

ADMINISTRACIÓN DE SERVICIOS DE DIRECTORIO

Raúl Arribas Redondo

Administración de Sistemas
Operativos

26/10/2024

Contenido

1	ACTIVE DIRECTORY	3
1.1	Instalar funcionalidad del Servidor AD	3
1.1.1	Promover el servidor como Controlador de dominio	4
1.2	Instalar los servicios necesarios en el dominio Windows para que los equipos con sistema operativo Windows se agreguen como clientes del dominio.	5
1.2.1	Primero comprobamos que Active Directory está activo.....	5
1.2.2	Configurar la política de red para los equipos clientes	6
1.2.3	Agregar un equipo al dominio	7
1.3	Configuración del servidor DNS local	9
2	OBJETOS DE AD EN WINDOWS SERVER	11
2.1	Crear unidades organizativas	11
2.1.1	Crear Usuarios	11
2.2	Crear una GPO para Impedir la Instalación de Aplicaciones en UO FCT	12
2.3	GPO para Deshabilitar Dispositivos USB en UO MKT	14
2.4	GPO para Redirigir Carpetas (Documentos y Escritorio)	15
2.5	Política de Contraseñas para Exigir Requisitos de Complejidad y Longitud Mínima de 9 Caracteres.....	20
2.6	Investigar Otras Dos GPOs Adicionales para Establecer Políticas en Clientes del Dominio.....	22
2.6.1	Limitar el acceso a los paneles de control y configuración del sistema:	22
2.6.2	Política de actualizaciones automáticas	23
3	INSTALAR UBUNTU SERVER CON OPENLDAP	24
3.1	Instalación LDAP	25
3.2	Instalar los servicios necesarios para que los equipos con sistema op Ubuntu se agreguen como clientes del dominio	36
3.3	Instalación de FreeIPA	40
4	OBJETOS DE OPENLDAP Y FREEIPA.....	41
4.1	Generar dos Unidades Organizativas distintas con un usuario cada una	41
4.1.1	Creamos la OU.....	41
4.1.2	Crear usuarios dentro de la UO.....	41
4.2	Crear Políticas.....	43
5	VIRTUALIZACIÓN EN LA NUBE Y CONCLUSIONES.....	43
5.1	Crear una maquina virtual en Azure	43
5.2	Comparativa de los servicios en la nube mas conocidos	52

1 ACTIVE DIRECTORY

En este apartado, configuraremos un Directorio con Windows Server 2019 (o cualquier versión a partir de WS 2012) [Windows Server 2019 | Microsoft Evaluation Center](https://www.microsoft.com/evalcenter/evaluate-windows-server-2019-evaluation) y conectaremos un cliente con Windows10 al servidor.

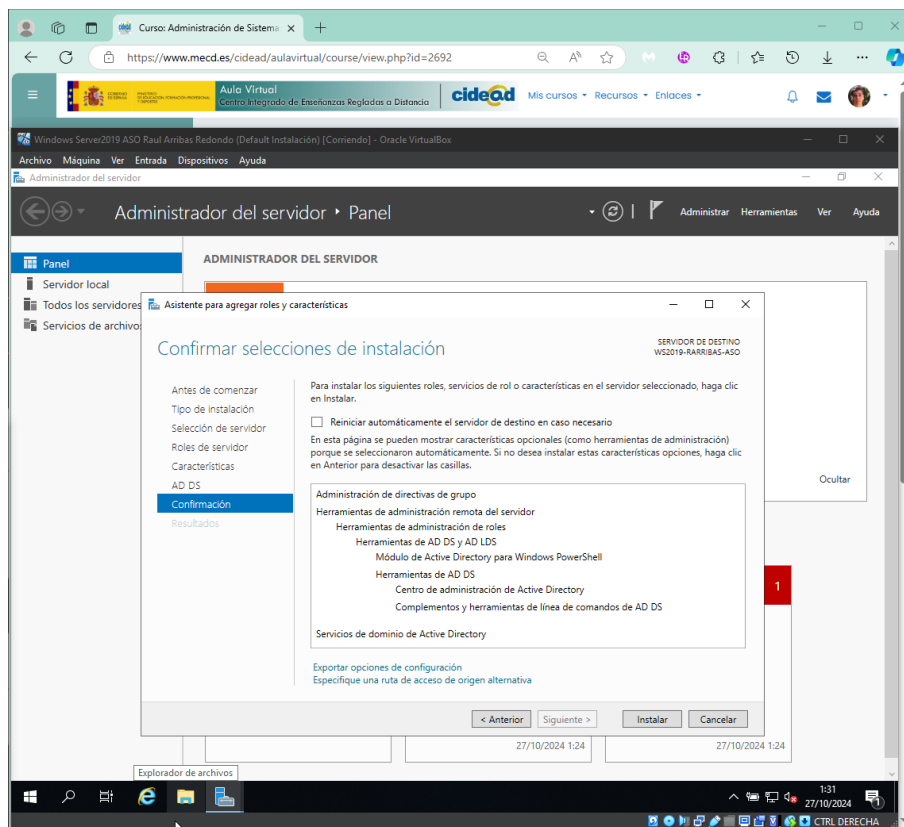
Primero nos crearemos la maquina virtual con Windows Server 2019, vamos a trabajar desde Virtual box. Una vez tenemos instalado Windows Server 2019 vamos a cambiar el nombre del servidor por uno nuestro: **WS2019-RARRIBAS-ASO**, seguimos los pasos siguientes para instalar Active directory (AD).

1.1 Instalar funcionalidad del Servidor AD

En primer lugar vamos a instalar el servidor AD, para ello nos vamos a:

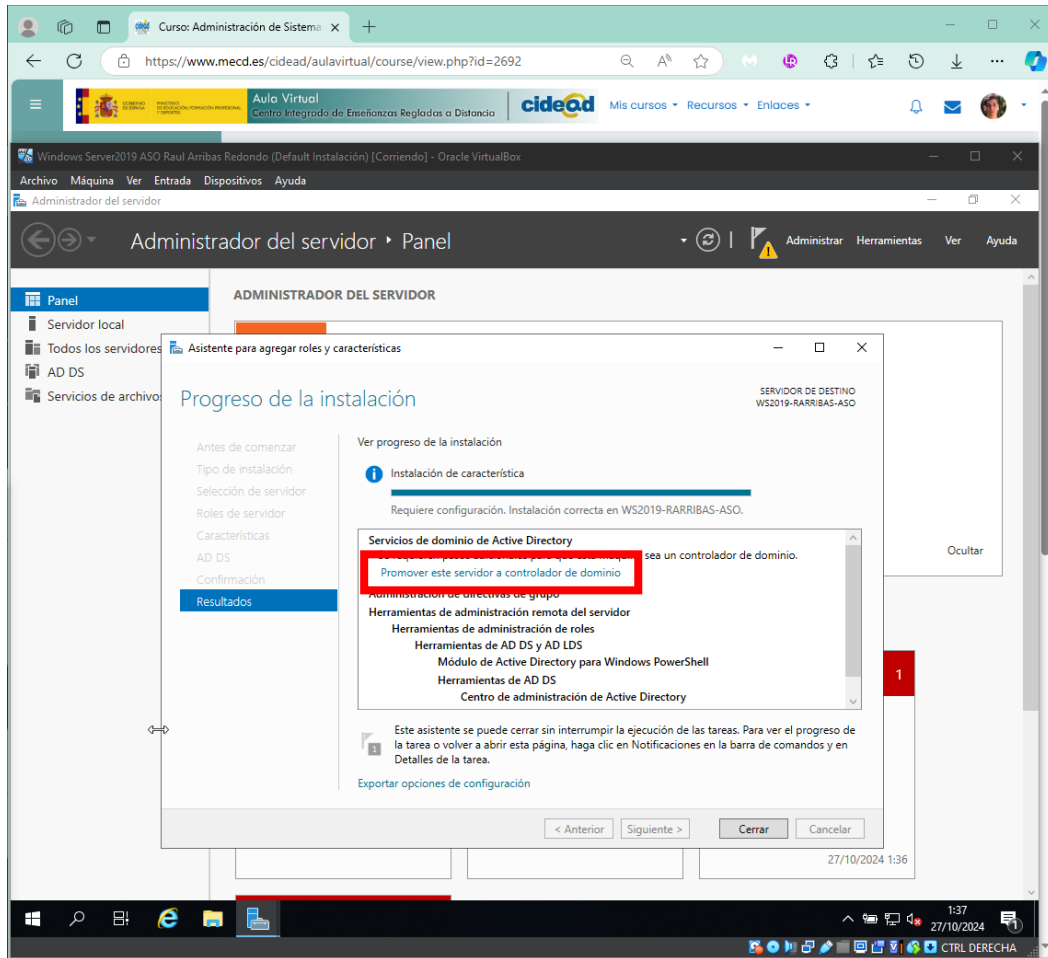
Administrador del Servidor → Agregar roles y características

- **Seleccionar tipo de instalación:** *Instalación basada en características o roles.*
- **Selección de servidor de destino:** Seleccionar *un servidor del grupo de servidores*, seleccionamos nuestro equipo que en este caso solo no aparecerá nuestro servidor **WS2019-RARRIBAS-ASO**
- **Seleccionar roles de servidor:** Marcamos la opción *Servicios de dominio de Active Directory*, se agregarán características requeridas, hacemos click en agregar características.
- **Seleccionar características:** Lo dejamos como está por default.
- **Servicios de dominio de AD:** Le damos siguiente .
- **Confirmar selecciones de instalación:** Confirmamos lo que se va a instalar.

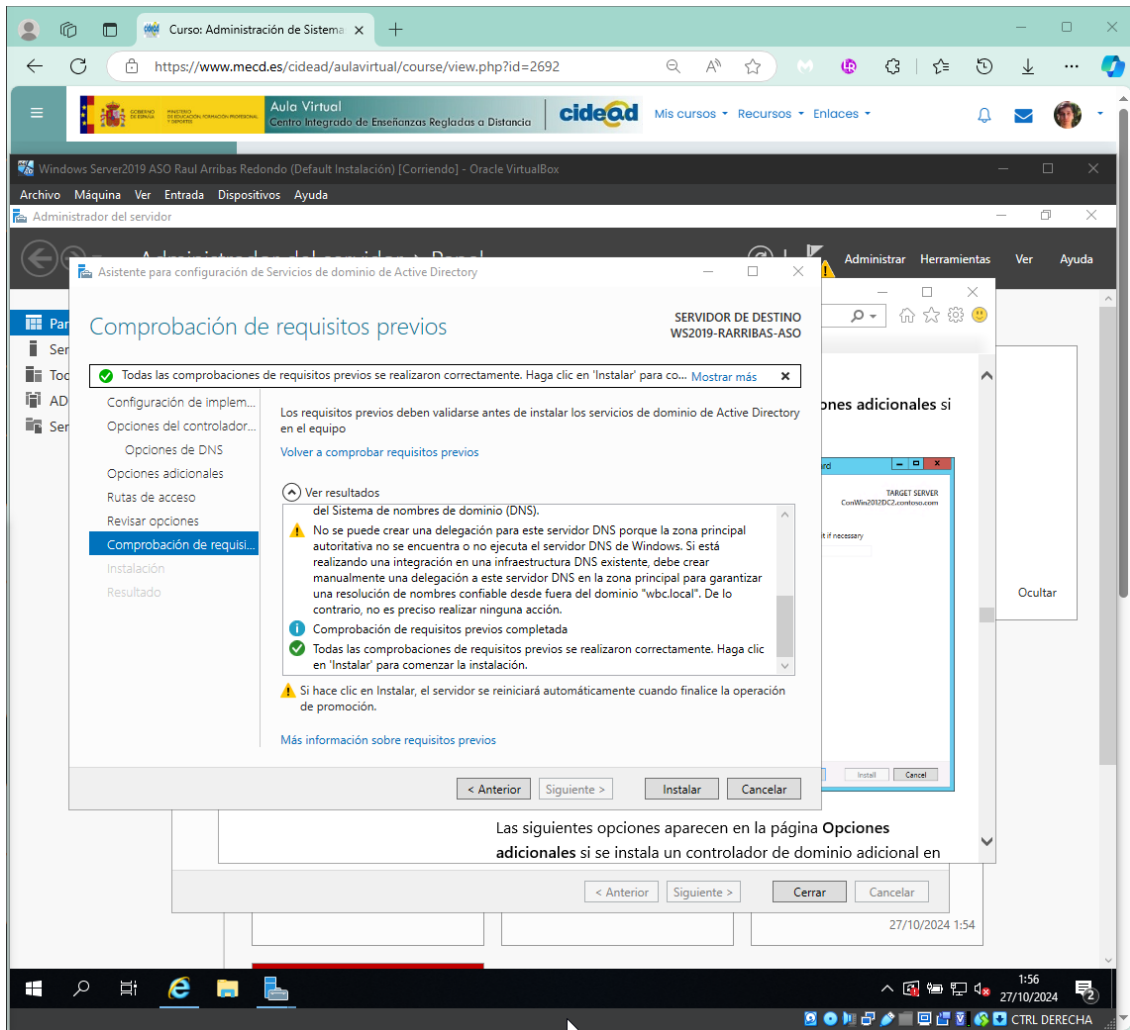


1.1.1 Promover el servidor como Controlador de dominio

Una vez terminada la instalación le damos a ***promover este servidor a controlador de dominio***



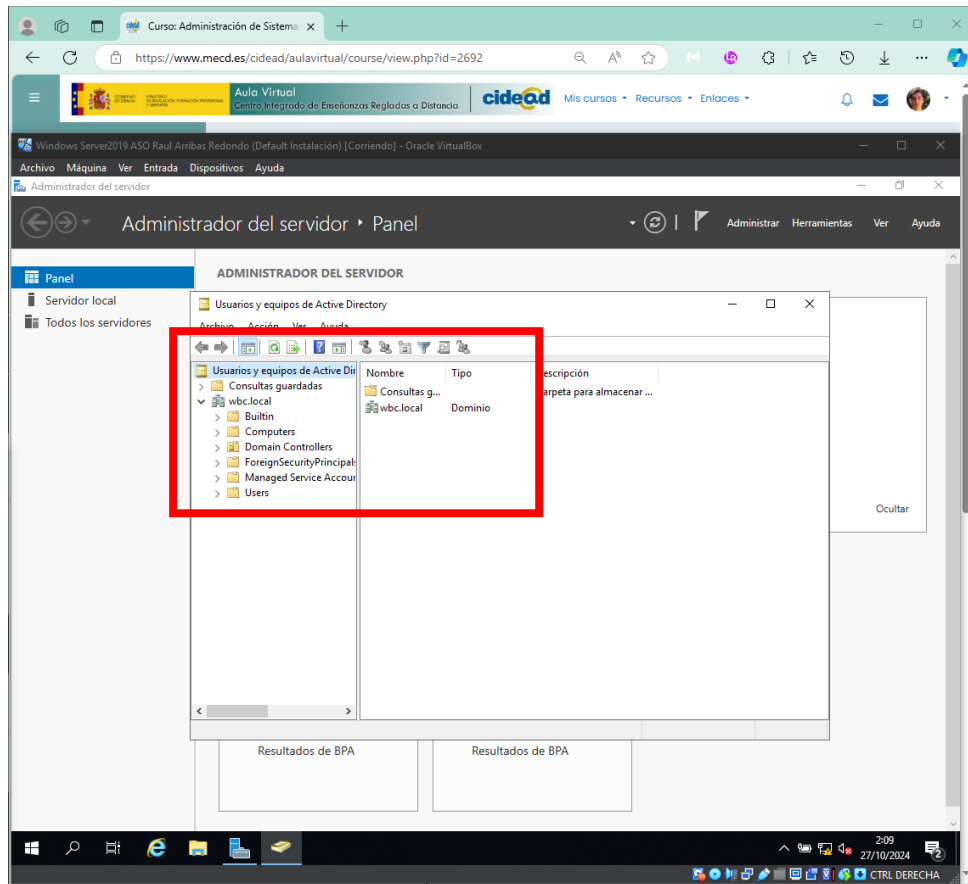
- **Configuración de implementación:**
 - **Agregar un nuevo bosque:** Ponemos el nombre **wbc.local**
 - **Opciones del controlador de dominio:** Seleccionamos la versión Windows Server 2016, marcamos la opción de **DNS Y GC** y ponemos una contraseña de restauración.
 - **Opciones de DNS:** Lo dejamos por default (no nos dejará aún)
 - **Opciones adicionales:** Nombre del dominio NetBIOS: WBC
 - **Rutas de acceso:** Lo dejamos por defecto, es donde se creará la base de datos de AD DS, archivos de registro y SYSVOL.
 - **Revisar opciones:** Revisamos las opciones que hemos puesto anteriormente.
 - **Comprobación de requisitos previos:** Comprobamos los requisitos y si todo esta ok nos debería de salir un mensaje de OK, le damos a instalar y cuando termine reiniciamos el servidor.



1.2 Instalar los servicios necesarios en el dominio Windows para que los equipos con sistema operativo Windows se agreguen como clientes del dominio.

1.2.1 Primero comprobamos que Active Directory está activo

Administrador del servidor → Herramientas → Usuarios y equipos de Active Directory y nos tiene que aparecer el dominio wbc.local

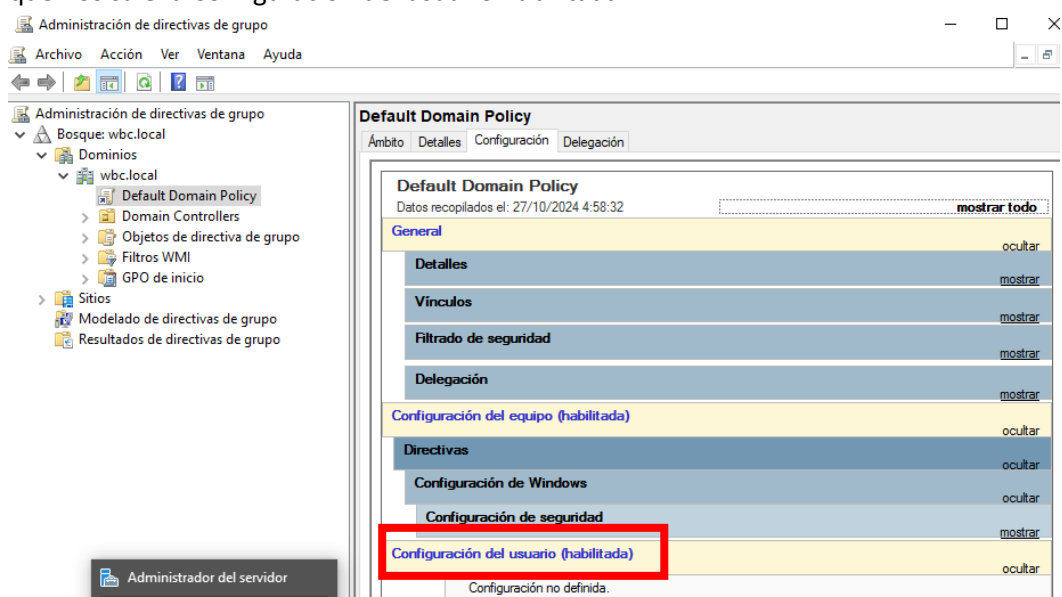


1.2.2 Configurar la política de red para los equipos clientes

Vamos a comprobar que los equipos con Windows se puedan unir a nuestro dominio.

Herramientas → Administración de directivas de grupo y verificamos cuales son los permisos necesarios:

- **Bosque → Dominios → wbc.local → Default Domain Policy → Configuración** veremos que nos sale la Configuración del usuario habilitada.

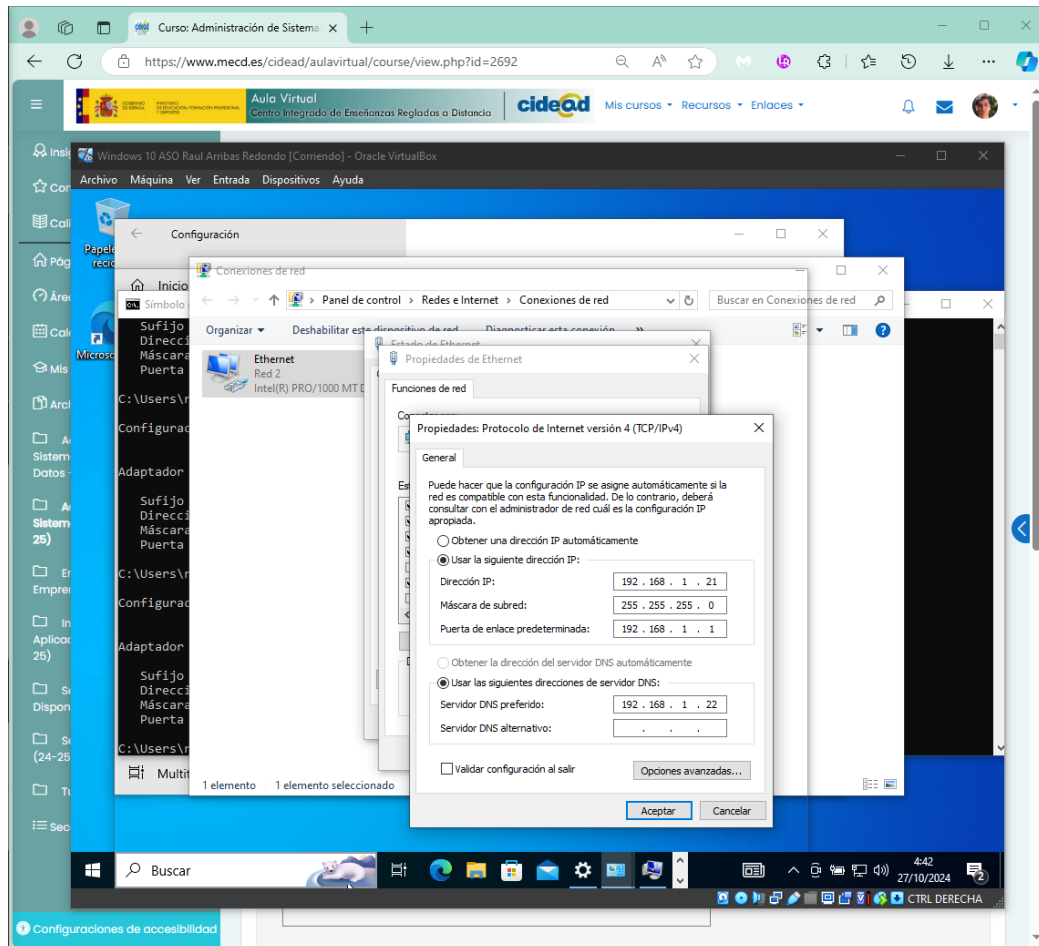


1.2.3 Agregar un equipo al dominio

Nos abrimos una nueva máquina virtual con sistema operativo Windows 10 y lo agregamos al dominio.

Cliente windows10:

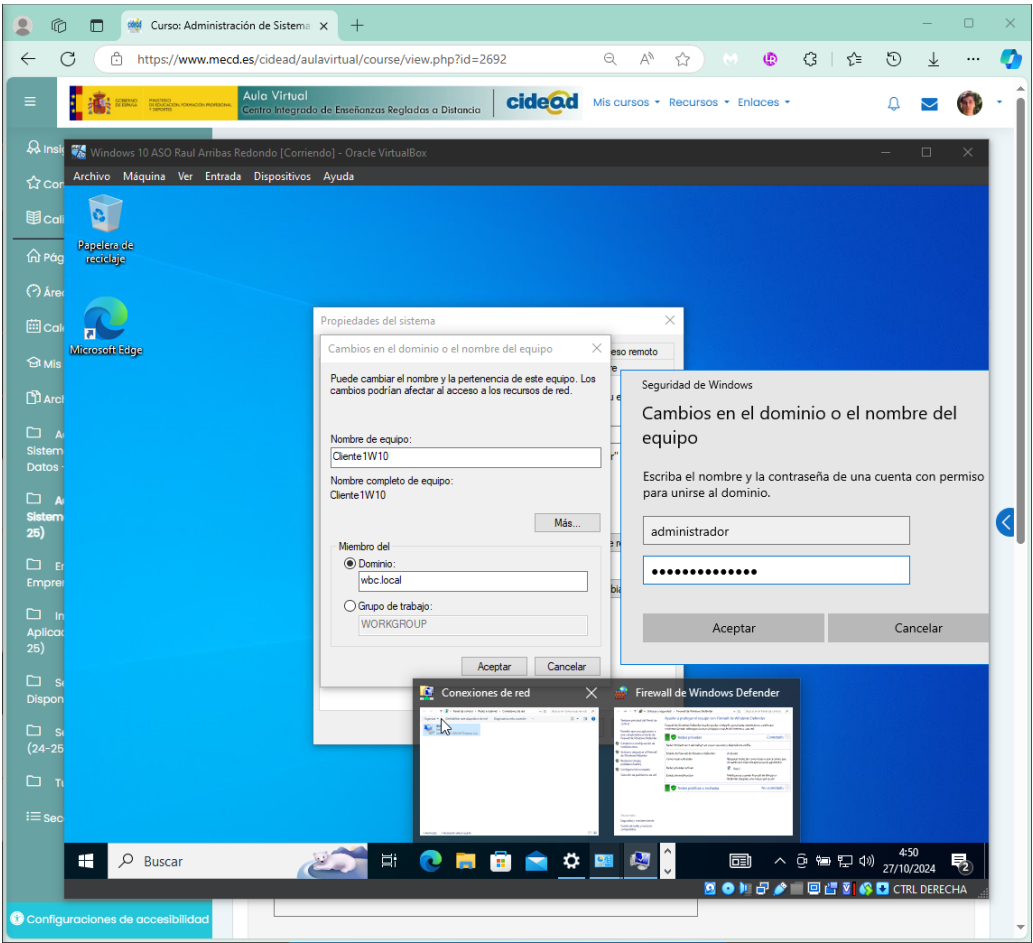
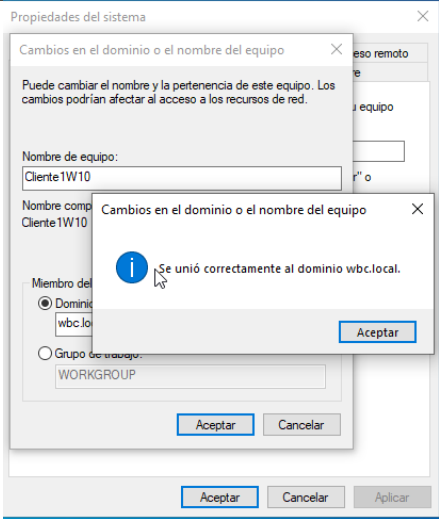
Primero configuramos la dirección Ip para que tenga la Ip del servidor DNS del servidor como en la imagen. (IP DEL SERVIDOR WINDOWS SERVER 192.168.1.22)



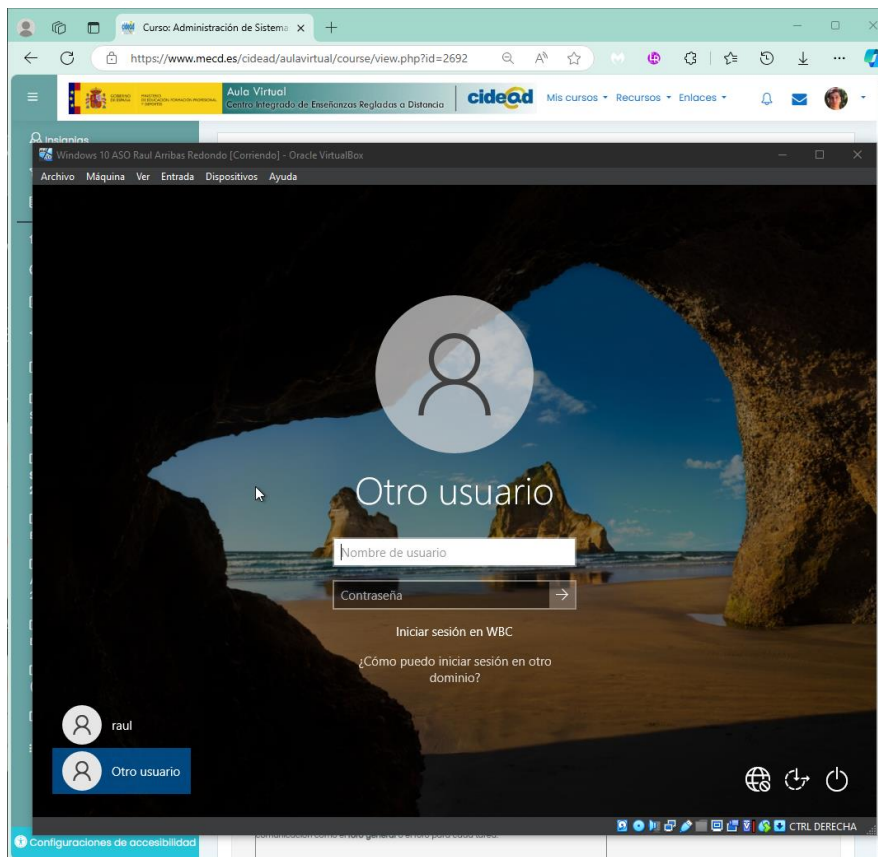
Ahora lo agregamos al dominio:

Acerca de tu PC → Cambiar el nombre de este equipo (avanzado) y seleccionamos la opción cambiar dominio o grupo de trabajo.

Cambiamos el nombre del cliente si queremos y en Dominio ponemos **wbc.local**, cuando nos unamos tenemos que reiniciar el equipo para que se apliquen los cambios.



Comprobamos que el cliente puede entrar con un usuario del dominio:



1.3 Configuración del servidor DNS local

****IMPORTANTE** EL SERVIDOR DE DNS YA SE NOS HA INSTALADO ANTES CON LA INSTALACIÓN DE AD DS**

Pero por si nos dio algún error y no lo tenemos instalado vemos cómo hacerlo. Vamos a instalar el servidor DNS para mejorar la resolución interna de nombres en el dominio wbc.local

Administrar → Agregar roles y características

- **Seleccionar tipo de instalación:** *Instalación basada en características o roles.*
- **Selección de servidor de destino:** Seleccionar *un servidor del grupo de servidores*, seleccionamos nuestro equipo que en este caso solo no aparecerá nuestro servidor **WS2019-RARRIBAS-ASO**
- **Seleccionar roles de servidor:** *Servidor DNS*
- **Todos los demás pasos son por defecto y le damos a Instalar.**

Una vez tengamos el servidor de DNS instalado nos vamos a:

Herramientas → DNS → WS2019-RARRIBAS → Zonas de búsqueda directa y creamos una nueva zona primaria con el nombre wbc.local (click derecho y zona nueva...)

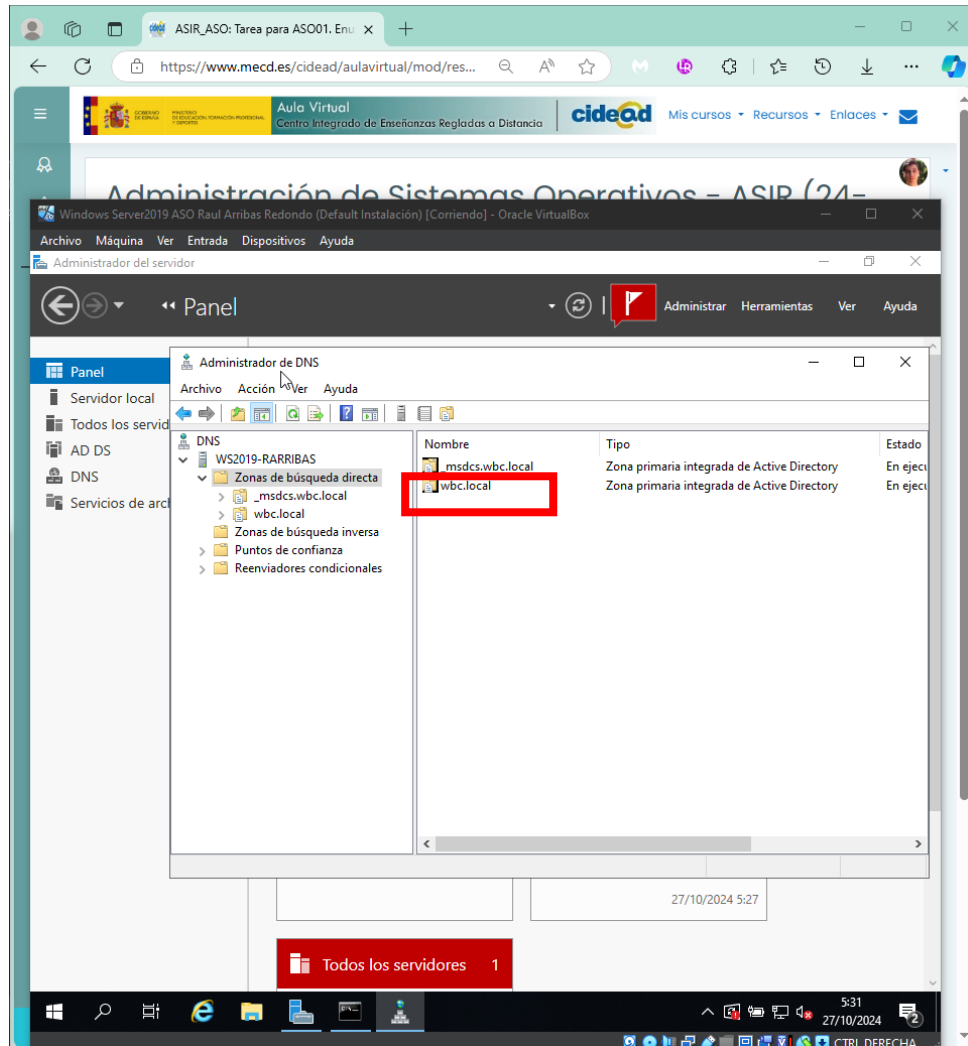
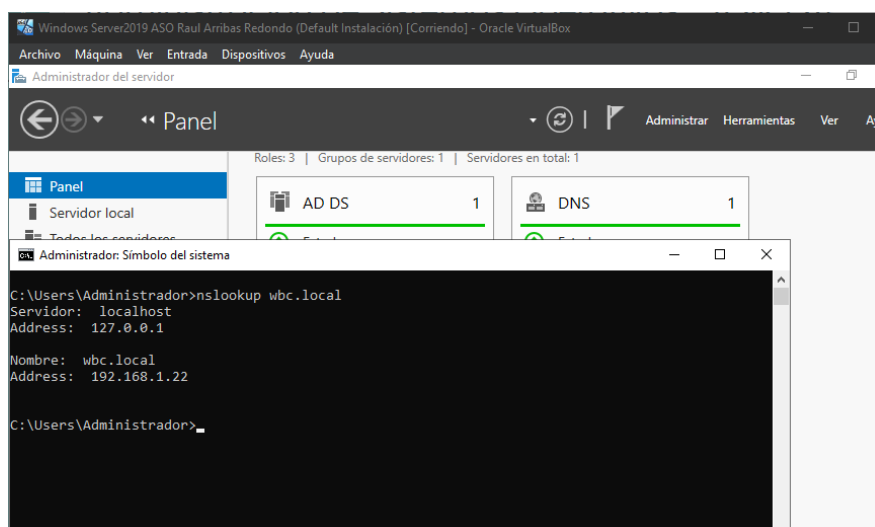
Seleccionamos Tipo de Zona:

- **Zona Principal**

ADMINISTRACIÓN DE SERVICIOS DE DIRECTORIO

- **Para todos los servidores DNS que se ejecutan en controladores de dominio en este dominio: wbc.local**
- **Nombre de zona: wbc.local**

Nos tiene que quedar así:



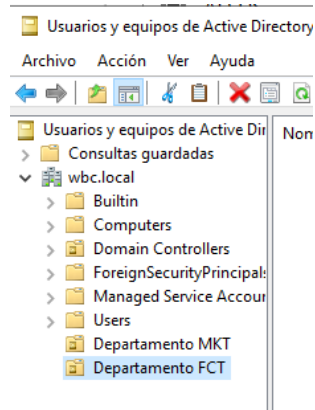
2 OBJETOS DE AD EN WINDOWS SERVER

2.1 Crear unidades organizativas

Administrador del servidor → Herramientas → Usuarios y equipos de Active Directory

Click derecho en el nombre de dominio wbc.local → Nuevo → Unidad Organizativa

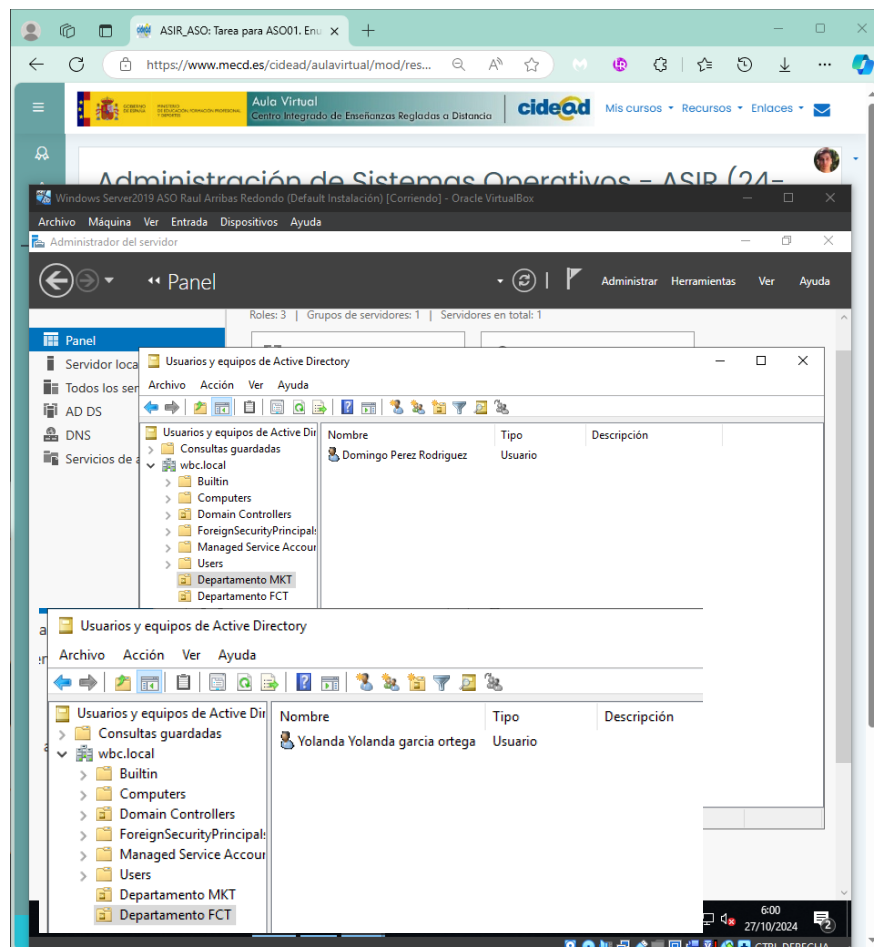
- Creamos el departamento MKT Y FCT



2.1.1 Crear Usuarios

Ahora vamos a crear 1 usuario para cada una de las UO que hemos creado previamente.

Click derecho en las UO nuevas, **Nuevo → Usuario**



2.2 Crear una GPO para Impedir la Instalación de Aplicaciones en UO FCT

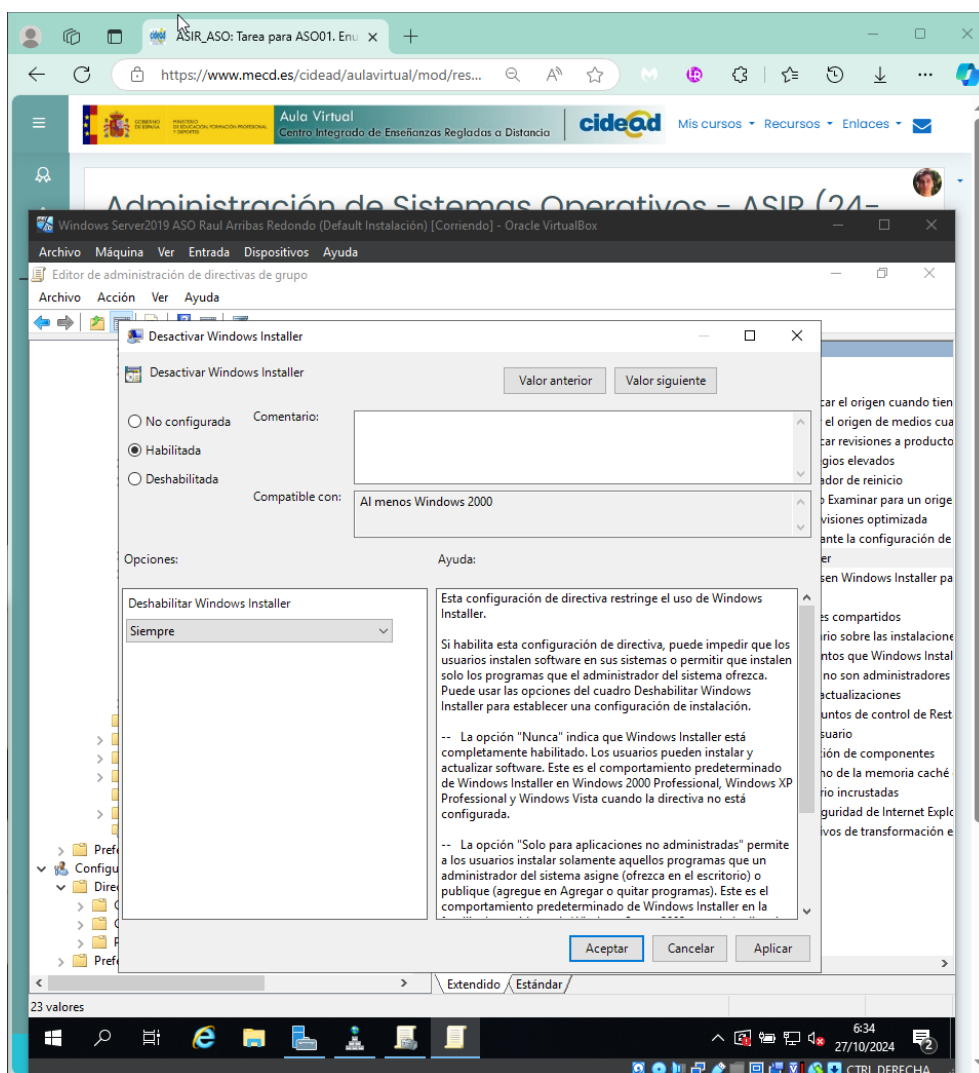
Vamos a crear una GPO en la UO de FCT para que no pueda instalar aplicaciones, para ello nos vamos a:

Herramientas → Administración de directivas de grupo → Bosque → Dominios → wbc.local → Departamento FCT

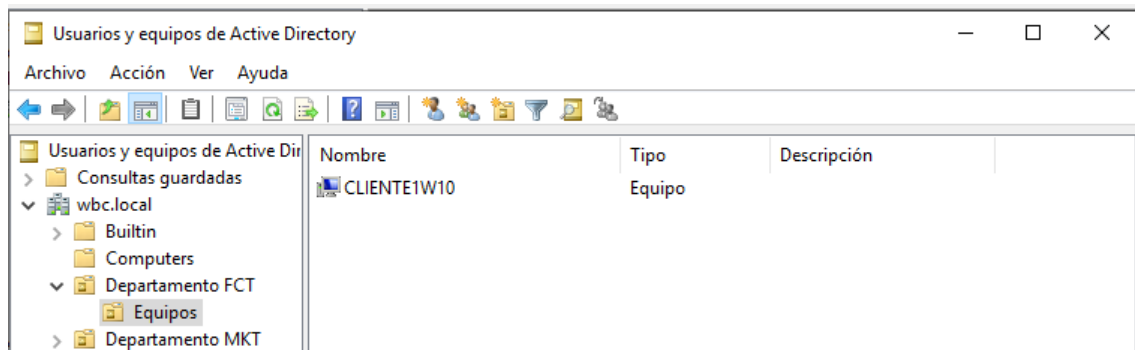
Damos click derecho en la UO Departamento FCT y **Crear un GPO en este dominio y vincularlo aquí.**

Una vez creada la GPO hacemos doble click y nos vamos a **Configuración del Usuario**, hacemos click derecho y Edición...

Configuración del equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Windows Installer → Desactivar Windows Installer

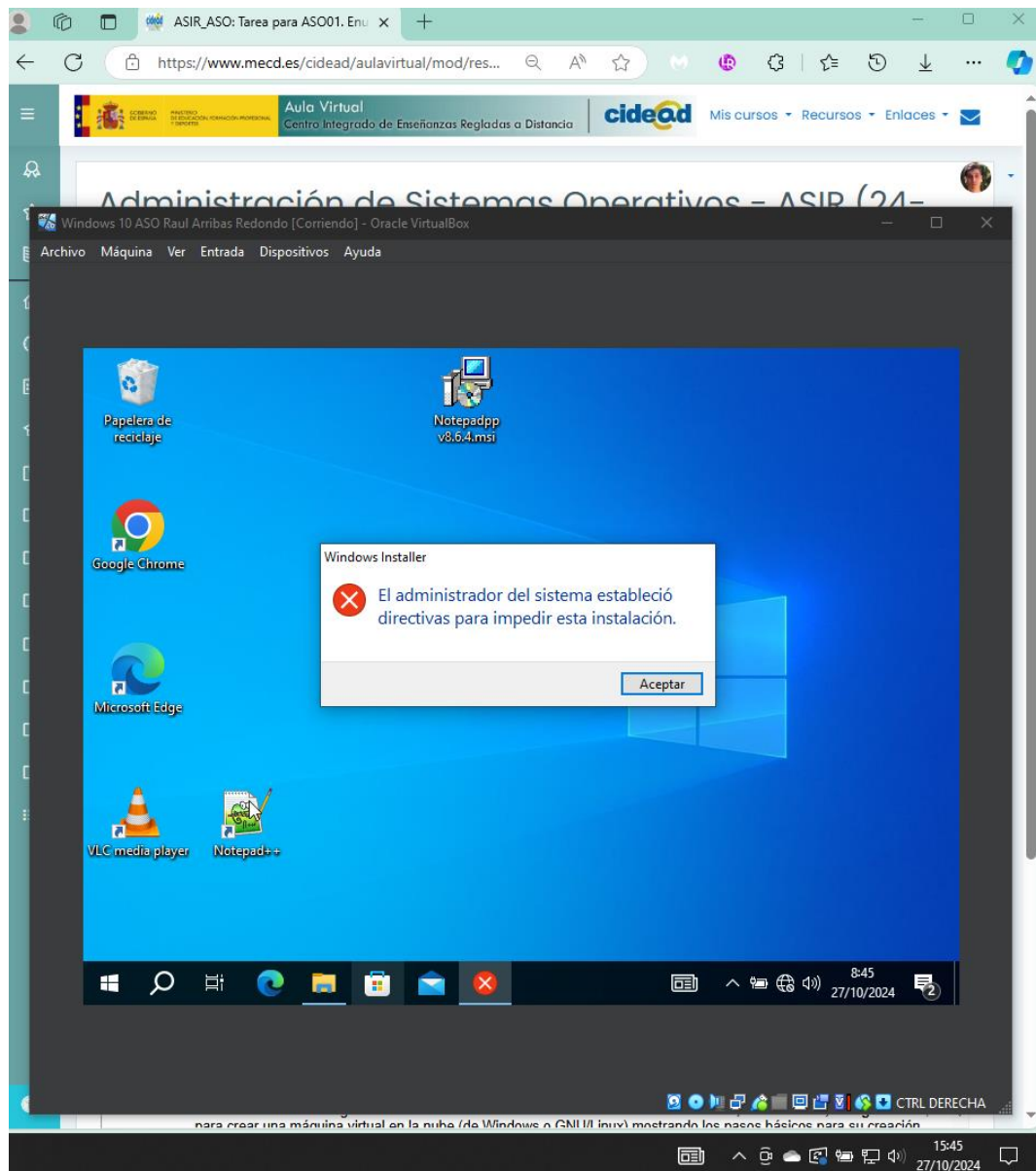


Antes de seguir tenemos que crear una nueva **UO** que se llame **“Equipos”** y dentro metemos el equipo con el que hemos iniciado sesión del departamento FCT:



Aplicamos un **gpupdate /force** para que se aplique la directiva nueva que hemos creado.

Ahora vamos a comprobar que el usuario de FCT no puede ejecutar software:



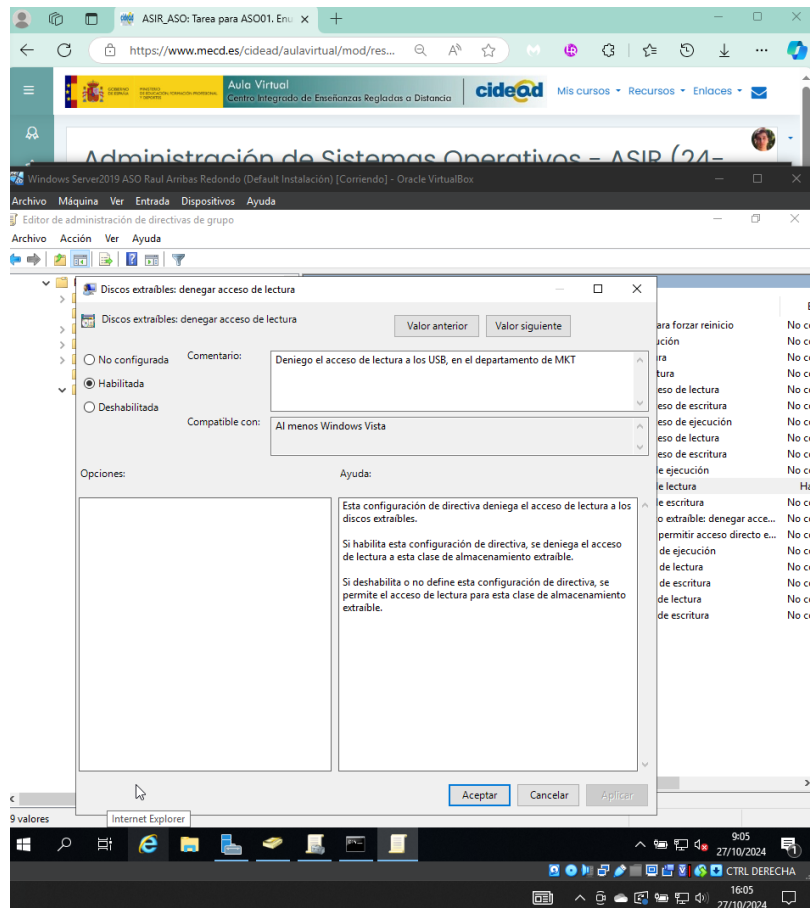
2.3 GPO para Deshabilitar Dispositivos USB en UO MKT

Para deshabilitar los dispositivos USB nos vamos a:

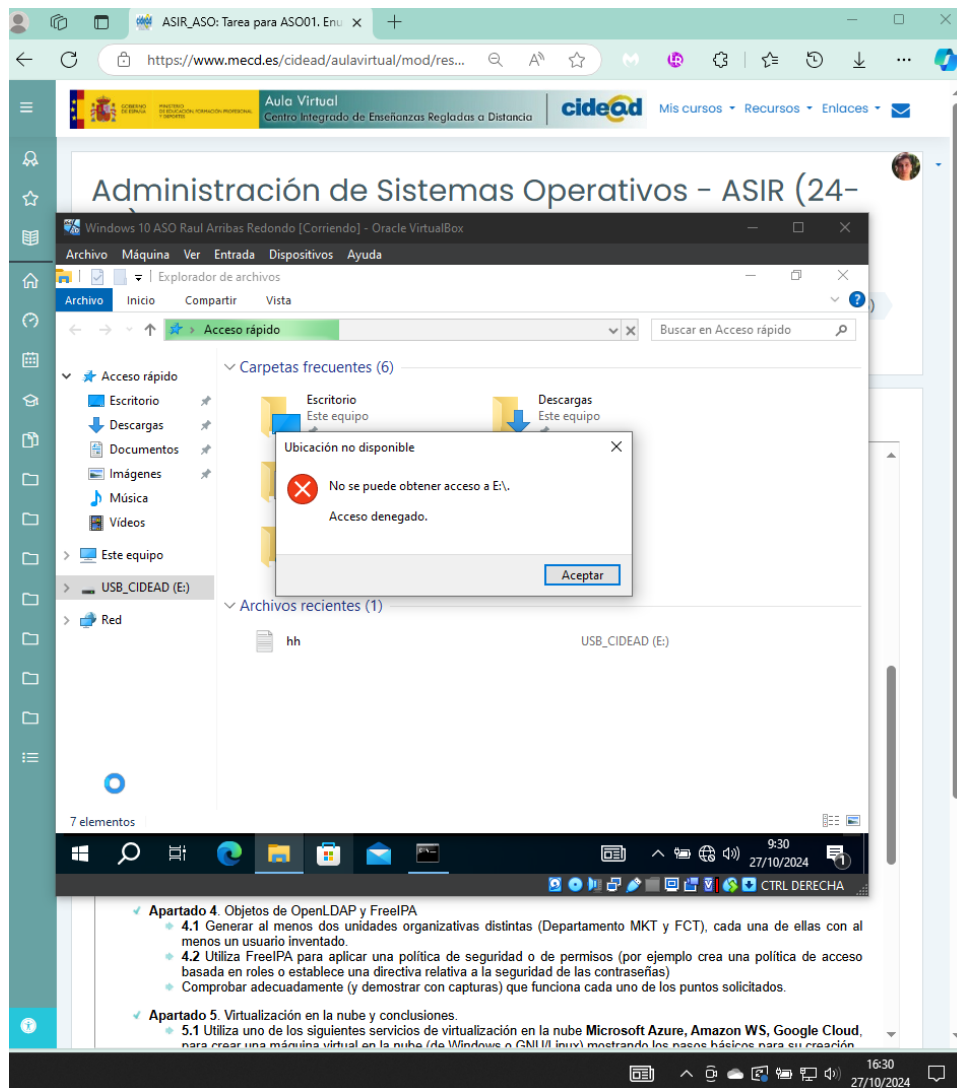
Administración de directivas de grupo → Departamento MKT → Crear un GPO en este dominio y vincularlo aquí

Una vez lo tengamos creado entramos dentro de el y le damos a **configuración**, pinchamos click derecho en configuración del equipo y **Edición...**

Directivas → Plantillas Administrativas → Sistema → Acceso de almacenamiento extraíble → Discos Extraíbles denegar acceso de lectura



Hacemos gpupdate /force y probamos en el usuario de MKT:



2.4 GPO para Redirigir Carpetas (Documentos y Escritorio)

Vamos a crear una GPO para que cada usuario que se conecte vea las carpetas de Documentos y Escritorio de los usuarios conectados.

Herramientas → Administración de directivas de grupo

Hacemos click derecho en el dominio **wbc.local** y seleccionamos **Crear una GPO en este dominio y vincularlo aquí...**

Cuando la tengamos creada damos click derecho en la Configuración del equipo y **Editar...**

Configuración de usuario → Directivas → Configuración de Windows → Redirección de carpetas

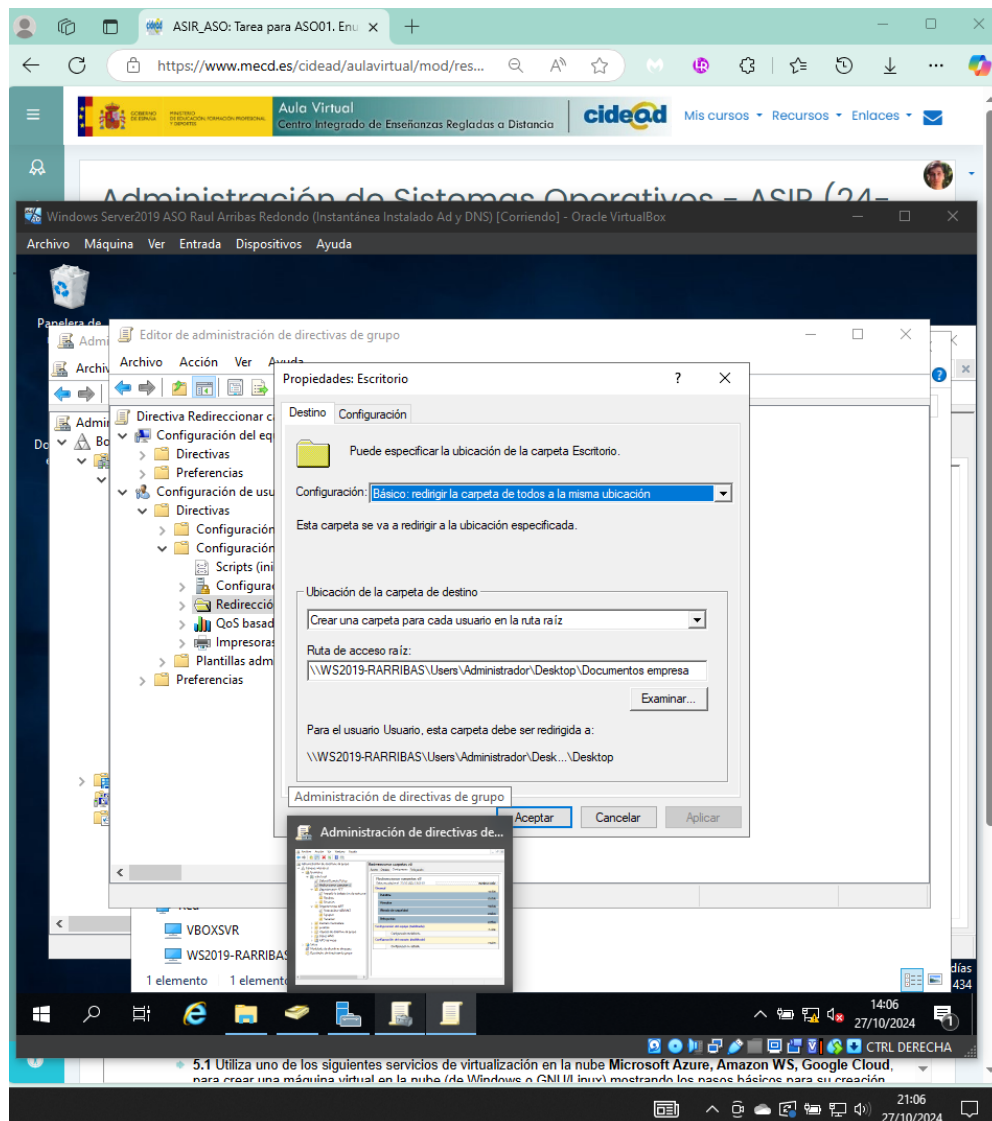
- Redirección de Escritorio:

Primero creamos una carpeta en **c:\users\Administrador\Desktop\Documentos empresa** y la compartimos, click derecho **Conceder acceso a...** → **Usuarios Específicos**

Agregamos: **Usuarios del Dominio** y le ponemos permisos de lectura y escritura.

Volvemos al editor de administración de directivas de grupo en la redirección de carpetas de antes

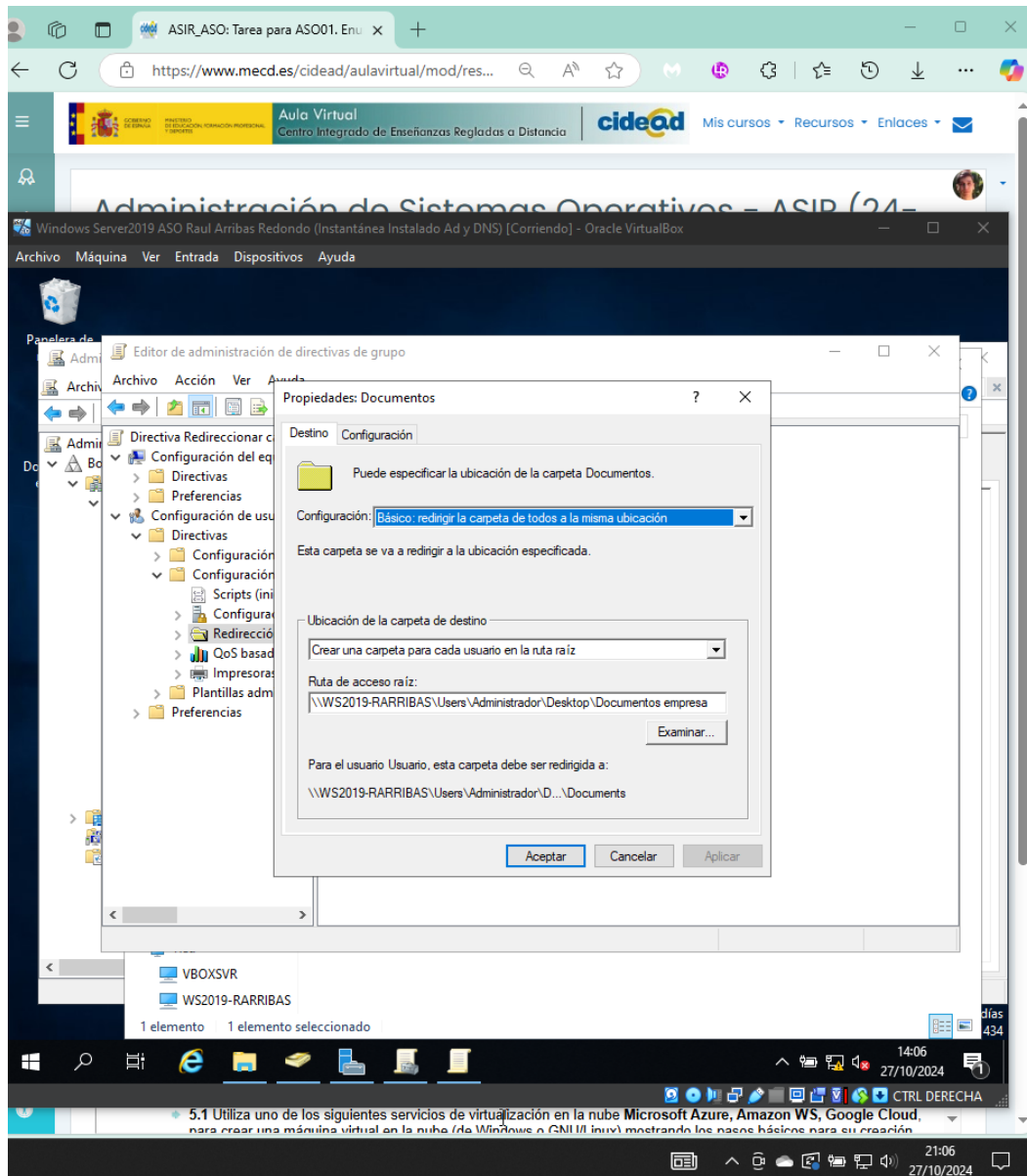
- Click derecho en **Escritorio** → **Propiedades**
 - Básico: **redirigir la carpeta de todos a la misma ubicación**
 - Ubicación de la carpeta de destino: **Crear una carpeta para cada usuario en la ruta raíz**
 - Ruta de acceso Raíz: **\\WS2019-RARRIBAS\users\administrador\Desktop\Documentos empresa**



- Redirección de Documentos

Click derecho en Documentos desde la redirección de carpetas y hacemos los mismos pasos que en la del Escritorio, pero poniendo la siguiente ruta en las propiedades de Documentos.

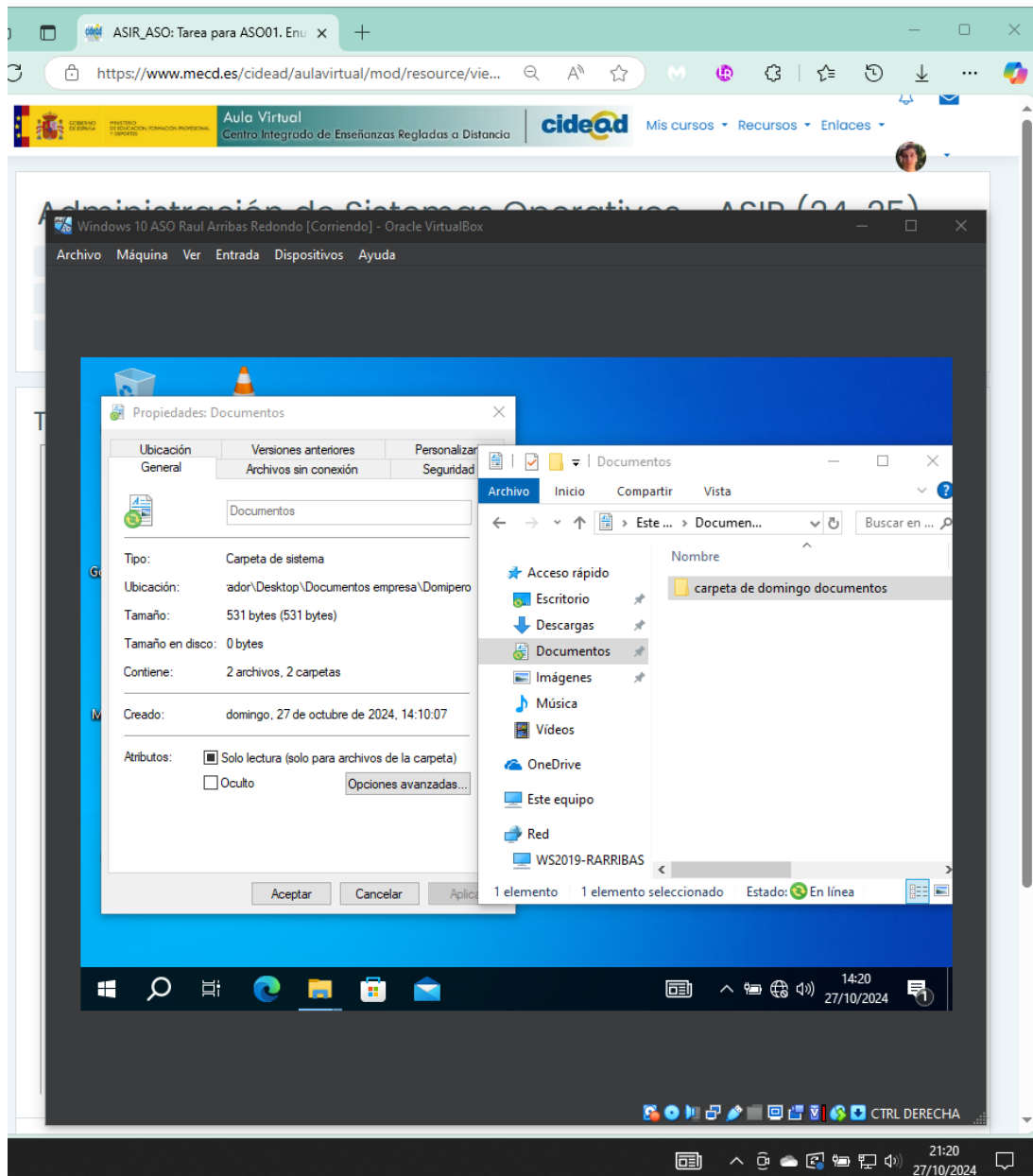
\\WS2019-RARRIBAS\users\administrador\Desktop\Documentos empresa



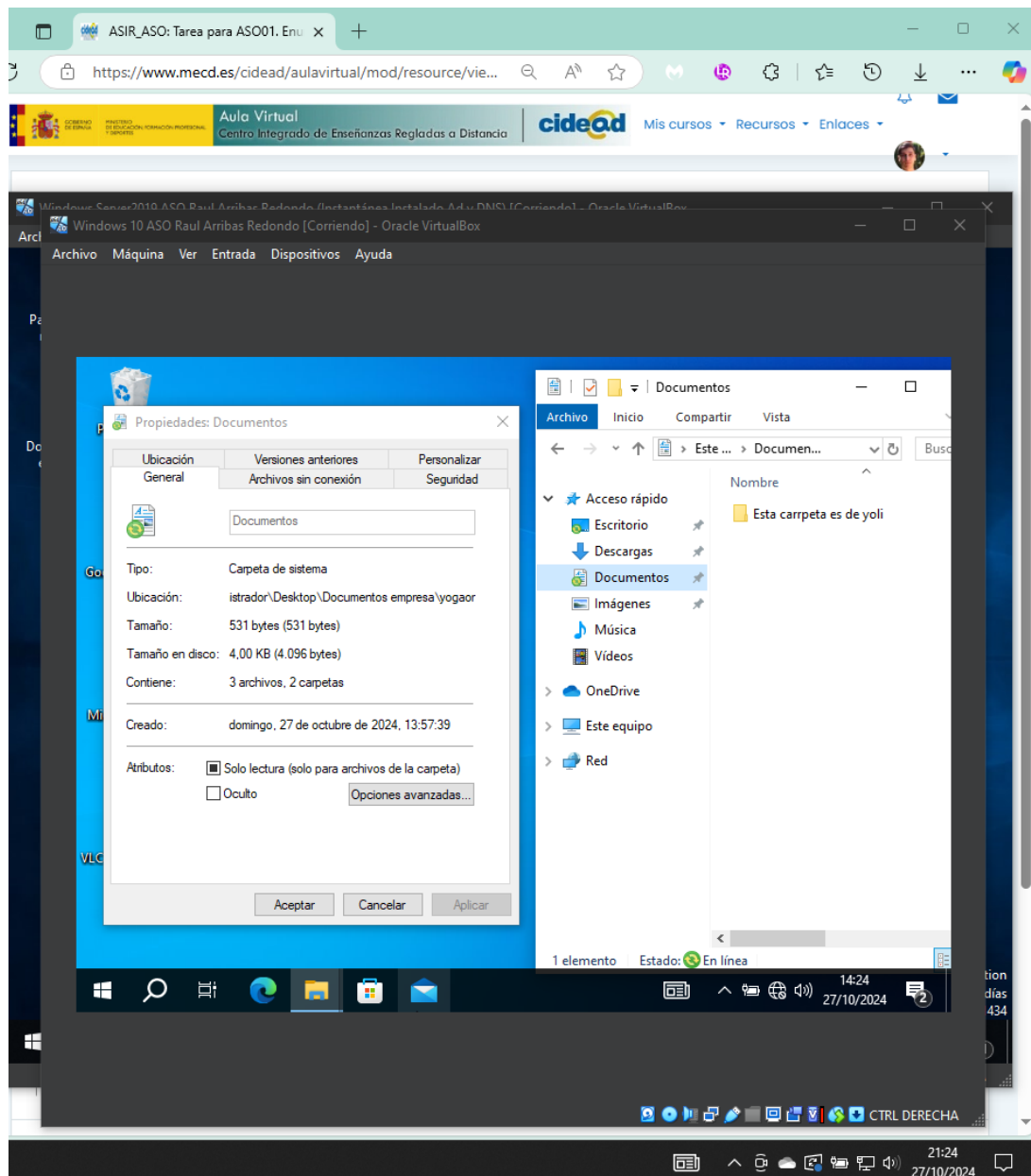
ADMINISTRACIÓN DE SERVICIOS DE DIRECTORIO

Vamos a comprobar que funciona correctamente:

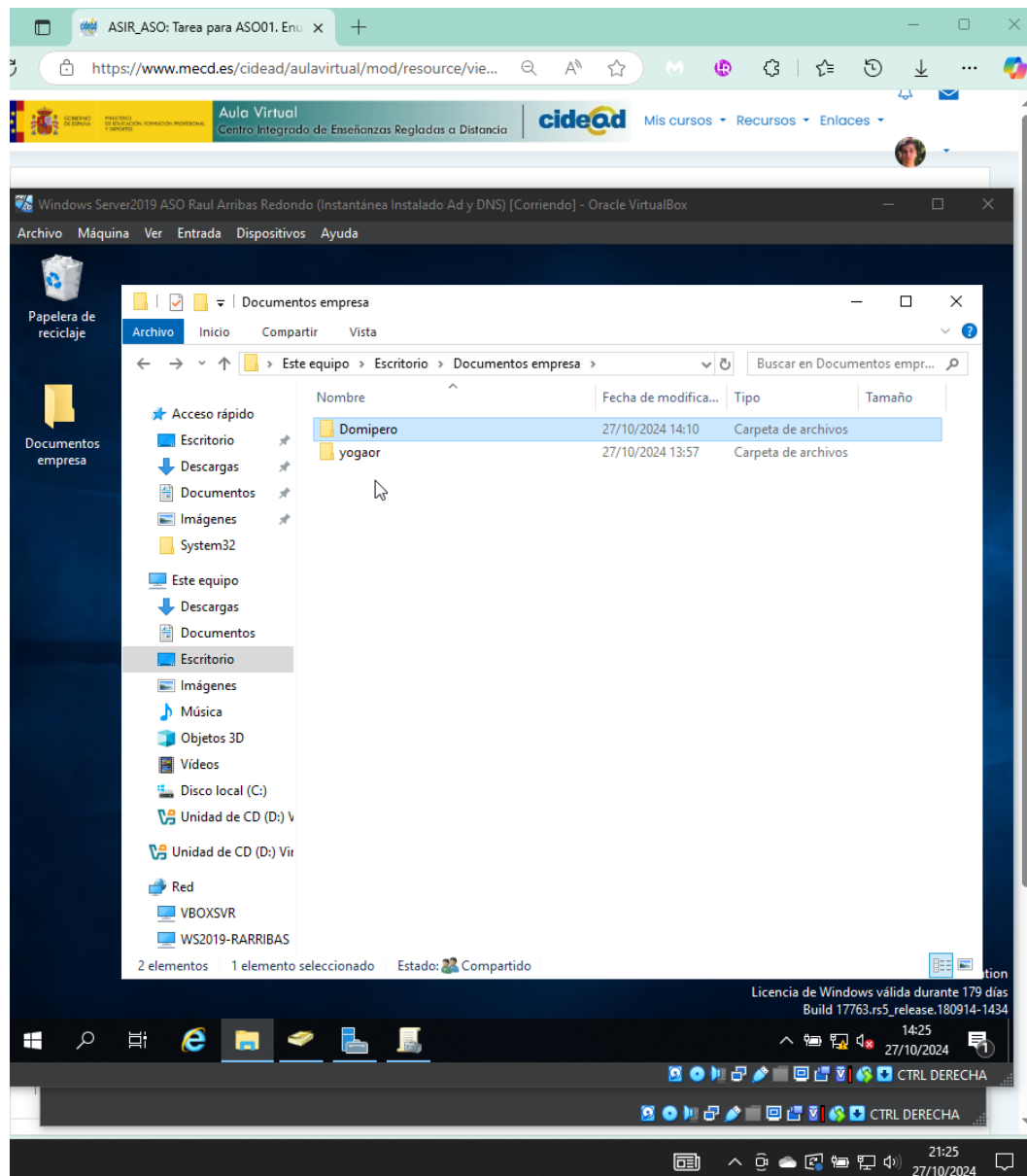
En el usuario de domingo:



Desde la cuenta de yolanda:



Desde el servidor las carpetas que se generan de los usuarios que han iniciado sesión:



2.5 Política de Contraseñas para Exigir Requisitos de Complejidad y Longitud Mínima de 9 Caracteres

Vamos a poner un requisito para que las contraseñas sean mas complejat y tengan mínimo de 9 caracteres.

Herramientas → Administración de directivas de grupo → Dominios → wbc.local → Default Domain Policy le damos click derecho y seleccionamos **Editar**

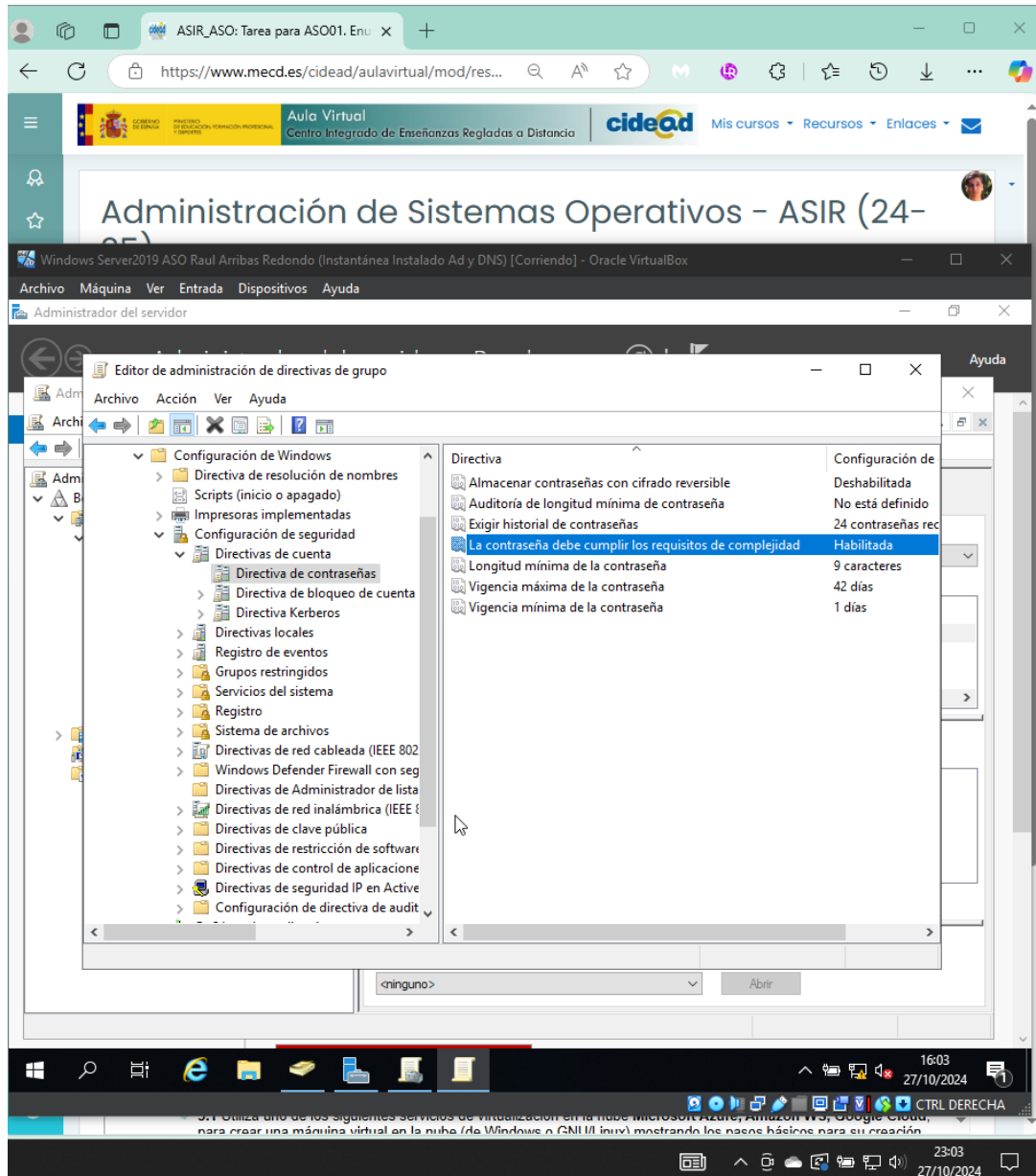
Se nos abrirá el editor de directivas de grupo, nos vamos a **Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas de cuenta → Directiva de contraseña**

Editamos las directivas y ponemos:

ADMINISTRACIÓN DE SERVICIOS DE DIRECTORIO

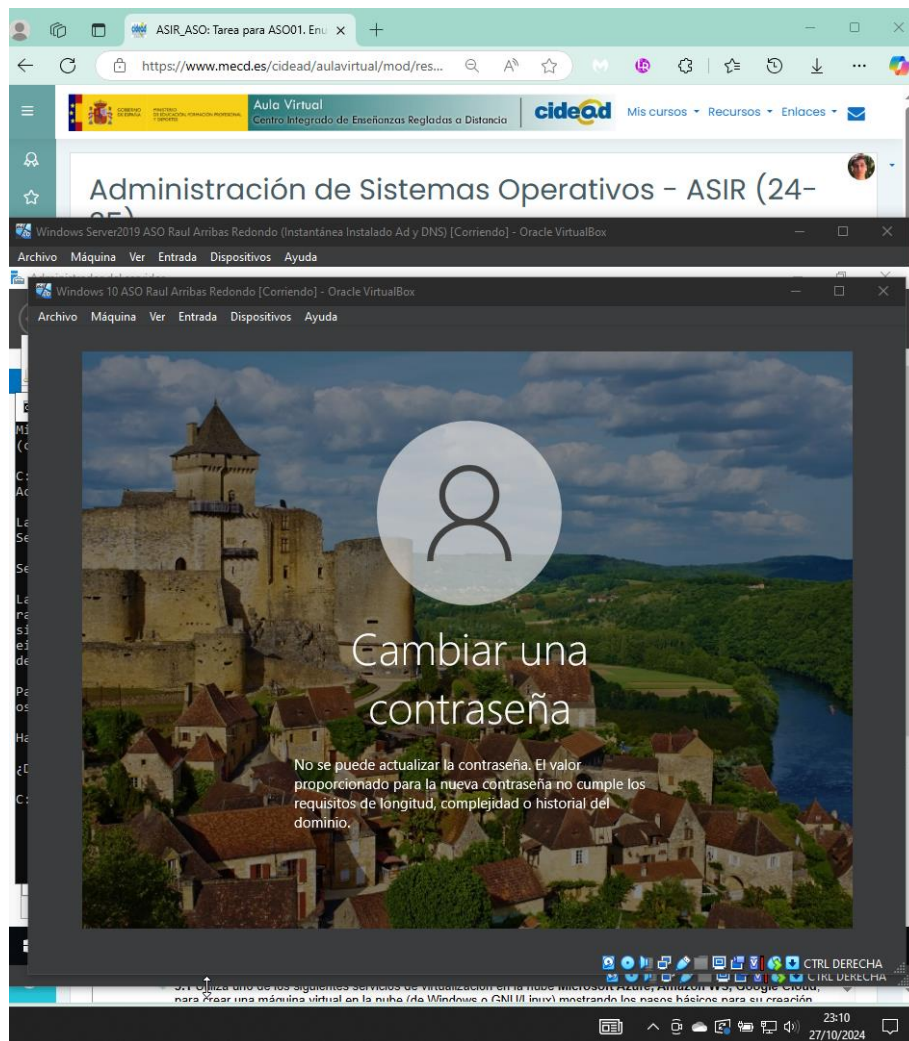
- Longitud mínima de contraseña: 9 caracteres
- La contraseña debe de cumplir los requisitos de complejidad: Habilitada

(Uso de letras mayúsculas y minúsculas, Números y caracteres especiales, No se permiten contraseñas iguales al nombre de usuario.)



Ahora para que se apliquen los cambios hacemos en servidor un **gupdate /force**.

Comprobamos que efectivamente funciona probando a cambiar una contraseña de los usuarios que tenemos creados.



2.6 Investigar Otras Dos GPOs Adicionales para Establecer Políticas en Clientes del Dominio

Vamos a crear la política para **Limitar el acceso a los paneles de control y configuración del sistema**.

Y la política de **Actualizaciones automáticas**.

2.6.1 Limitar el acceso a los paneles de control y configuración del sistema:

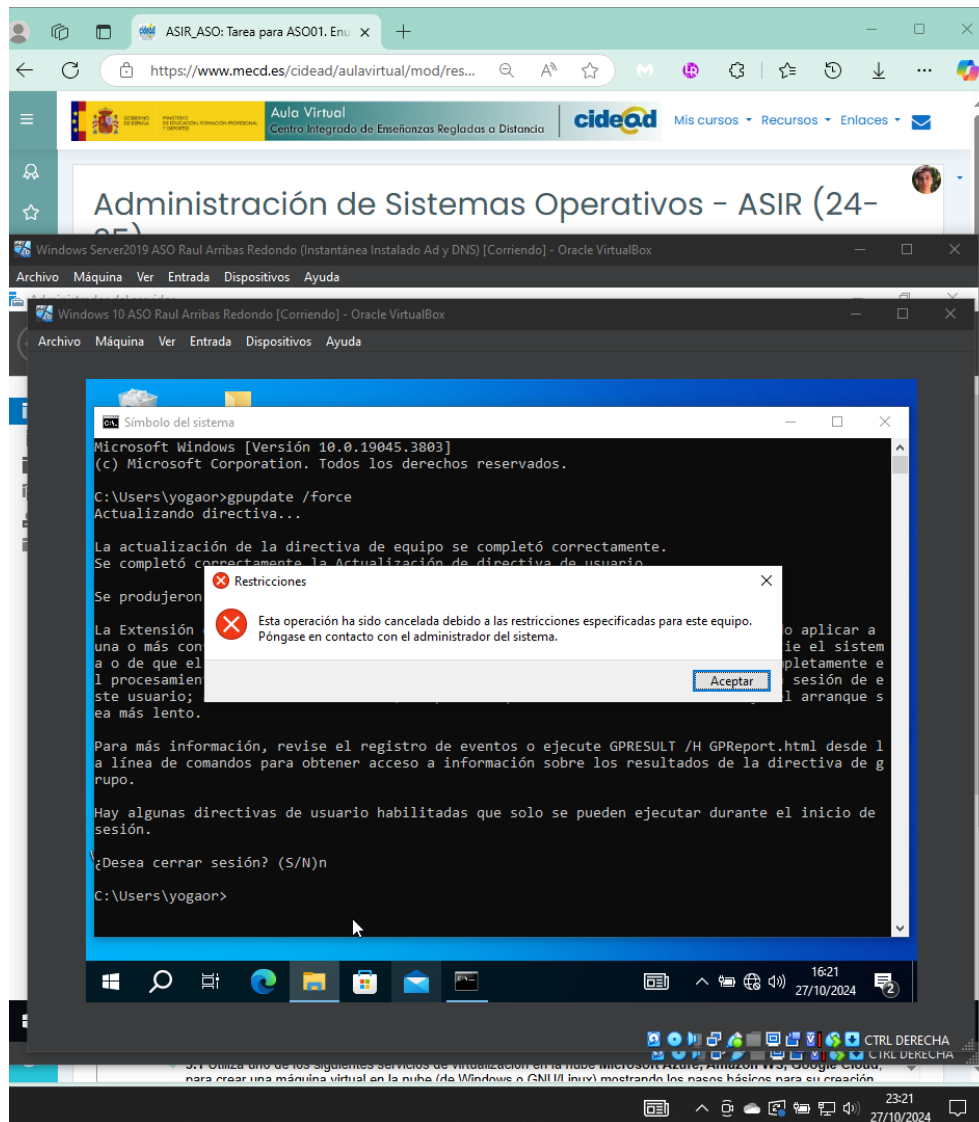
Creamos la política en el bosque `wbc.local`, una vez la creamos le damos a editar y nos vamos a la siguiente ruta:

Configuración de Usuario → Directivas → Plantillas administrativas → Panel de control

Seleccionamos Prohibir el acceso a configuración de PC y a Panel de control, y la habilitamos.

Comprobación que funciona:

Hacemos `gpupdate /force` en la maquina cliente y probamos a abrir el panel de control y la configuración. (la aplicación de configuración se debería de abrir y cerrar instantáneamente)



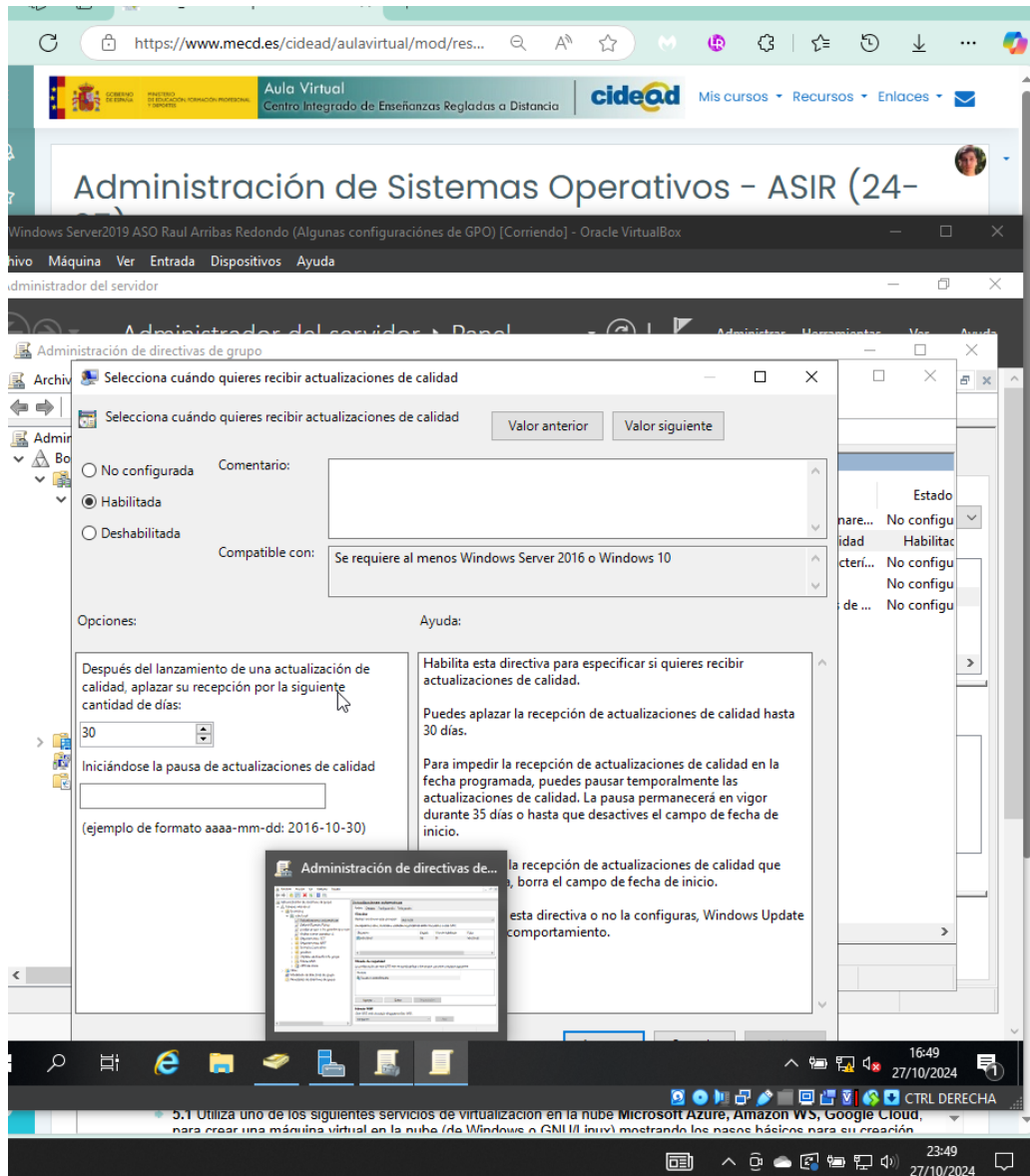
2.6.2 Política de actualizaciones automáticas

Vamos a gestionar las actualizaciones mediante una GPO, seguimos los siguientes pasos.

Herramientas → Administrador de directivas de grupo y creamos la política “Actualizaciones Windows” en el bosque `wbc.local`

Le damos a editar la política que hayamos creado y nos dirigimos a **Configuración del equipo → Plantillas administrativas → Componentes de Windows → Windows Update → Actualización de Windows para empresas** y seleccionamos cuando quieres recibir las actualizaciones de caidad.

Vamos a poner el máximo que son 30 días mas tarde.

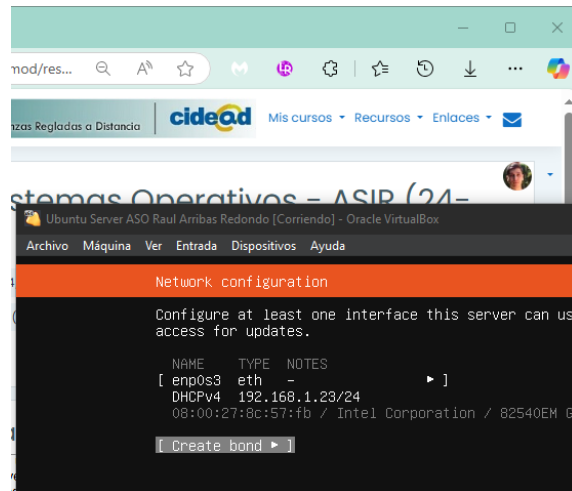


3 INSTALAR UBUNTU SERVER CON OPENLDAP

Primero nos descargamos Ubuntu Server desde la siguiente URL: [Get Ubuntu Server | Download | Ubuntu](#)

Instalamos Ubuntu server siguiendo los siguientes pasos:

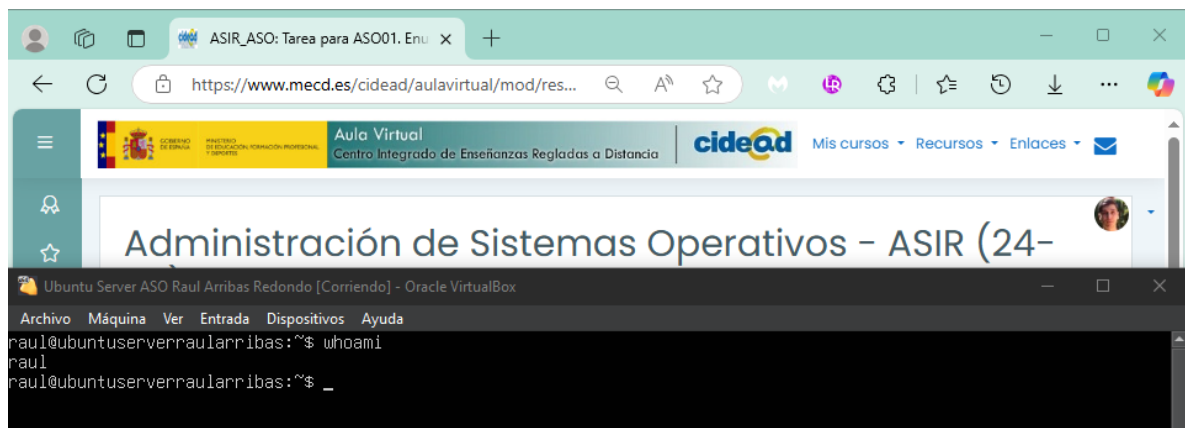
- Elegimos Idioma: Español
- Instalamos la última versión disponible si nos lo pide
- Network Configuration



- Proxy address: Lo dejamos vacío
- Mirror Configuration: Elegimos el que viene por defecto
- Configuración de almacenamiento: Utilizamos el disco completo y como LVM Group
- Nombre del servidor: ubuntuerverraularribas
- SSH configuration: Lo marcamos para la instalación

Al finalizar la instalación nos pedirá reiniciarlo.

Ya tenemos nuestro servidor instalado:



3.1 Instalación LDAP

Vamos a instalar LDAP y sus utilidades principales, para ello sigue los siguientes pasos desde la terminal:

sudo apt update

sudo apt upgrade

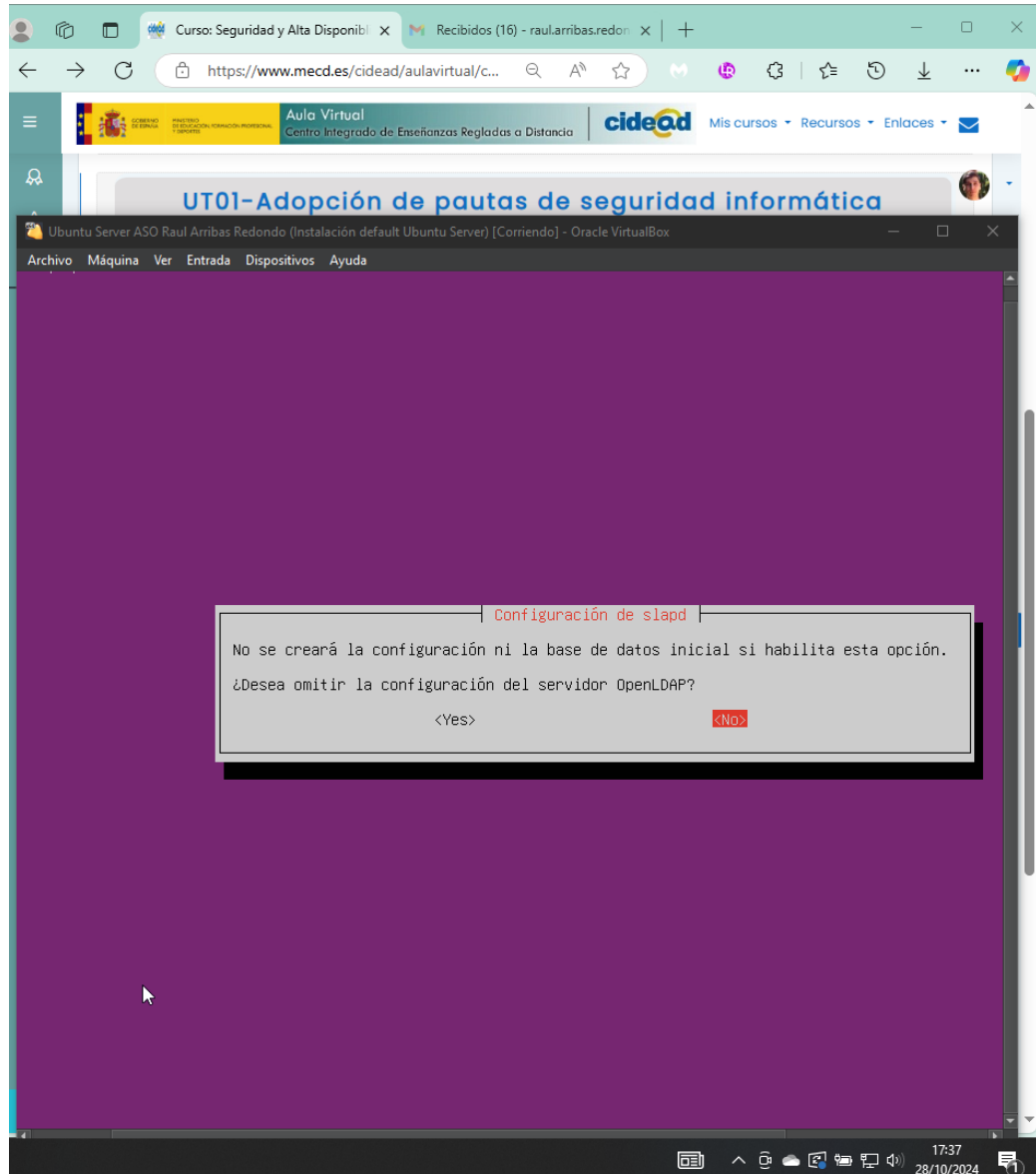
sudo apt install slapd ldap-utils -y

Tras ejecutarlo nos pedirá que introduzcamos la contraseña del usuario administrador del dominio.

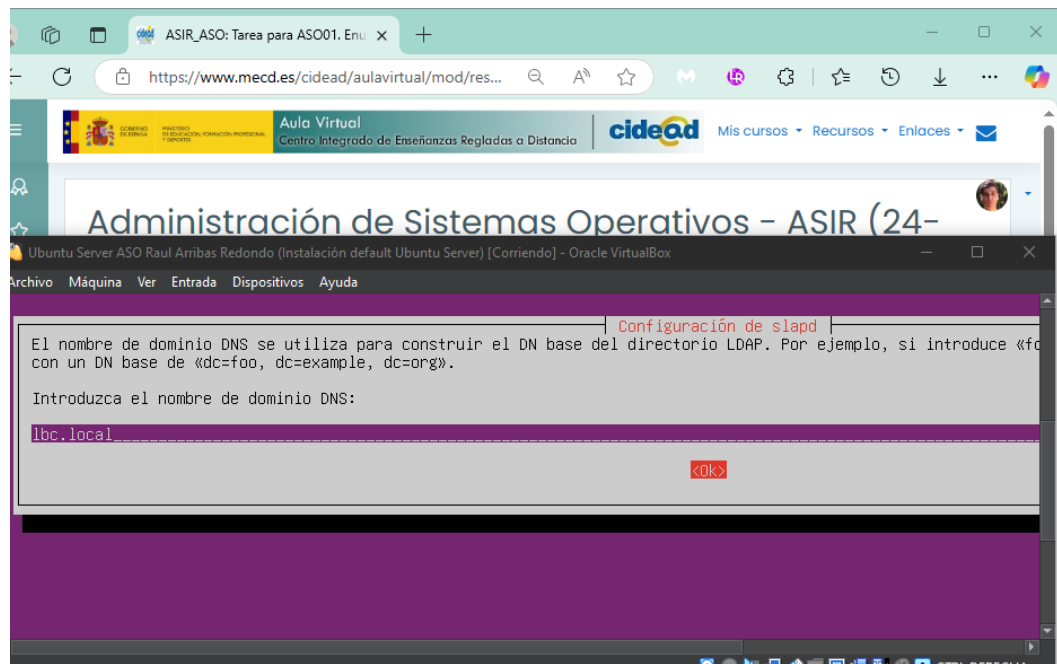
➤ Configuración del servidor LDAP

Sudo dpkg-reconfigure slapd

Desea Omitir la configuración, le damos que no



Nos pedirá que introduzcamos el nombre del dominio: lbc.local



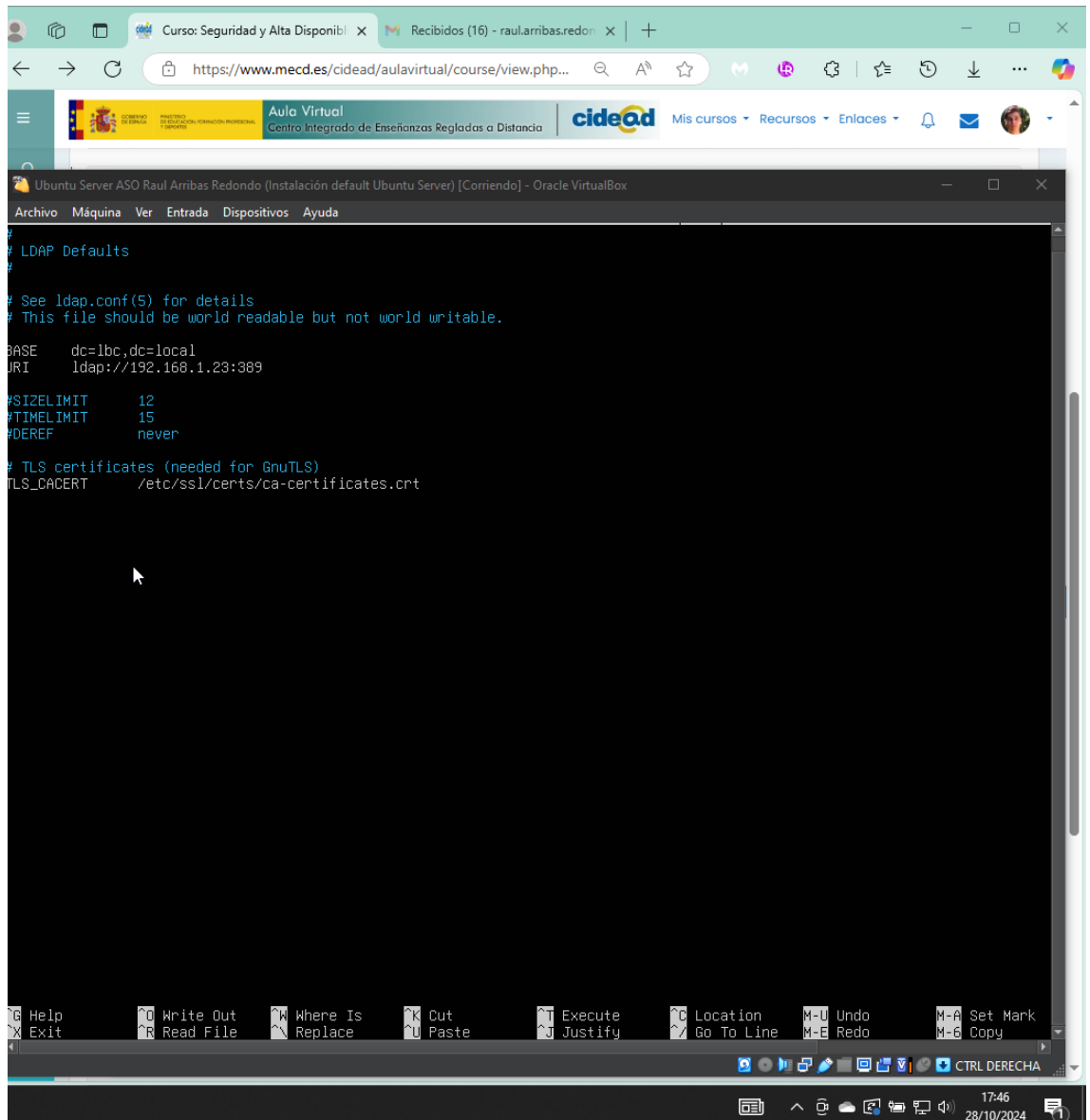
Ahora nos pedirá el nombre de la organización: lbclocal y la contraseña.

Nos pedirá si queremos que borre la base de datos: seleccionamos NO

Desea mover la base de datos antigua: Si

Una vez terminamos la configuración abrimos el fichero de configuración `ldap.conf` y lo dejamos como se muestra en la imagen

`sudo nano /etc/ldap/ldap.conf`

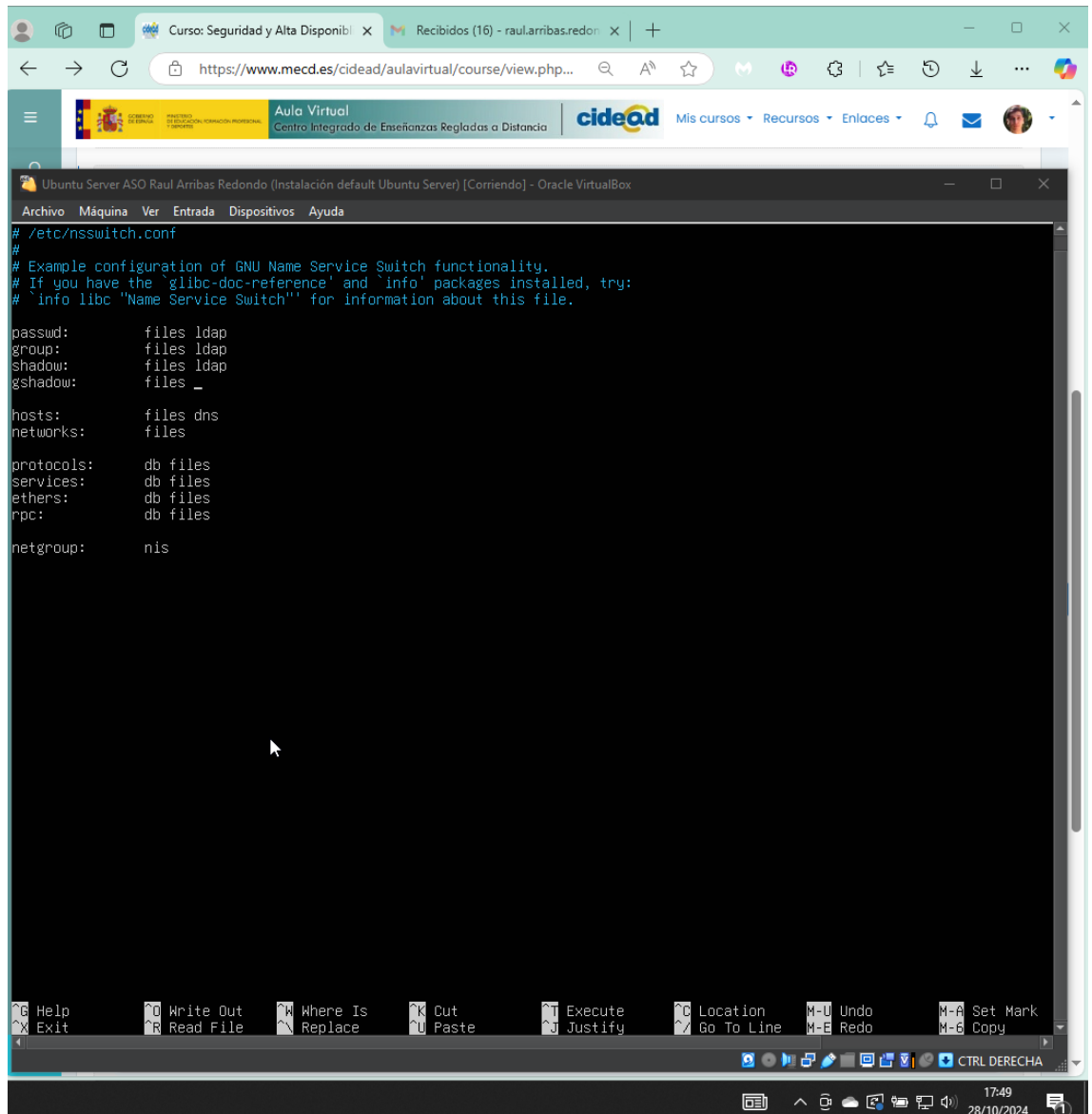


The image shows a web browser window at the top and a terminal window below it. The browser window displays a course page from MEC D (Ministerio de Educación, Cultura y Deporte) titled "Curso: Seguridad y Alta Disponibilidad". The terminal window is titled "Ubuntu Server ASO Raul Arribas Redondo (Instalación default Ubuntu Server) [Corriendo] - Oracle VirtualBox". It shows the contents of the /etc/ldap/ldap.conf file, which includes LDAP Defaults, BASE, URI, and TLS certificates.

```
# LDAP Defaults
#
# See ldap.conf(5) for details
# This file should be world readable but not world writable.
BASE    dc=lbc,dc=local
URI      ldap://192.168.1.23:389
#SIZELIMIT    12
#TIMELIMIT    15
#DEREF        never
# TLS certificates (needed for GnuTLS)
TLS_CACERT  /etc/ssl/certs/ca-certificates.crt
```

Ahora editamos el siguiente fichero: `nsswitch.conf` y lo dejamos como en la imagen

Sudo nano /etc/nsswitch.conf



The screenshot shows a web browser window with the URL <https://www.mecd.es/cidead/aulavirtual/course/view.php...>. The page header includes the logo of the Ministerio de Educación and the text "Aula Virtual Centro Integrado de Enseñanzas Regladas a Distancia". Below the browser, a terminal window titled "Ubuntu Server ASO Raul Arribas Redondo (Instalación default Ubuntu Server) [Corriendo] - Oracle VirtualBox" is open. The terminal displays the contents of the `/etc/nsswitch.conf` file:

```
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the 'glibc-doc-reference' and 'info' packages installed, try:
# 'info libc "Name Service Switch"' for information about this file.

passwd:      files ldap
group:       files ldap
shadow:      files ldap
gshadow:     files _

hosts:       files dns
networks:    files

protocols:   db files
services:    db files
ethers:      db files
rpc:         db files

netgroup:    nis
```

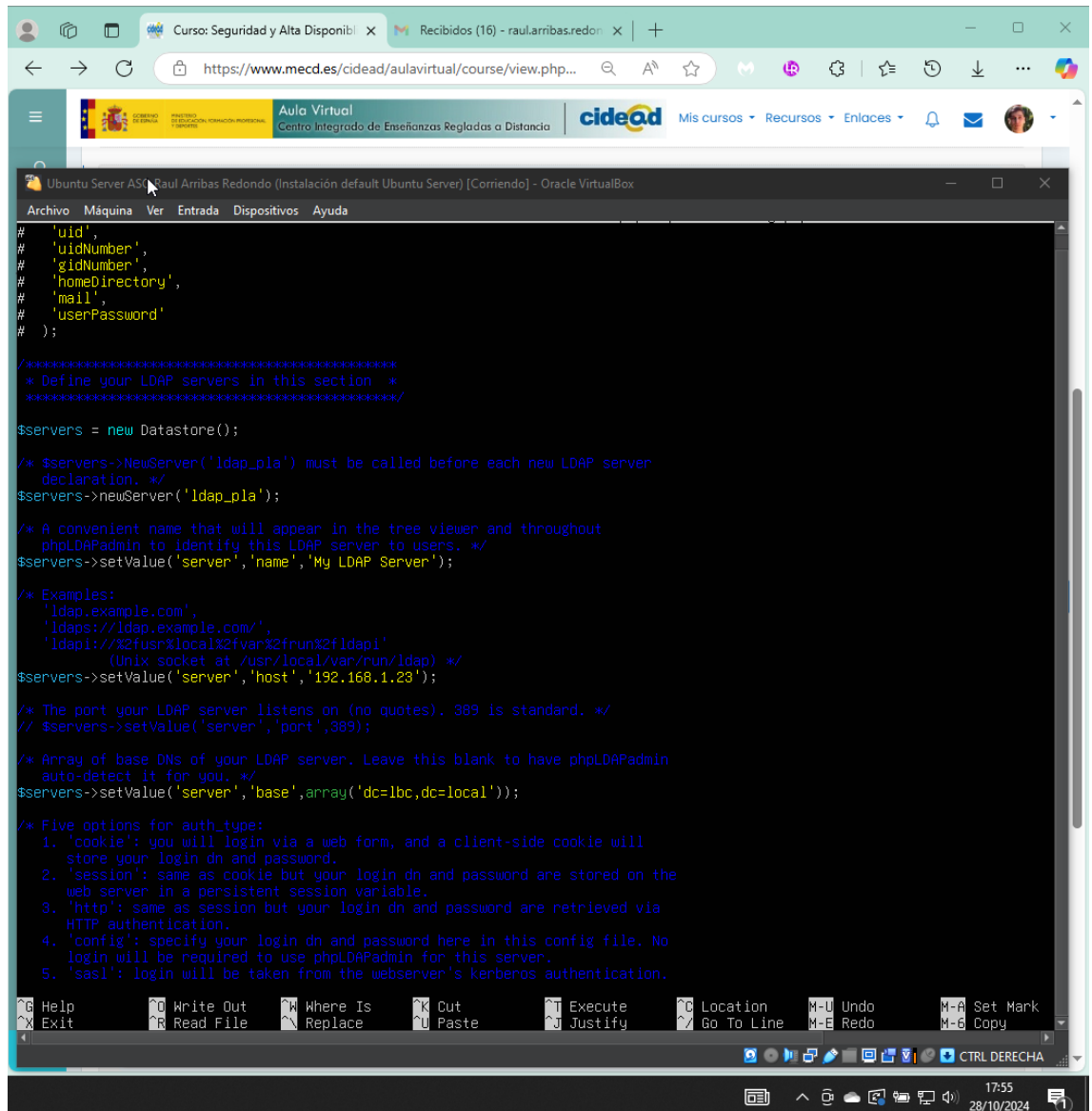
The terminal window also shows a menu bar with options like "Archivo", "Máquina", "Ver", "Entrada", "Dispositivos", and "Ayuda". At the bottom, there is a status bar with the time "17:49" and the date "28/10/2024".

Después de editar el fichero anterior vamos a instalar `phpldapadmin`:

Sudo apt install phpldapadmin

Ahora nos metemos al archivo de configuración para cambiar la ip que viene por defecto a la nuestra y nuestro dominio `lbc.local`

Sudo nano /etc/phpldapadmin/Config.php



The screenshot shows a web browser window with the URL <https://www.mecd.es/cidead/aulavirtual/course/view.php...>. The page displays the 'Aula Virtual' interface for 'Centro Integrado de Enseñanzas Regladas a Distancia'. Below the browser, a terminal window titled 'Ubuntu Server AS Raul Arribas Redondo (Instalación default Ubuntu Server) [Corriendo] - Oracle VirtualBox' is open. The terminal shows the following code:

```
# 'uid',
# 'uidNumber',
# 'gidNumber',
# 'homeDirectory',
# 'mail',
# 'userPassword'
# );

/* Define your LDAP servers in this section */
/* ===== */

$servers = new Datastore();

/* $servers->NewServer('ldap_pla') must be called before each new LDAP server
   declaration. */
$servers->newServer('ldap_pla');

/* A convenient name that will appear in the tree viewer and throughout
   phpLDAPAdmin to identify this LDAP server to users. */
$servers->setValue('server','name','My LDAP Server');

/* Examples:
   'ldap.example.com',
   'ldaps://ldap.example.com/',
   'ldapi://%2fusr%2flocal%2fvar%2frun%2fldapi'
   (Unix socket at /usr/local/var/run/ldap) */
$servers->setValue('server','host','192.168.1.23');

/* The port your LDAP server listens on (no quotes). 389 is standard. */
// $servers->setValue('server','port',389);

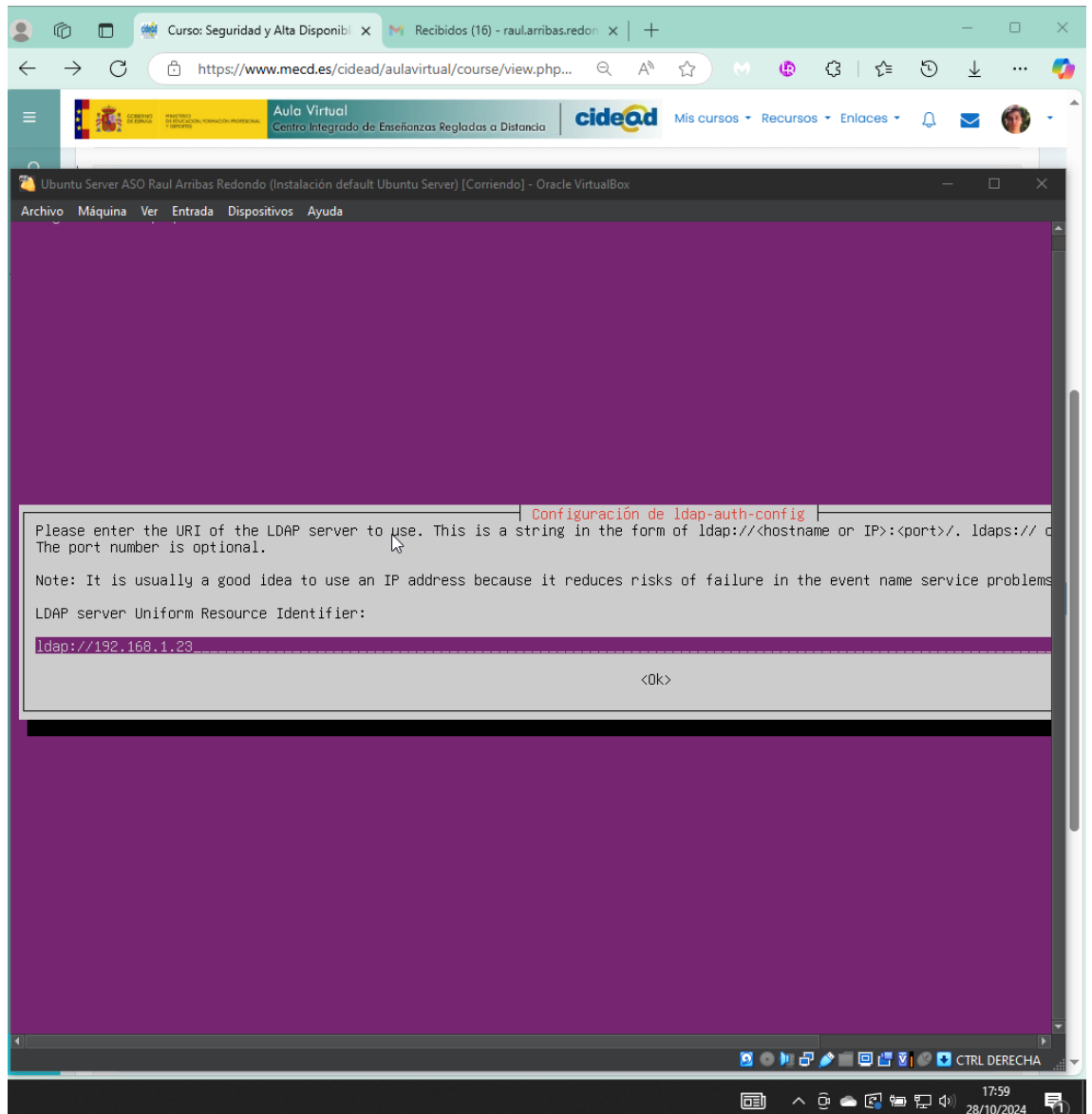
/* Array of base DN's of your LDAP server. Leave this blank to have phpLDAPAdmin
   auto-detect it for you. */
$servers->setValue('server','base',array('dc=lbc,dc=local'));

/* Five options for auth_type:
   1. 'cookie': you will login via a web form, and a client-side cookie will
      store your login dn and password.
   2. 'session': same as cookie but your login dn and password are stored on the
      web server in a persistent session variable.
   3. 'http': same as session but your login dn and password are retrieved via
      HTTP authentication.
   4. 'config': specify your login dn and password here in this config file. No
      login will be required to use phpLDAPAdmin for this server.
   5. 'sasl': login will be taken from the webserver's kerberos authentication.
```

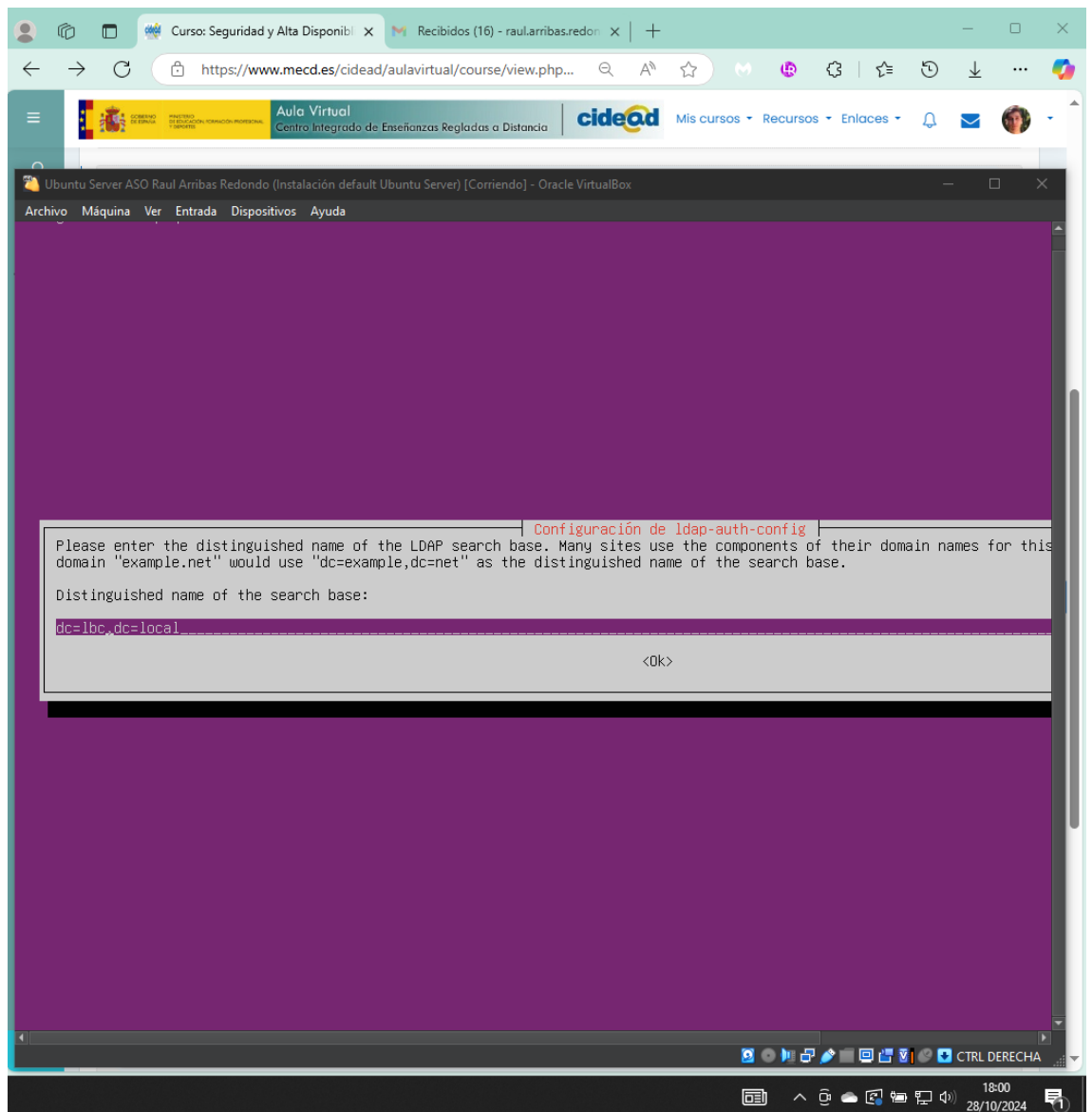
Ahora instalamos algunas librerías:

Sudo apt install libnss-ldap libpam-ldap

Ponemos la siguiente Uri: **ldap://192.168.1.23**

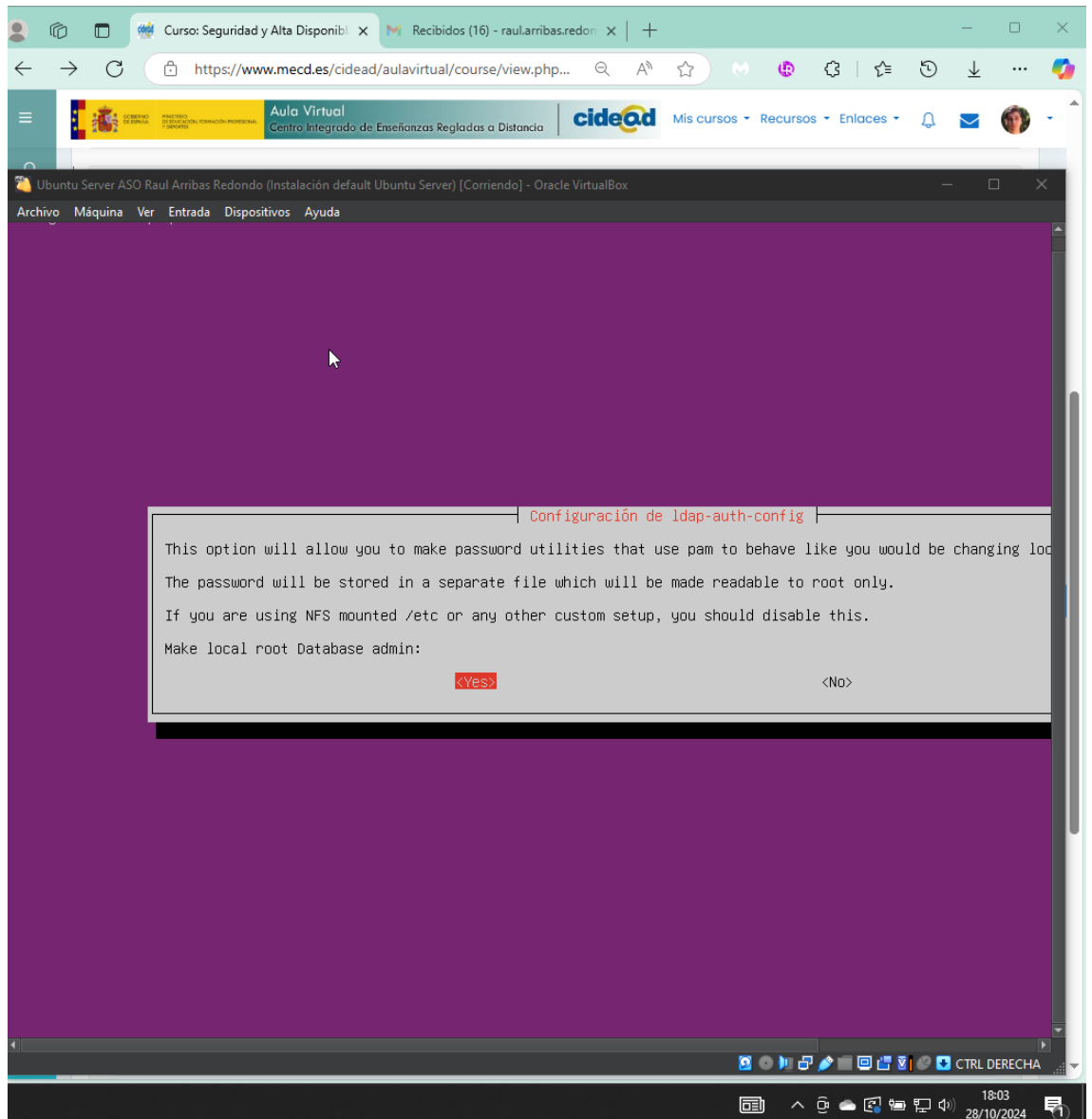


Ponemos nuestro nombre de dominio: **dc=lbc,dc=local**

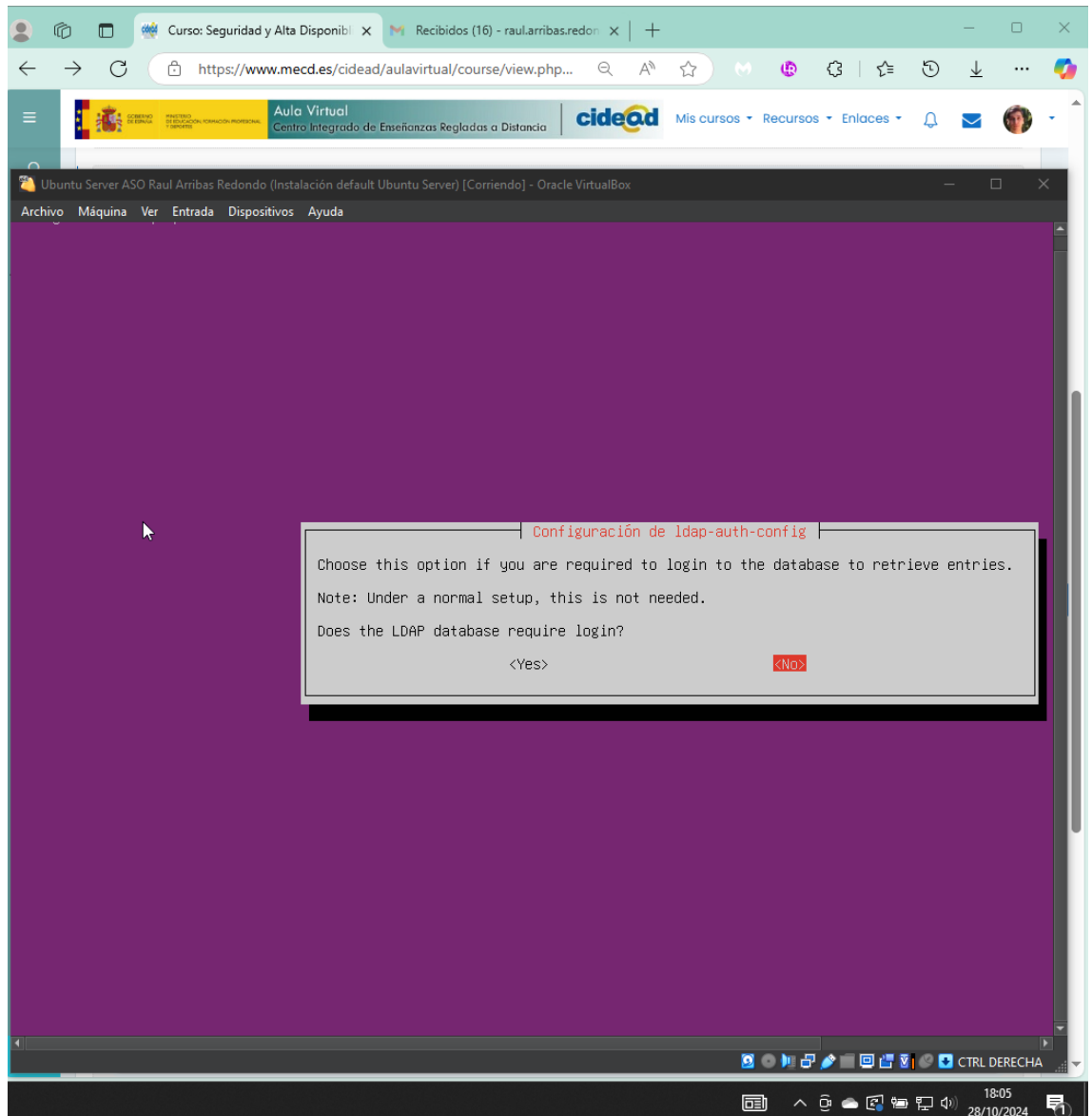


Escogemos la **Version 3** de ldap

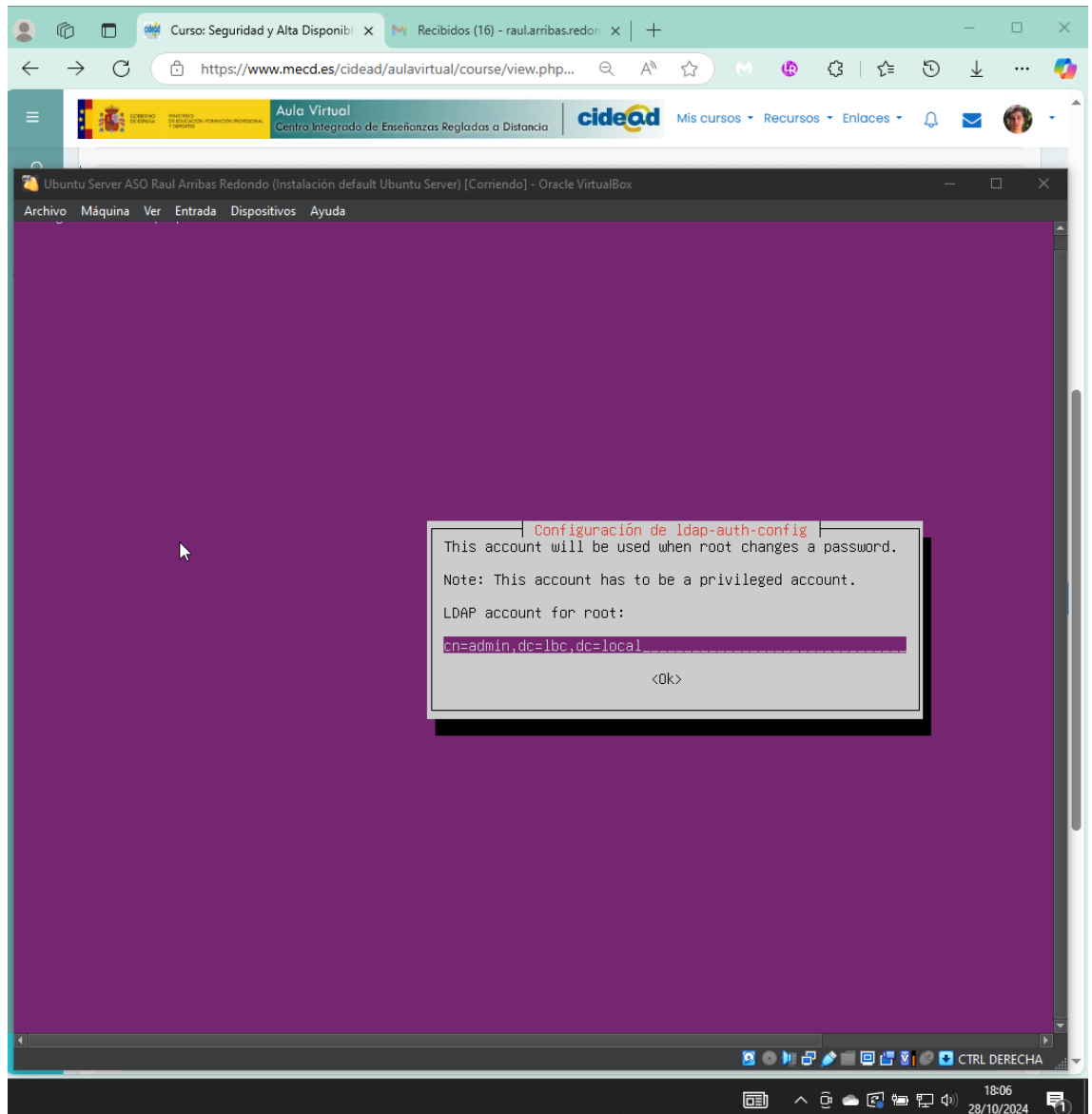
Hacemos el usuario local root como admin: **Yes**



Nos preguntará si queremos que nos requiera logearnos: **No**

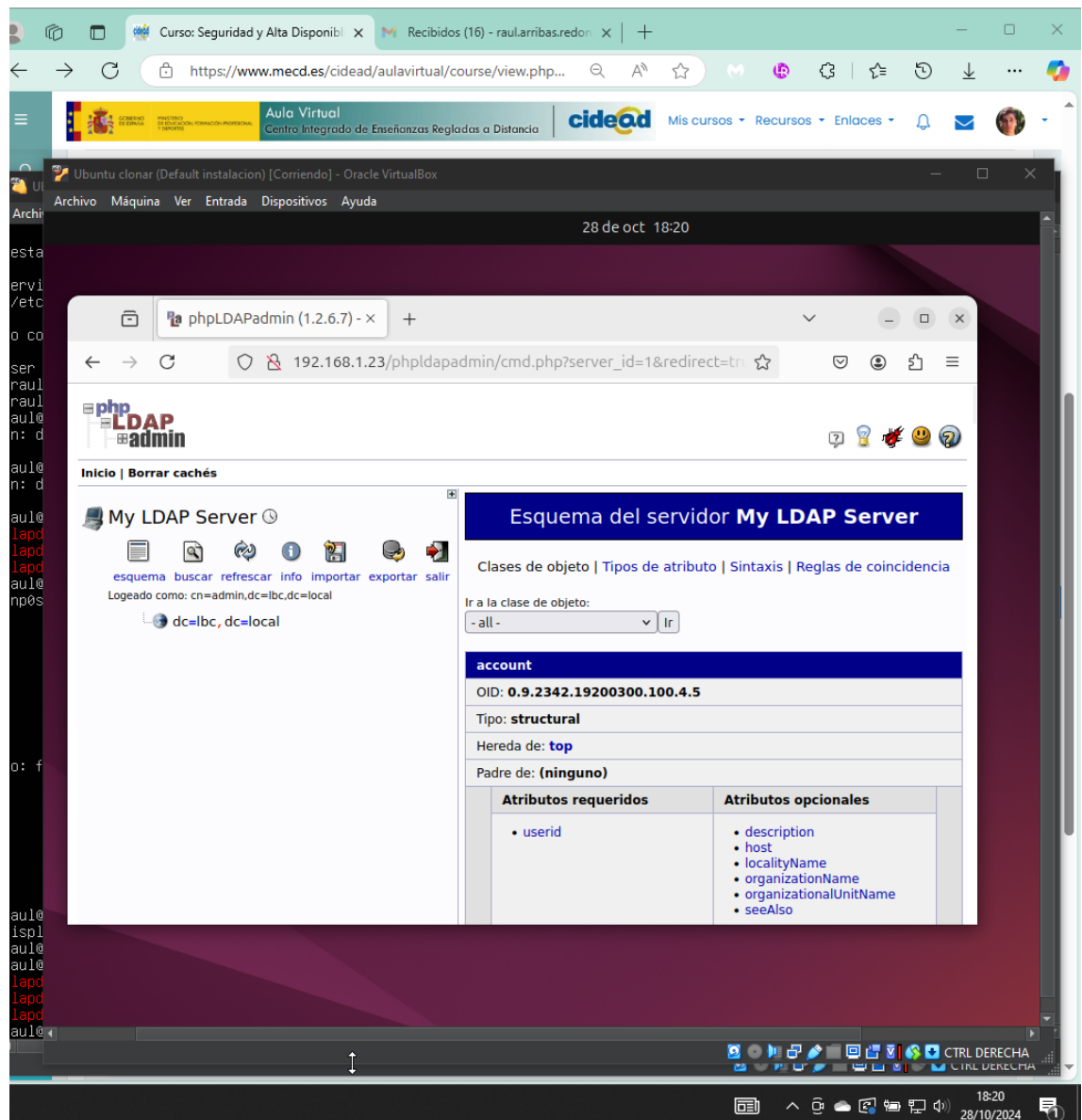


Ponemos la cuenta de LDAP para root:



Y por último nos pedirá que introduzcamos la contraseña.

Una vez terminamos la configuración nos vamos a un navegador web y comprobamos que podemos acceder.



Otra verificación que Podemos hacer para ver si está escuchando en el puerto 389 es:

Sudo lsof -i -P -n | grep slapd

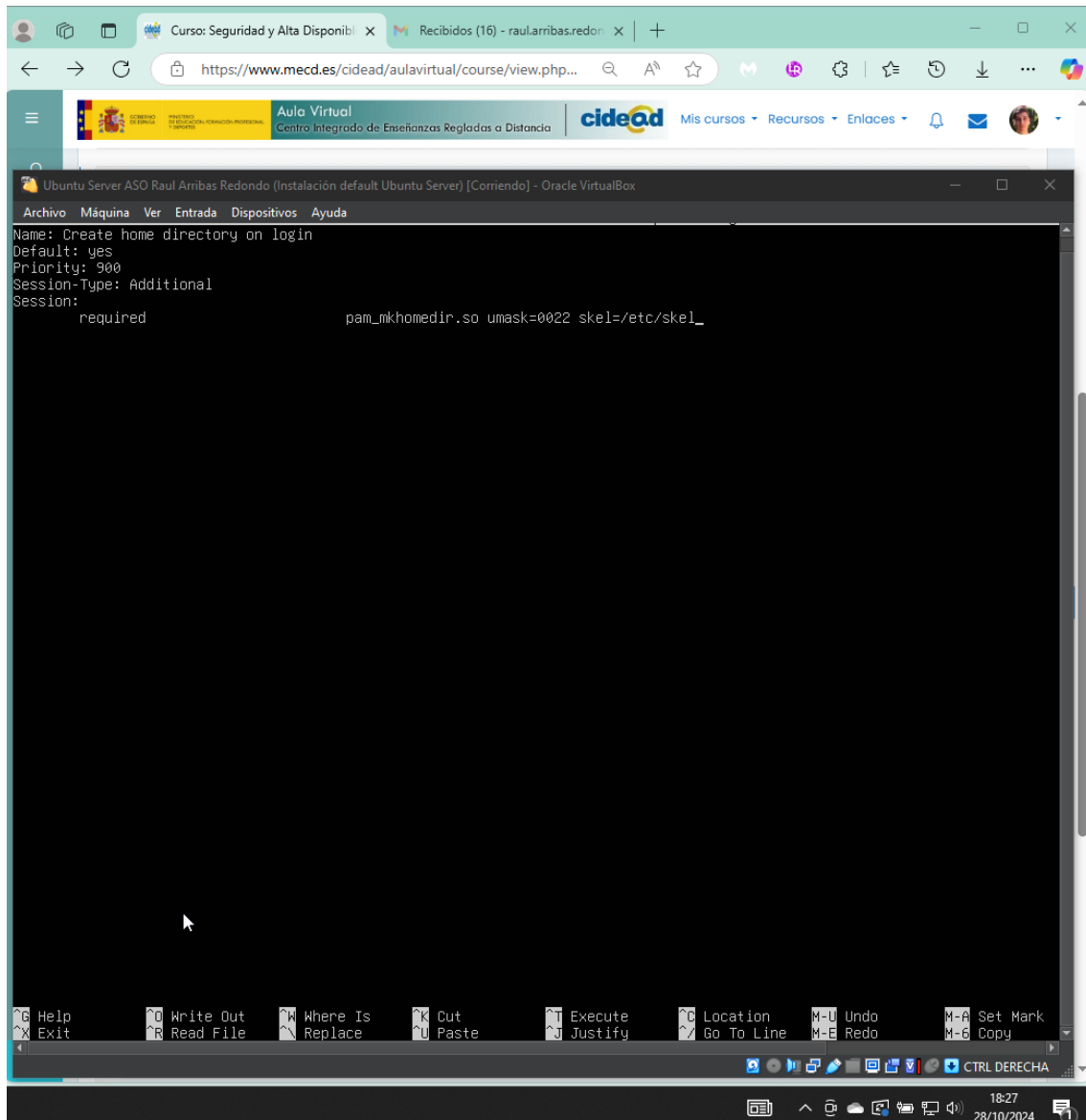
Nos tiene que salir lo siguiente:

```
raul@ubuntu-server-raul-arribas:~$ sudo lsof -i -P -n | grep slapd
slapd  10978      openldap    8u  IPv4  26592      0t0  TCP *:389 (LISTEN)
slapd  10978      openldap    9u  IPv6  26593      0t0  TCP *:389 (LISTEN)
slapd  10978      openldap   12u  IPv4  41870      0t0  TCP 192.168.1.23:389->192.168.1.23:44432 (ESTABLISHED)
raul@ubuntu-server-raul-arribas:~$
```

3.2 Instalar los servicios necesarios para que los equipos con sistema op Ubuntu se agreguen como clientes del dominio

Vamos a modificar el fichero mkhomedir, para que cuando un usuario se una al dominio se genere automáticamente un /home/usuario. Nos vamos a esta ruta y editamos el archivo como en la imagen:

Sudo nano /usr/share/pam-configs/mkhomedir



Ahora ejecutamos:

Pam-auth-update y seleccionamos con el espacio, create home directory on login.

El siguiente paso sería entrar en el directorio de common-account y agregar en la ultima fila:
account required pam_unix.so

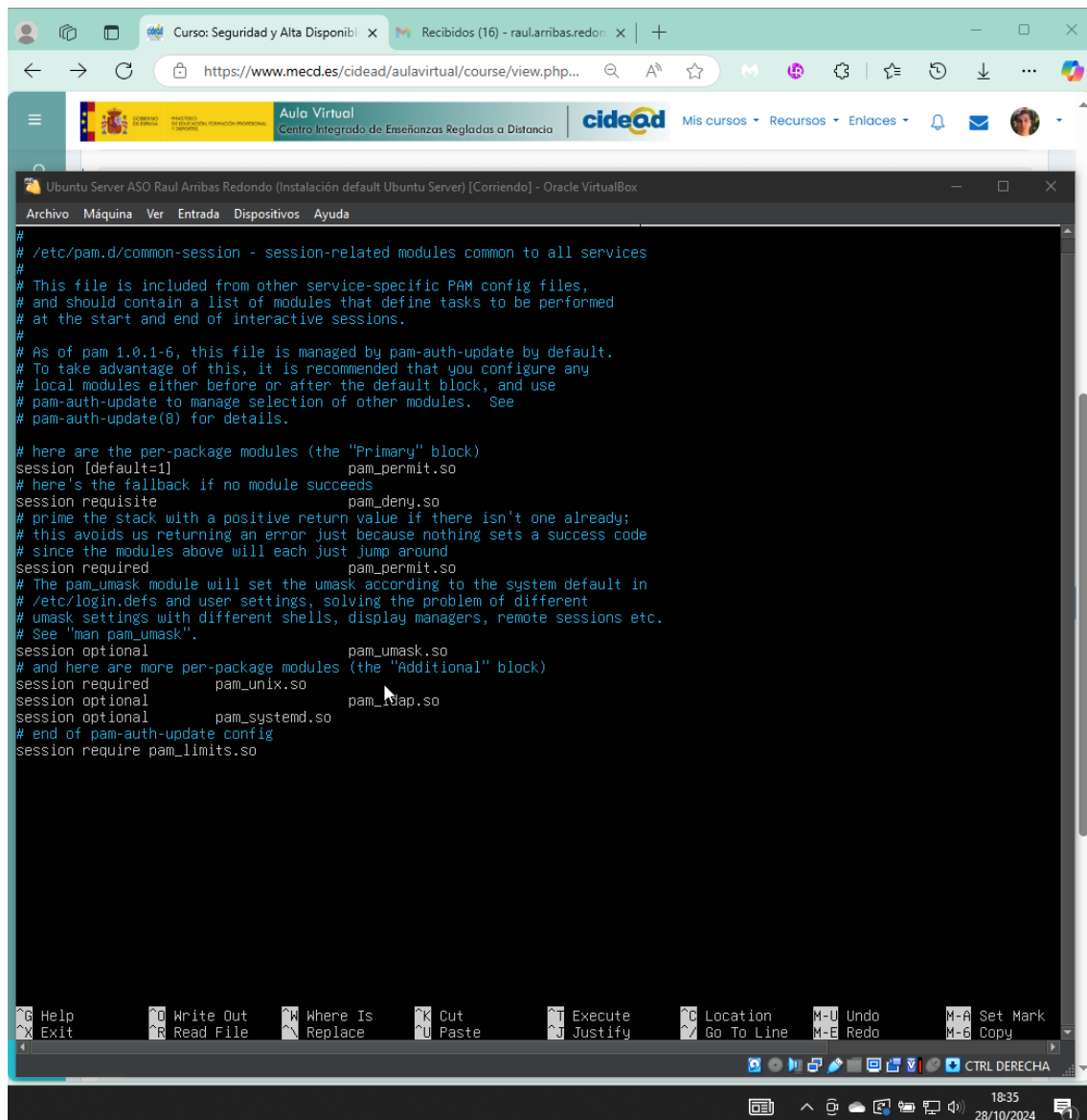
Sudo nano /etc/pam.d/common-account

The screenshot shows a web browser window with the URL <https://www.mecd.es/cidead/aulavirtual/course/view.php...>. The browser displays a course page for 'Curso: Seguridad y Alta Disponibilidad' with a user profile 'Recibidos (16) - raul.arribas.redondo'. Below the browser, a terminal window titled 'Ubuntu Server ASO Raul Arribas Redondo (Instalación default Ubuntu Server) [Corriendo] - Oracle VirtualBox' is open. The terminal shows the contents of the `/etc/pam.d/common-account` file, which defines authorization settings for all services. The file includes comments explaining its purpose and lists various PAM modules like `pam_unix.so`, `pam_ldap.so`, `pam_deny.so`, and `pam_permit.so`.

```
# /etc/pam.d/common-account - authorization settings common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of the authorization modules that define
# the central access policy for use on the system. The default is to
# only deny service to users whose accounts are expired in /etc/shadow.
#
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules. See
# pam-auth-update(8) for details.
#
# here are the per-package modules (the "Primary" block)
account [success=2 new_authtok_reqd=done default=ignore]      pam_unix.so
account [success=1 default=ignore]      pam_ldap.so
# here's the fallback if no module succeeds
account requisite      pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
account required      pam_permit.so
# and here are more per-package modules (the "Additional" block)
# end of pam-auth-update config
account required pam_unix.so_
```

Ahora nos vamos al fichero de sesión y escribimos en la ultima fila: session require pam_limits.so

Sudo nano /etc/pam.d/common-session



The screenshot shows a web browser window with the URL <https://www.mecd.es/cidead/aulavirtual/course/view.php...>. The browser displays the 'Aula Virtual' interface of the 'Centro Integrado de Enseñanzas Regladas a Distancia' (CIDEAD). Below the browser window, a terminal window titled 'Ubuntu Server ASO Raul Arribas Redondo (Instalación default Ubuntu Server) [Corriendo] - Oracle VirtualBox' is open. The terminal displays the contents of the `/etc/pam.d/common-session` file, which configures PAM modules for session management. The configuration includes a 'Primary' block with `pam_permit.so` and `pam_unix.so`, and an 'Additional' block with `pam_unix.so` and `pam_systemd.so`. The terminal also shows a status bar with various keyboard shortcuts and a system tray at the bottom indicating the time as 18:35 on 28/10/2024.

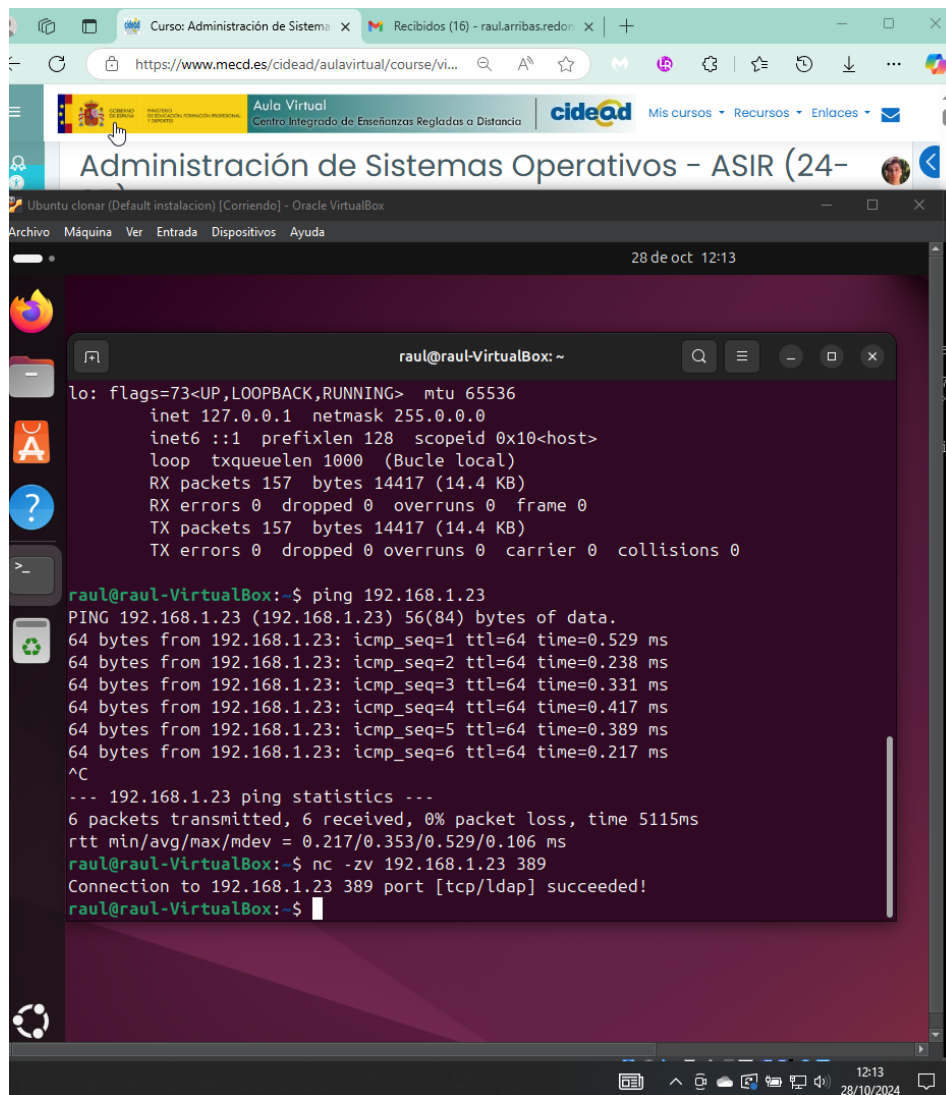
```
# /etc/pam.d/common-session - session-related modules common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of modules that define tasks to be performed
# at the start and end of interactive sessions.
#
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules. See
# pam-auth-update(8) for details.
#
# here are the per-package modules (the "Primary" block)
session [default=1]      pam_permit.so
# here's the fallback if no module succeeds
session requisite        pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
session required         pam_permit.so
# The pam_umask module will set the umask according to the system default in
# /etc/login.defs and user settings, solving the problem of different
# umask settings with different shells, display managers, remote sessions etc.
# See "man pam_umask".
session optional         pam_umask.so
# and here are more per-package modules (the "Additional" block)
session required         pam_unix.so
session optional         pam_unix.so
session optional         pam_systemd.so
# end of pam-auth-update config
session require pam_limits.so
```

Con esta configuración los usuarios con Ubuntu se podrán logear en nuestro dominio.

Comprobamos en un cliente Ubuntu que la conexión con el LDAP se hace correctamente, hacemos un ping y un Netcat:

Ping 192.168.1.23

Nc -zv 192.168.1.23 389



3.3 Instalación de FreeIPA

IMPORTANTE: He intentado de muchas formas posibles instalar esta utilidad, pero no me ha sido posible, ni con Docker, ni instalando desde GitHub un repositorio para instalarlo desde ahí. Según he investigado en la versión de Ubuntu 22.04 no se puede instalar, tiene que ser en una versión mas antigua. O en Fedora y CentOS ya que está mas orientado a estas distribuciones.

```
E: El paquete «freeipa» no tiene un candidato para la instalación
raul@ubuntu-server-raularribas:~$ sudo apt install freeipa-
freeipa-client      freeipa-client-epn  freeipa-client-samba freeipa-common      freeipa-healthcheck
raul@ubuntu-server-raularribas:~$ sudo apt install freeipa-
freeipa-client      freeipa-client-epn  freeipa-client-samba freeipa-common      freeipa-healthcheck
raul@ubuntu-server-raularribas:~$ sudo apt install freeipa-
```

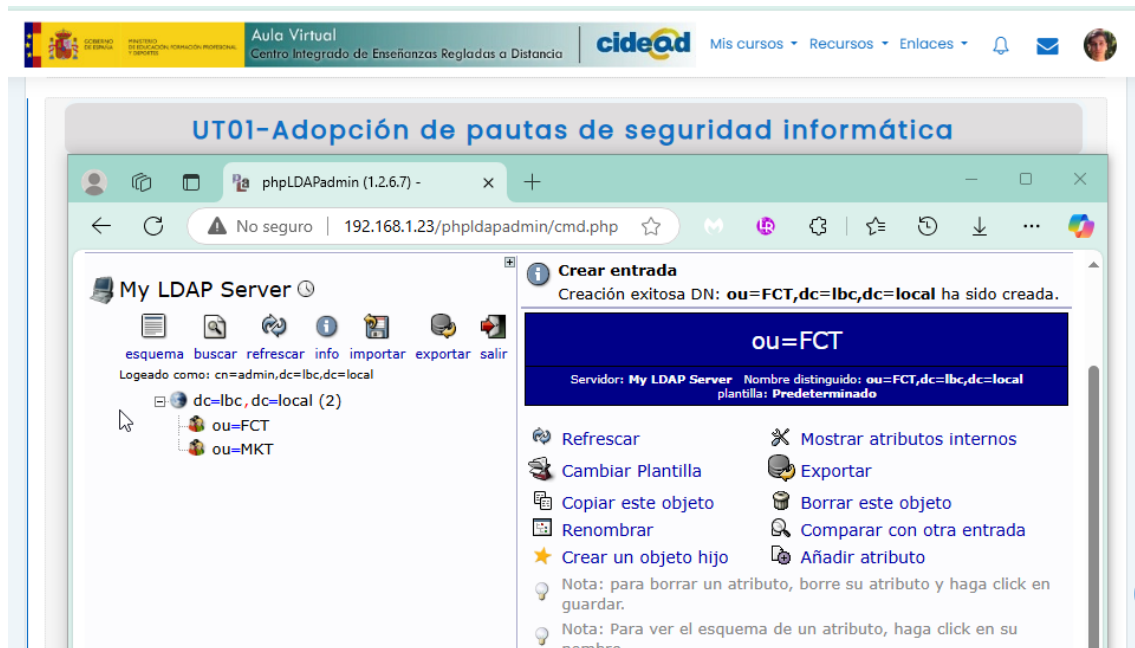
He investigado y desde el phpLDAPadmin se puede gestionar políticas y autenticación en los equipos, ya lo hemos instalado anteriormente.

4 OBJETOS DE OPENLDAP Y FREEIPA

4.1 Generar dos Unidades Organizativas distintitas con un usuario cada una
Vamos a generar 2 OU desde el phpldapadmin que hemos creado previamente, para ellos nos vamos a un navegador y escribimos <http://192.168.1.23/phpldapadmin/cmd>

4.1.1 Creamos la OU

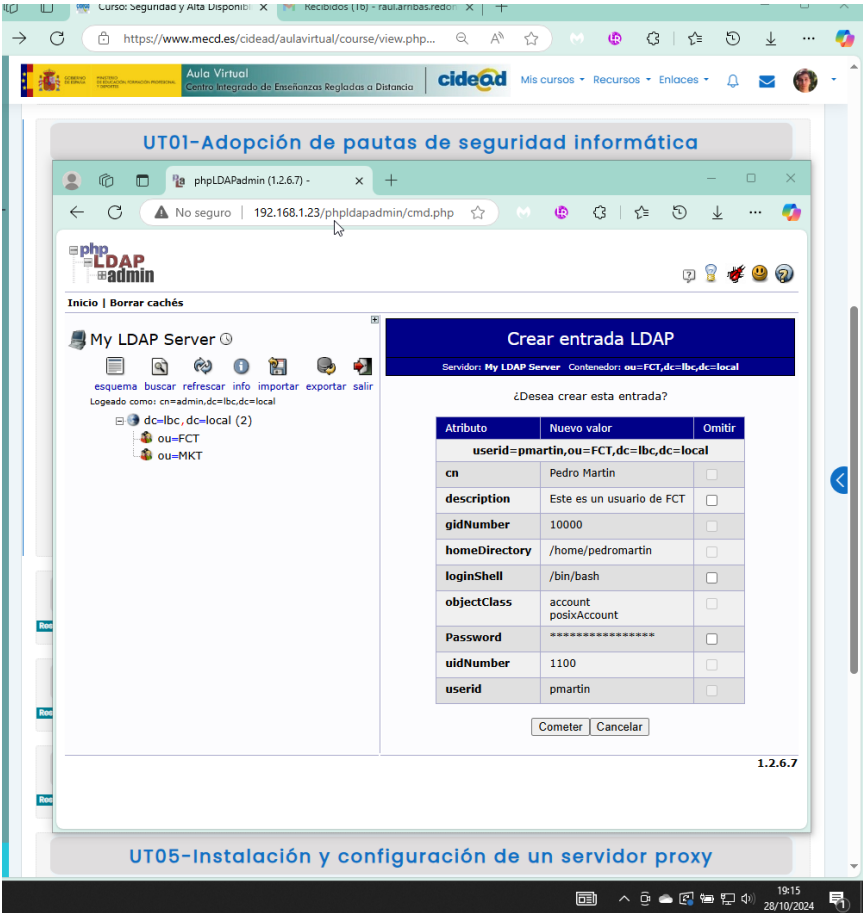
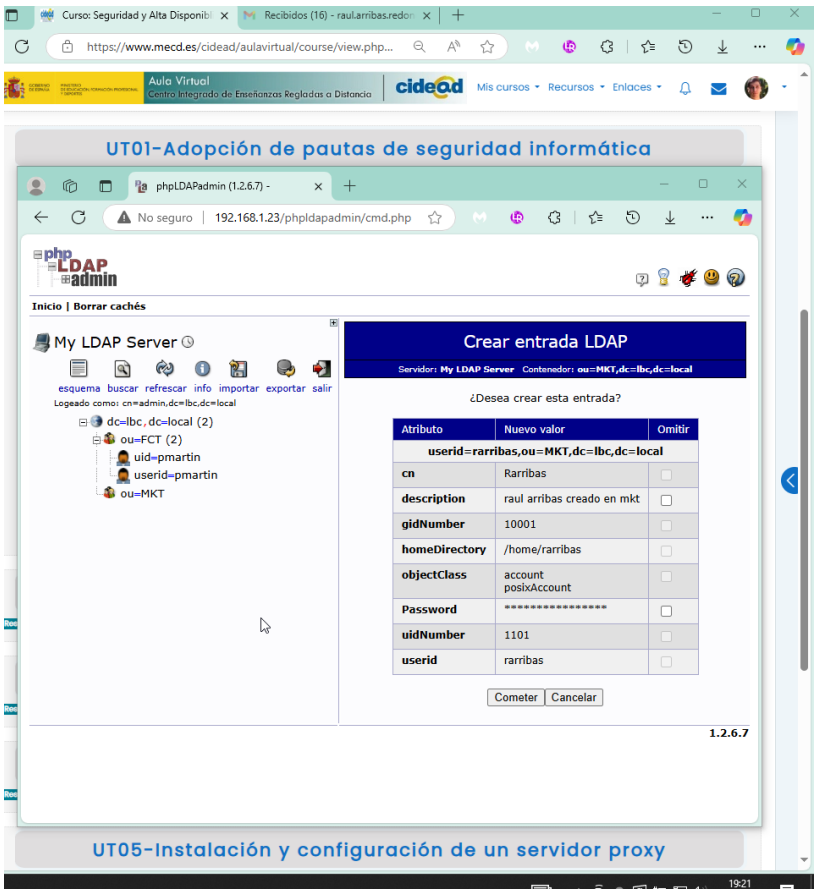
- Hacemos click en “Crear un objeto hijo”
- Seleccionamos **Generic Organizational Unit**



Repetimos el mismo paso con la UO de FCT.

4.1.2 Crear usuarios dentro de la UO

- Seleccionamos crear un objeto hijo
- Seleccionamos Predeterminado
- Seleccionamos Account y PoxixAccount con ctrl podemos seleccionar los dos y le damos proceder
- Rellenamos los datos:
 - CN: Pedro Martin
 - Gidnumber: 10000
 - homeDirectory: /home/pedroMartin
 - uidnumber1100
 - userid: pmartin
 - loginshell: /bin/bash
 - contraseña: pedro123



Podemos comprobar el usuario creado en el servidor:

```
raul@ubuntuserverraularribas:~$ ldapsearch -x -LLL -b "dc=lbc,dc=local" "(uid=rarribas)"
dn: uid=rarribas,ou=MKT,dc=lbc,dc=local
cn: Rarribas
description: raul arribas creado en mkt
gidNumber: 10001
homeDirectory: /home/rarribas
objectClass: account
objectClass: posixAccount
objectClass: top
uidNumber: 1101
uid: rarribas
```

4.2 Crear Políticas

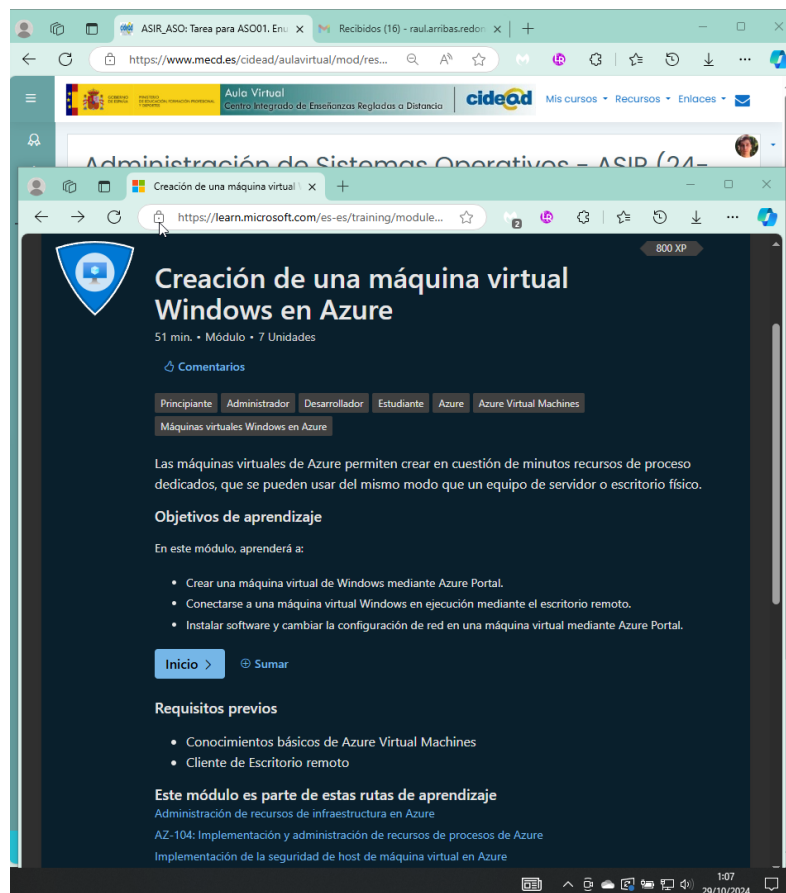
He intentado crear políticas pero no lo he conseguido.. he intentado con OPendap con directory server, pero no hay forma de que funcionen correctamente en Ubuntu server.

5 VIRTUALIZACIÓN EN LA NUBE Y CONCLUSIONES

5.1 Crear una maquina virtual en Azure

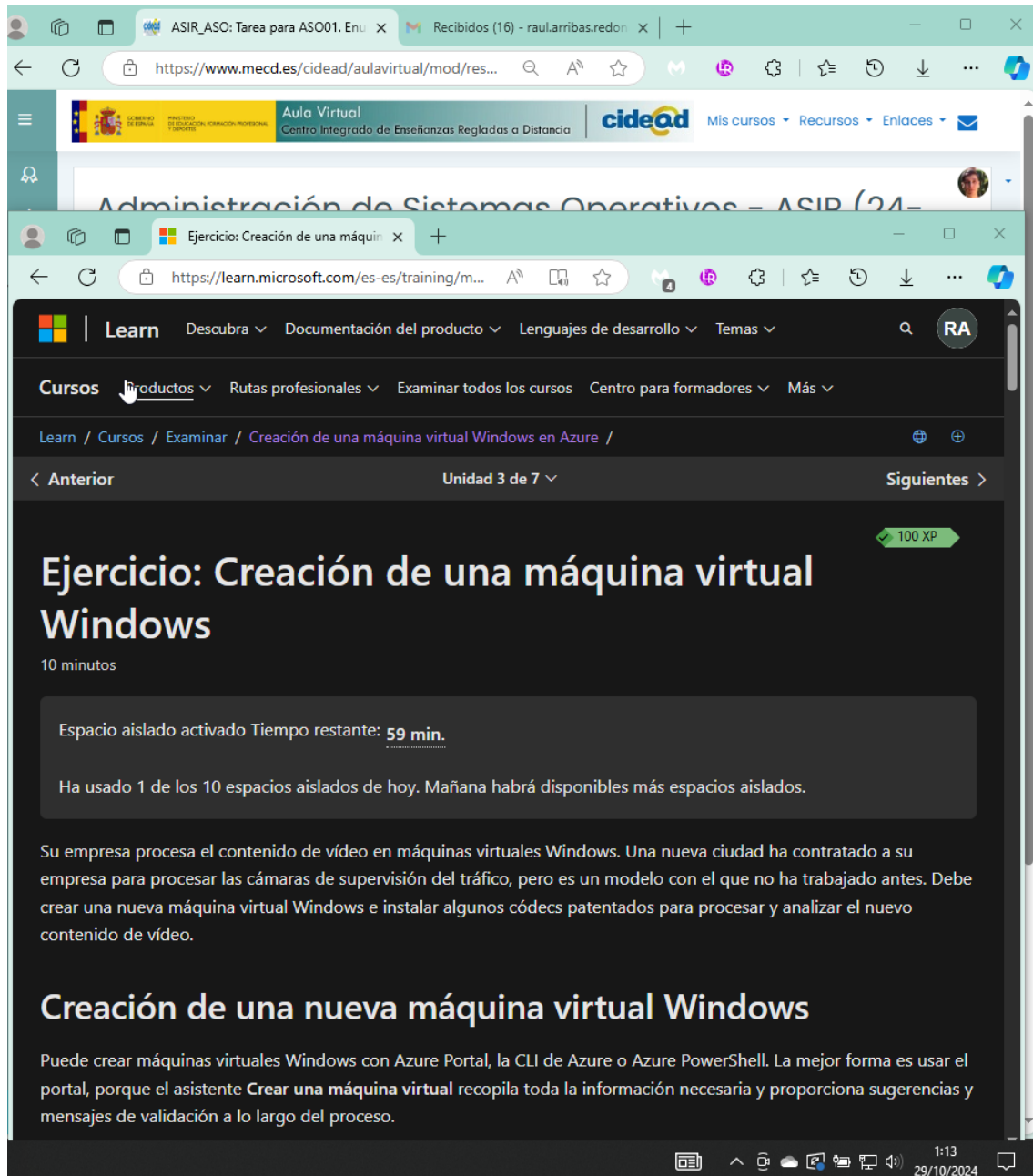
Entramos al siguiente enlace: <https://learn.microsoft.com/es-es/training/modules/create-windows-virtual-machine-in-azure/>

Le damos **Inicio** y comenzamos con los pasos que nos piden:



Después de leer la documentación nos sale que **iniciemos sesión para activar el espacio aislado**.

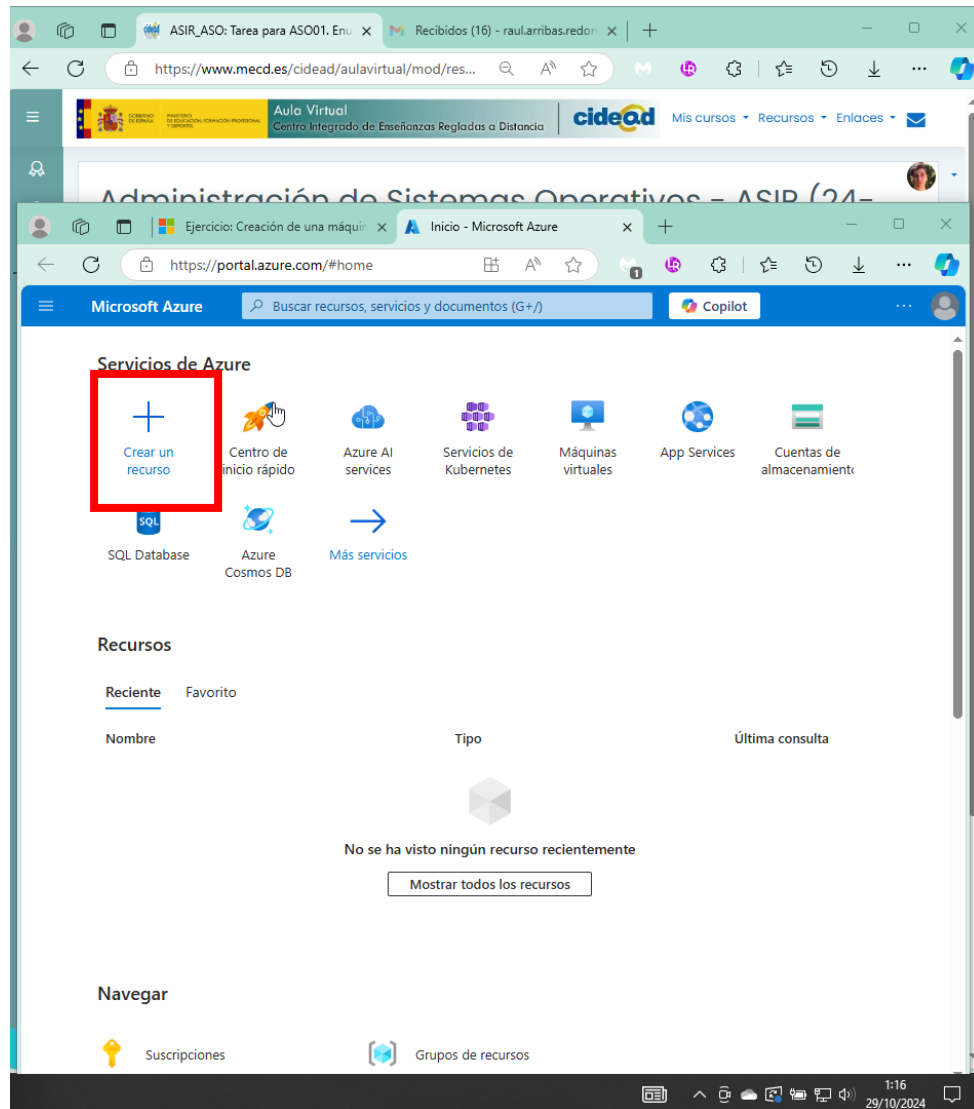
Cuando iniciemos sesión con una cuenta de Microsoft y verificar un proceso de seguridad nos deberá de salir lo siguiente:



Ahora tenemos que iniciar sesión en Azure Portal con la misma cuenta que hemos utilizado para logearnos anteriormente:

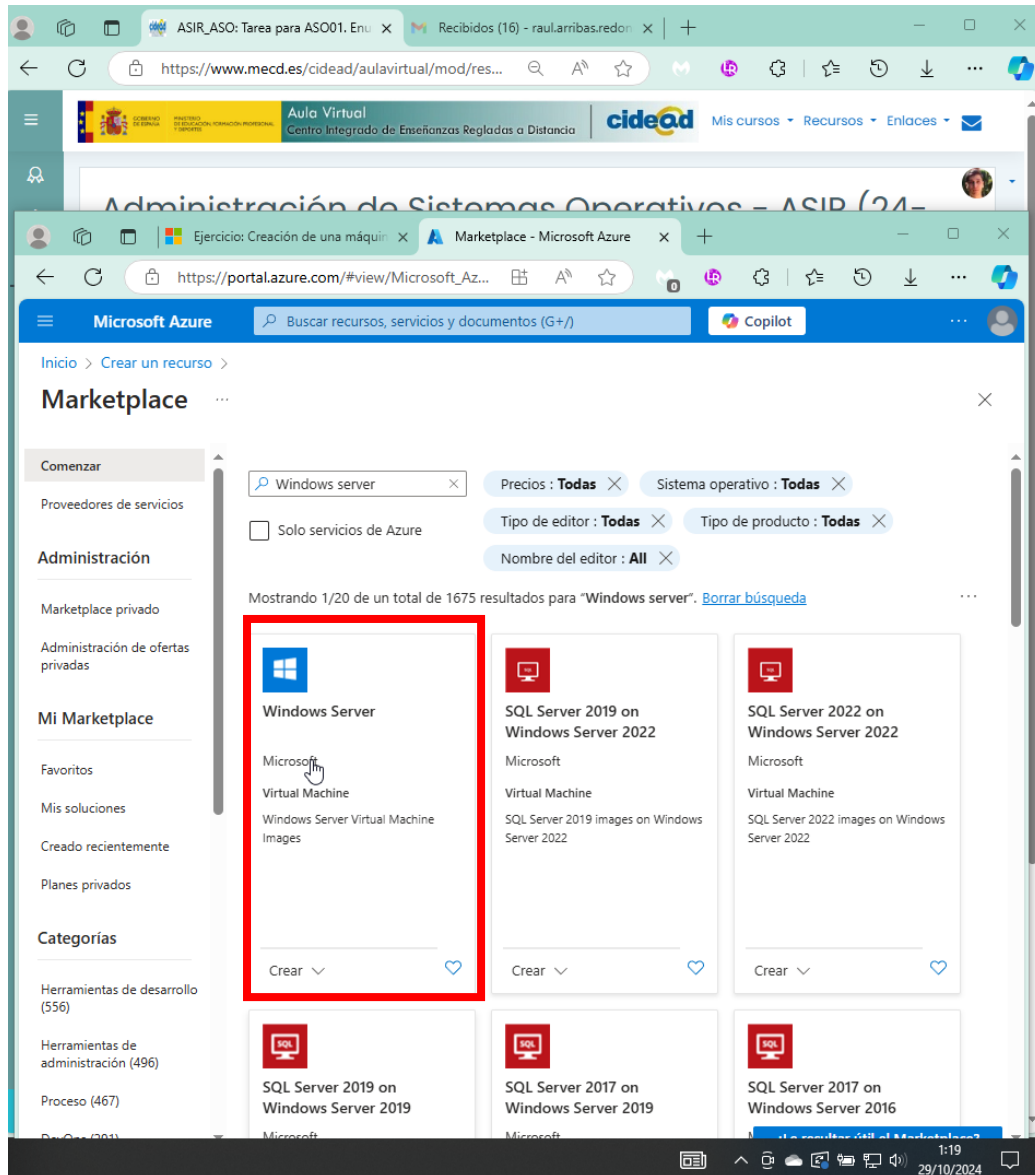
[Inicio - Microsoft Azure](#)

Una vez dentro seleccionamos **Crear recurso**



ADMINISTRACIÓN DE SERVICIOS DE DIRECTORIO

En el cuadro de búsqueda buscamos Windows Server y presionamos intro. Seleccionamos Windows server de Microsoft. Se nos abrirá un Panel.



En el panel seleccionamos Plan y elegimos **[Smalldisk] Windows server 2019 Datacenter** y seleccionamos **Crear**.

The screenshot shows the Microsoft Azure portal interface. At the top, there are browser tabs for 'ASIR_ASO: Tarea para ASO01: Enu...' and 'Recibidos (16) - raul.arribas.redon...'. The address bar shows 'https://www.mecd.es/cidead/aulavirtual/mod/res...'. Below this is a header for 'Aula Virtual' and 'cidead'. The main content area is titled 'Windows Server' and 'Microsoft | Virtual Machine'. It shows a rating of 4.8 (12 clasificaciones). The 'Plan' dropdown is set to '[smalldisk] Windows Server 2019 Dat...' and the 'Crear' button is highlighted with a red box. Below the plan selection, there are tabs for 'Información general', 'Planes', 'Información de uso y soporte técnico', and 'Clasificaciones + reseñas'. The 'Información general' tab is active, showing a description of Windows Server and a list of features. The 'Planes' tab is also visible, showing the selected plan.

Windows Server is the operating system that bridges on-premises environments with Azure services enabling hybrid scenarios and maximizing existing investments, including:

- The latest is security innovation including Secured-core to minimize risk from firmware vulnerabilities and advanced malware.
- Unique hybrid capabilities with Azure to extend your datacenter and maximize investments.
- File server security and performance increased with SMB AES-256 encryption and SMB on-the-fly compression.
- Azure Edition images with additional functionality optimized to run in Azure.
- Improvements to Windows container runtime such as cross-version compatibility and containerization tools for .NET, ASP.NET and IIS applications.

Available Images

Windows Server 2022 is the latest Long-Term Servicing Channel (LTSC) release with five years of mainstream support + five years of extended support. Choose the image that is right for your application needs.

- Server with Desktop Experience includes all roles and a graphical user interface (GUI).
- **Server Core** omits the GUI for a smaller OS footprint.
- Azure Edition with Desktop Experience - includes additional new functionality such as Hotpatch, SMB over QUIC, extended network for Azure, and is optimized to run in Azure.
- Azure Edition Core - includes additional new functionality such as Hotpatch, SMB over QUIC, extended network for Azure, and is optimized to run in Azure.

Elegimos los Aspectos básicos como se muestran en la imagen siguiente y le damos a Revisar y crear:

ASIR_ASO: Tarea para ASO01. Enu x Recibidos (16) - raul.arribas.redon x

https://www.mecd.es/cidead/aulavirtual/mod/res...

Aula Virtual
Centro Integrado de Enseñanzas Regladas a Distancia

cidead Mis cursos Recursos Enlaces

Administración de Sistemas Operativos - ASIR (24-

Ejercicio: Creación de una máquina x Crear una máquina virtual - Micro x

https://portal.azure.com/#create/Microsoft.s...

Microsoft Azure Buscar recursos, servicios y documentos (G+)

Copilot

Inicio > Crear un recurso > Marketplace > Windows Server >

Crear una máquina virtual

Al cambiar opciones básicas se pueden restablecer las selecciones realizadas. Revise todas las opciones antes de crear la máquina virtual.

Ayuda para crear una máquina virtual de bajo coste Ayuda para crear una VM optimizada para alta disponibilidad

Ayudarme a elegir el tamaño de VM adecuado para mi carga de trabajo

Seleccione los puertos de red de máquina virtual que son accesibles desde la red Internet pública. Puede especificar acceso de red más limitado o granular en la pestaña Red.

Puertos de entrada públicos * Ninguno ☒ Permitir los puertos seleccionados

Seleccionar puertos de entrada * RDP (3389)

Se bloquea todo el tráfico de Internet de forma predeterminada. Puede cambiar las reglas del puerto de entrada en la página VM > Redes.

Licencias

Ahorre hasta un 49 % con una licencia de su propiedad con Ventaja híbrida de Azure. Más información

¿Quiere usar una licencia de Windows Server existente? ☐

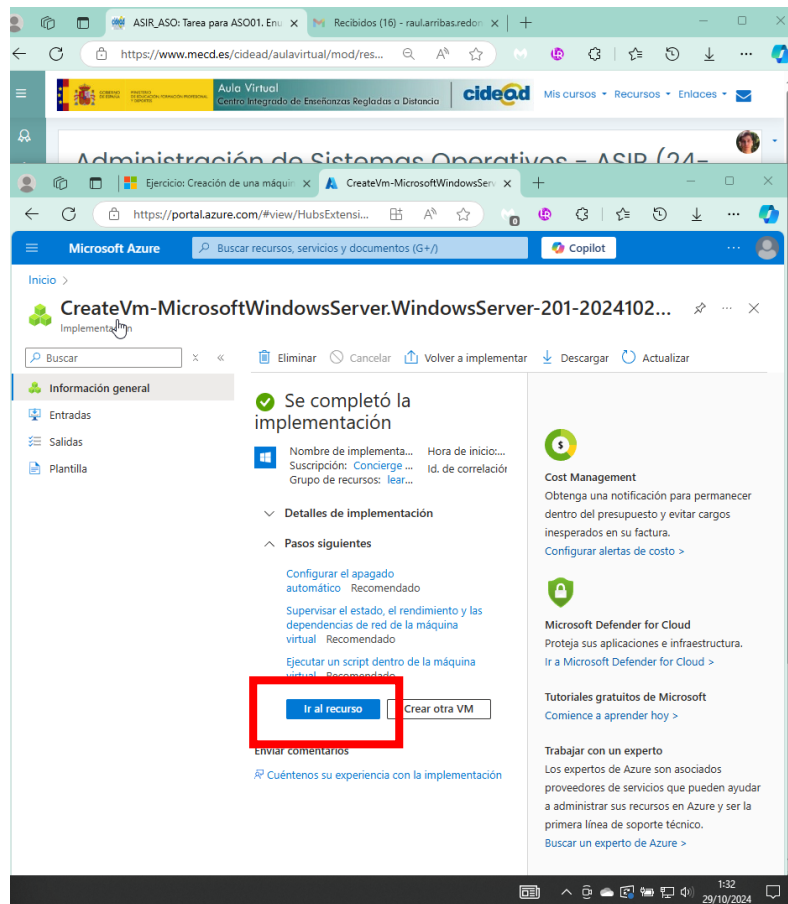
Revisar conformidad de la Ventaja híbrida de Azure

< Anterior Siguiente: Discos > **Revisar y crear** Enviar comentarios

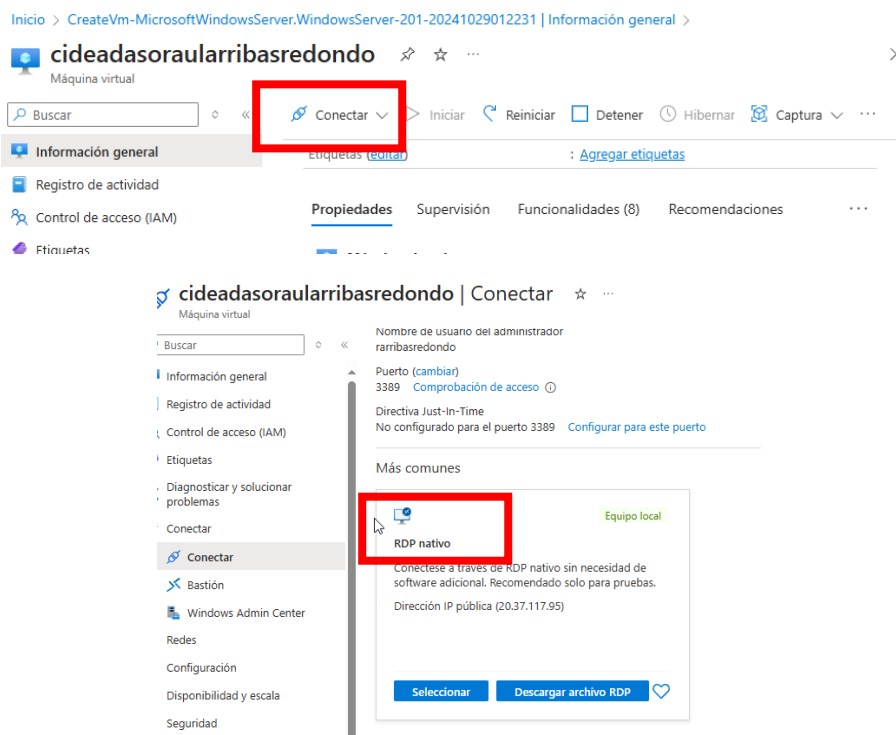
1:27 29/10/2024

ADMINISTRACIÓN DE SERVICIOS DE DIRECTORIO

Nos aparecerá un resumen de nuestra información y le damos a **Crear**. Nos empezará a crear la implementación, tardará unos minutos hasta que termine. **Seleccionamos Ir al Recurso**.

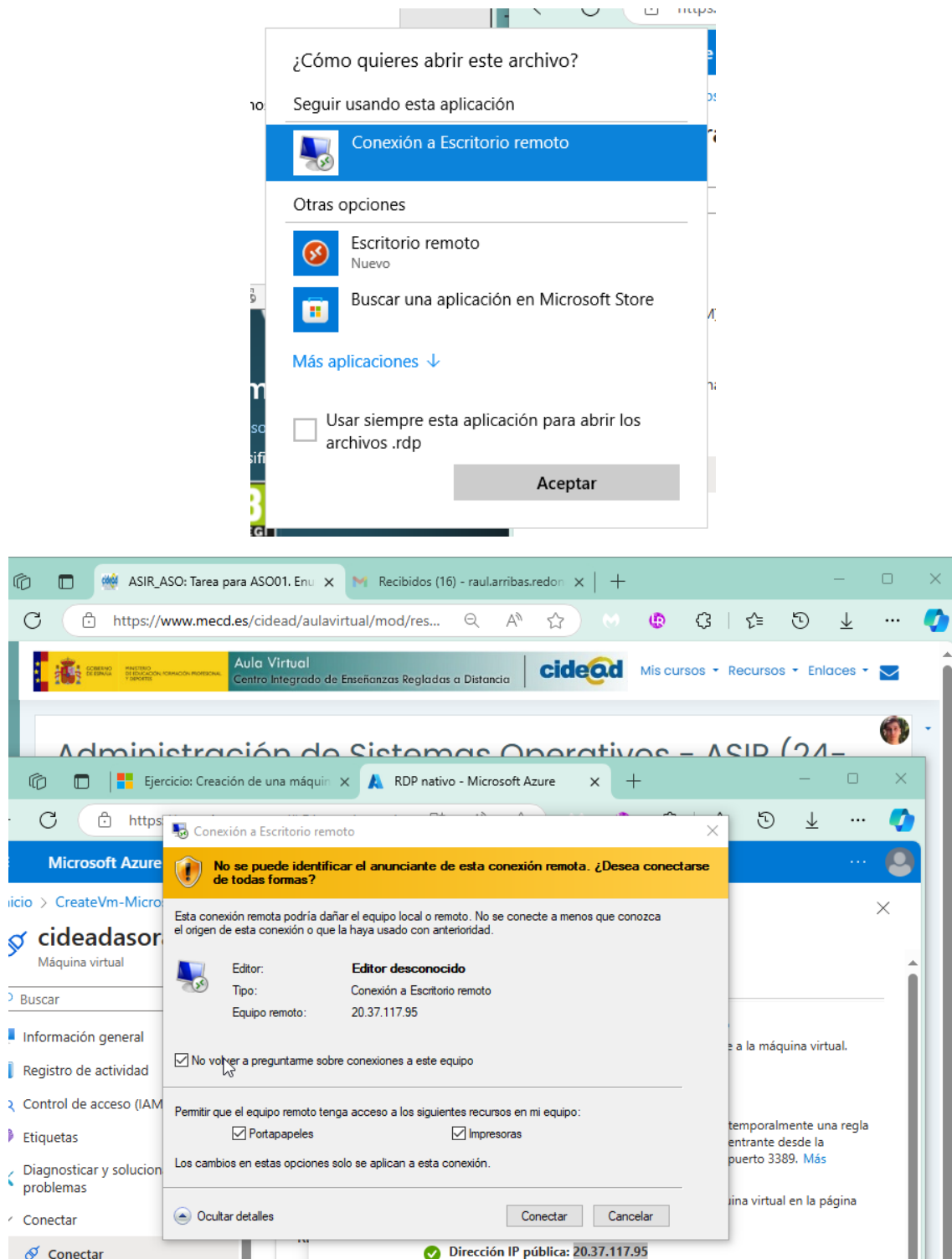


Una vez dentro del recurso le damos a **conectar**, nos conectamos mediante **RDP Nativo**.

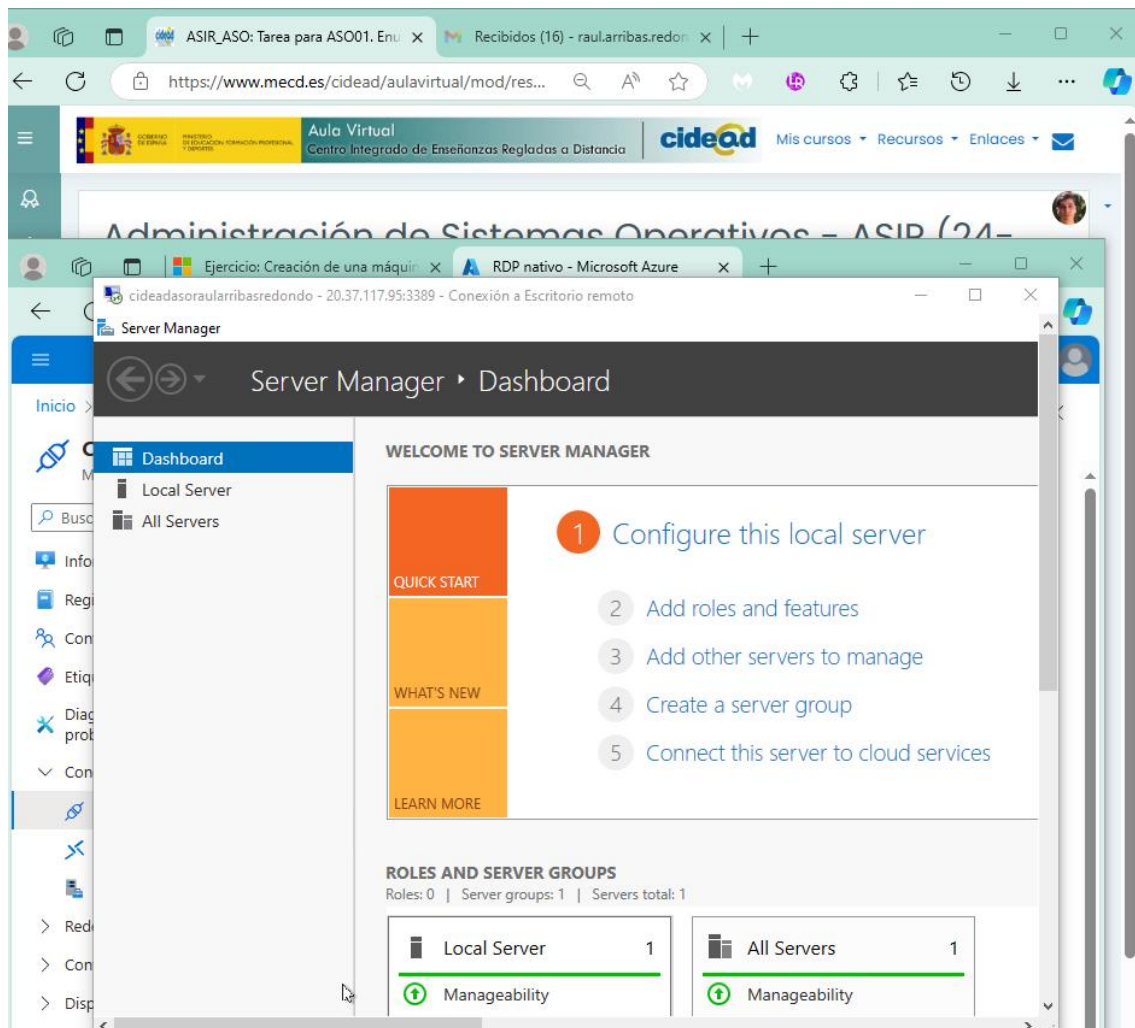


ADMINISTRACIÓN DE SERVICIOS DE DIRECTORIO

Para conectarnos seguimos los pasos, en mi caso vamos a descargarnos el Archivo RDP que nos deja descargar y lo ejecutamos con la aplicación de Windows de escritorio remoto.



Nos pedirá la contraseña y el usuario que creamos anteriormente junto con la maquina virtual.



Ya tenemos la maquina virtual funcionando.

5.2 Comparativa de los servicios en la nube mas conocidos

Aspecto	Microsoft Azure	Amazon Web Services (AWS)	Google Cloud Platform (GCP)
Facilidad de uso	Bien integrado con productos Microsoft como Office y Active Directory	Complejo al inicio, pero muy potente para proyectos avanzados	Interfaz sencilla y amigable, ideal para quienes usan Google Workspace
Precio	Pago por uso, planes reservados y suscripciones	Pago por uso con descuentos para instancias reservadas	Pago por uso con ahorros en instancias comprometidas
Capa gratuita	12 meses con máquinas B1S y servicios básicos gratuitos	Instancia t2.micro gratuita por 12 meses	Instancia f1-micro gratuita por 12 meses
Soporte de Sistemas Operativos	Windows y Linux	Windows y Linux	Windows y Linux
Almacenamiento	Azure Blob Storage, Files, y Discos	S3, EBS, Glacier	Cloud Storage, Filestore
Redes	VNet (Virtual Network)	VPC (Virtual Private Cloud)	VPC
Opciones para migración híbrida	Azure Arc y Azure Stack	AWS Outposts	Anthos y Kubernetes Engine
IA y Machine Learning	Azure Machine Learning	SageMaker	Vertex AI

Mercado de aplicaciones	Azure Marketplace	AWS Marketplace	Google Cloud Marketplace
Presencia global	60+ regiones	Más de 100 zonas de disponibilidad	35+ regiones, y sigue creciendo
Seguridad	Integración fuerte con Active Directory	Amplias herramientas de gestión de seguridad	Enfoque en identidad y permisos
Escalabilidad	Ideal para empresas con infraestructura Microsoft	Excelente para proyectos a gran escala	Perfecto para empresas que buscan agilidad

Para una PyME pequeña:

Google Cloud Platform (GCP) es una opción muy buena porque:

- Es fácil de usar y tiene un entorno sencillo que no complica las cosas.
- Ofrece servicios gratuitos por un año, incluyendo máquinas f1-micro sin coste.
- Funciona bien con las herramientas de Google, como Google Workspace, lo que facilita el trabajo en equipo.

Conclusión: Si la PyME necesita una solución simple y económica, **GCP** es una excelente opción.

Para una empresa en expansión internacional y con migración híbrida:

- **Microsoft Azure** es ideal si la empresa ya utiliza herramientas de Microsoft como **Office 365** o **Active Directory**, ya que se integra fácilmente. Además, **Azure Arc** y **Azure Stack** permiten combinar sistemas locales y en la nube sin problemas.
- **AWS** es una gran opción para empresas que necesiten **crecer rápido** y usar **muchos servicios especializados**. Con **AWS Outposts**, pueden llevar la infraestructura de AWS a sus centros de datos locales, algo útil para operaciones en varios países.

Conclusión:

- **Azure** es la mejor opción si la empresa ya depende de Microsoft.
- **AWS** es más adecuado para proyectos internacionales que necesiten flexibilidad y alta capacidad.

