- hmdrv: Specifies the home directory drive letter (for example, E:) of the user that you want to add.
- hmdir: Specifies the home directory location of the user that you want to add.
- Profile: Specifies the profile path of the user that you want to add.

6.3.6.2.6 Engadir usuario a grupo

```
dsmod                                group                                "cn=G-
Profesores,ou=profesores,ou=usuarios,ou=IESLOSADA,dc=IES,dc=local"
-addmbr "cn=profel,ou=profesores,ou=usuarios,ou=ieslosada,dc=ies,dc=local"
```

6.3.6.2.7 Borrar elementos

```
dsrm "ou=profesores,ou=usuarios,ou=IESLOSADA,dc=ies,dc=local"
```