

Implantación de Sistemas Operativos

U6. Administración de dominios y recursos compartidos.

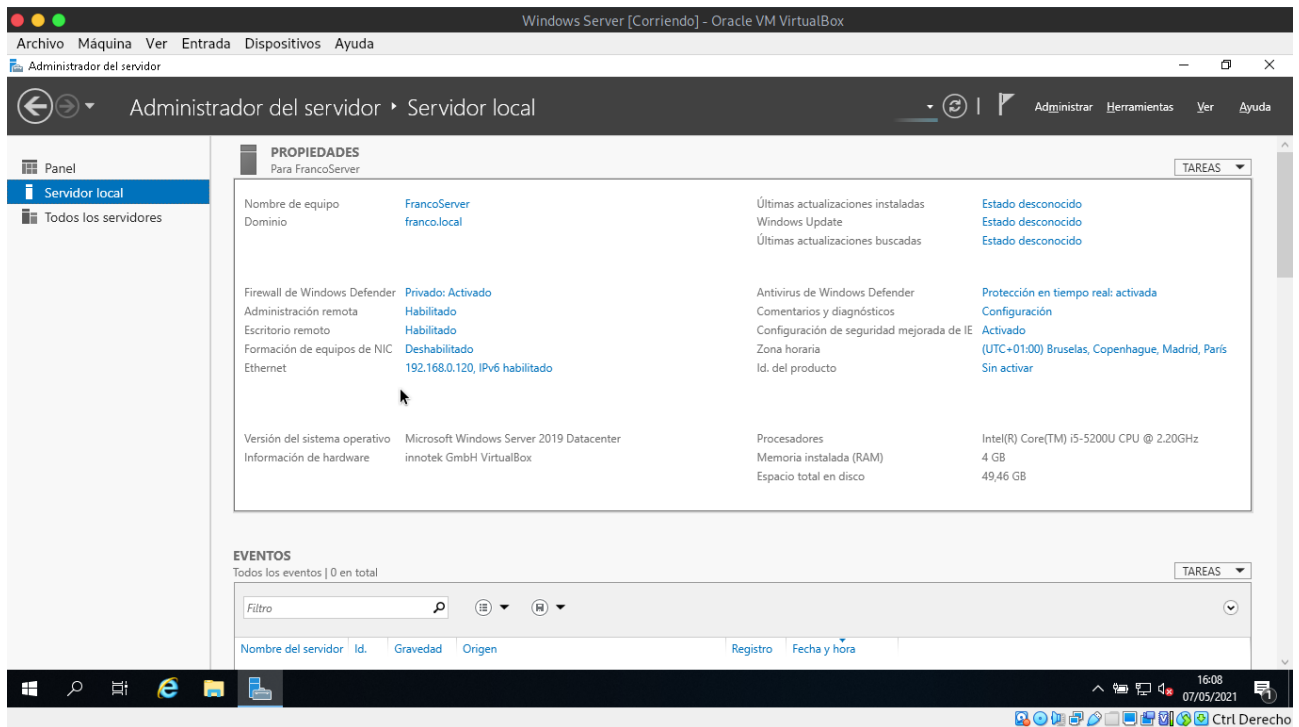
Práctica 1. ACTIVE DIRECTORY.

Franco Larrea - 1ºASIR

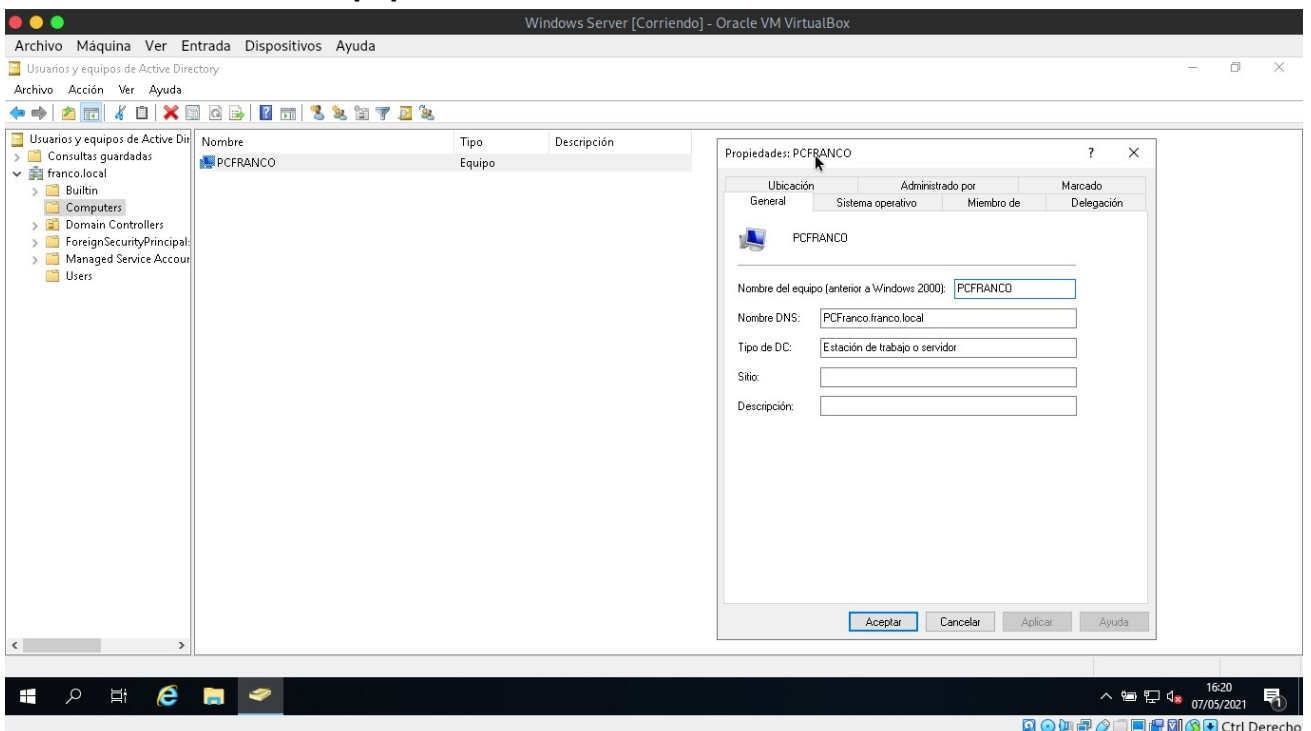
Para esta práctica voy a usar las maquinas virtuales que use en la anterior practica:

['U5. Práctica1. Instalación W10 y Wserver2019'](#)

1. Intalación del servidor.

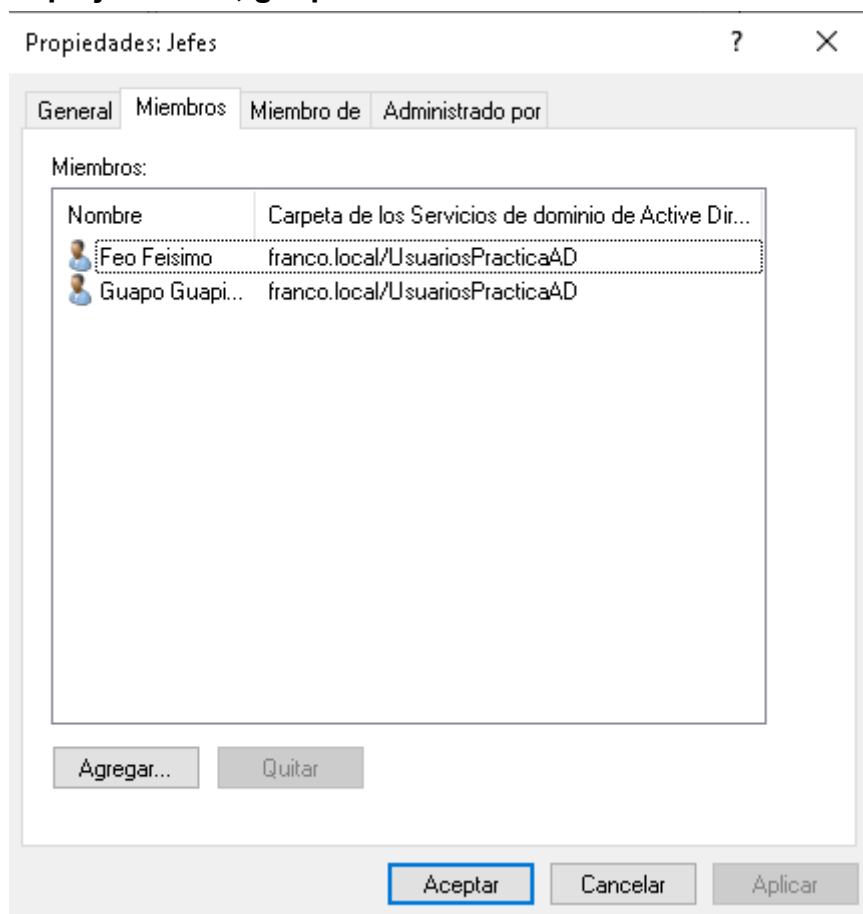


2. Validación de equipo

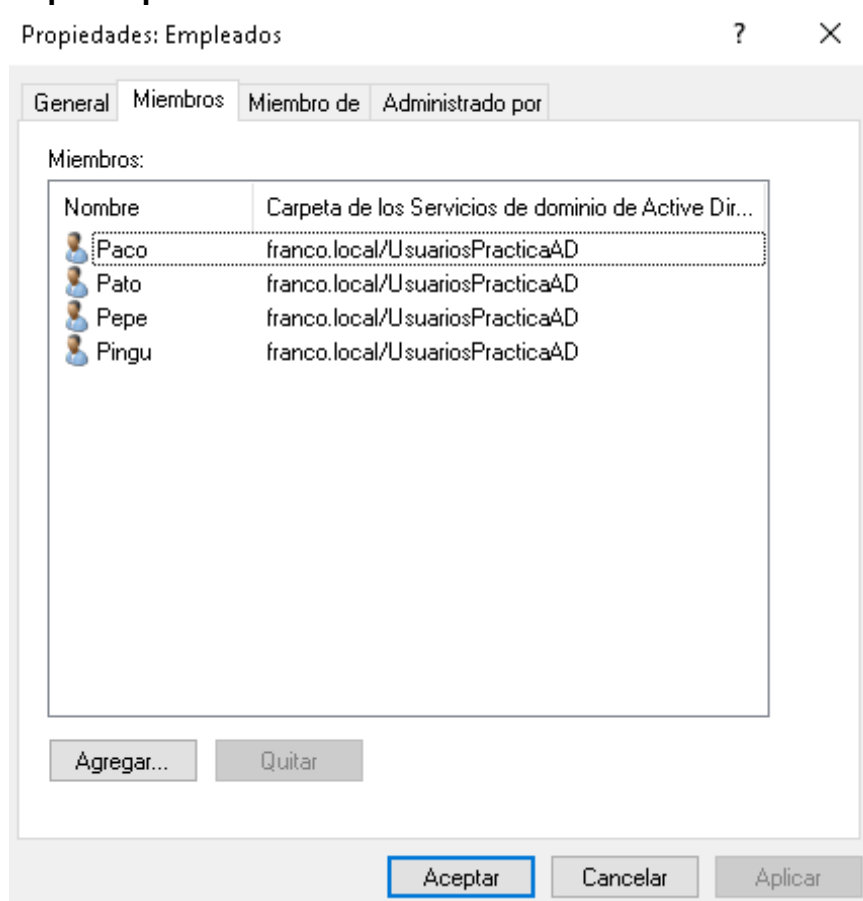


3. Usuarios de dominio

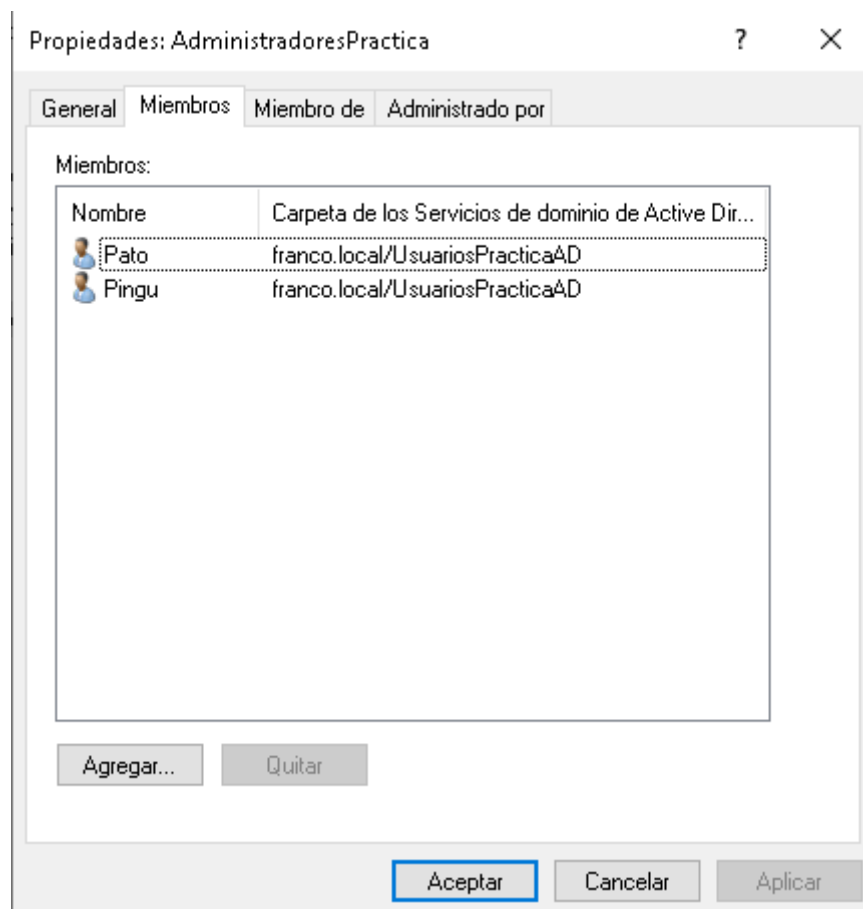
a) Grupo jefes: feo, guapo



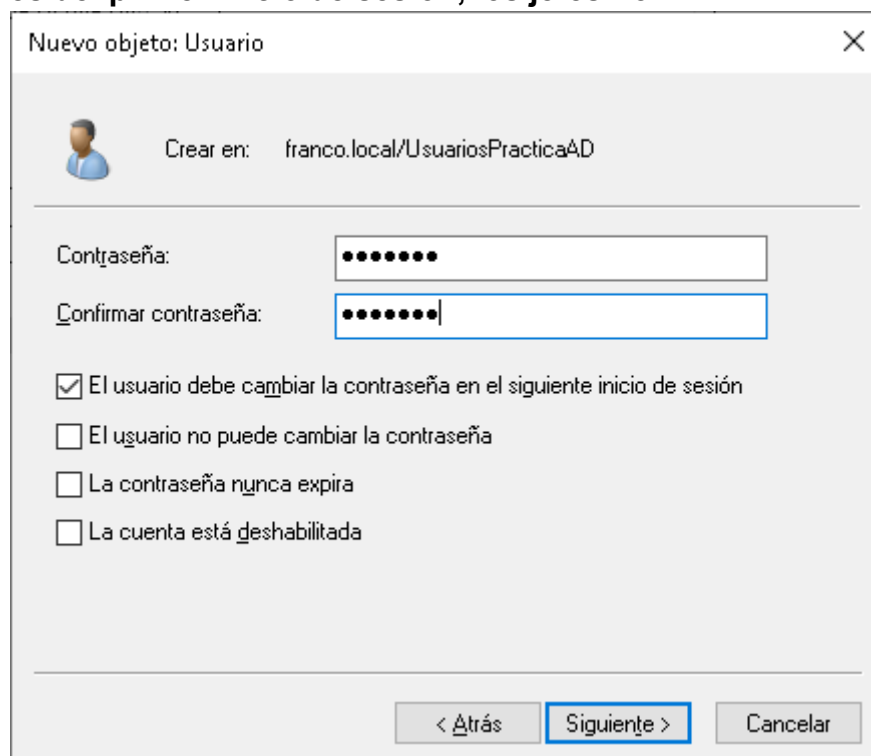
b) Grupo empleados:

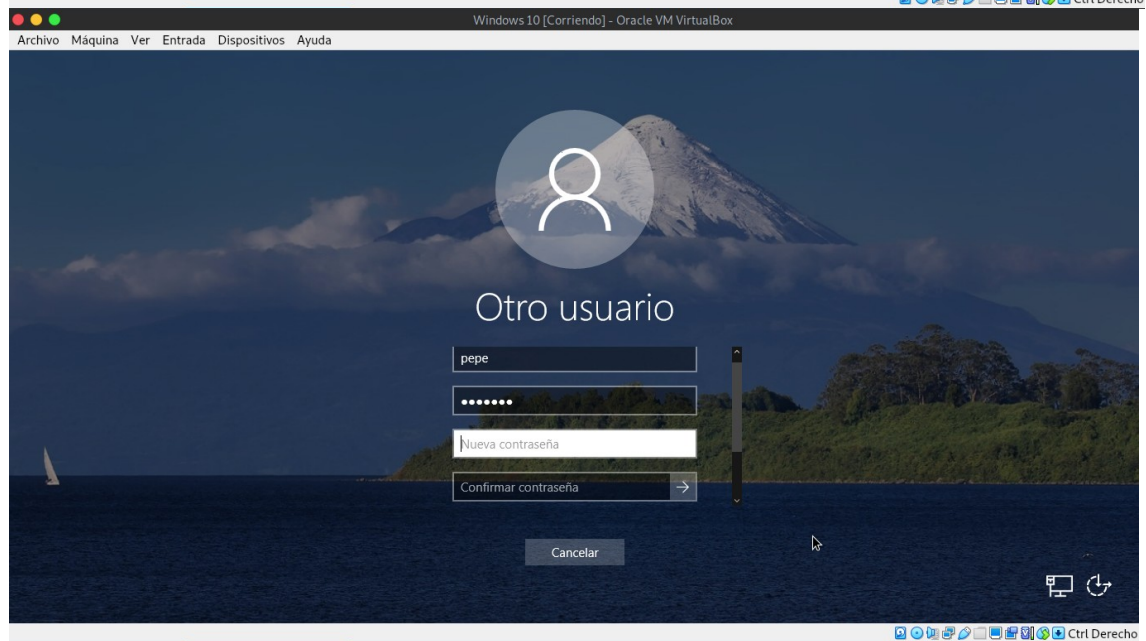
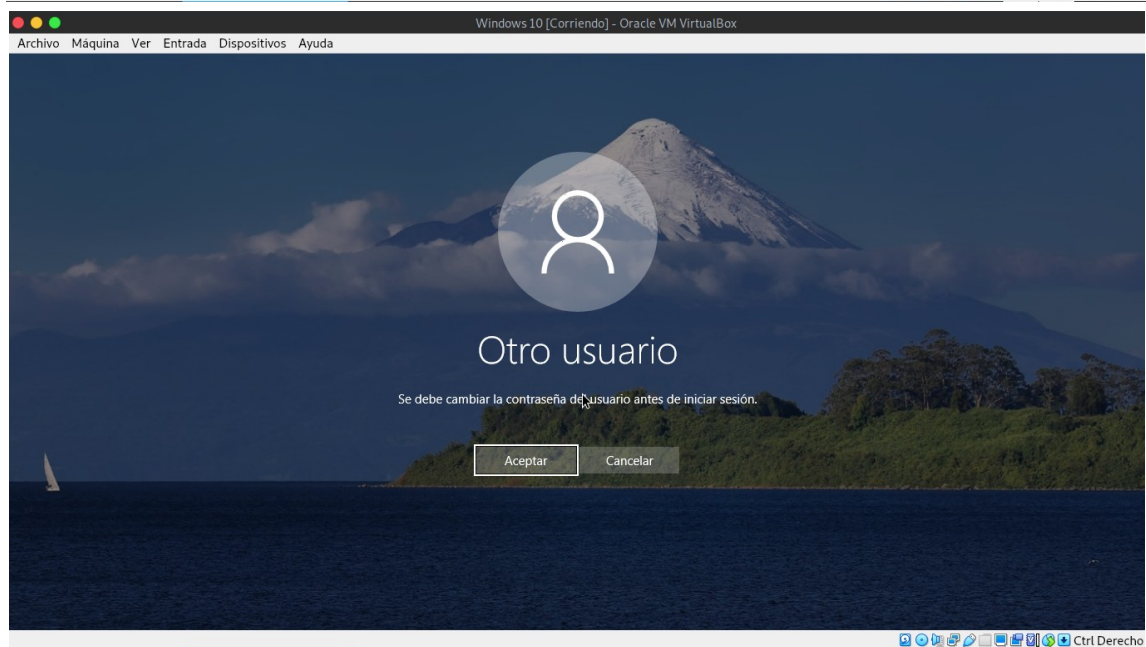
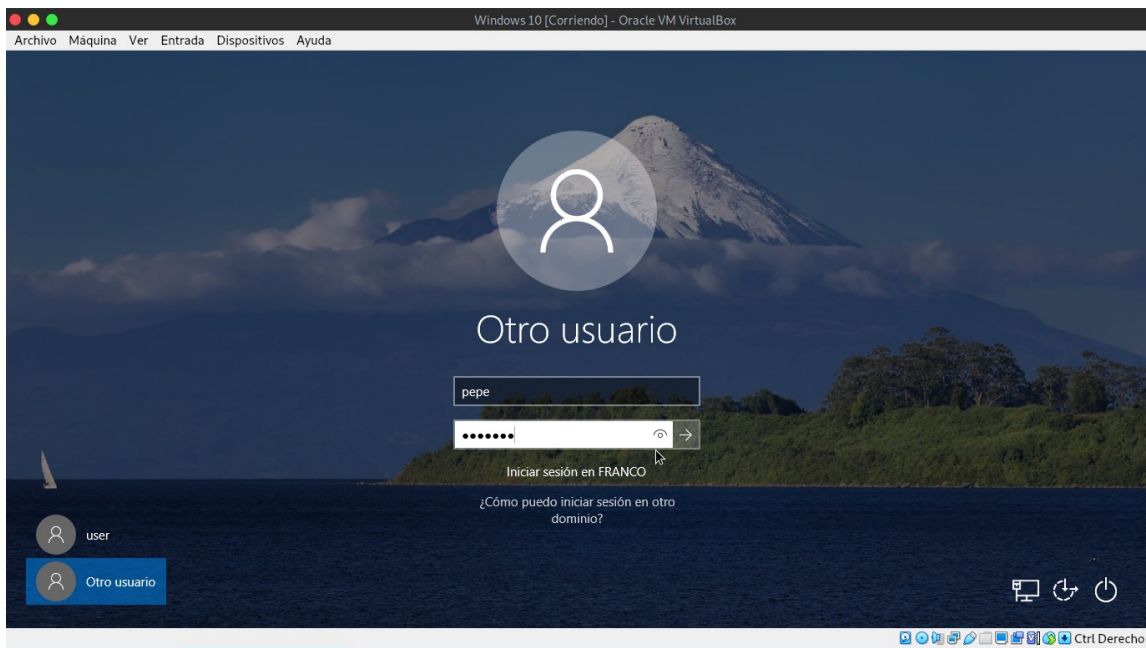


c) **Grupo administradores:**



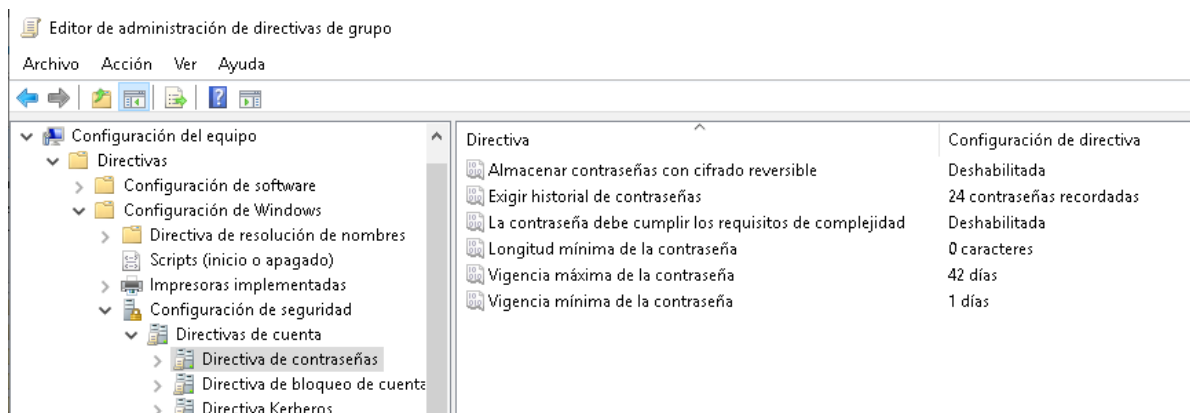
d) **Los usuarios del grupo empleados deberán cambiar la contraseña después del primer inicio de sesión, los jefes no.**





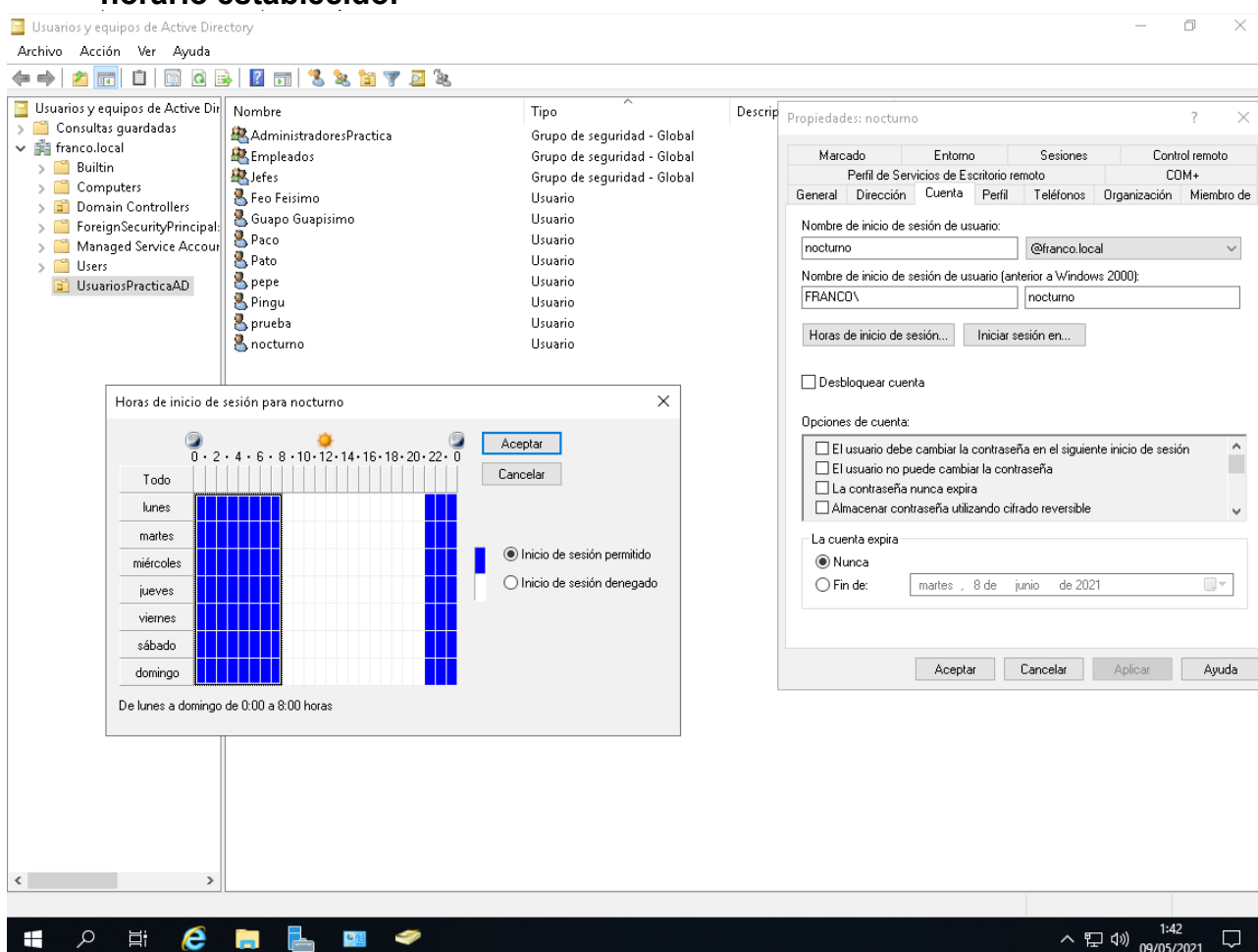
e) Crea un usuario llamado prueba sin contraseña. Prueba a acceder con él.

Para poder crearlo hay que modificar las directivas de contraseña.

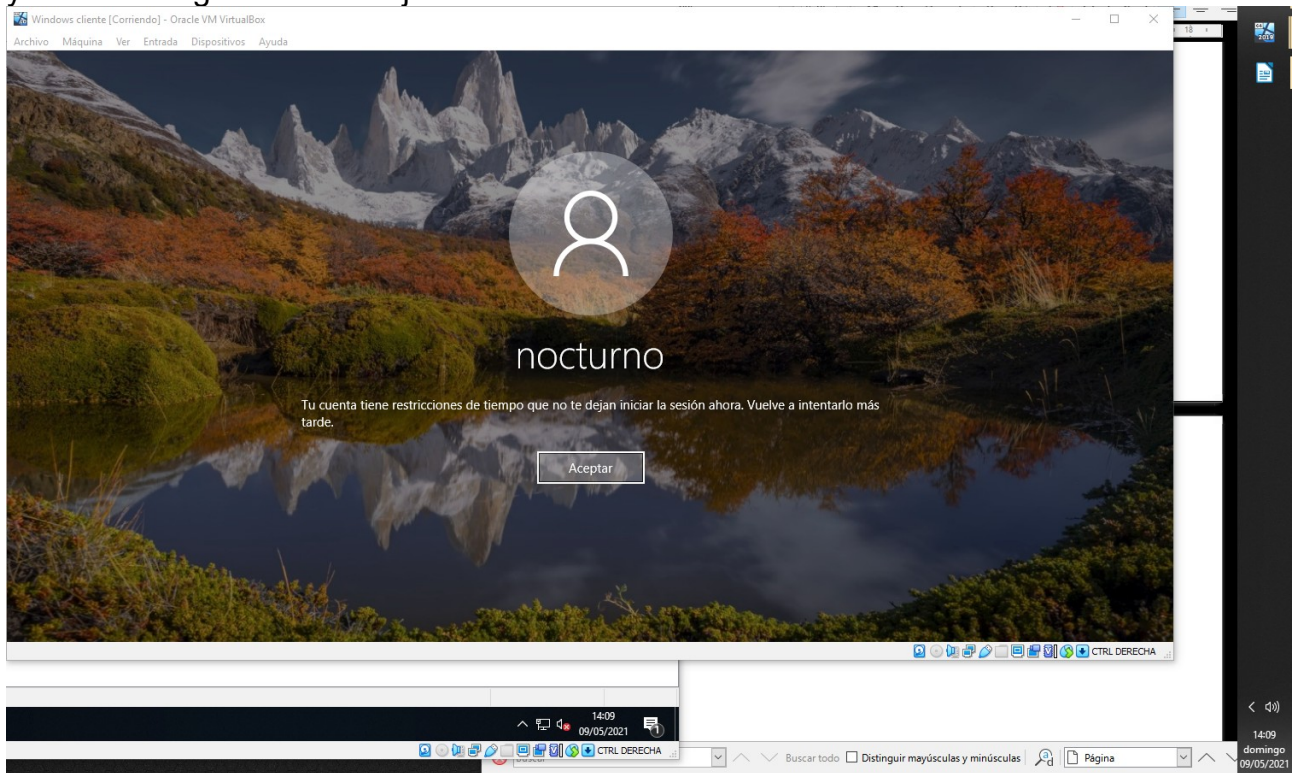


He accedido con el usuario prueba, sin ingresar ninguna contraseña, correctamente.

f) Crea el usuario nocturno dentro del grupo de jefes que solo pueda iniciar sesión de 21 a 8 horas. Prueba a iniciar sesión dentro y fuera del horario establecido.

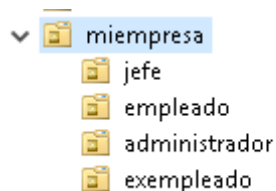


Se puede iniciar sesión con el usuario nocturno en las horas establecidas sin problemas. En cambio si intentamos iniciar sesión fuera de las horas activas vemos que no podemos y nos da el siguiente mensaje:

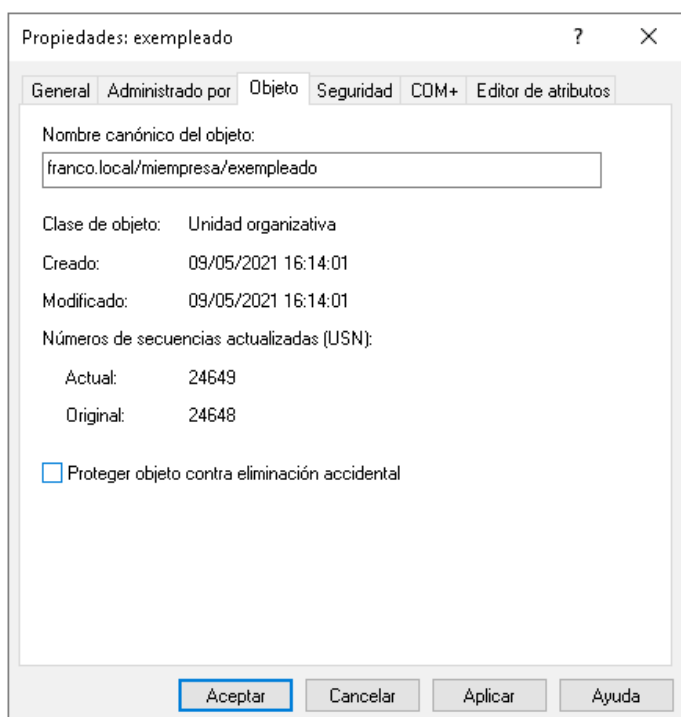


4. Unidades organizativas y GPO

a) **Crea la unidad organizativa miempresa y dentro de esta, cuatro unidades organizativas: jefe, empleado, expleado y administrador. Incluye los grupos jefes, empleados y administradores dentro de sus respectivas unidades organizativas.**



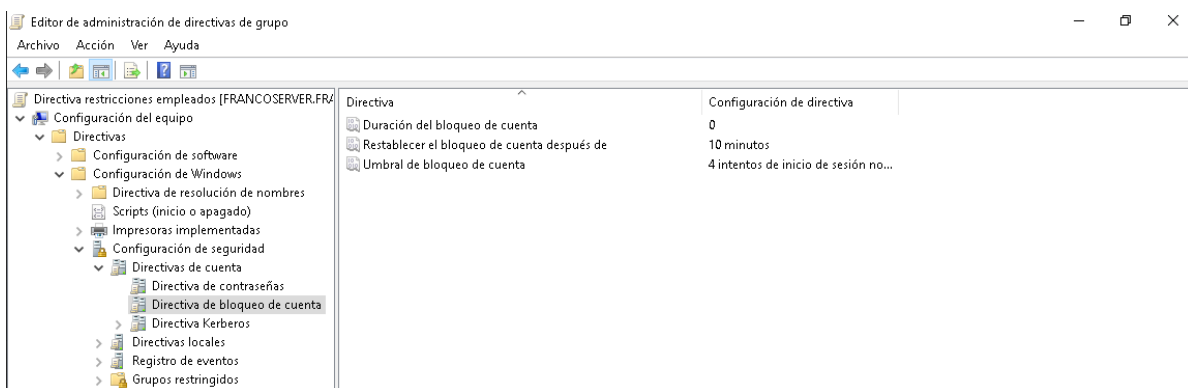
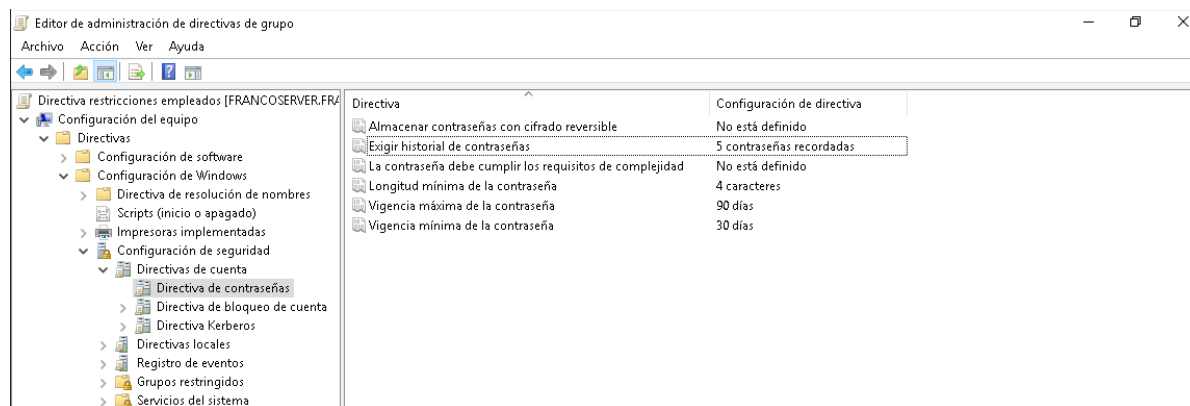
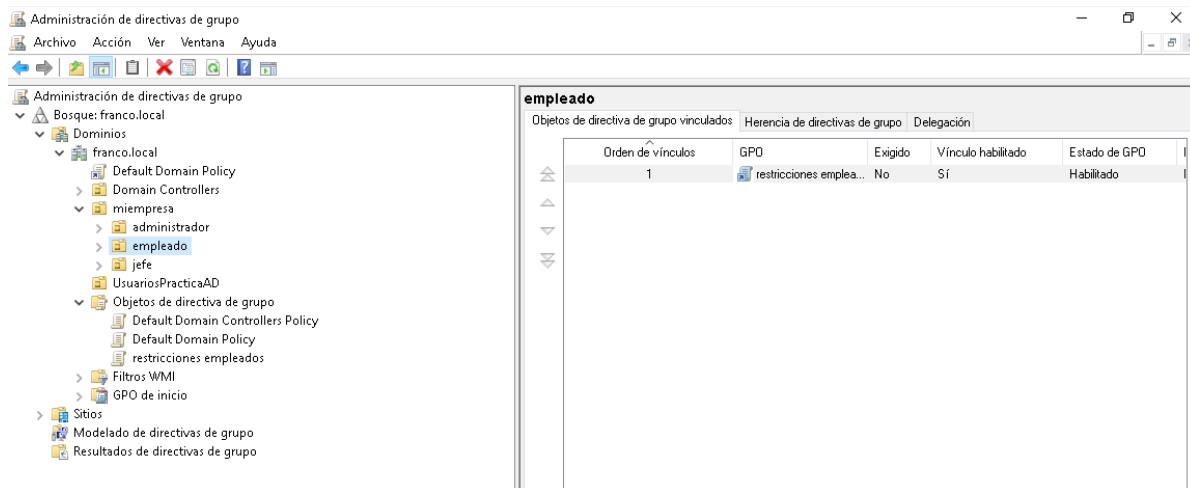
b) **Elimina la unidad organizativa expleado.**



c) **Deshabilita la cuenta del usuario prueba. ¿Qué diferencia hay entre deshabilitarla y eliminarla?**

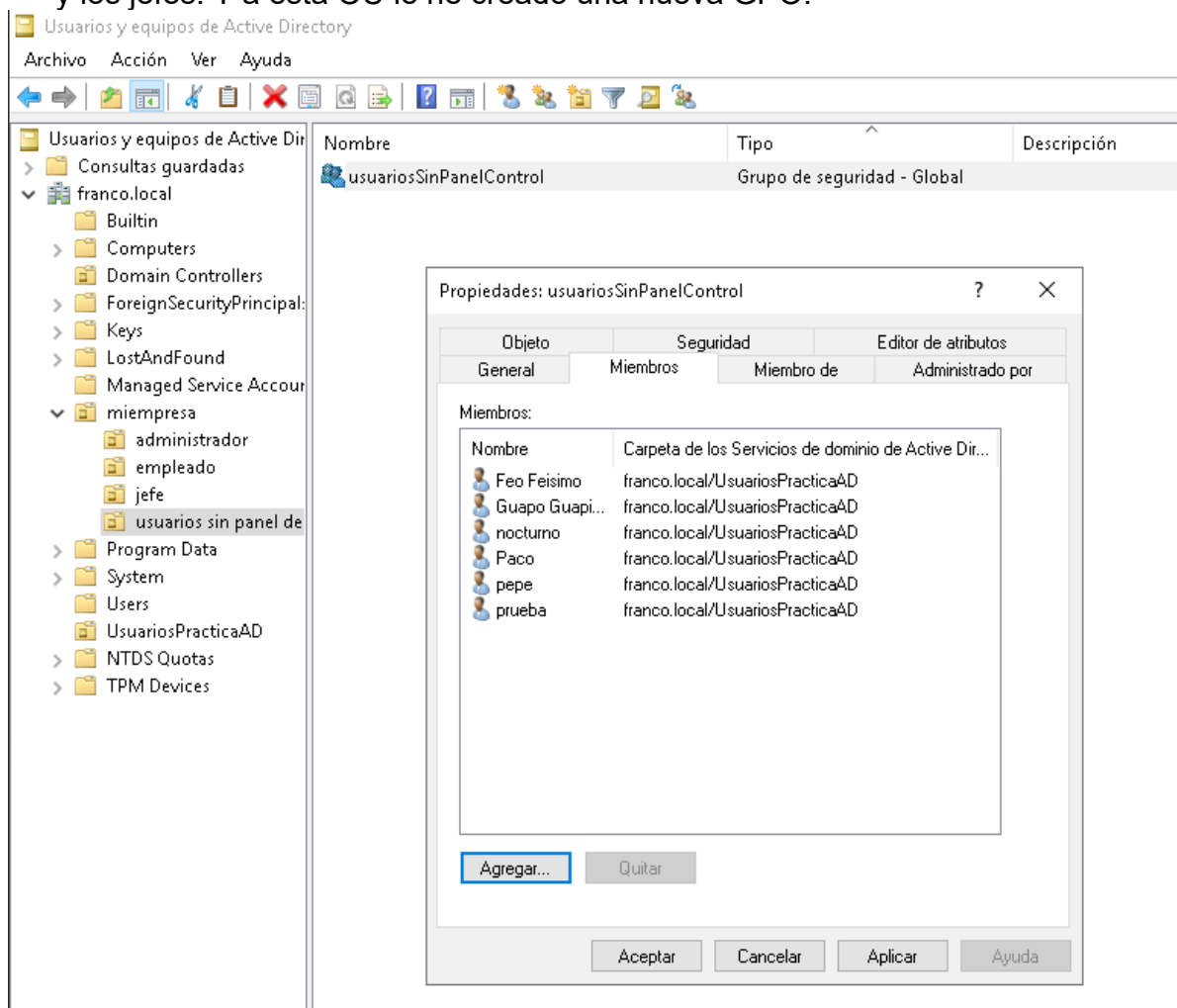
Deshabilitarla la deja inactiva con opción a volver a activarla, eliminarla en cambio, es una acción irreversible.

d) Crea una directiva de seguridad sobre el grupo empleados que impida contraseñas menores de 4 caracteres y que obligue a cambiar la contraseña cada 90 días con un historial de 5 contraseñas. Además, para evitar posibles robos de contraseña y ataques mal intencionados, cuando un usuario intenta 4 veces introducir de manera incorrecta su contraseña, debe bloquear la cuenta hasta que el administrador la desbloquee. Se reestablecerá el contador de inicios de sesión erróneos a los 10 minutos. Haz un pantallazo de las directivas.



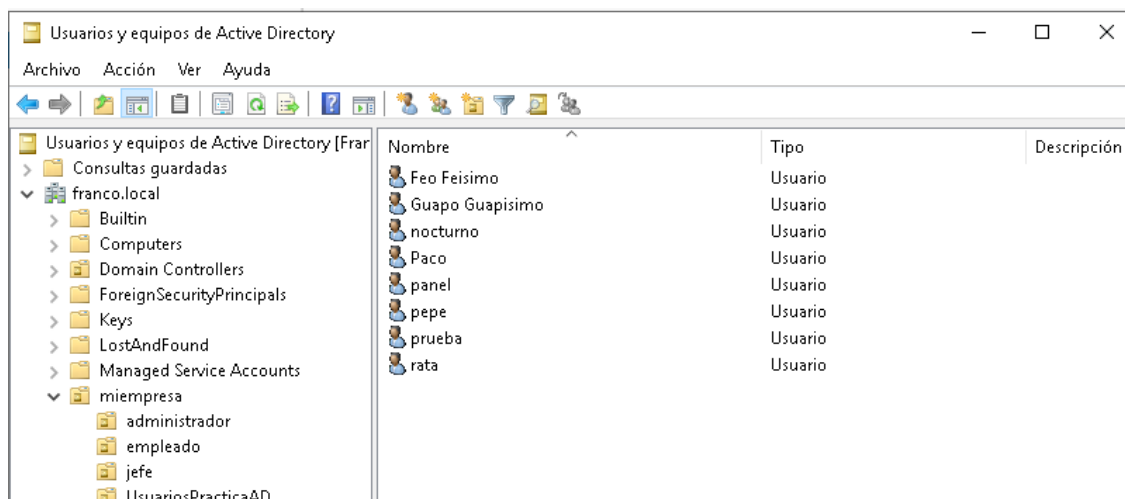
e) **Deniega el acceso al panel de control a todos los usuarios excepto a los administradores.**

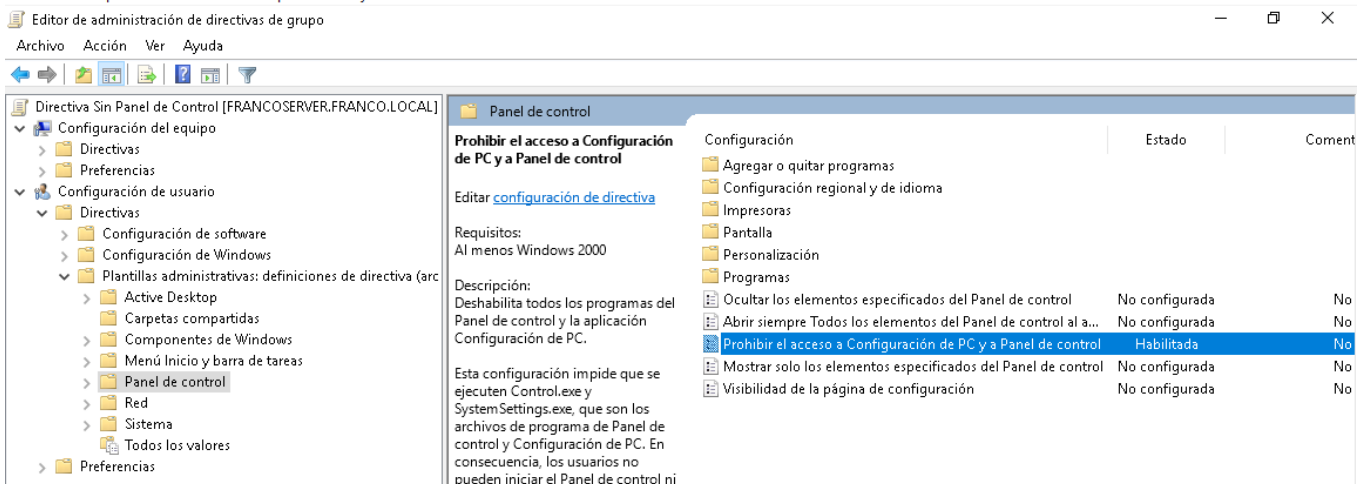
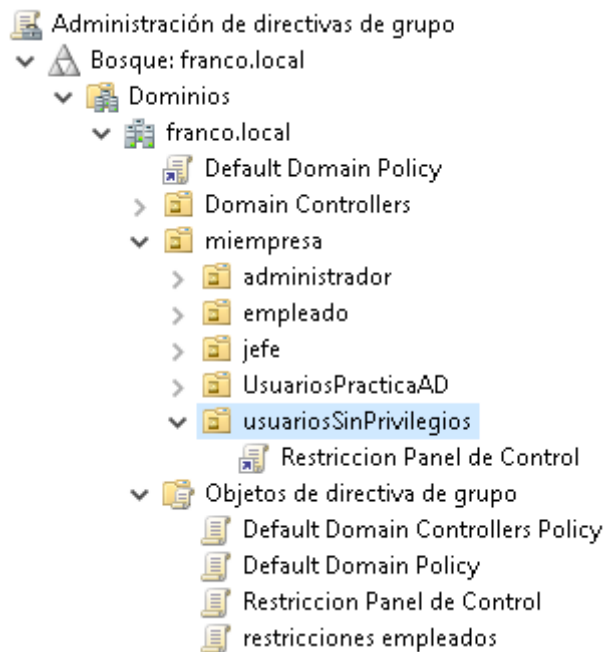
He creado una nueva OU donde esten los empleados que no son administradores y los jefes. Y a esta OU le he creado una nueva GPO.



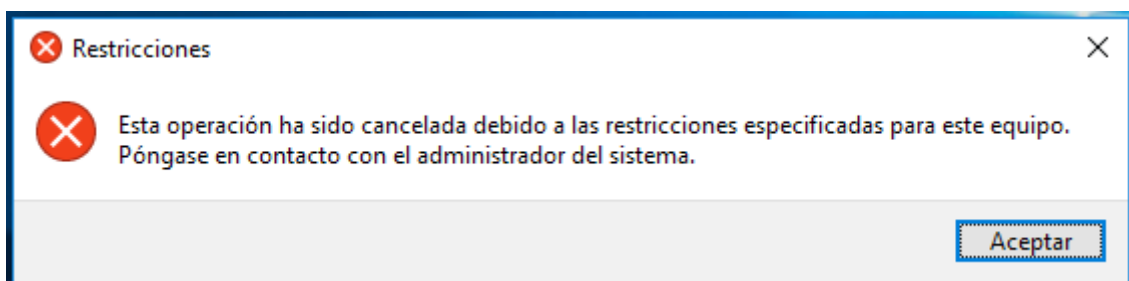
Lo anterior no funciona, por alguna razón las GPO afectan a los usuarios dentro de una OU pero no afecta a los usuarios miembros de un grupo dentro de una OU.

Así que simplemente moveré los usuarios a los que quiero aplicar la restricción del panel de control a una OU. Al final llame a esta OU 'usuariosSinPrivilegios'.





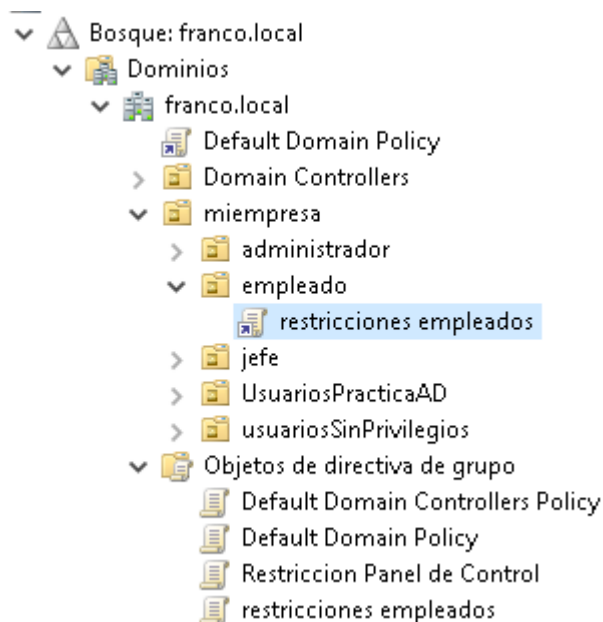
Despues de esto, probamos iniciar sesión con un usuario que NO sea administrador (Feo) y al intentar abrir el panel de control nos sale la siguiente alerta:



En cambio, si iniciamos sesión con un usuario Administrador (Pato), debería dejarnos acceder al panel de control.

f) Configura un fondo de pantalla personalizado para el grupo de empleados y que no lo puedan modificar.

He añadido las restricciones a una GPO existente.



Directiva restricciones empleados	Configuración	Estado	Comentario
▼ Configuración del equipo	Habilitar Active Desktop	Habilitada	No
> Directivas	Deshabilitar Active Desktop	No configurada	No
> Preferencias	No permitir cambios	Habilitada	No
▼ Configuración de usuario	Tapiz del escritorio	Habilitada	No
> Directivas	Prohibir agregar elementos	No configurada	No
> Configuración de sol	Prohibir cerrar elementos	No configurada	No
> Configuración de Wi	Prohibir eliminar elementos	No configurada	No
> Plantillas administrat	Prohibir modificar elementos	No configurada	No
> Active Desktop	Deshabilitar todos los elementos	No configurada	No
> Active Desktop	Agregar o quitar elementos	No configurada	No
> Carpetas compart	Permitir solo papel tapiz de mapa de bits	No configurada	No

‘Habilitar Active Desktop’ tiene que estar habilitado. ‘Tapiz del escritorio’ tiene que estar habilitado y tenemos que indicar la ruta del fondo de pantalla a utilizar.

Si establecemos una ruta local, el archivo tiene que estar en cada maquina cliente donde queramos poner el fondo.

Lo suyo es que este en una carpeta compartida.

(Siguen sin aplicarse las GPO a los miembros de grupos)

g) Denegar el acceso al USB (unidades extraíbles) para todos los empleados, excepto los administradores.

Modificaré la restricción que cree para restringir el acceso al panel de control para todos los empleados, excepto los administradores.

Editor de administración de directivas de grupo

Archivo Acción Ver Ayuda

← → ↶ ↷ ↸ ↹

Directiva Restricción Panel de Control [FRANCOSERVER.F

▼ Configuración del equipo

▼ Directivas

► Configuración de software

► Configuración de Windows

▼ Plantillas administrativas: definiciones de direc

► Componentes de Windows

► Impresoras

► Menú Inicio y barra de tareas

► Panel de control

► Red

► Servidor

▼ Sistema

► Acceso a Almacenamiento mejorado

► Acceso de almacenamiento extraíble

► Administración de comunicaciones de

► Administración de energía

► Administrador del servidor

► Antimalware de inicio temprano

► Apagado

► App-V

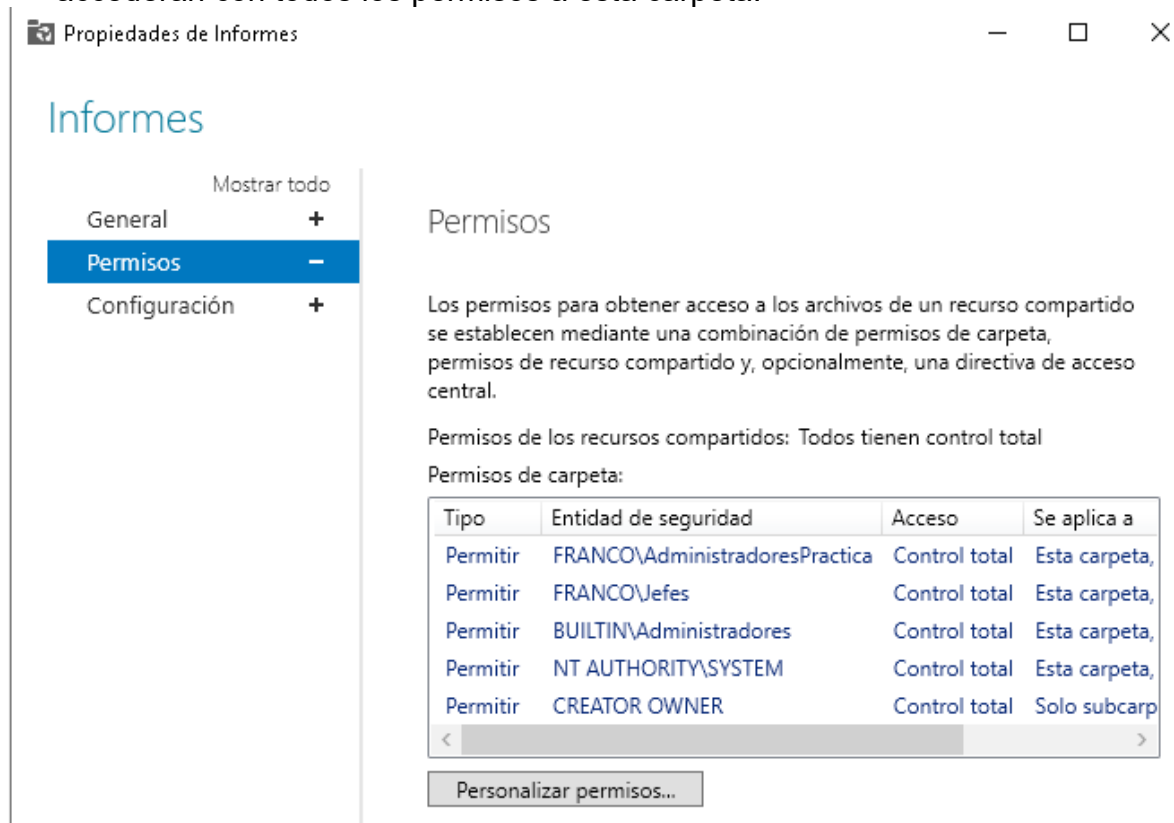
► Asistencia de acceso denegado

► Asistencia remota

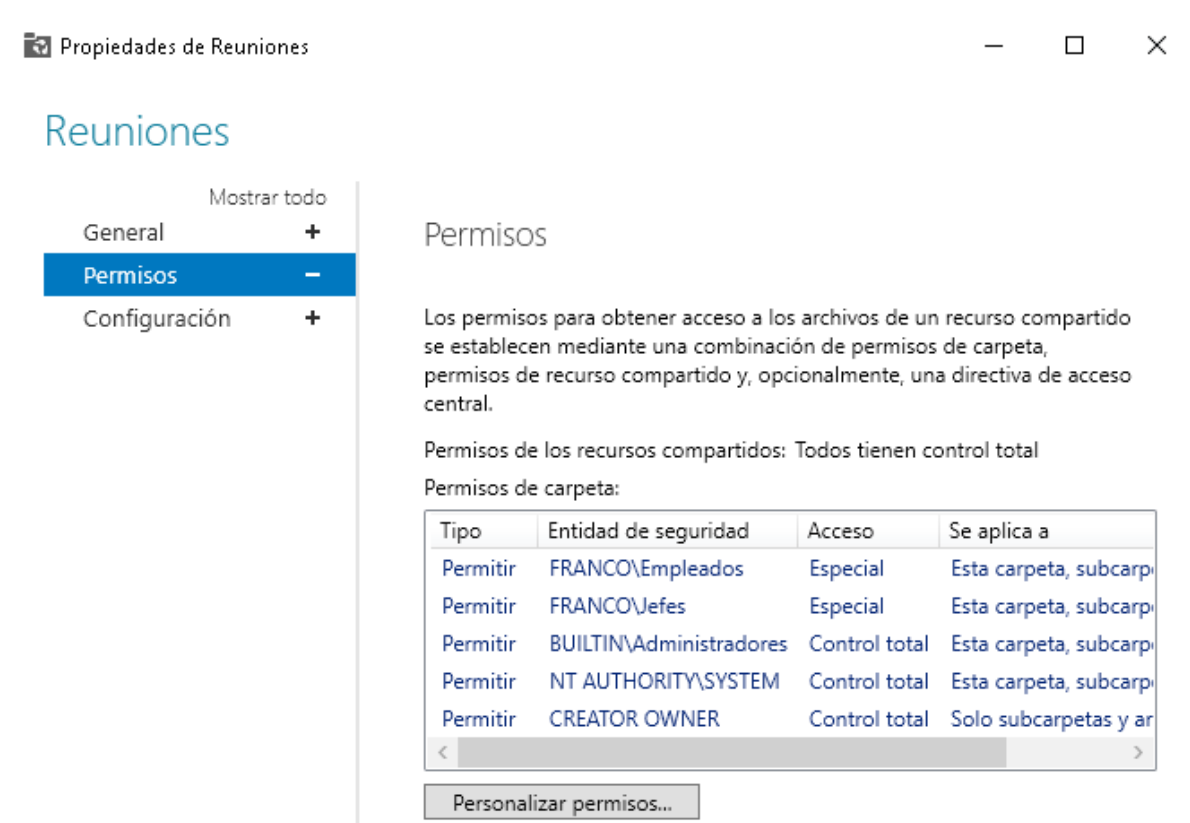
Configuración	Estado	Comentario
Establecer tiempo (en segundos) para forzar reinicio	No configurada	No
CD y DVD: denegar acceso de ejecución	No configurada	No
CD y DVD: denegar acceso de lectura	No configurada	No
CD y DVD: denegar acceso de escritura	No configurada	No
Clases personalizadas: denegar acceso de lectura	No configurada	No
Clases personalizadas: denegar acceso de escritura	No configurada	No
Unidades de disquete: denegar acceso de ejecución	No configurada	No
Unidades de disquete: denegar acceso de lectura	No configurada	No
Unidades de disquete: denegar acceso de escritura	No configurada	No
Discos extraíbles: denegar acceso de ejecución	Habilitada	No
Discos extraíbles: denegar acceso de lectura	Habilitada	No
Discos extraíbles: denegar acceso de escritura	No configurada	No
Todas las clases de almacenamiento extraíble: denegar acce...	No configurada	No
Todo el almacenamiento extraíble: permitir acceso directo e...	No configurada	No
Unidades de cinta: denegar acceso de ejecución	No configurada	No
Unidades de cinta: denegar acceso de lectura	No configurada	No
Unidades de cinta: denegar acceso de escritura	No configurada	No
Dispositivos WPD: denegar acceso de lectura	No configurada	No
Dispositivos WPD: denegar acceso de escritura	No configurada	No

5. Servicios de archivos


- a) **Informes:** Sólo los usuarios administradores y jefes podrán acceder y accederán con todos los permisos a esta carpeta.



- b) **Reuniones:** Los jefes y empleados podrán acceder a leer y escribir.



- c) **Anuncios:** Los administradores y jefes podrán entrar a leer y escribir. Los empleados solo podrán leer.

 Propiedades de Anuncios

Mostrar todo

General +

Permisos -

Configuración +

Anuncios

Permisos

Los permisos para obtener acceso a los archivos de un recurso compartido se establecen mediante una combinación de permisos de carpeta, permisos de recurso compartido y, opcionalmente, una directiva de acceso central.


Permisos de los recursos compartidos: Todos tienen control total

Permisos de carpeta:

Tipo	Entidad de seguridad	Acceso	Se aplica a
Permitir	FRANCO\AdministradoresPracti...	Especial	Esta carpeta,
Permitir	FRANCO\Empleados	Leer	Esta carpeta,
Permitir	FRANCO\Jefes	Especial	Esta carpeta,
Permitir	BUILTIN\Administradores	Control total	Esta carpeta,
Permitir	NT AUTHORITY\SYSTEM	Control total	Esta carpeta,
Permitir	CREATOR OWNER	Control total	Solo subcarp

< Personalizar permisos... >

- d) **Pruebas:** Todos podrán leer y escribir.

 Propiedades de Pruebas

Mostrar todo

General +

Permisos -

Configuración +

Pruebas

Permisos

Los permisos para obtener acceso a los archivos de un recurso compartido se establecen mediante una combinación de permisos de carpeta, permisos de recurso compartido y, opcionalmente, una directiva de acceso central.

Permisos de los recursos compartidos: Todos tienen control total

Permisos de carpeta:

Tipo	Entidad de seguridad	Acceso	Se aplica a
Permitir	FRANCO\Usuarios del dominio	Especial	Esta carpeta, su
Permitir	BUILTIN\Administradores	Control total	Esta carpeta, su
Permitir	NT AUTHORITY\SYSTEM	Control total	Esta carpeta, su
Permitir	CREATOR OWNER	Control total	Solo subcarpeta

< Personalizar permisos... >