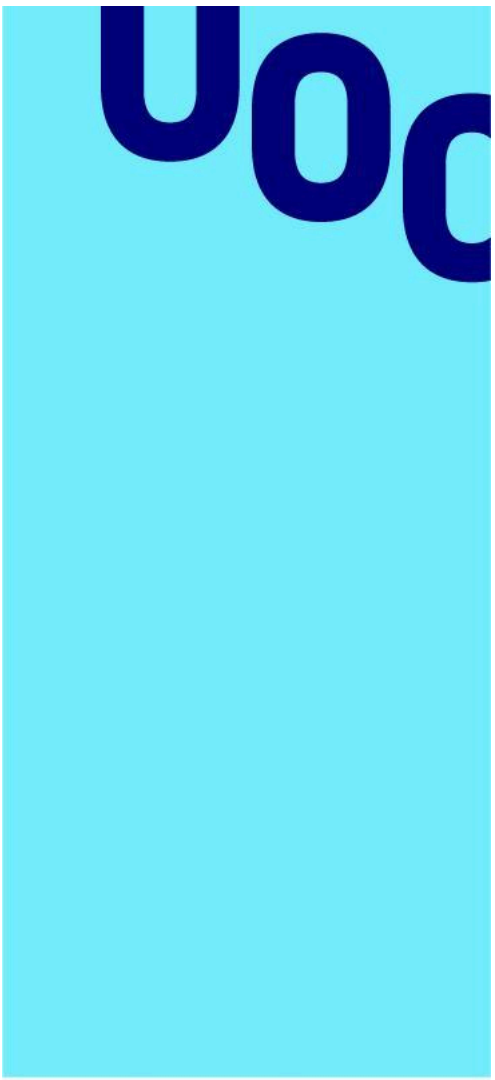
FP.048 - (P) Administración de servidores empresariales

Producto 2. Instalación, configuración y administración de servicios y recursos de red

Fast&Query

- Pau Cabanillas
- Vicent Melero
- Rubén Vicente Gilabert
- Andrei Vasiliu



Universitat Oberta de Catalunya

Descripción

Una vez diseñado el sistema, implementada la parte de infraestructura y el servicio de directorio instalado, ya estamos en posición de completar la implementación del servicio de directorio diseñado en el producto anterior.

Para ello, según el diseño realizado en el producto 1, crearemos las unidades organizativas y objetos necesarios e incorporaremos equipos con sistemas operativos propietarios y libres a nuestro sistema.

Con esto dejaremos un sistema informático con un servicio de directorio desde donde podremos gestionar y administrar todos los recursos y servicios que éste ofrece.

Objetivos

Implantar servicios de red configurando su acceso y seguridad, integrando sistemas operativos libre y propietarios y garantizando la operabilidad.

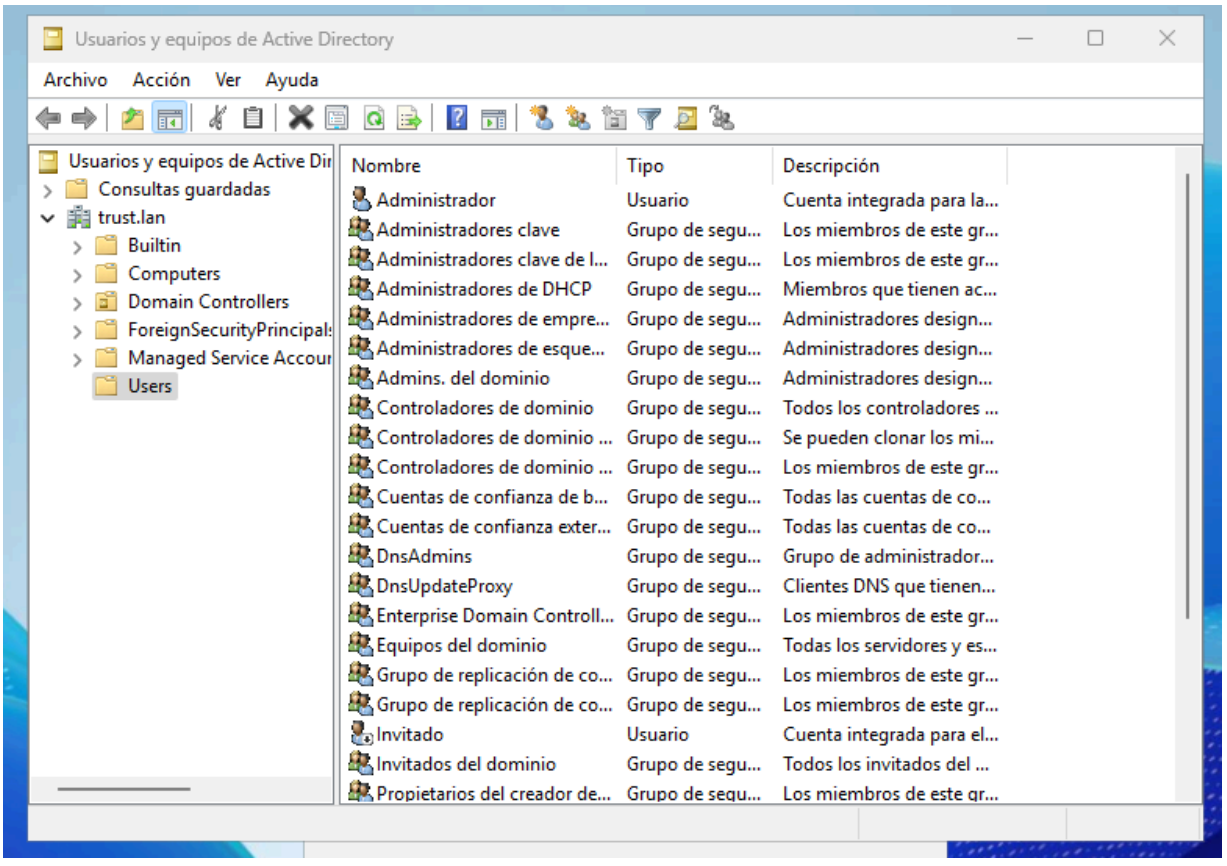
1. Introducción

En este producto se lleva a cabo la implementación completa de los servicios y recursos de red del dominio trust.lan, siguiendo el diseño establecido en el Producto 1. El objetivo es integrar sistemas operativos propietarios y libres, configurar unidades organizativas, usuarios, grupos y permisos, así como implementar servicios como carpetas compartidas y el servidor de impresión centralizado.

2. Bloque 1 – Implementación de la estructura del servicio de directorio

2.1 Criterios de diseño

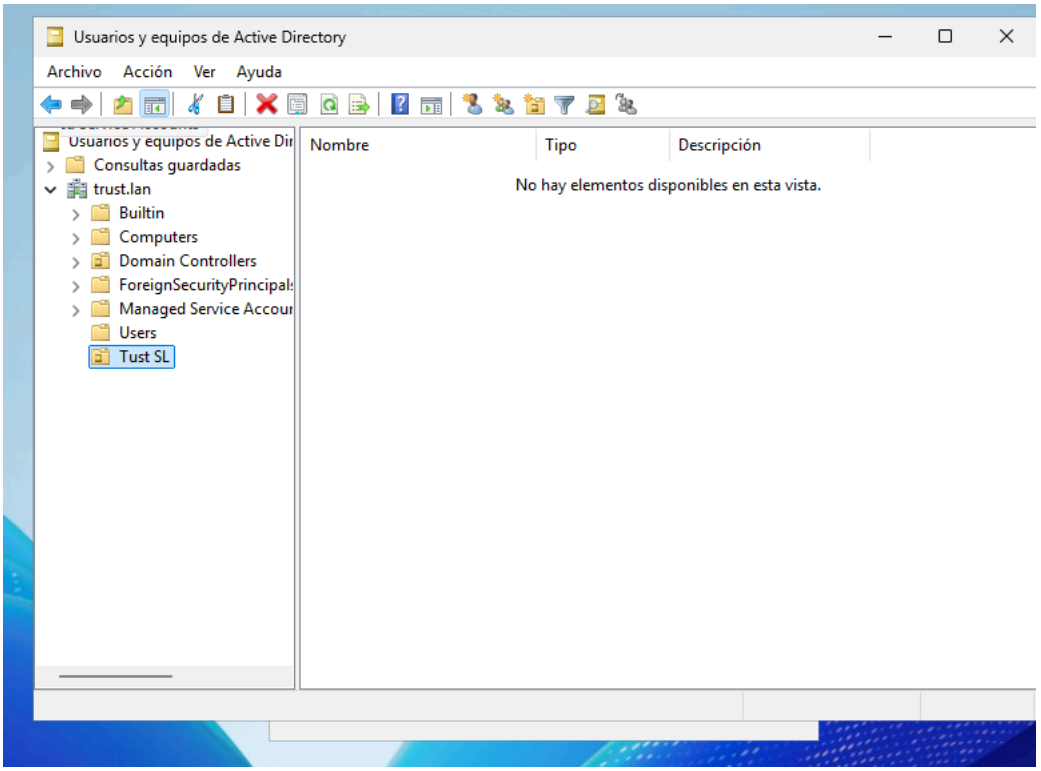
La estructura del directorio se ha diseñado en base a la organización real de la empresa, separando usuarios, grupos y equipos, y permitiendo la delegación de tareas, aplicación de GPOs y escalabilidad. Se han creado OUs por departamentos y se han protegido contra eliminación accidental.



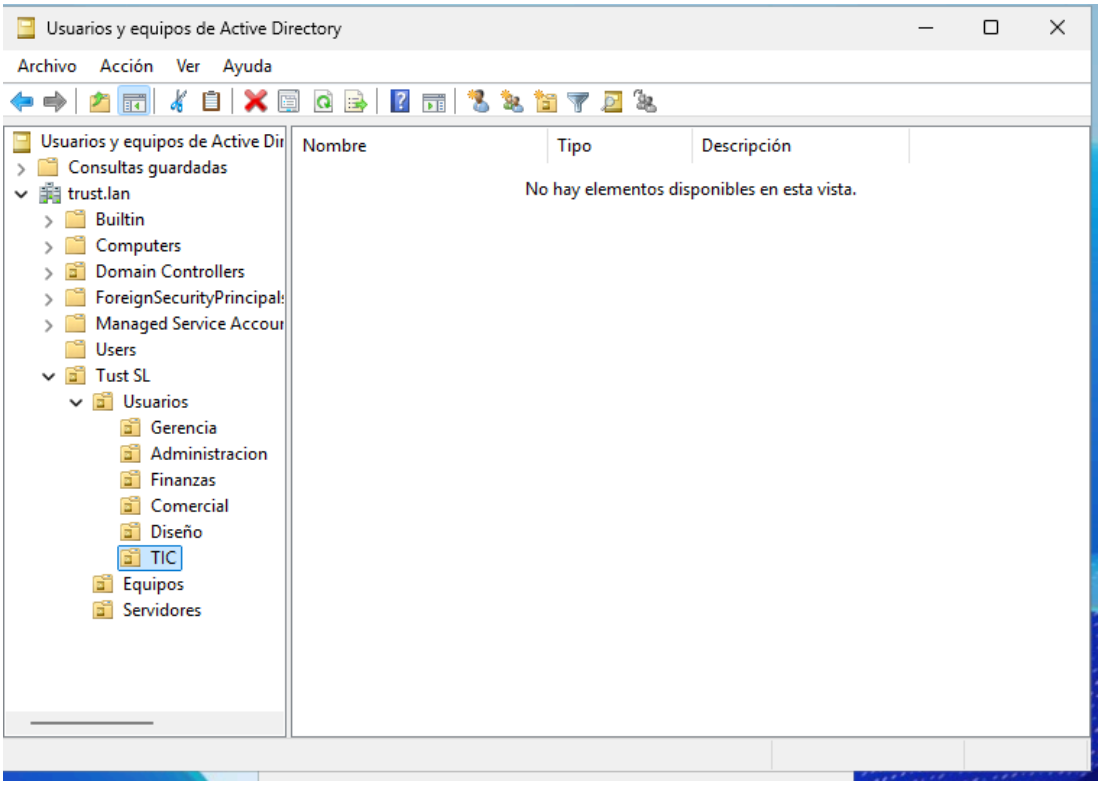
Se accede a la consola *Usuarios y equipos de Active Directory* desde el servidor principal para iniciar la creación de la estructura organizativa del dominio **trust.lan**.

2.2 Objetos creados

• Unidades Organizativas: Gerencia, Administración y Finanzas, Comercial, Diseño, TIC, Equipos.
• Sub-OUs para equipos Windows y Linux.
• Grupos globales de seguridad de cada departamento.
• Usuarios con contraseña inicial Trust2025*.



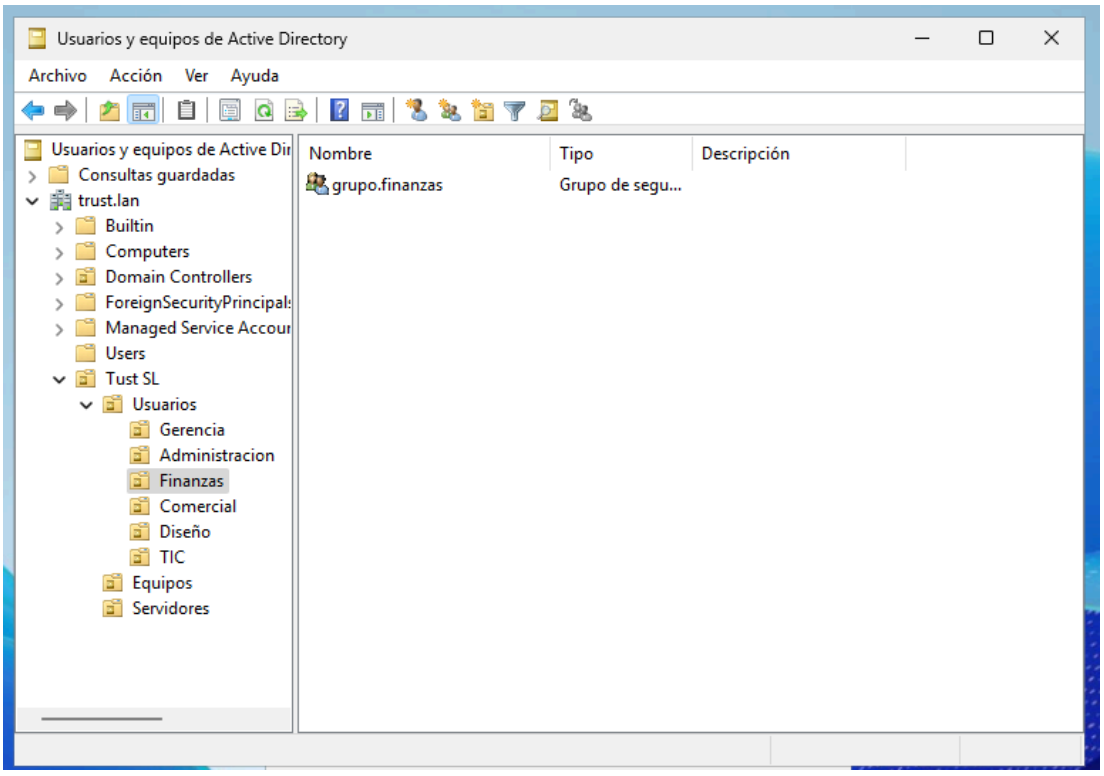
Se crea la unidad organizativa principal *Trust SL*, que actuará como contenedor global de todos los objetos de la empresa.

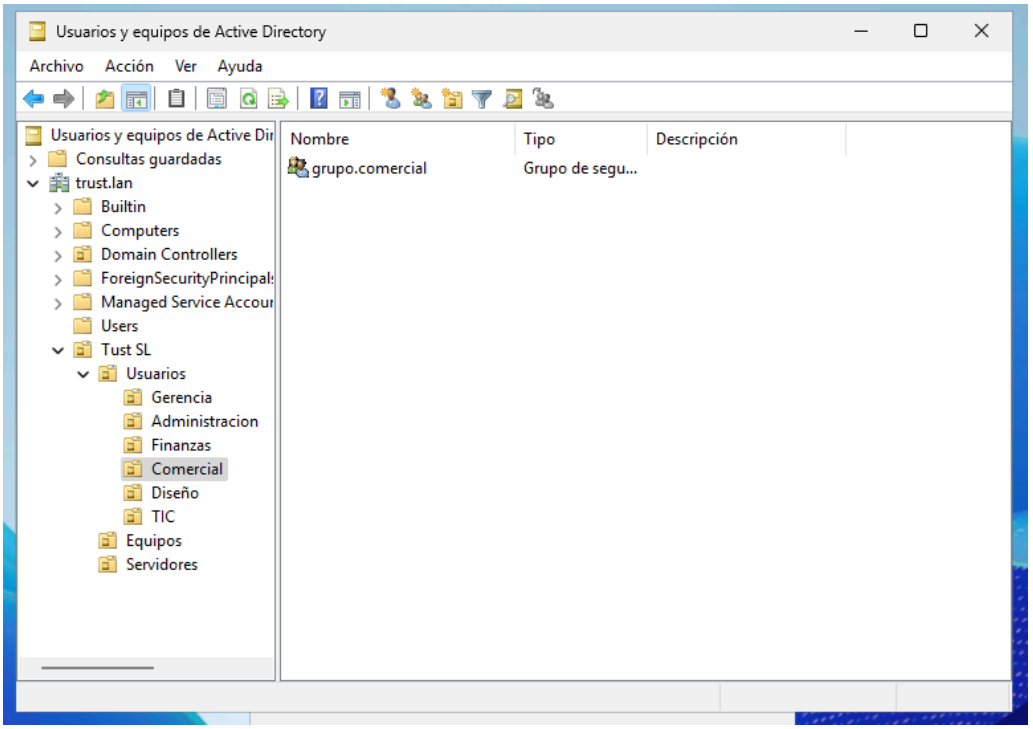


Se generan las Unidades Organizativas que reflejan la estructura de la empresa. Esta jerarquía permite aplicar políticas y delegar permisos por departamento.

2.3 Ejemplo: creación de la OU Administración y Finanzas

Desde Usuarios y Equipos de Active Directory → Nuevo → Unidad Organizativa. Se crea la OU y se activa la protección de eliminación accidental.

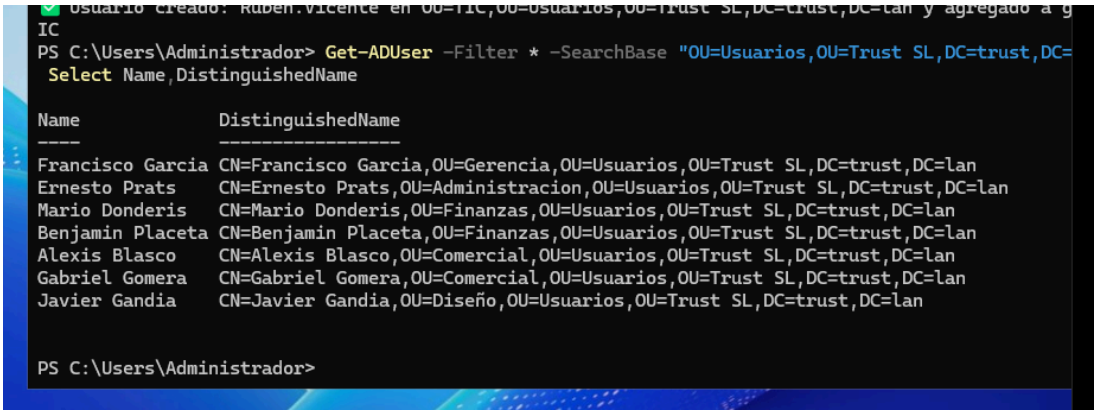




Se crean los grupos de seguridad globales que agrupan a los miembros de cada departamento.
Estos grupos se utilizarán para asignar permisos sobre recursos de red de forma centralizada.

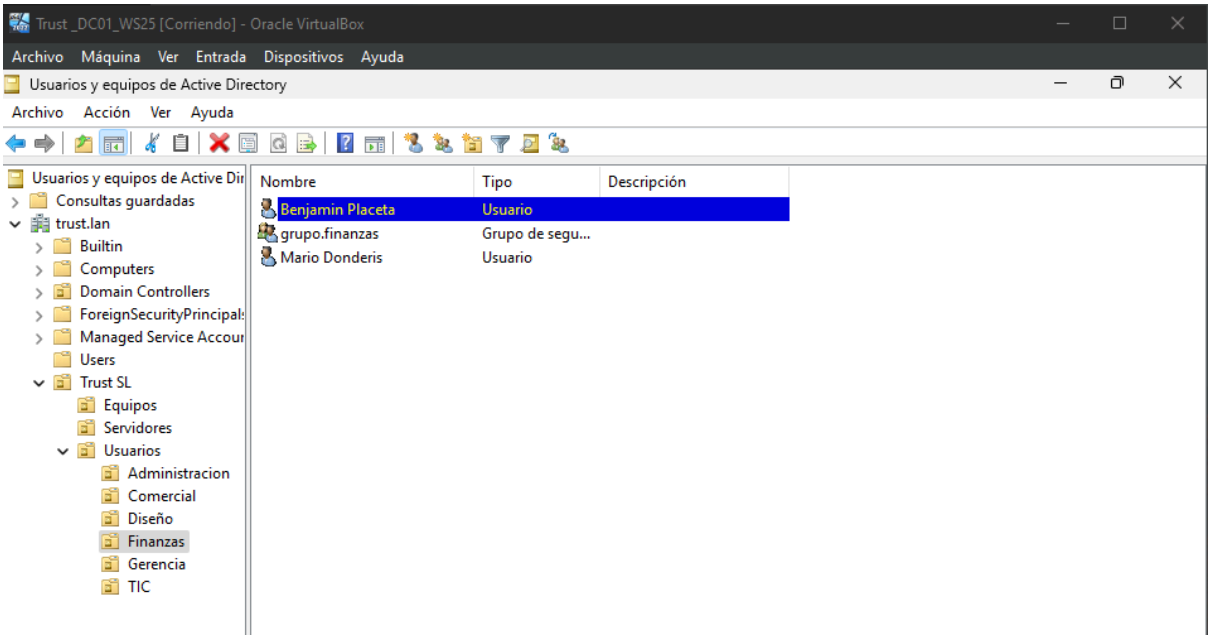
2.4 Automatización mediante PowerShell

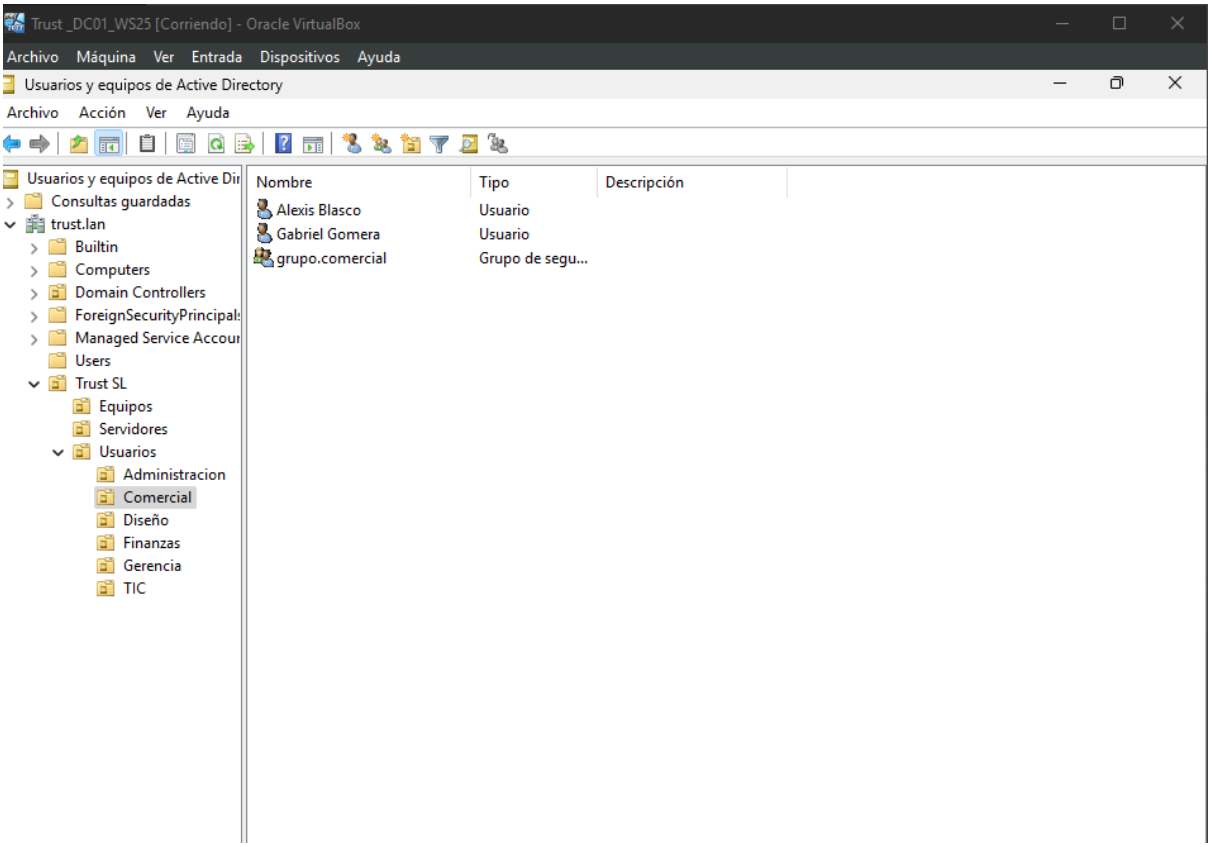
Se empleó un script para crear OUs, grupos y usuarios, garantizando homogeneidad.



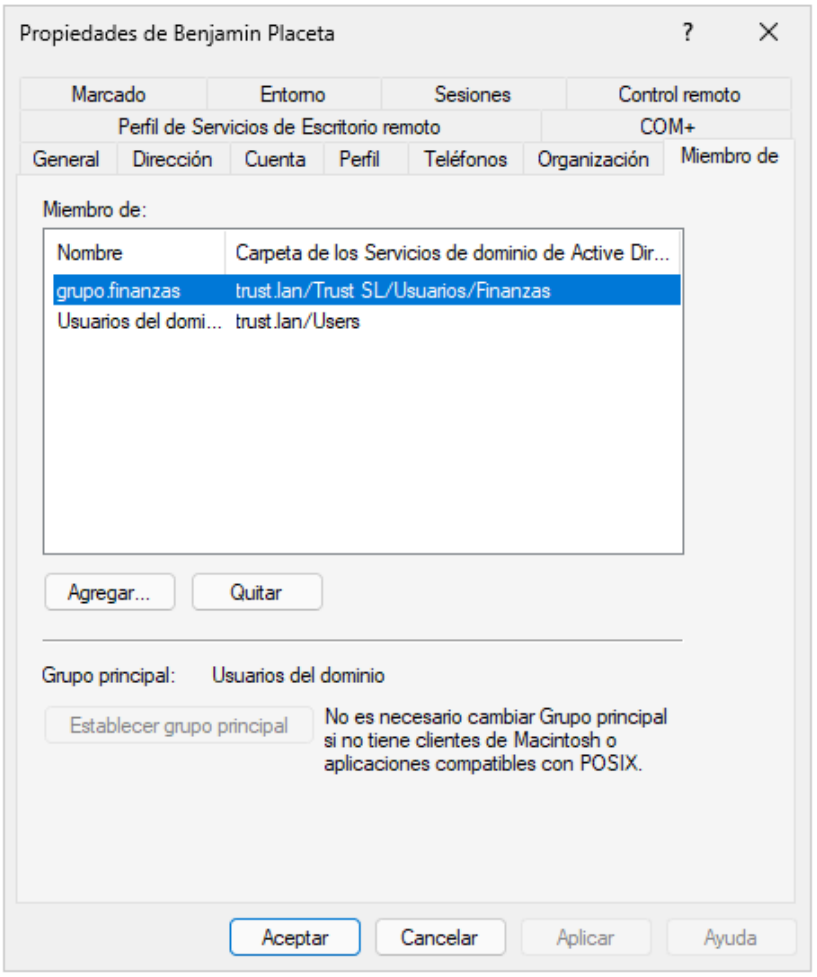
Se ejecuta el script de PowerShell corregido tras la validación de las rutas de las Unidades Organizativas.
El resultado muestra la creación exitosa de los ocho usuarios dentro de sus OUs correspondientes y su asociación automática con los grupos de cada departamento.

Se verifica mediante PowerShell que todos los usuarios se han creado correctamente dentro de las Unidades Organizativas del dominio *trust.lan*.





etc



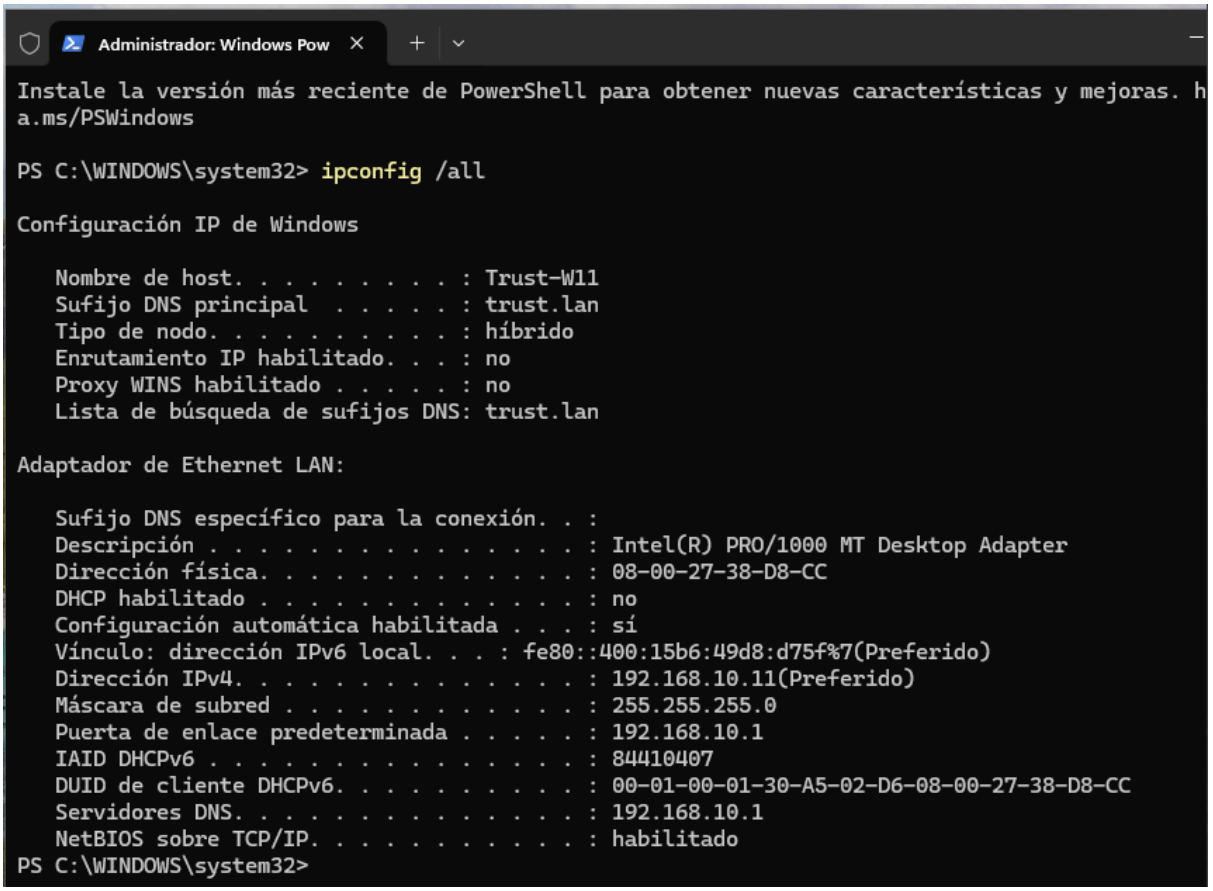
A través de la consola de Active Directory se confirma la correcta ubicación de los usuarios en sus departamentos y su pertenencia a los grupos de seguridad globales.
Esta estructura garantiza una gestión ordenada y facilita la asignación de permisos en los recursos compartidos.

Conclusión del Bloque 1

Tras completar la creación de las OUs, grupos y usuarios, la estructura del dominio *trust.lan* refleja fielmente la organización de la empresa Trust SL. Esta configuración servirá de base para aplicar políticas, permisos y recursos en los bloques siguientes del proyecto.

3. Bloque 2 – Unión de un equipo Windows 11 al dominio

Se configuró el cliente Windows 11 para usar como DNS la IP del DC (192.168.10.1). Tras comprobar la resolución de trust.lan mediante ping, se unió el equipo al dominio a través de Configuración → Acceso laboral. Tras el reinicio, se pudo iniciar sesión con un usuario del dominio.



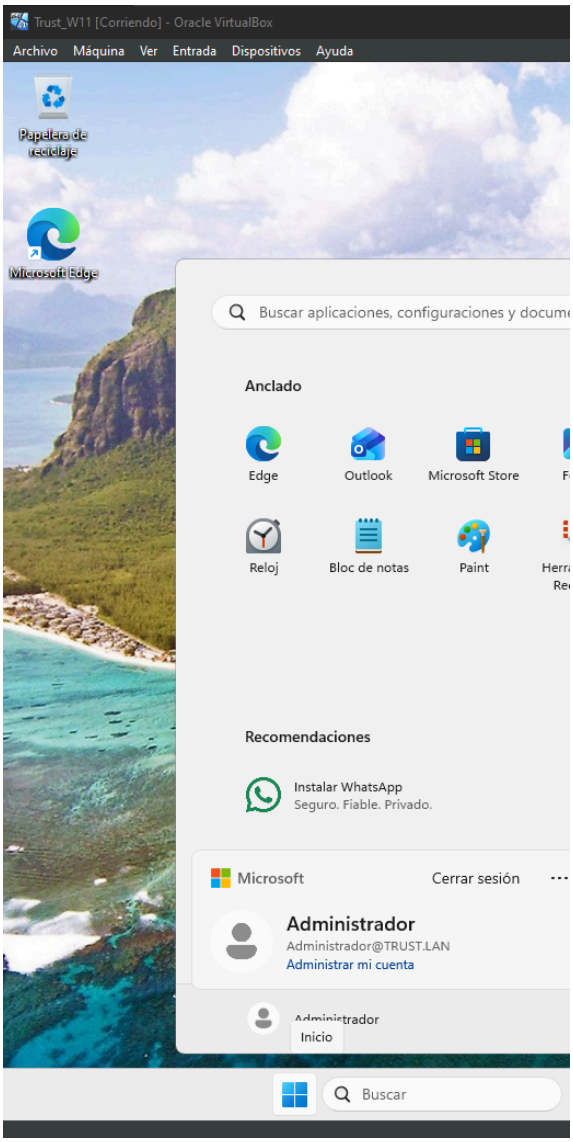
Se comprueba la configuración de red del equipo Windows 11, confirmando que pertenece a la red interna del dominio. El servidor DNS apunta al controlador de dominio (192.168.10.1), permitiendo la resolución correcta de *trust.lan* y la autenticación mediante Kerberos.

Resultado del comando nltest /dsgetdc:trust.lan.

El comando nltest /dsgetdc:trust.lan confirma que el equipo Windows 11 detecta correctamente al controlador de dominio DC-TRUST-01.trust.lan. Esto valida la comunicación entre el cliente y el servicio de directorio a través de DNS y LDAP.

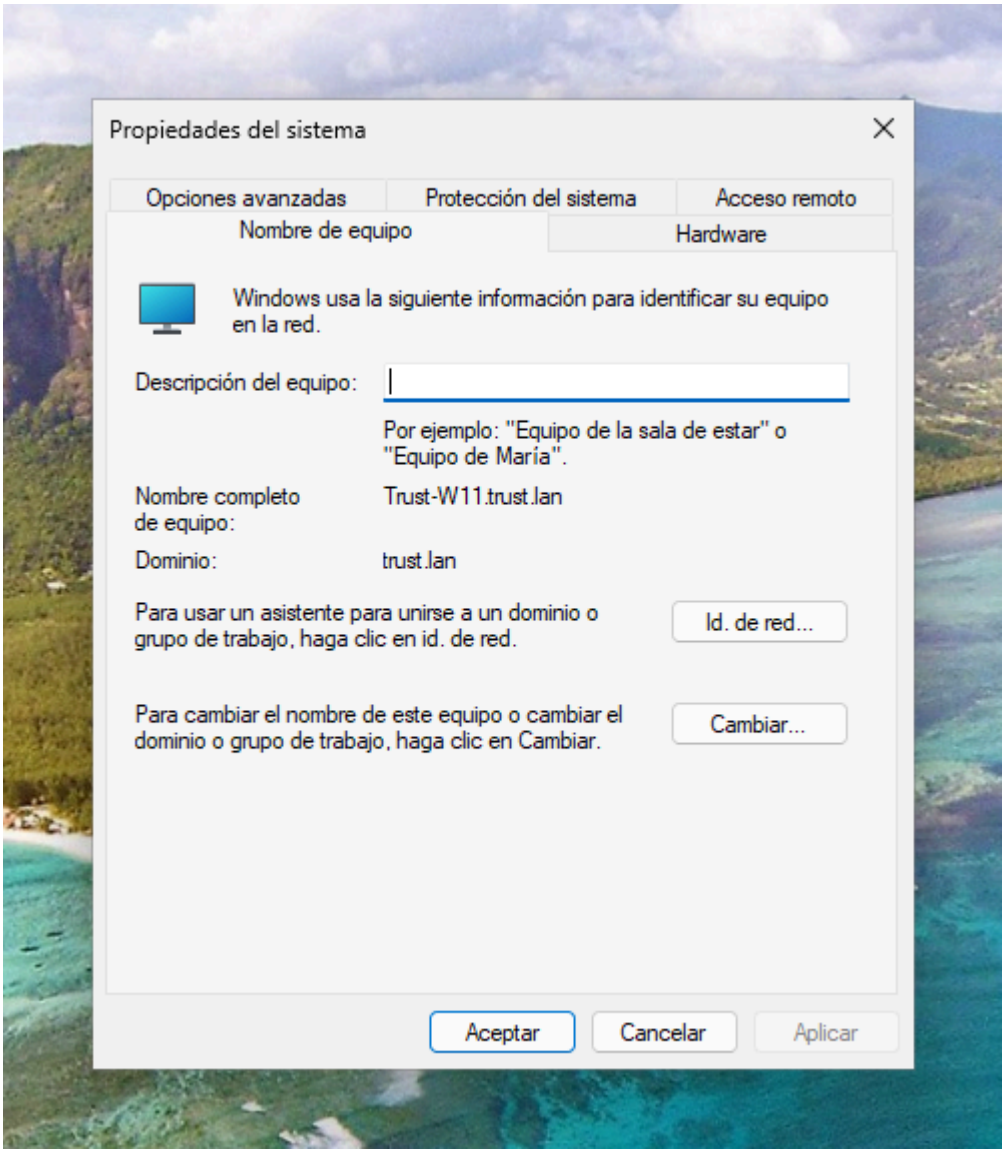
```
El comando se completó correctamente
PS C:\WINDOWS\system32> w32tm /query /status
Indicador de salto: 0(ninguna advertencia)
Capa: 2 (referencia secundaria - sincronizada mediante (S)NTP)
Precisión: -23 (119.209ns por tick)
Demora de raíz: 0.0014839s
Dispersión de raíz: 11.9015155s
Id. de referencia: 0xC0A80A01 (IP de origen:  192.168.10.1)
Última sincronización de hora correcta: 12/11/2025 18:41:45
Origen: DC-TRUST-01.trust.lan
Intervalo de sondeo: 10 (1024s)

PS C:\WINDOWS\system32>
```

La sincronización horaria entre el cliente y el controlador de dominio es esencial para la autenticación Kerberos. El equipo Windows 11 toma la hora del servidor DC-TRUST-01, garantizando la validez de los tickets Kerberos y evitando errores de inicio de sesión.



El equipo Windows 11 se une satisfactoriamente al dominio y permite el inicio de sesión con credenciales de dominio (Administrador@trust.lan).

Este proceso confirma que el cliente propietario está correctamente integrado en el entorno de Active Directory y puede autenticarse mediante el servicio de directorio.



Desde las propiedades del sistema se verifica que el equipo pertenece al dominio **trust.lan**, lo que permite aplicar políticas centralizadas y compartir recursos en red.

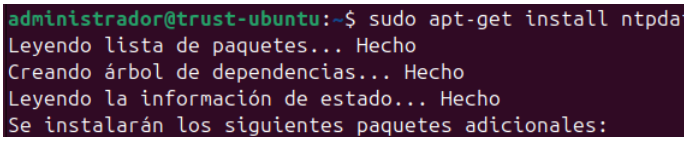
Conclusión del Bloque 2

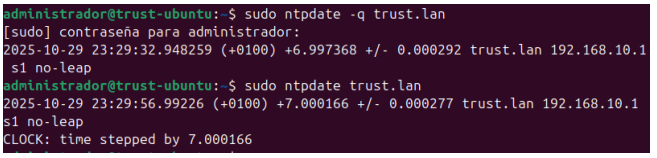
Tras la incorporación del equipo Windows 11 al dominio, se confirma la correcta comunicación con el servidor de directorio y la autenticación de usuarios mediante Kerberos. Este proceso sienta las bases para el acceso seguro a recursos compartidos y la aplicación de directivas de grupo en el entorno corporativo.

4. Bloque 3 – Unión de Ubuntu al dominio

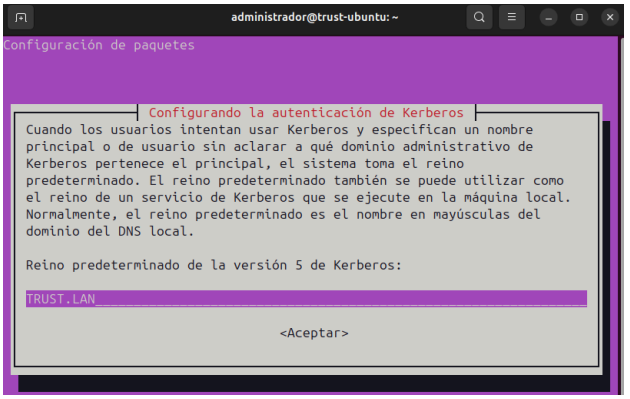
Se instalaron paquetes: samba, winbind, krb5-user, libpam-winbind, libnss-winbind.
Se configuraron los archivos /etc/krb5.conf, /etc/samba/smb.conf y /etc/nsswitch.conf.
La unión al dominio se realizó mediante sudo net ads join -U Administrador.

Instalar NTPDATE
sudo apt-get install ntpdate
sudo ntpdate -q trust.lan
sudo ntpdate trust.lan





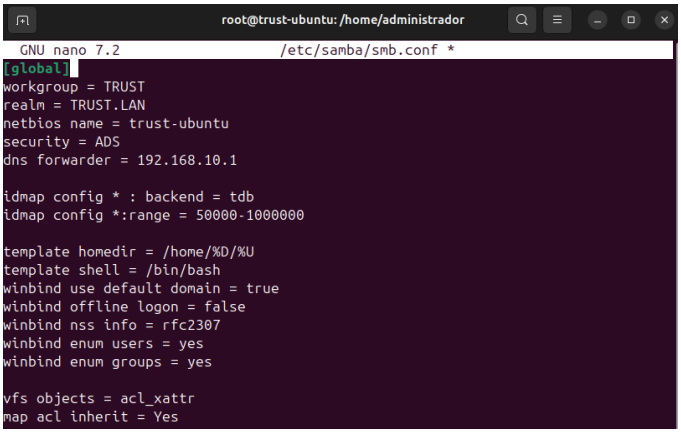
Instalar paquetes necesarios
sudo apt-get install samba krb5-config krb5-user winbind libpam-winbind libnss-winbind



Comprobar autenticación en el servidor de Kerberos mediante el administrador de usuarios
kinit Administrador@TRUST.LAN

Mover archivo smb.conf y crear copia de seguridad
sudo mv /etc/samba/smb.conf /etc/samba/smb.conf.initial

sudo nano /etc/samba/smb.conf



Reiniciar todos los daemons de samba
sudo systemctl restart smbd nmbd

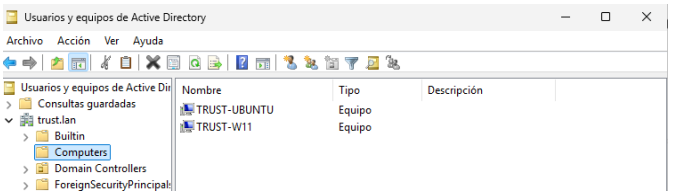
Habilitar los servicios de samba
sudo systemctl enable smbd nmbd

```
root@trust-ubuntu:/home/administrador# sudo systemctl restart smbd nmbd
root@trust-ubuntu:/home/administrador# sudo systemctl enable smbd nmbd
Synchronizing state of smbd.service with SysV service script with /usr/lib/syste
md/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable smbd
Synchronizing state of nmbd.service with SysV service script with /usr/lib/syste
md/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable nmbd
root@trust-ubuntu:/home/administrador#
```

Unir Ubuntu Desktop a SAMBA AD DC
sudo net ads join -U Administrador

```
root@trust-ubuntu:/home/administrador# sudo net ads join -U Administrador
Password for [TRUST\Administrador]:
Using short domain name -- TRUST
Joined 'TRUST-UBUNTU' to dns domain 'trust.lan'
No DNS domain configured for trust-ubuntu. Unable to perform DNS Update.
DNS update failed: NT_STATUS_INVALID_PARAMETER
root@trust-ubuntu:/home/administrador#
```

Vemos como en Usuarios y equipos de Active Directory aparece nuestro equipo TRUST-UBUNTU



sudo nano /etc/nsswitch.conf

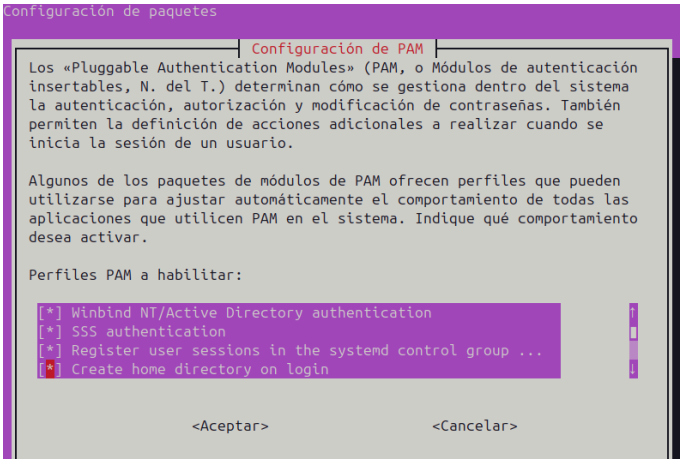
```
 GNU nano 7.2                    /etc/nsswitch.conf *
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the `glibc-doc-reference' and `info' packages installed, try:
# `info libc "Name Service Switch"' for information about this file.

passwd:         compat winbind
group:          compat winbind
shadow:         compat winbinf
gshadow:        files systemd

hosts:          files dns
networks:       files

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

netgroup:       nis sss
automount:  sss
```

Reinicar servicio winbind
sudo systemctl restart winbind

Listar usuarios y grupos del dominio.
wbinfo -u

```
root@trust-ubuntu:/home/administrador# sudo systemctl restart winbind
root@trust-ubuntu:/home/administrador# wbinfo -u
administrador
invitado
```

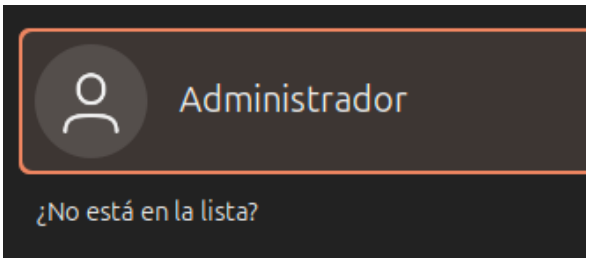
Configurar pam-auth-update para autenticarnos con cuentas de dominio y que se creen automáticamente los directorios.
sudo pam-auth-update



Editar el archivo /etc/pam.d/common-account para crear automáticamente directorios.
nano /etc/pam.d/common-account

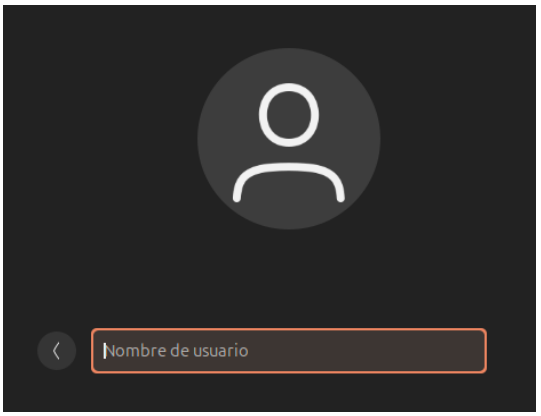
```
 GNU nano 7.2                  /etc/pam.d/common-account *
# only deny service to users whose accounts are expired in /etc/shadow.
#
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either 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 new_authtok_reqd=done default=ignore]        pam_winbind.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)
account sufficient                      pam_localuser.so
account [default=bad success=ok user_unknown=ignore]    pam_sss.so
# end of pam-auth-update config
session    required    pam_mkhomedir.so    skel=/etc/skel/    umask=0022
```

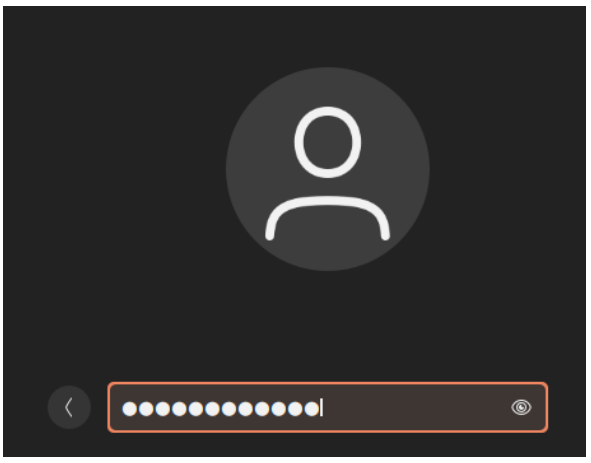
Pulsamos en ¿No está en la lista?



Ingresamos las credenciales del usuario deseado en nuestro caso ruben.vicente@trust.lan

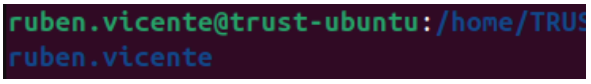
junto con su contraseña





Mensaje de Ubuntu al ser la primera vez que iniciamos sesión.

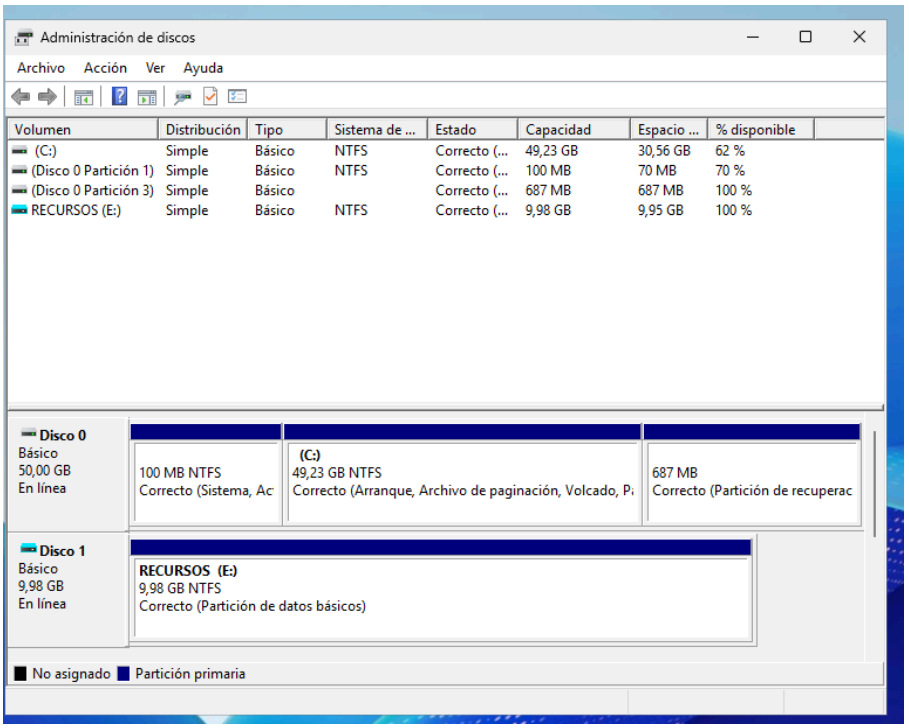
Al iniciar sesión se crean nuestras carpetas personales dentro de la máquina Ubuntu



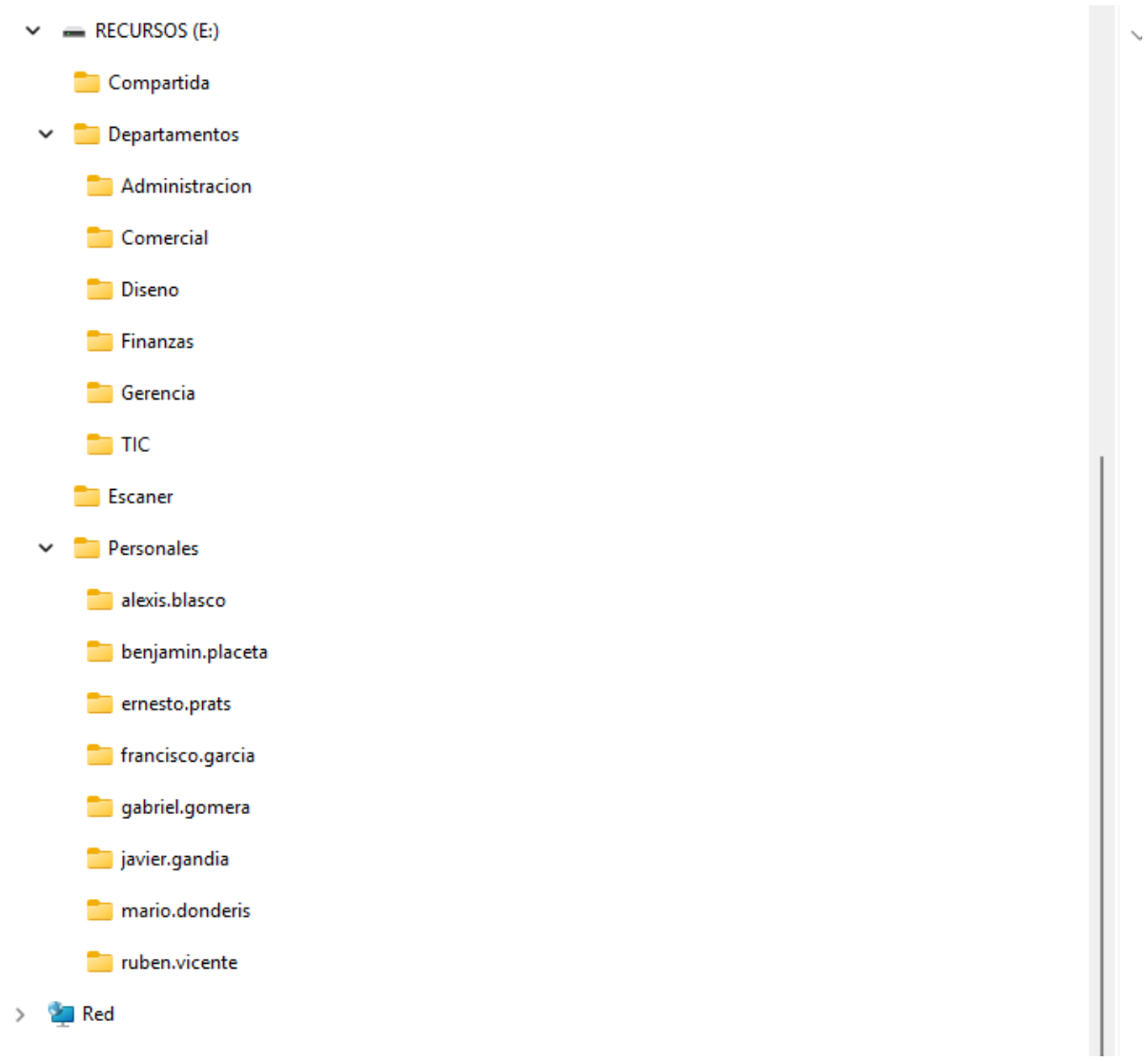
Estos resultados confirman que la integración con el servicio de directorio es completa y funcional.

5. Bloque 4 – Disco de red y carpetas compartidas

Se añadió un segundo disco virtual E: en el DC. En él se creó la estructura: Administración y Finanzas, Comercial, Diseño, TIC, Gerencia, Pública, Recursos y Personales.



Captura del Administrador de discos mostrando el nuevo disco E: creado y formateado como NTFS. Se agrega un nuevo disco virtual VHD al servidor principal, destinado a almacenar las carpetas compartidas del dominio. El volumen se inicializa en formato NTFS bajo la letra **E:** y se nombra *RECURSOS*, sirviendo como disco compartido central.



En el disco **E:** del servidor se crea la estructura completa de carpetas correspondiente a los recursos compartidos del dominio.

Se incluyen los directorios departamentales (Administración, Finanzas, Comercial, Diseño, Gerencia y TIC), junto con carpetas comunes (*Compartida* y *Escáner*) y un área *Personales* con subcarpetas individuales para cada usuario.

Esta jerarquía refleja la estructura organizativa de la empresa *Trust SL* y facilita la gestión de permisos centralizados por grupo o usuario.

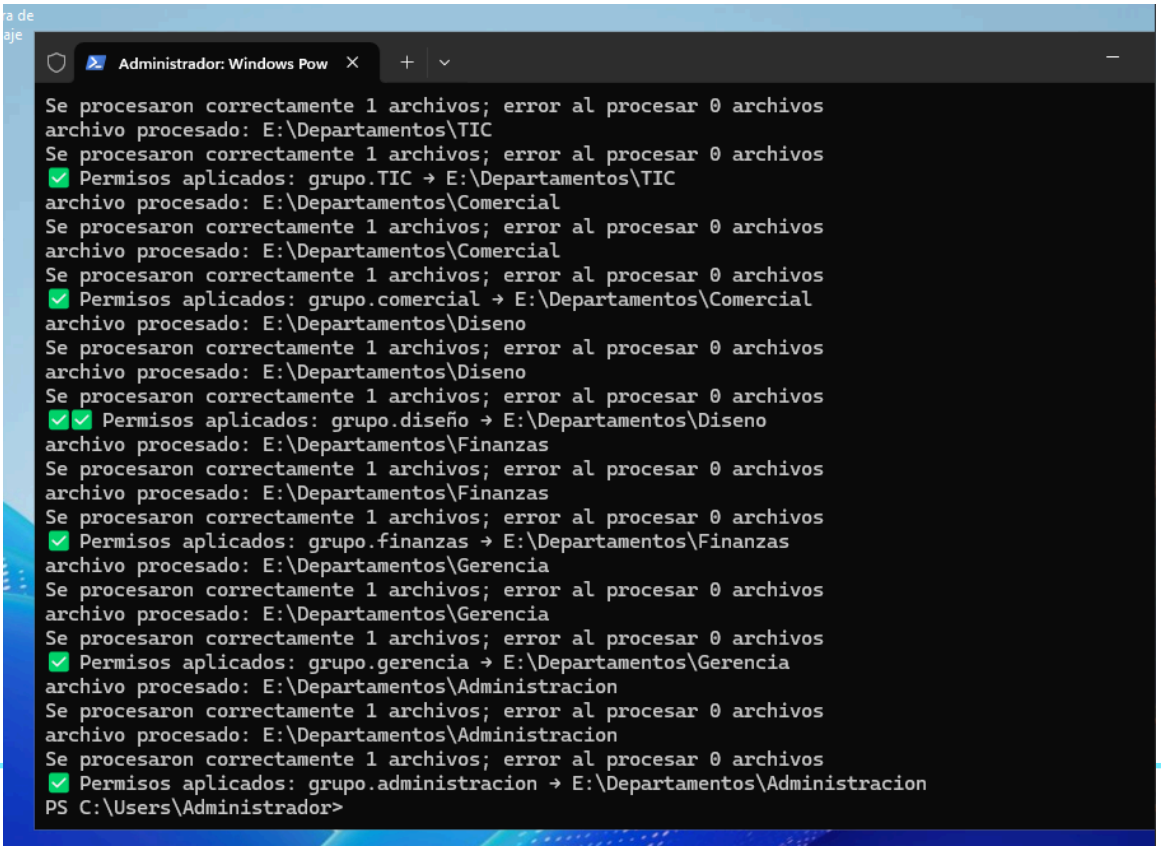
Se genera de forma automatizada la estructura de carpetas personales para cada usuario dentro del directorio **E:\Personales**.

El script de PowerShell crea una carpeta para cada cuenta del dominio, siguiendo la nomenclatura *nombre.apellido*, garantizando una correspondencia directa entre las cuentas de Active Directory y sus directorios personales en el servidor. Esta automatización permite ahorrar tiempo y mantener una estructura uniforme y ordenada.

5.1 Configuración de recursos compartidos SMB

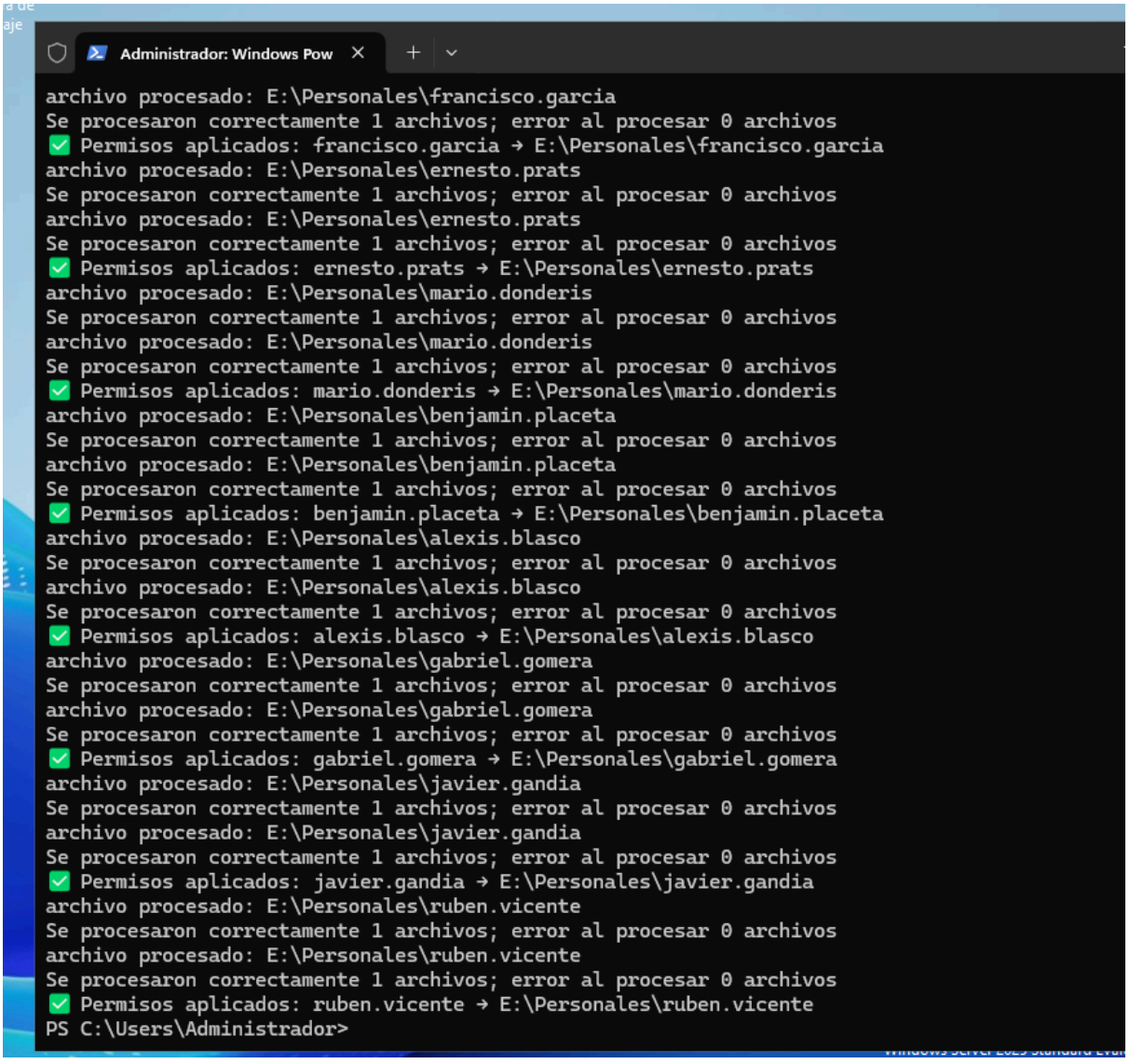
Desde Administrador del servidor → Servicios de archivos y almacenamiento → Recursos compartidos. Para cada carpeta se creó un recurso compartido SMB y se personalizaron permisos NTFS deshabilitando herencia.

Asignación automática de permisos NTFS



Se aplican automáticamente los permisos NTFS a las carpetas del dominio mediante un script de PowerShell. El script asigna a cada grupo departamental control total sobre su carpeta y crea un grupo global (*grupo.todos*) con permisos de modificación en las carpetas *Compartida* y *Escáner*. Este método garantiza que los permisos se gestionen desde Active Directory, evitando asignaciones manuales y mejorando la seguridad y coherencia de la red corporativa.

Asignación automática de permisos NTFS para carpetas personales:

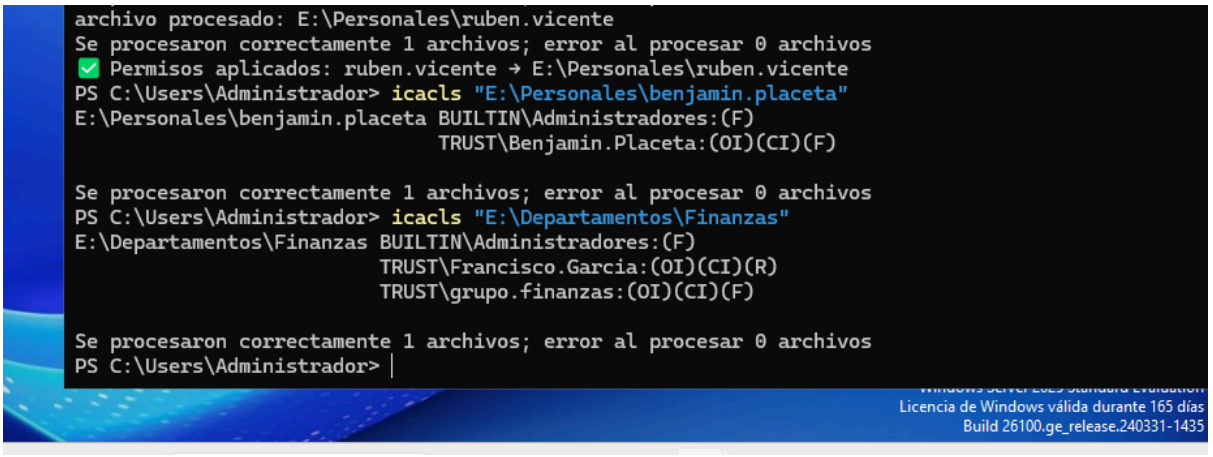


Se aplican automáticamente los permisos NTFS en las carpetas personales mediante PowerShell.

Cada usuario del dominio obtiene control total sobre su carpeta individual dentro de **E:\Personales**, eliminando la herencia de permisos y garantizando la privacidad de su espacio de trabajo. Este proceso automatizado asegura una configuración coherente, rápida y alineada con la política de seguridad del sistema.

5.3 Ejemplo práctico – Usuario Benjamín Placeta

Benjamín pertenece a TIC y Administración y Finanzas. Al iniciar sesión en Windows 11, se mapean automáticamente sus unidades de red y puede crear archivos en las carpetas de sus departamentos.



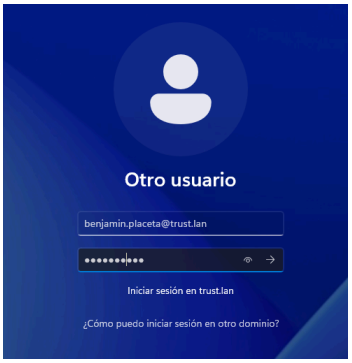
En la carpeta *E:\Personales\benjamin.placeta*, únicamente el usuario *Benjamín Placeta* y los administradores tienen control total. En *E:\Departamentos\Finanzas*, el grupo *grupo.finanzas* dispone de control total mientras que el gerente *Francisco García* cuenta únicamente con permisos de lectura. Esta verificación demuestra la correcta aplicación de la política de seguridad y la segmentación de acceso por departamentos.

Se verifican los permisos NTFS mediante el comando icacls, confirmando que cada carpeta posee los permisos correctos según la matriz de control de acceso del dominio.

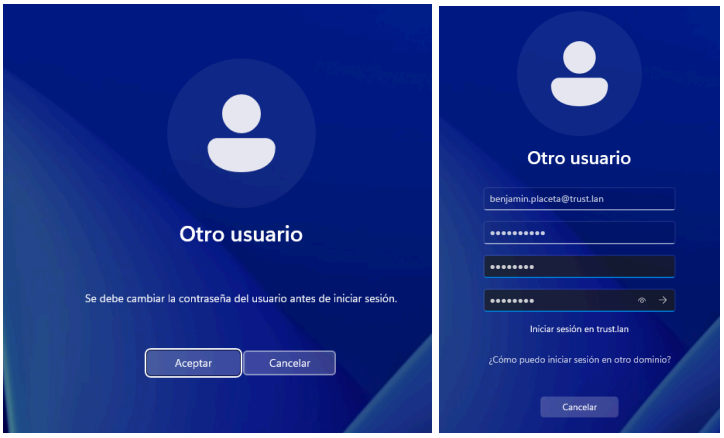
Como ejemplo de prueba de funcionamiento del sistema de archivos y permisos del dominio **Trust.lan**, se utilizó la cuenta de dominio del usuario **Benjamín Placeta**.

Este usuario pertenece simultáneamente a los grupos de seguridad **grupo.administracionyfinanzas** y **grupo.tic**, lo que le concede permisos de **lectura y escritura (RW)** sobre las carpetas compartidas de ambos departamentos, de acuerdo con la matriz de control de acceso definida.

Al iniciar sesión en un **equipo con Windows 11** unido al dominio, se introducen las credenciales de Benjamín en formato **benjamin.placeta@trust.lan**, autenticándose correctamente en el controlador de dominio **DC-TRUST-01**.

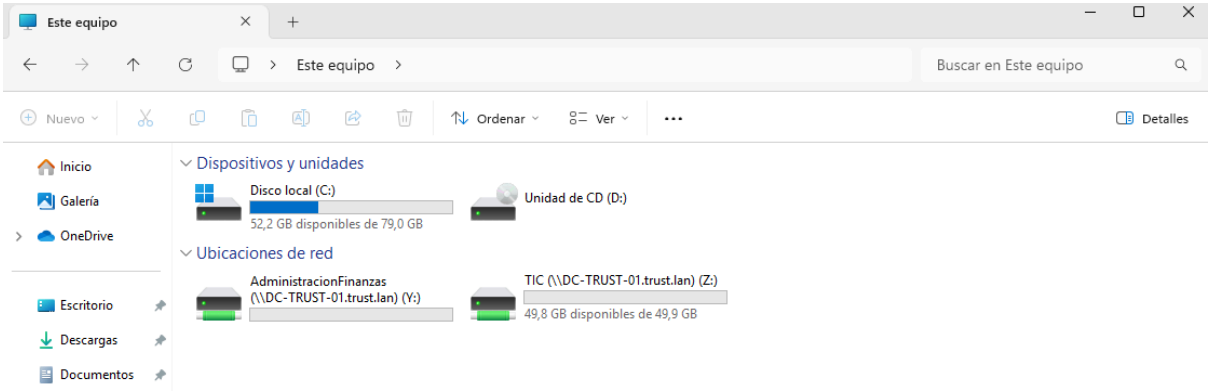


Durante el primer inicio de sesión, el sistema solicita el **cambio de contraseña**, tal y como establecen las políticas de seguridad de Active Directory, lo cual garantiza que la cuenta esté protegida con una clave personalizada.



Una vez completado el inicio de sesión, el sistema sincroniza el perfil de usuario y, tras unos segundos, el escritorio se carga completamente.
Al acceder al **Explorador de archivos** y seleccionar **Este equipo**, se puede comprobar que las unidades de red configuradas en el servidor aparecen automáticamente mapeadas.
En este caso, el usuario Benjamín dispone de acceso a las siguientes carpetas compartidas:

- \\DC-TRUST-01\AdminFinanzas
- \\DC-TRUST-01\TIC



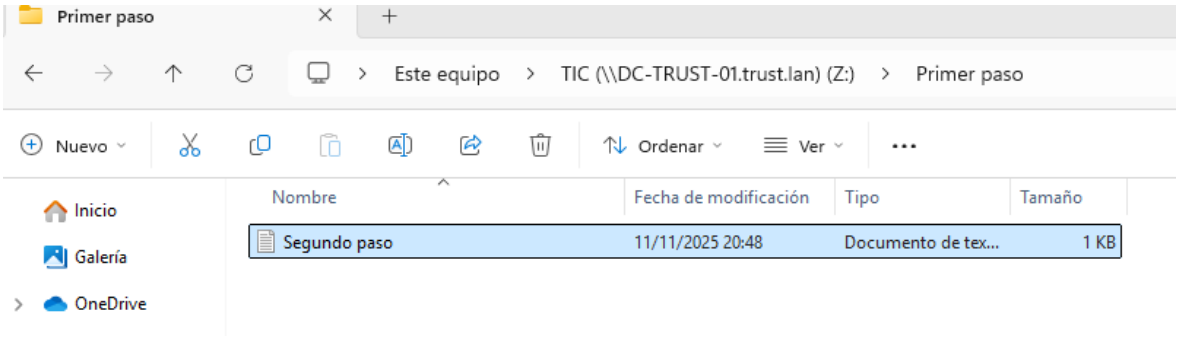
Estas unidades corresponden a las carpetas departamentales de **Administración y Finanzas y TIC**, respectivamente.
El usuario puede abrir, modificar y guardar documentos dentro de ambas rutas, tal como permiten los permisos **NTFS y SMB** aplicados en el servidor.

5.3 Ejemplo práctico – Usuario Benjamín Placeta

Benjamín pertenece a TIC y Administración y Finanzas. Al iniciar sesión en Windows 11, se mapean automáticamente sus unidades de red y puede crear archivos en las carpetas de sus departamentos.

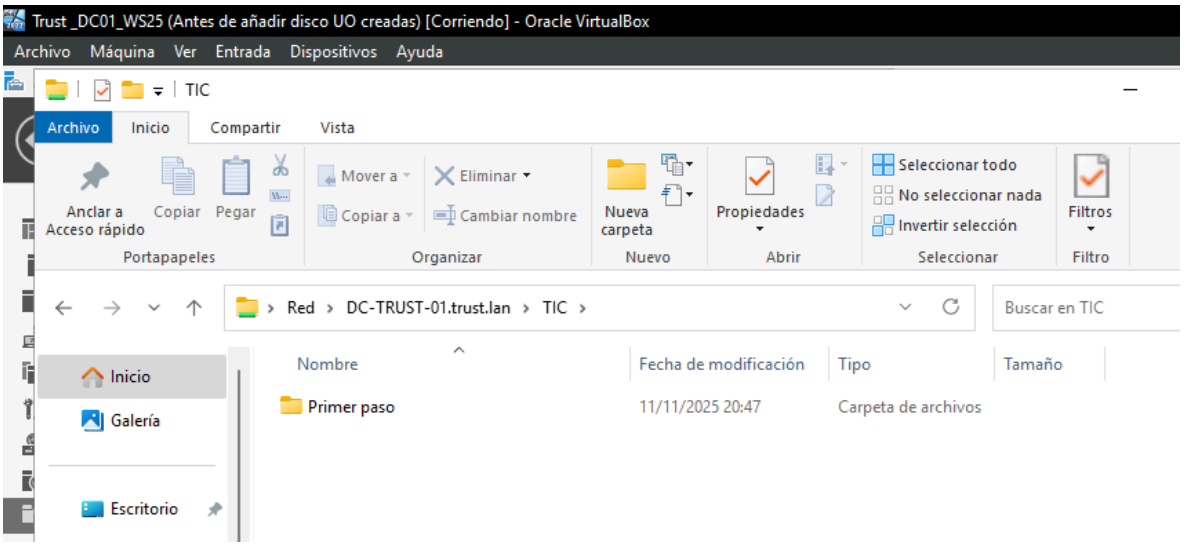
Desde su equipo unido al dominio (Windows 11), Benjamín accede correctamente a las unidades de red mapeadas que corresponden a estas rutas, confirmando la conexión establecida mediante el protocolo **SMB**.

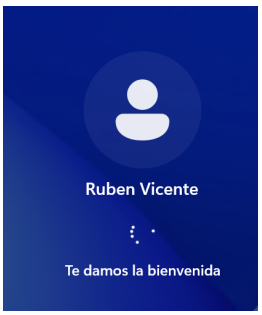
Dentro de la carpeta **TIC**, crea un nuevo directorio denominado *"Primer paso"* y en su interior genera un archivo de texto (*Segundo paso.txt*) con contenido explicativo, demostrando que posee permisos de creación y modificación en la carpeta compartida.



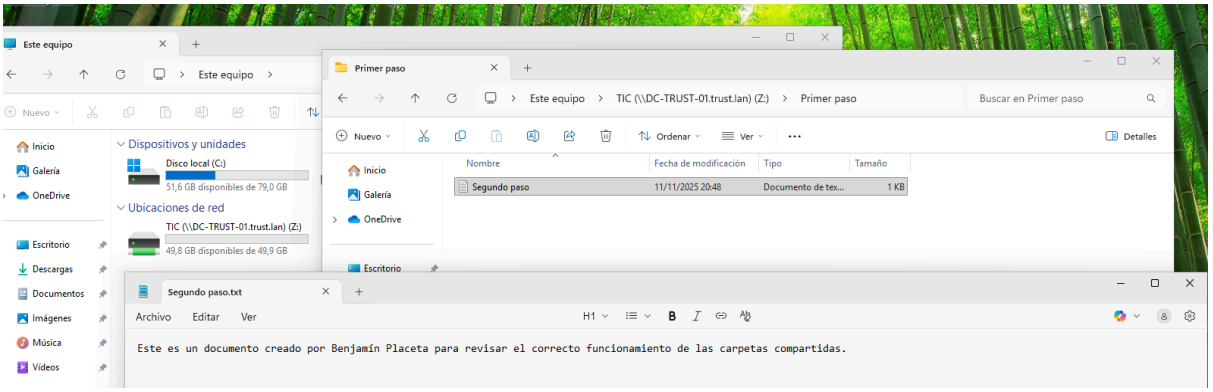
El contenido del archivo, creado por Benjamín, se guarda correctamente en la ruta de red, y posteriormente se verifica su existencia desde el **Administrador de archivos del servidor DC-TRUST-01**, donde el archivo aparece almacenado en la carpeta correspondiente.

Esta comprobación evidencia que las operaciones realizadas desde el cliente se reflejan directamente en el servidor, garantizando la sincronización correcta entre los recursos compartidos y los permisos NTFS.





A continuación, se realizó una segunda verificación iniciando sesión con otro usuario del dominio, **Rubén Vicente**, perteneciente también al grupo **TIC**.
Desde su sesión, Rubén accede a la misma carpeta compartida \\DC-TRUST-01\TIC, localiza el archivo Segundo paso.txt creado por Benjamín y puede abrirlo y leerlo sin problemas.



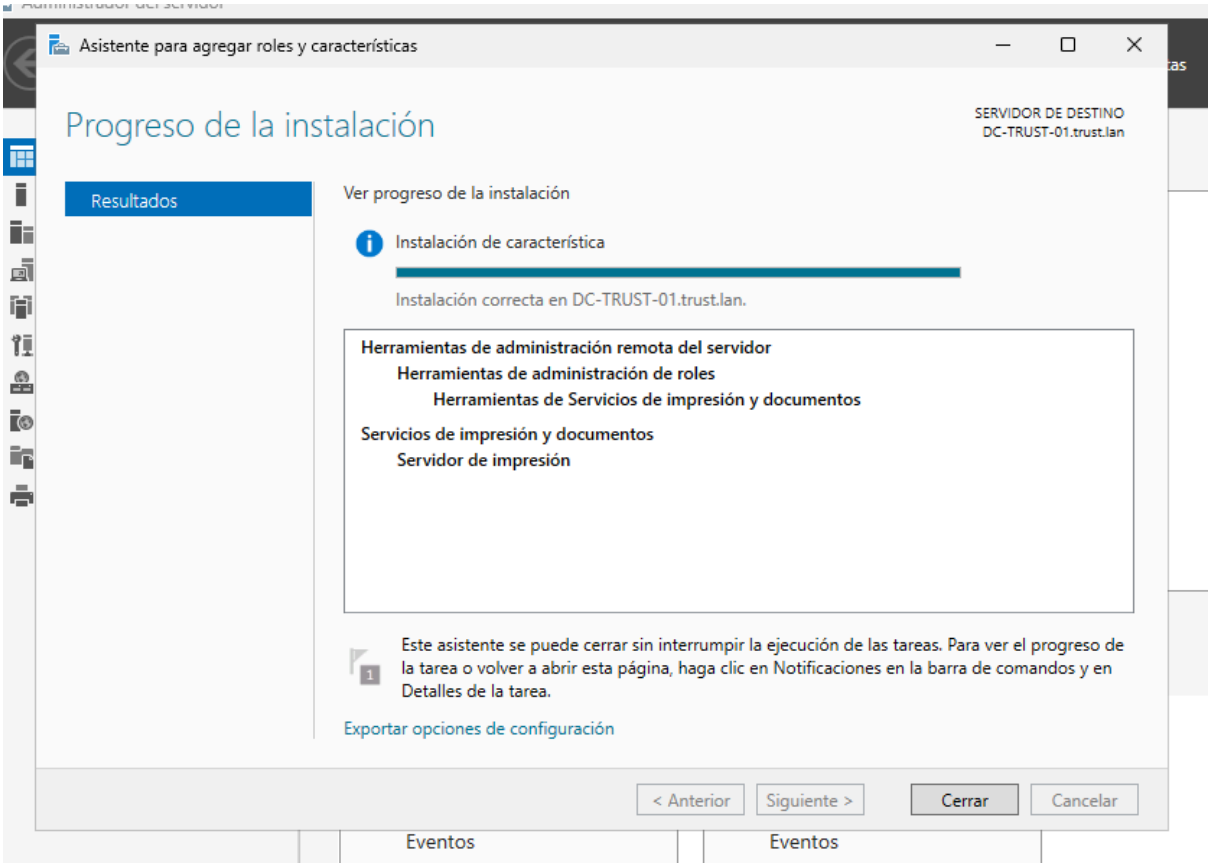
En este bloque se configura el servicio de impresión en red dentro del dominio trust.lan, siguiendo la estructura y la asignación de permisos definidas en el diseño inicial.

Se instalan las impresoras departamentales (multifunción, láser color A3 y plotter), junto con una impresora virtual PDF compartida para todos los usuarios del dominio.

Los permisos se aplican de forma centralizada desde el servidor, permitiendo que cada departamento administre únicamente sus dispositivos asignados.

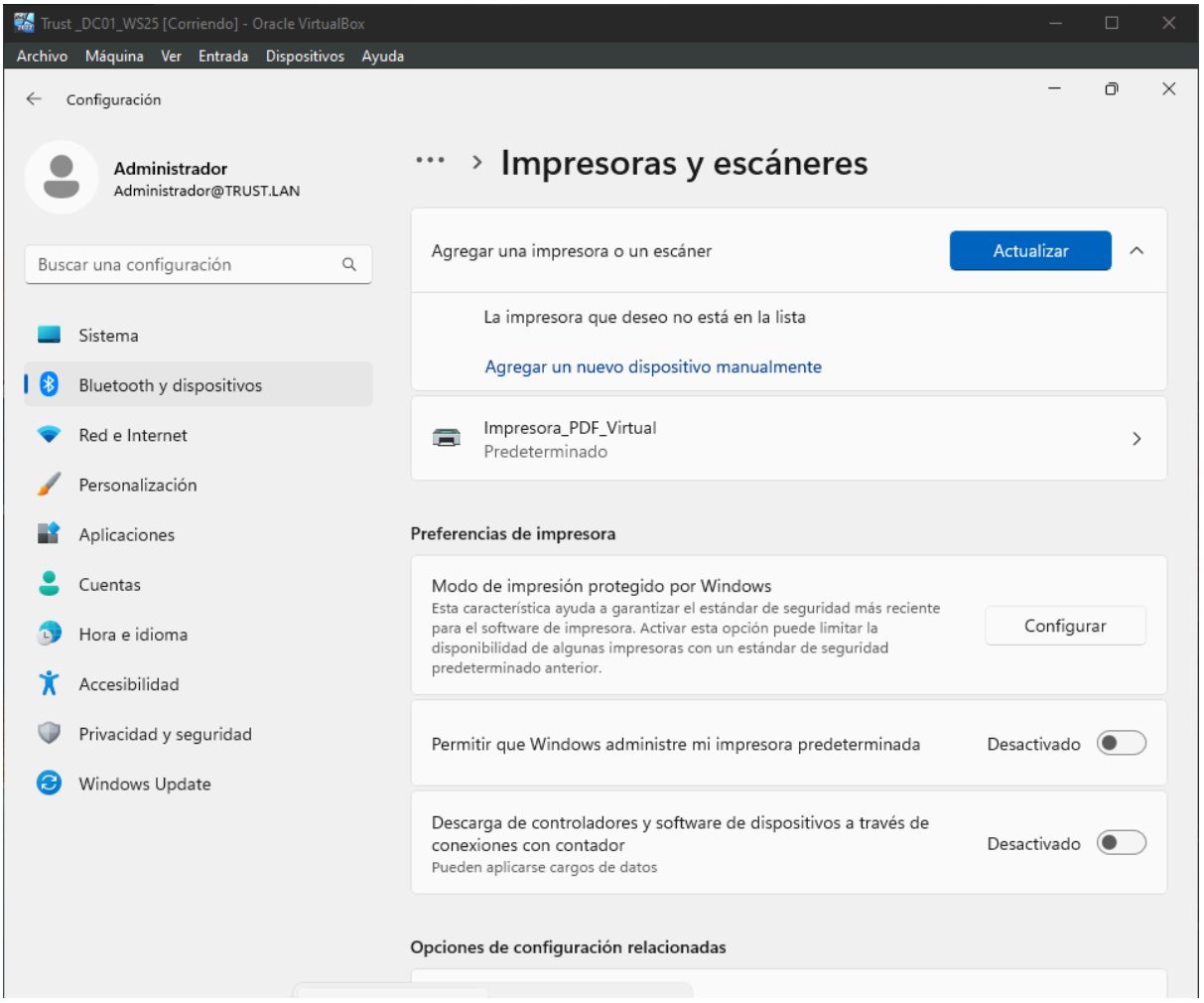
6. Bloque 5 – Servicio de impresión en red

Se instaló el rol de Servicios de impresión y documentos. Se añadieron las impresoras departamentales y una impresora PDF virtual usando el puerto NUL: y un controlador genérico. Las impresoras se publicaron en Active Directory y se asignaron permisos según departamentos. Todos los usuarios tienen acceso a la impresora PDF.



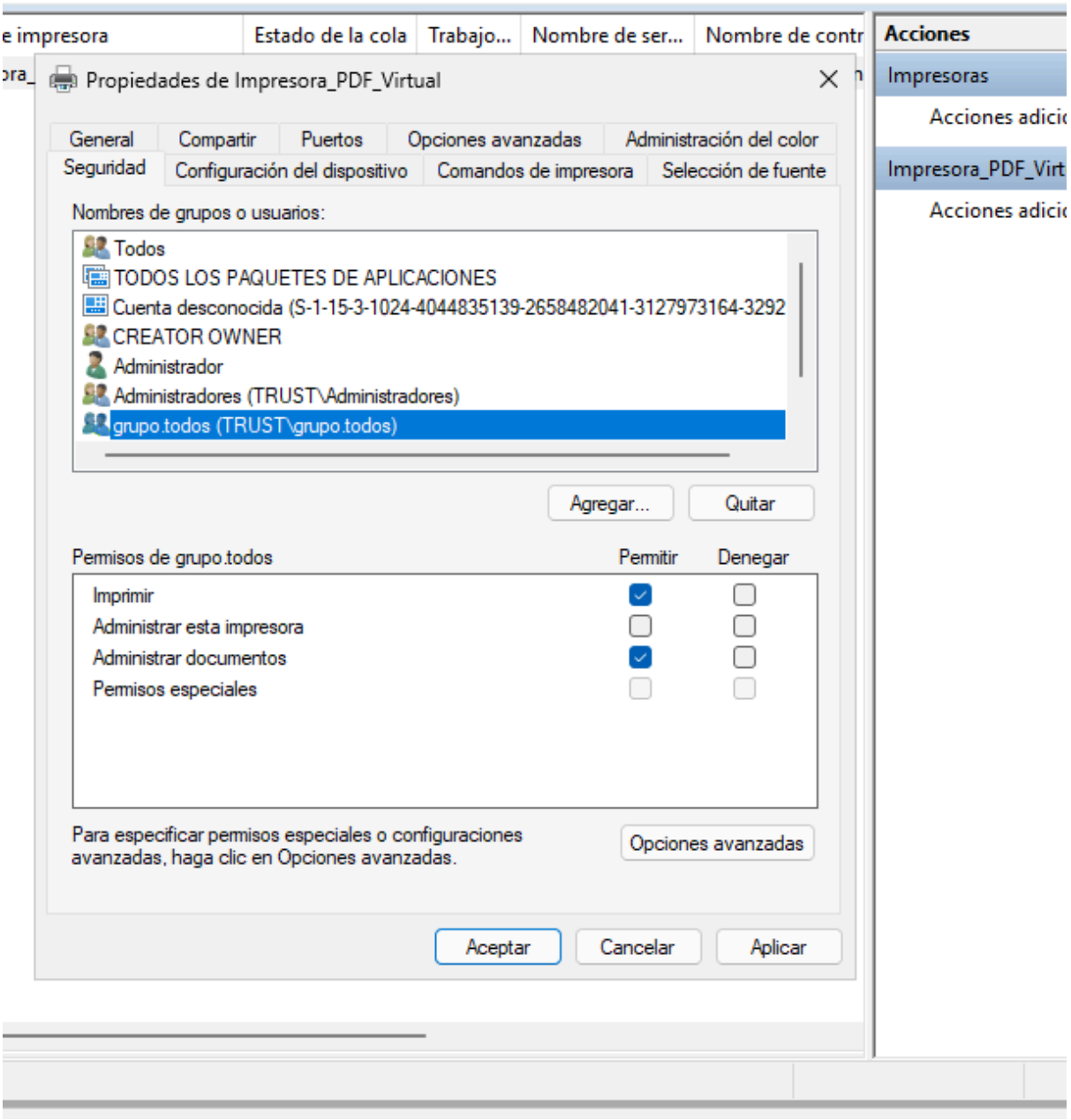
Se instala el rol de Servicios de impresión y documentos en el servidor principal del dominio.

Este rol habilita la administración centralizada de impresoras, colas de impresión y permisos de acceso desde el propio servidor de dominio.



Se instala una impresora virtual PDF utilizando el puerto local NUL: ya existente y el controlador *Generic / Text Only*.

Esta impresora permite generar documentos en formato PDF de manera simulada dentro del entorno de dominio, funcionando como una impresora compartida accesible desde cualquier equipo del dominio trust.lan.

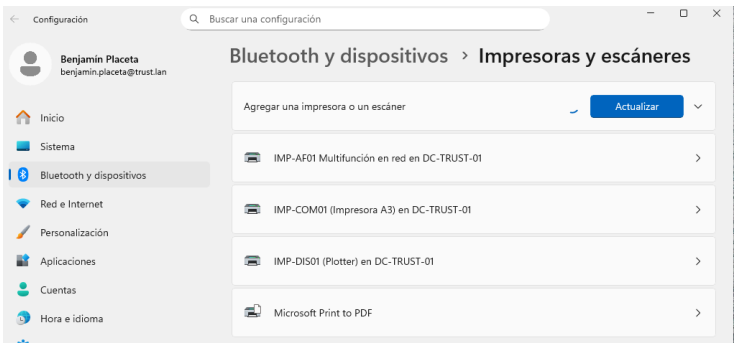


Se asignan los permisos de impresión a la impresora virtual PDF, otorgando al grupo global grupo.todos permisos de Imprimir y Administrar documentos.
De este modo, todos los usuarios del dominio pueden utilizar la impresora, mientras que la administración de la cola de impresión queda restringida a los administradores del dominio.
Este control centralizado garantiza una gestión segura y eficiente de los servicios de impresión en red.

6.1 Uso de las impresoras desde un usuario del dominio

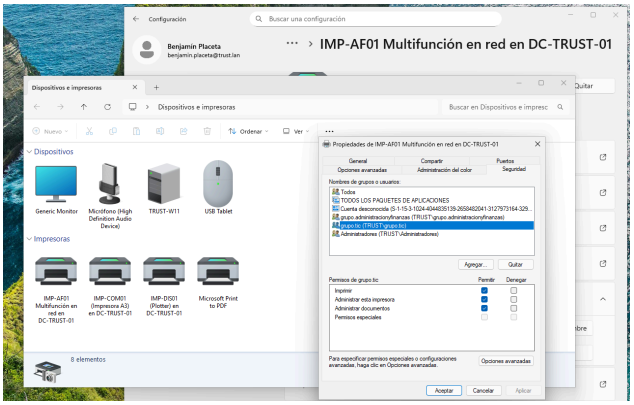
Benjamín puede ver las impresoras, imprimir documentos y administrar colas de impresión según sus permisos.

Desde su sesión en un equipo cliente **Windows 11** unido al dominio, se accede a la ruta de configuración:
Inicio > Configuración > Bluetooth y dispositivos > Impresoras y escáneres



En esta sección se muestran todas las impresoras disponibles en el servidor **DC-TRUST-01**, correctamente desplegadas mediante el Administración de impresión:

- **IMP-AF01** – Impresora multifunción (departamento Administración y Finanzas)
- **IMP-COM01** – Impresora A3 (departamento Comercial)
- **IMP-DIS01** – Plotter (departamento Diseño)
- **Microsoft Print to PDF** – Impresora virtual PDF compartida para todos los usuarios



El usuario **Benjamín Placeta** puede visualizar y seleccionar cualquiera de las impresoras asignadas, tal y como se aprecia en la captura.

Al acceder a las propiedades de la impresora **IMP-AF01**, se comprueba que su cuenta tiene los siguientes **permisos efectivos:**

- Imprimir documentos
- Administrar impresoras
- Administrar documentos

Estos privilegios le permiten no solo imprimir archivos desde las carpetas compartidas del dominio, sino también pausar, reanudar o cancelar documentos en cola, así como modificar las preferencias del dispositivo.

7. Conclusiones

El dominio trust.lan queda completamente implementado: equipos unidos, recursos compartidos configurados, permisos aplicados, servicio de impresión operativo y estructura del directorio optimizada. Todo el entorno puede administrarse de forma centralizada conforme a las buenas prácticas.

7. Bloque 6 – Video Instalación, configuración y administración de servicios y recursos de red (trust.lan)

En este vídeo se muestra la implementación completa del Producto 2 del proyecto de Administración de Servidores Empresariales.

Se demuestra la estructura del servicio de directorio del dominio trust.lan, la incorporación de un equipo con sistema operativo propietario (Windows 11) y un equipo con sistema operativo libre (Ubuntu) al dominio, la creación y configuración de un disco de red con carpetas compartidas y permisos, así como la instalación y administración del servicio de impresión en red.

Link: https://youtu.be/pzOYe208f_I