Asignatura	Datos del alumno	Fecha
Seguridad en Sistemas Operativos	Apellidos: Mehrez Garcia	16-01-2022
	Nombre: Amir Fernando Mamdouh	

FORTIFICACIÓN DE UN ENTORNO WINDOWS

Integrantes:

Espiritu Zarate, Danny Jonathan

Mehrez Garcia, Amir Fernando Mamdouh

Asignatura	Datos del alumno	Fecha
Seguridad en Sistemas Operativos	Apellidos: Mehrez Garcia	16-01-2022
	Nombre: Amir Fernando Mamdouh	

Tabla de contenido

Asignatura	Datos del alumno	Fecha
Seguridad en Sistemas Operativos	Apellidos: Mehrez Garcia	16-01-2022
	Nombre: Amir Fernando Mamdouh	

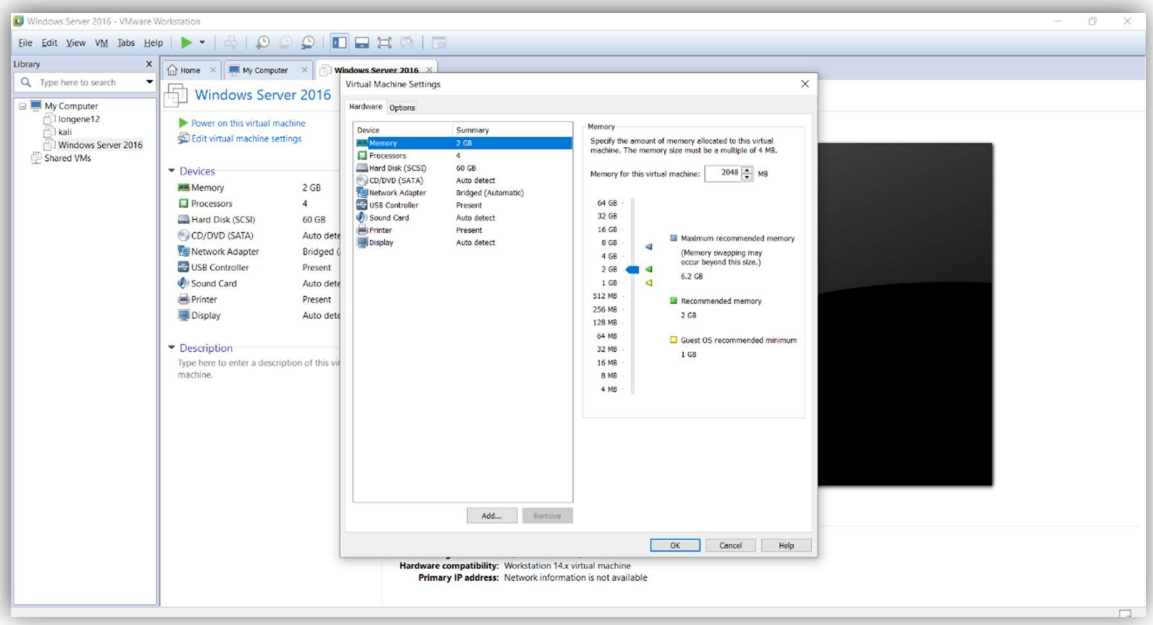
1 INTRODUCIÓN

En esta actividad se nos pide poner en práctica los conocimientos adquiridos en el primer tema de la asignatura de seguridad en sistemas operativos, mediante una actividad de grupo. Se nos pide desplegar un controlador de dominio y un equipo unido a este en el que aplicaremos diferentes medidas de seguridad, tanto a nivel de dominio como en el propio equipo. Para ello se ha realizado el laboratorio sobre una máquina virtual Windows Server 2016 y una maquina cliente Windows 7.

2 DESPLIEGUE DE UN CONTROLADOR DE DOMINIO

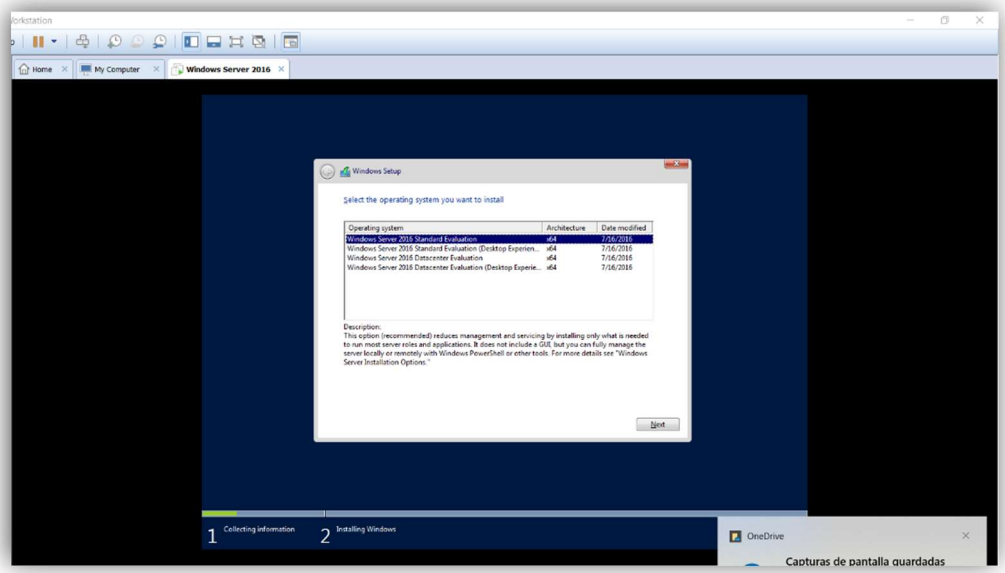
Se procedió con la descarga de la ISO de Windows Server 2016, la cual utilizaremos para la implementación del laboratorio de la actividad solicitada.

Luego procedemos con la configuración de hardware virtual que utilizaremos para poder implementar nuestra máquina virtual.



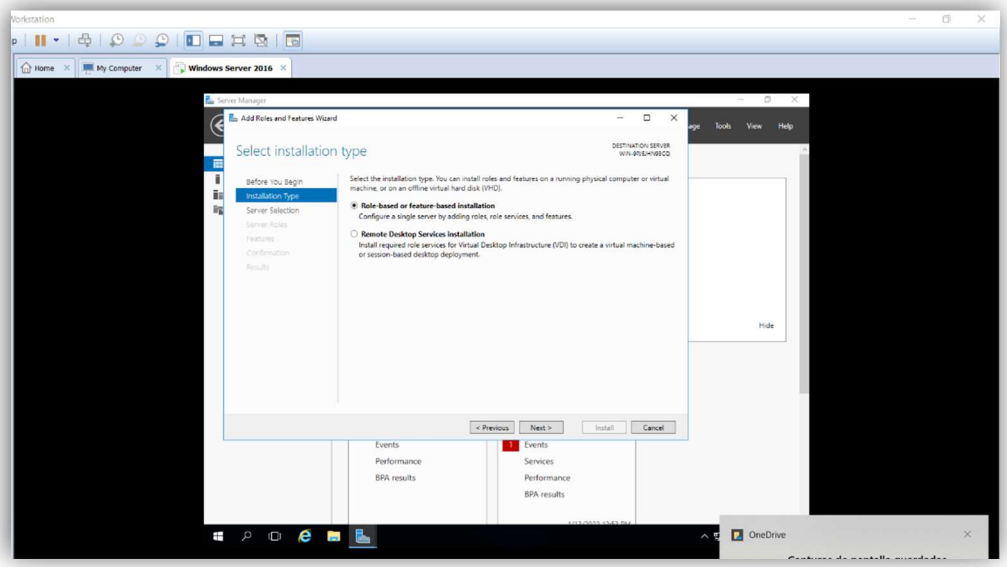
Para el presente laboratorio se utilizó el sistema operativo Windows Server 2016 Datacenter (Desktop experience) y sobre el cual resolveremos las distintas actividades.

Asignatura	Datos del alumno	Fecha
Seguridad en Sistemas Operativos	Apellidos: Mehrez Garcia	16-01-2022
	Nombre: Amir Fernando Mamdouh	



2.1 Añadir Roles y Características

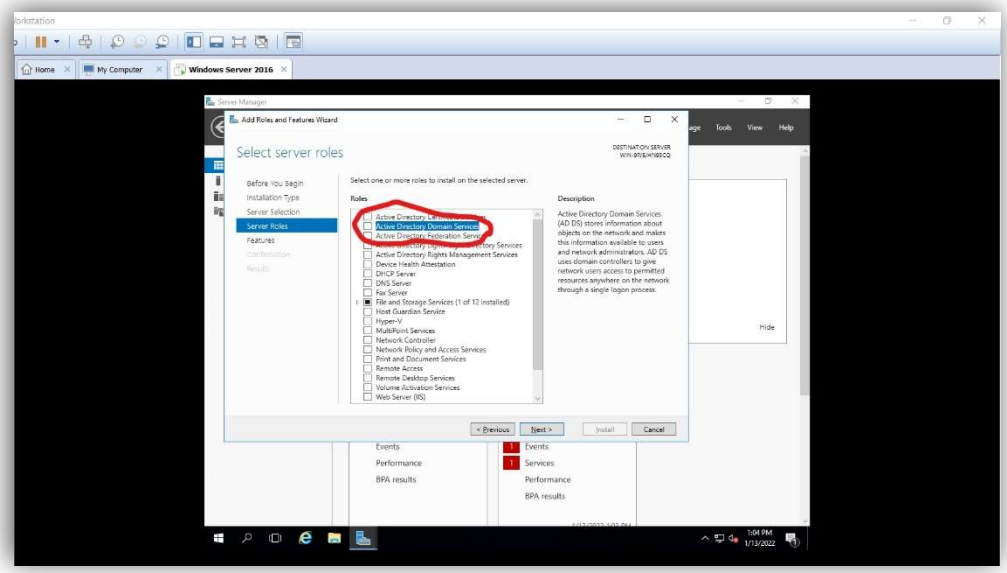
En primer lugar, accedemos al servidor Windows Server 2016 con la cuenta de administrador local y procedemos a agregar los roles necesarios a través del panel de administración del servidor, en concreto el rol de ACTIVE DIRECTORY DOMAIN SERVICES.



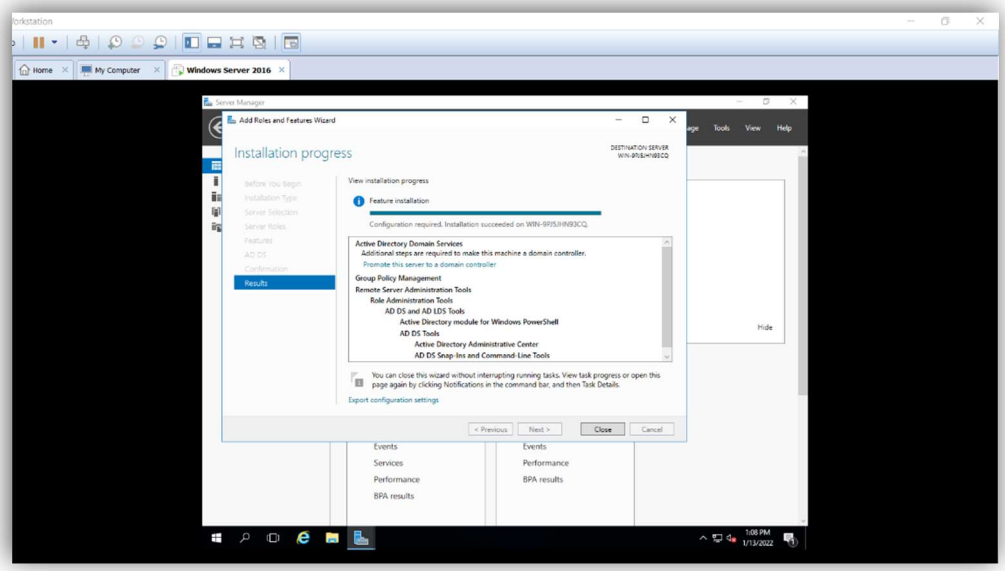
Seleccionamos el rol deseado y continuamos con el asistente.

Continuamos con el asistente confirmando la instalación de roles y características necesarias para implementar un servidor que sea controlador de dominio, tras el reinicio deberemos configurar el controlador.

Asignatura	Datos del alumno	Fecha
Seguridad en Sistemas Operativos	Apellidos: Mehrez Garcia	16-01-2022
	Nombre: Amir Fernando Mamdouh	



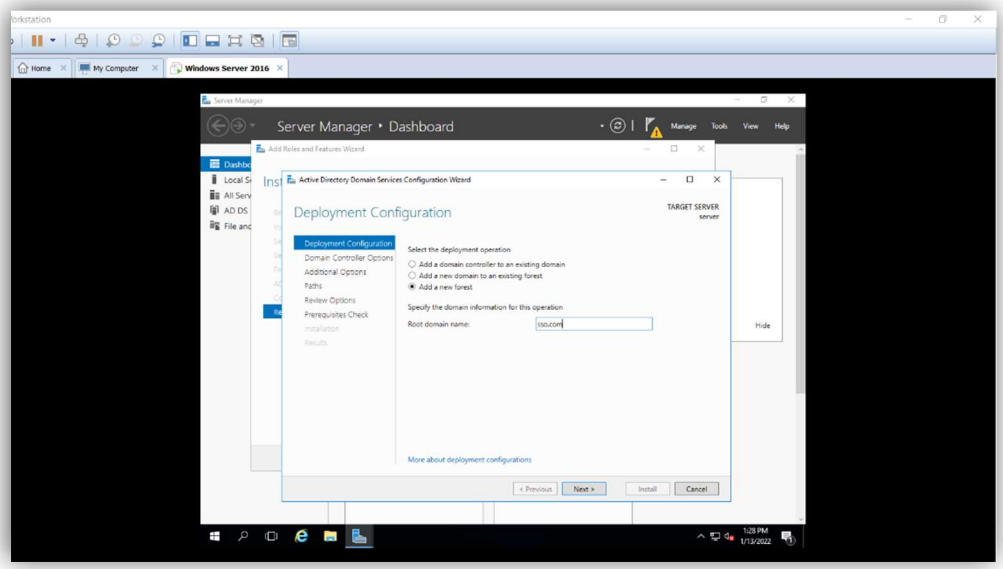
Vemos que la instalación a finalizado correctamente:



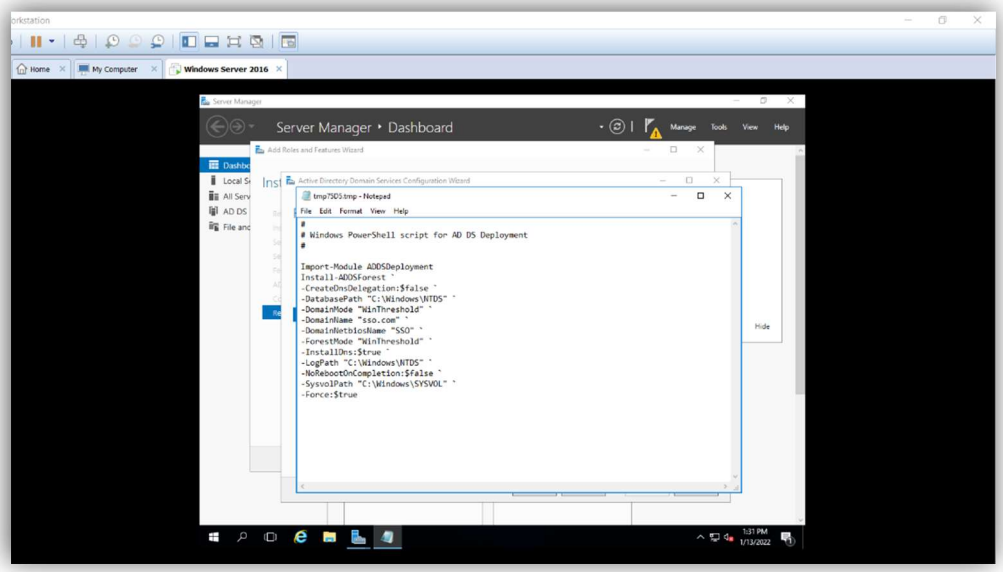
2.2 Promovemos el controlador de dominio

Tras el reinicio configuraremos el controlador de dominio tal cual se nos indica en la actividad, con el nombre de dominio **sso.com**

Asignatura	Datos del alumno	Fecha
Seguridad en Sistemas Operativos	Apellidos: Mehrez Garcia	16-01-2022
	Nombre: Amir Fernando Mamdouh	



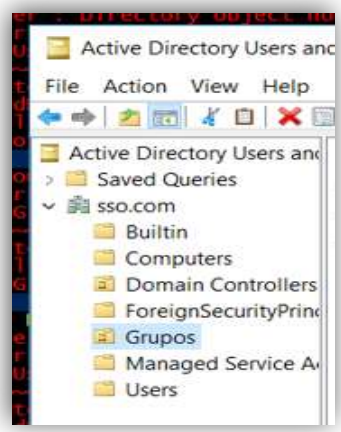
Luego de dar las opciones se crea este script por si se quiere autogenerar en otro servidor.



3 CONFIGURACIÓN DEL SERVIDOR WINDOWS 2012

Hemos optado por crear una OU (unidad organizativa) de nombre “Grupos” dentro del directorio activo, para la mejor gestión de los grupos y cuentas de usuario.

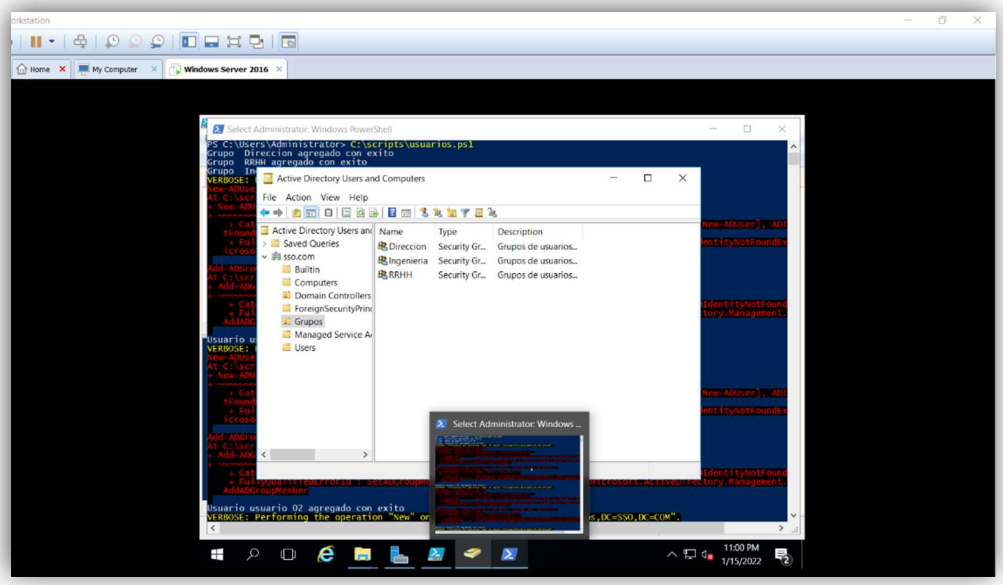
Asignatura	Datos del alumno	Fecha
Seguridad en Sistemas Operativos	Apellidos: Mehrez Garcia	16-01-2022
	Nombre: Amir Fernando Mamdouh	



3.1 Creación de grupos de trabajo

Se crea el script en el disco C, **"C:/scripts/usuarios.ps1".**

Con la primera parte del script se crean los Departamentos (grupos) que se solicita en la actividad y con la segunda parte del script se generan los usuarios.



Primera parte script - Departamentos (grupos)

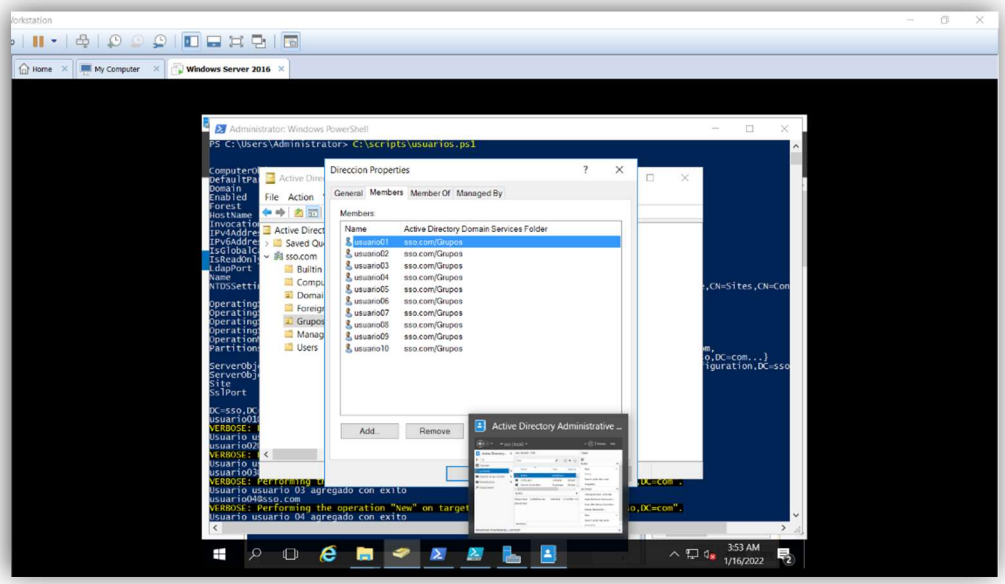
```
#Write-Host 'Hello from PowerShell!'
Import-Module ActiveDirectory
$data = @('Direccion','RRHH','Ingenieria') #arreglo de grupos
$cont = 0
#Get-ADDomainController -filter {IsGlobalCatalog -eq $True}
while($cont -lt 3)#este loop sirve para agregar los grupos basado en los arreglos
{
$grupo=""+$data[$cont]
New-ADGroup -Name $grupo -SamAccountName $grupo -GroupCategory Security -GroupScope Global -DisplayName "Departamento de $grupo" -Path "OU=Grupos,DC=sso,DC=com" -Description
"Grupos de usuarios de $grupo"
Write-Host "Grupo "$grupo" agregado con exito"
$cont++
}
```

Asignatura	Datos del alumno	Fecha
Seguridad en Sistemas Operativos	Apellidos: Mehrez Garcia	16-01-2022
	Nombre: Amir Fernando Mamdouh	

Segunda parte del script - creación de usuarios

```
$cont = 0 #reinicializar el contador de grupos en 0 para la asignacion del grupo cuando se agrega un nuevo usuario

#$ou="OU=Grupos,DC=sso,DC=com" Quise usar esta variable para el path pero mandaba error porque termina en :string

#Write-Host (Get-ADDomain).DistinguishedName ver controladores de dominio
$dominio= (Get-ADDomain).DNSRoot #obtener dominio
$usuario="0"
$cont2=.
while($cont2 -le 50) #loop para agregar usuarios sin usar un csv
{# las condicionales -le,-lt,etc estan documentadas en la bibliografia
if($cont2 -lt 10)
{$usuario="0"+$cont2}#si el usuario es menor de 10 se antepone el 0 para mantener los 2 digitos
if($cont2 -ge 10)
{$usuario=$cont2}

$grupo=""+$data[$cont]
$nombre="usuario"+$usuario
$UPN="usuario$usuario@$dominio"
Write-Host $UPN
New-ADUser -SamAccountName $nombre -UserPrincipalName ($UPN) -Name $nombre -DisplayName $nombre -Surname "Apellido$usuario" -GivenName "nombre$usuario" -Department "departamento$usuario" -
Description "descripcion del usuario$usuario" -AccountPassword (ConvertTo-SecureString "SSSO0-unli" -AsPlainText -Force) -Path "OU=Grupos,DC=sso,DC=com" -Enabled $true -
ChangePasswordAtLogon $true -Verbose

Add-ADGroupMember -Identity $grupo -Members $nombre #asignar el usuario a un grupo

Write-Host "Usuario usuario"$usuario" agregado con exito"

if($cont2 -eq 10)#al llegar al usuario nro 10 cambia de grupo de Direccion a RRHH
{$cont++}
if($cont2 -eq 30)#al llegar al usuario nro 10 cambia de grupo de RRHH a Ingenieria
{$cont++}
$cont2++

}
```

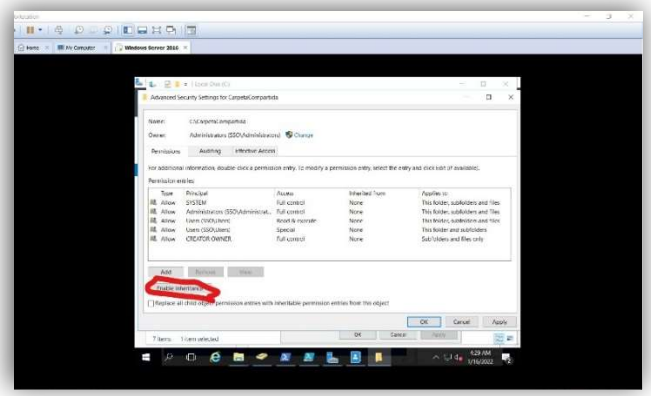
Se verifica si se crearon los usuarios de manera exitosa y si se asignaron los usuarios al grupo creado (“Grupos”).

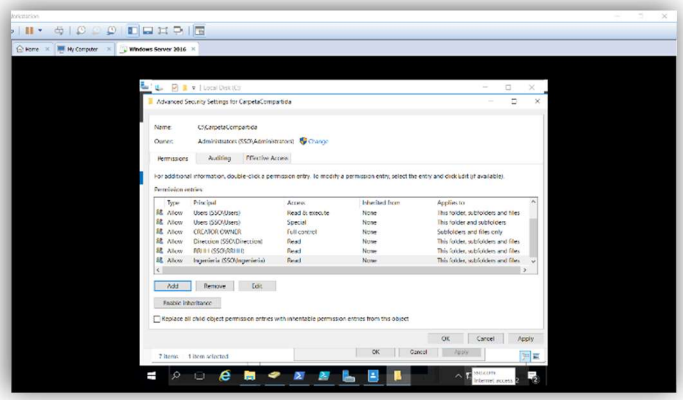


3.2 Creación de un recurso compartido

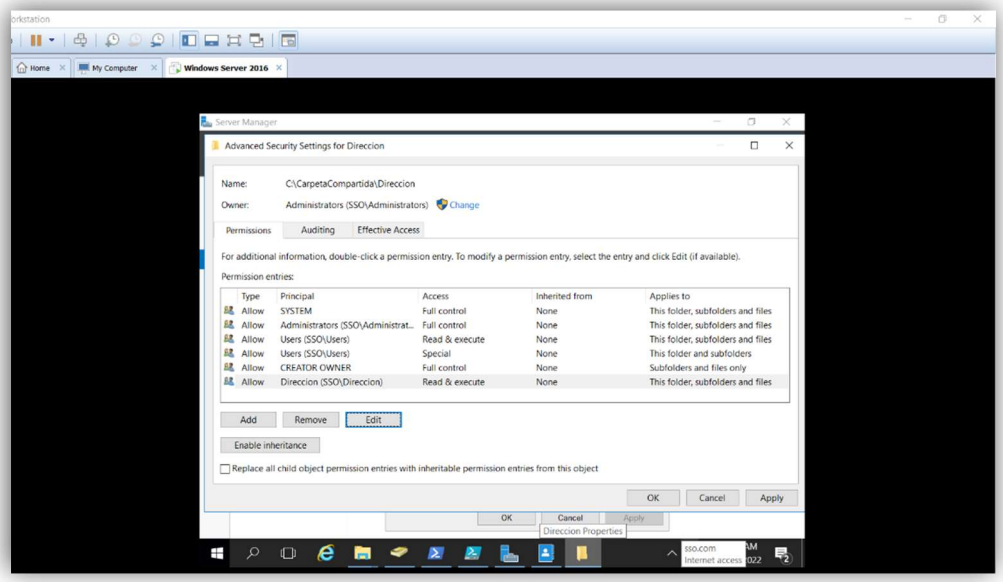
Se creo la carpeta llamada carpeta compartida y para que no haya problemas a largo plazo se desactivaron los permisos de herencia y a esta carpeta se le agregaron los 3 grupos en permiso “read”.

Asignatura	Datos del alumno	Fecha
Seguridad en Sistemas Operativos	Apellidos: Mehrez Garcia	16-01-2022
	Nombre: Amir Fernando Mamdouh	





Luego se crearon 3 carpetas dentro de esta y a cada una se le asignaros los permisos correspondientes, pero con read & execute que permite abrir, listar el contenido y ver la carpeta.

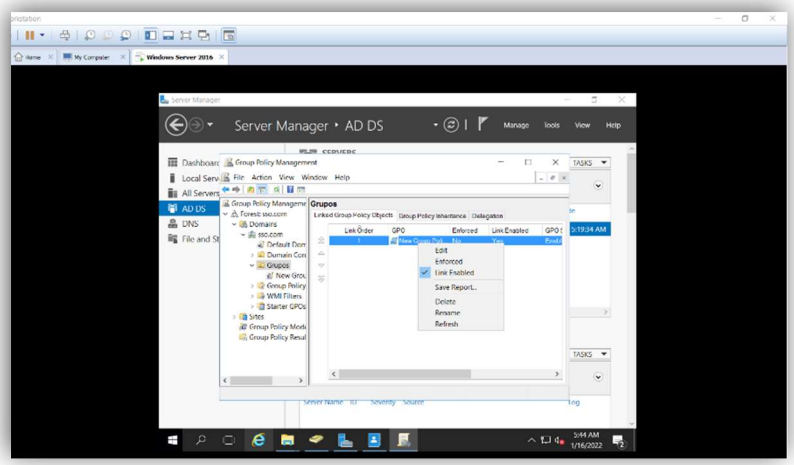


Asignatura	Datos del alumno	Fecha
Seguridad en Sistemas Operativos	Apellidos: Mehrez Garcia	16-01-2022
	Nombre: Amir Fernando Mamdouh	

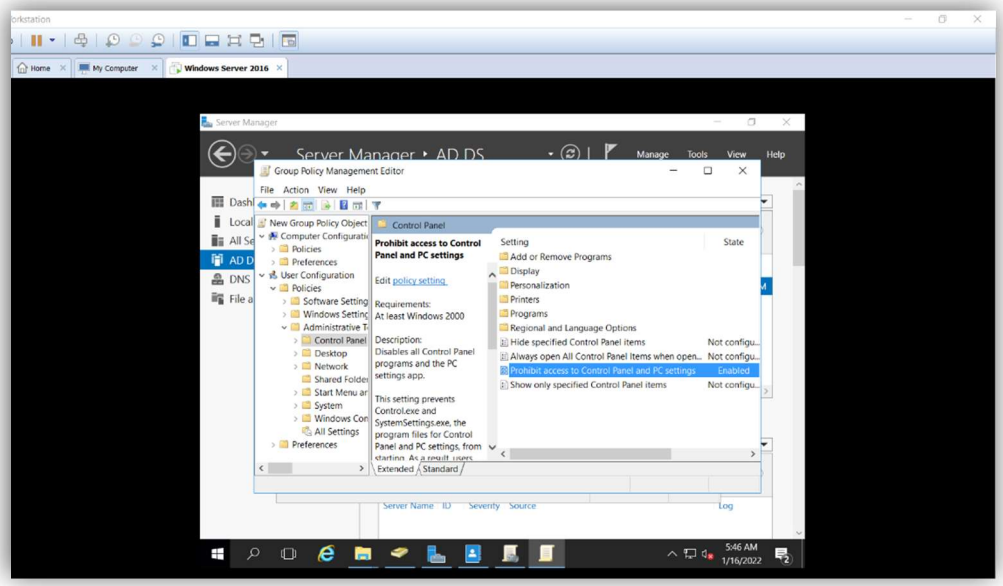
4 DIRECTIVAS DE SEGURIDAD EN EL DOMINIO

4.1 Panel de Control y fondo de pantalla

Se crea la política en group policy management.

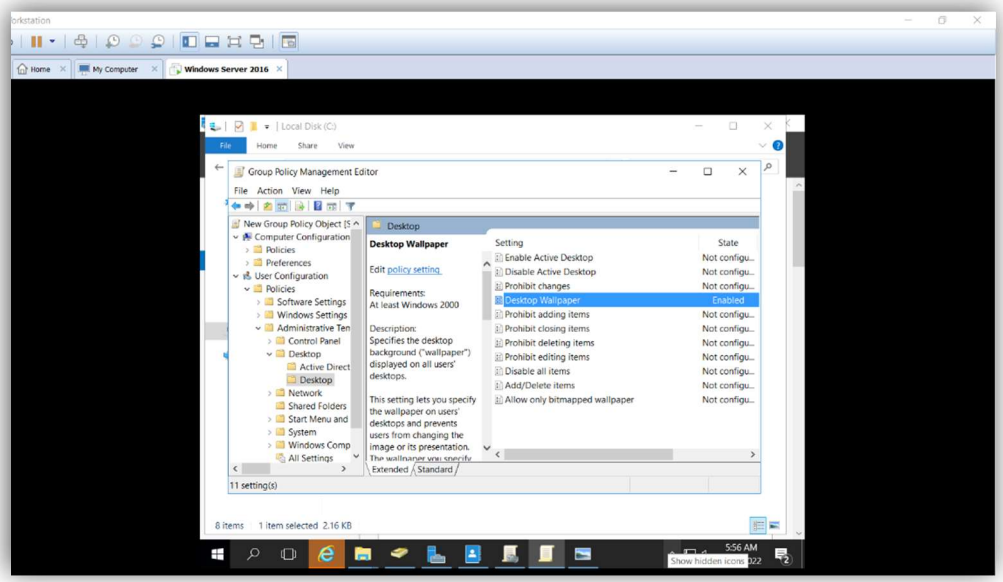


Para control panel se le da **"enable"** a este archivo "Prohibit Access to Control Panel and PC settings"



Y para desktop wallpaper es esta opción "Desktop Wallpaper".

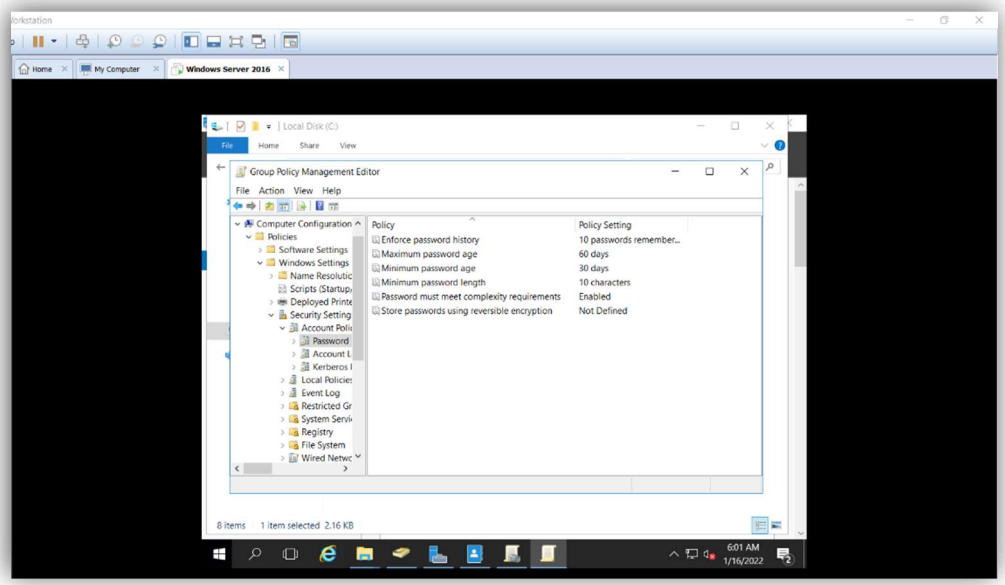
Asignatura	Datos del alumno	Fecha
Seguridad en Sistemas Operativos	Apellidos: Mehrez Garcia	16-01-2022
	Nombre: Amir Fernando Mamdouh	



4.2 Política de contraseñas en el directorio activo.

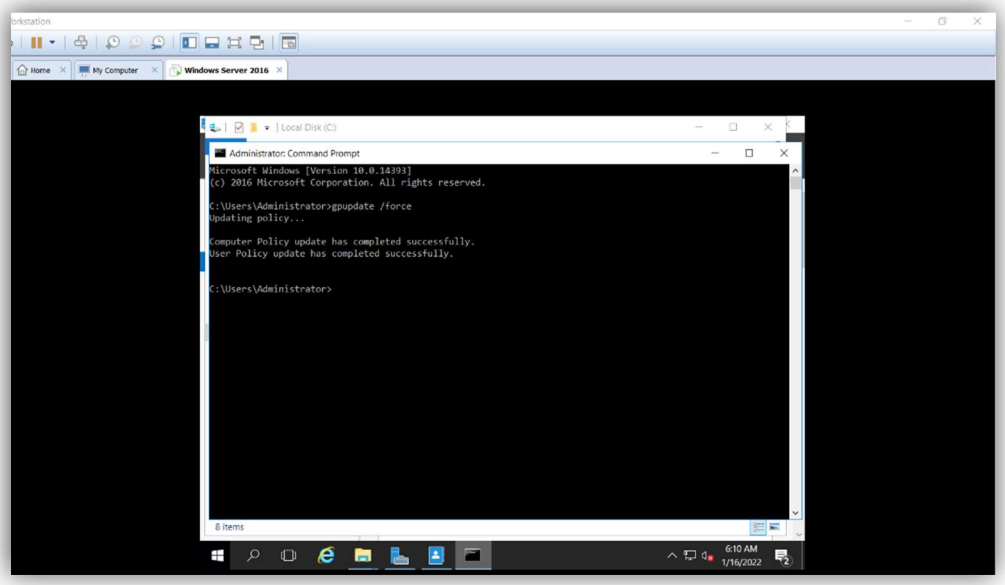
Configure los password de esta forma **"Minimum password lenght"** asegura que el tamaño mínimo de password si se quiere modificar sea de 10 y el enforce hace que la configuración de directiva Aplicara un historial de **contraseñas** determina el número de contraseñas nuevas únicas que deben asociarse a una cuenta de usuario antes de que se pueda reutilizar una contraseña antigua.

Aplicar el historial de contraseñas (Windows 10) - | de seguridad de Windows Documentos de Microsoft



Forzar la actualizacion de las políticas

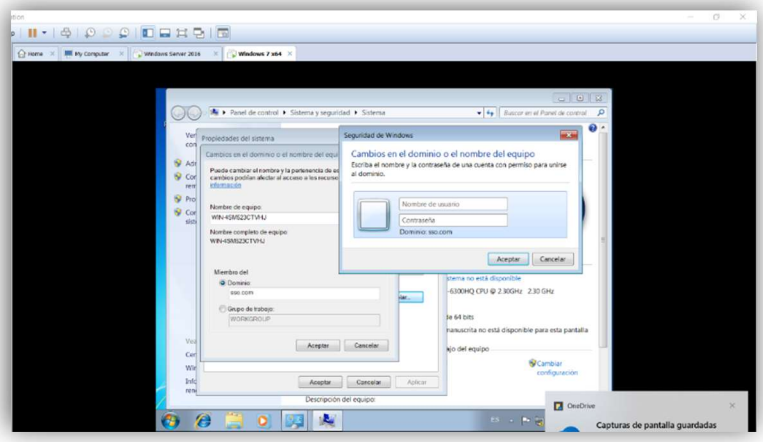
Asignatura	Datos del alumno	Fecha
Seguridad en Sistemas Operativos	Apellidos: Mehrez Garcia	16-01-2022
	Nombre: Amir Fernando Mamdouh	



5 COMPROBAR CONFIGURACIÓN EN WINDOWS 7

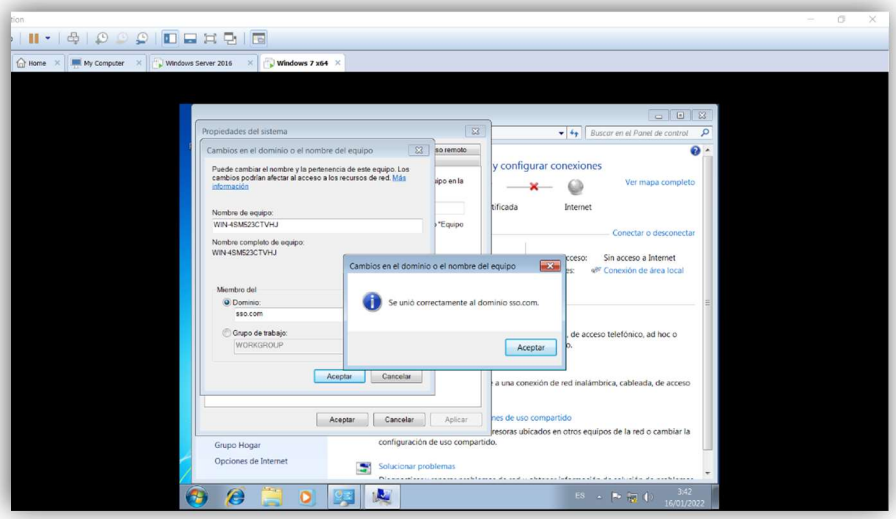
5.2 Unir Máquina al dominio

Para comprobar todas las configuraciones establecidas en los apartados anteriores uniremos un equipo con sistema operativo Windows 7 al dominio **sso.com** para ello accedemos a las propiedades del sistema y en la pestaña nombre del equipo con el botón cambiar, podemos modificar el nombre y con las credenciales del administrador de dominio podemos unirlo al dominio.



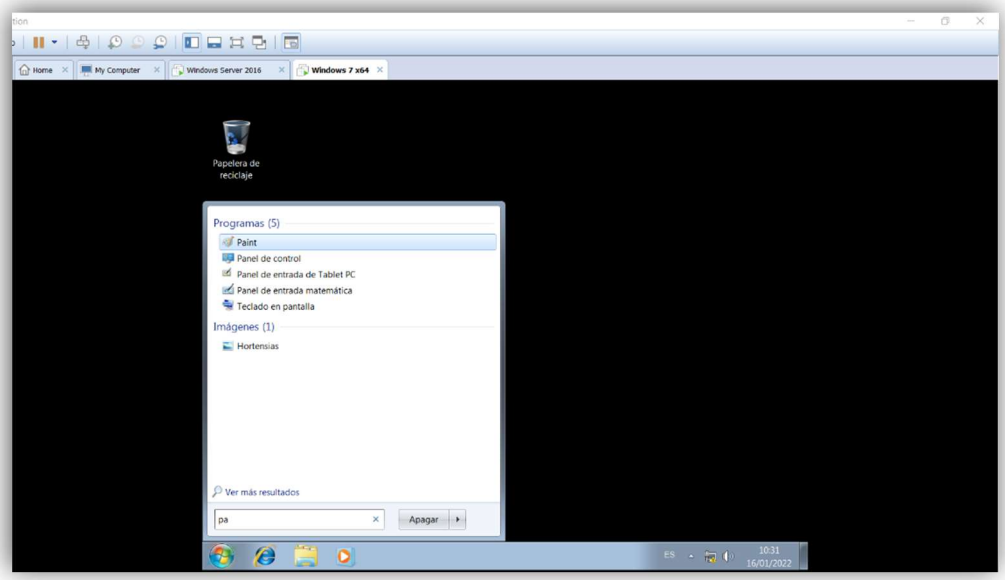
Y cuando te unes, ahora si ingresa de manera exitosa.

Asignatura	Datos del alumno	Fecha
Seguridad en Sistemas Operativos	Apellidos: Mehrez Garcia	16-01-2022
	Nombre: Amir Fernando Mamdouh	

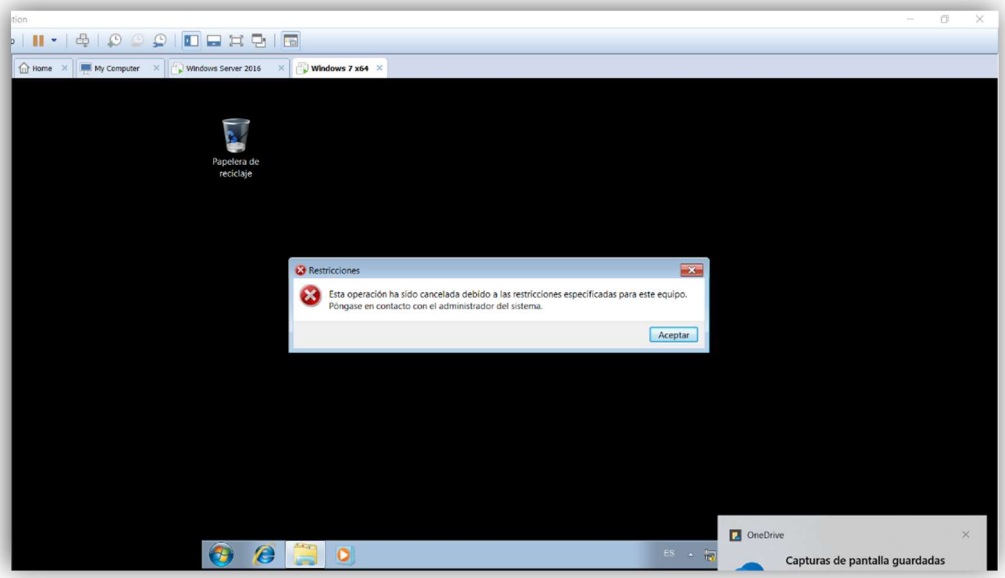


5.3 Políticas de panel de control y cambio de imagen

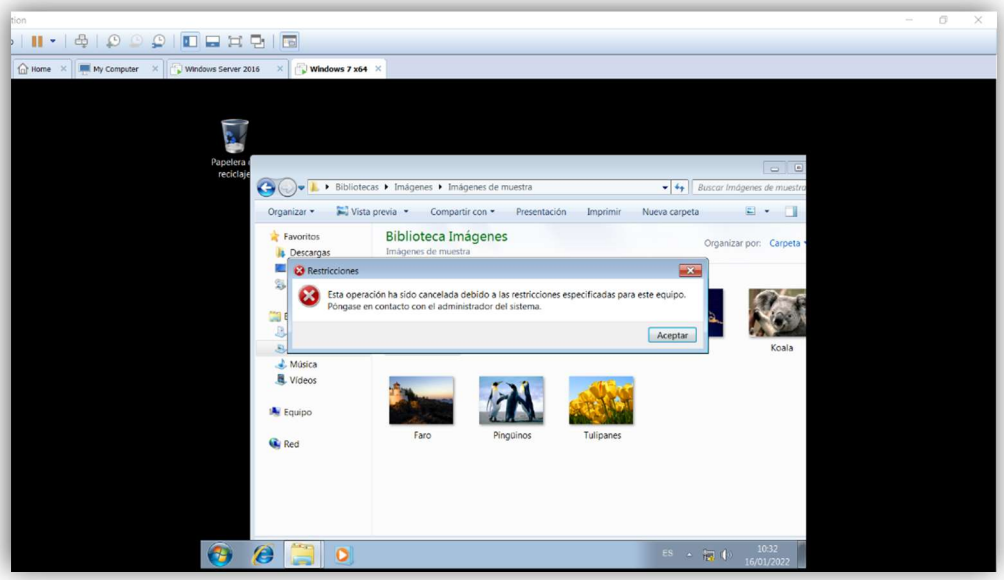
En este punto ya podemos comprobar que en el equipo se han configurado correctamente las políticas de seguridad y también que el usuario con el que accedemos dispone únicamente de los permisos necesarios para su grupo de pertenencia.



Asignatura	Datos del alumno	Fecha
Seguridad en Sistemas Operativos	Apellidos: Mehrez Garcia	16-01-2022
	Nombre: Amir Fernando Mamdouh	

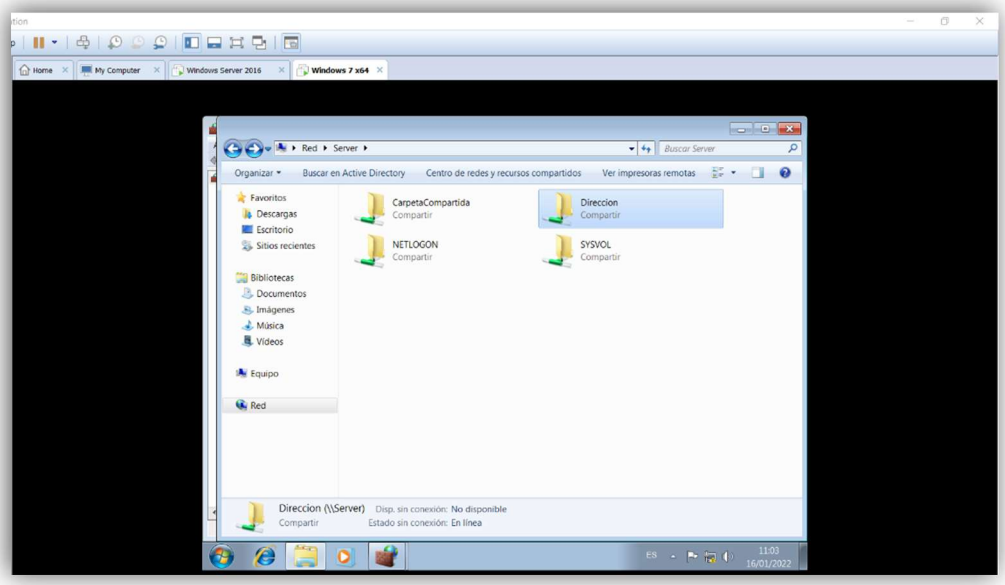


También evidenciamos la política generada “Desktop Wallpaper”

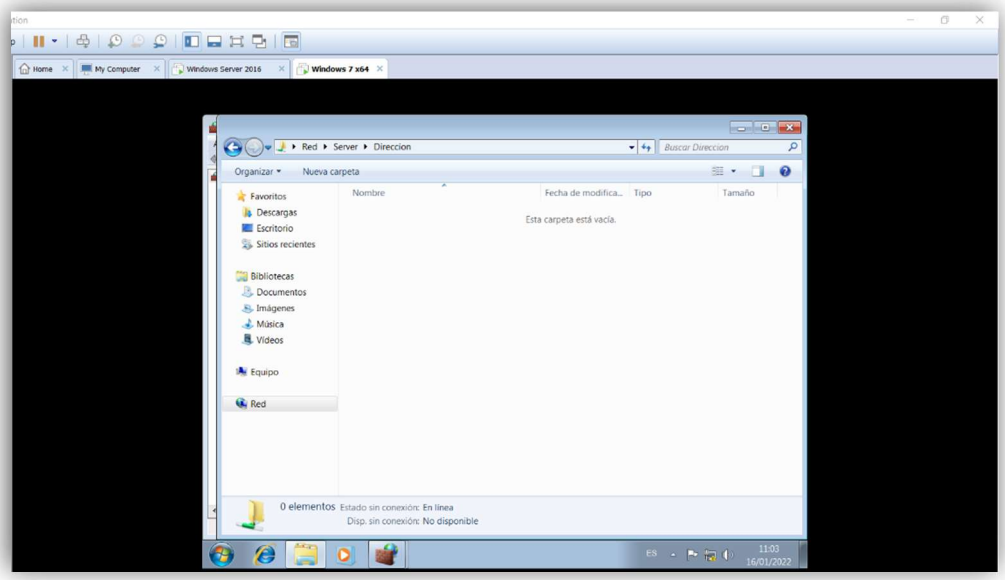


Explorar las carpetas que se pueden ver

Asignatura	Datos del alumno	Fecha
Seguridad en Sistemas Operativos	Apellidos: Mehrez Garcia	16-01-2022
	Nombre: Amir Fernando Mamdouh	



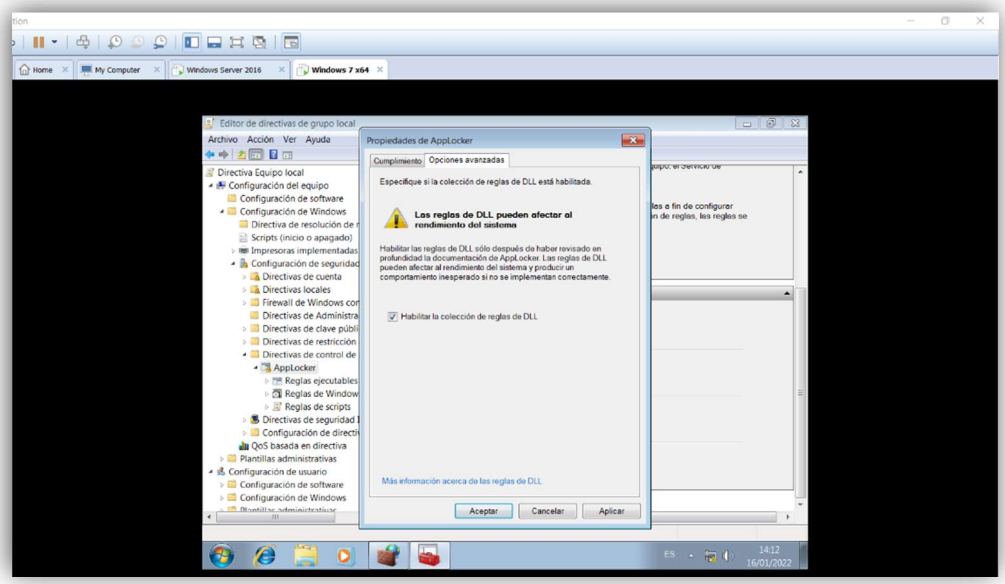
Como se hizo login con el usuario 01 solo se ve la carpeta dirección y permite abrirla.

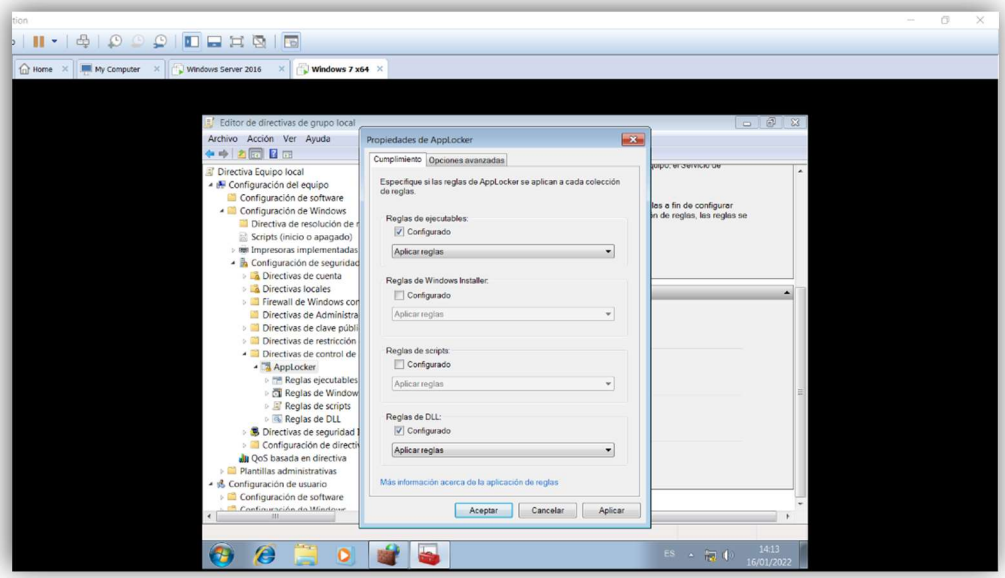


Asignatura	Datos del alumno	Fecha
Seguridad en Sistemas Operativos	Apellidos: Mehrez Garcia	16-01-2022
	Nombre: Amir Fernando Mamdouh	

6 CONFIGURACIÓN DE SEGURIDAD LOCAL EN WINDOWS 7

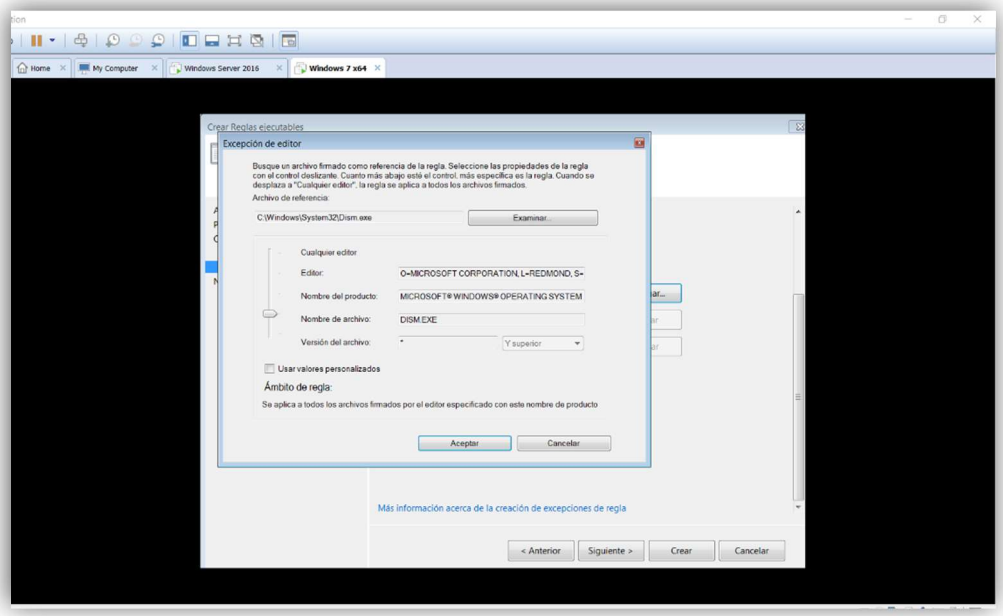
6.1 Reglas AppLocker

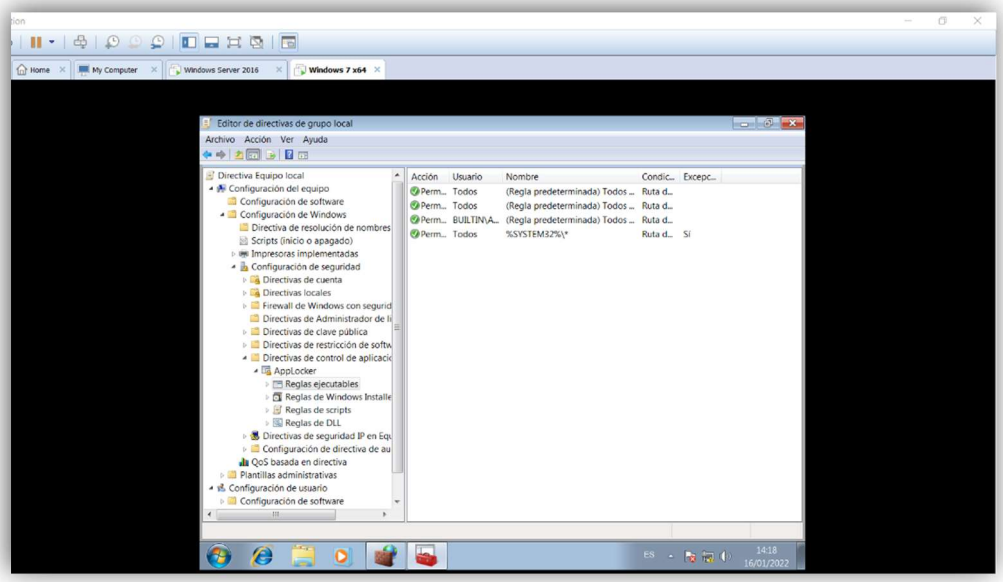




Permitir todo de la carpeta system32 y bloquear un archivo llamado “dism.exe”.

Asignatura	Datos del alumno	Fecha
Seguridad en Sistemas Operativos	Apellidos: Mehrez Garcia	16-01-2022
	Nombre: Amir Fernando Mamdouh	



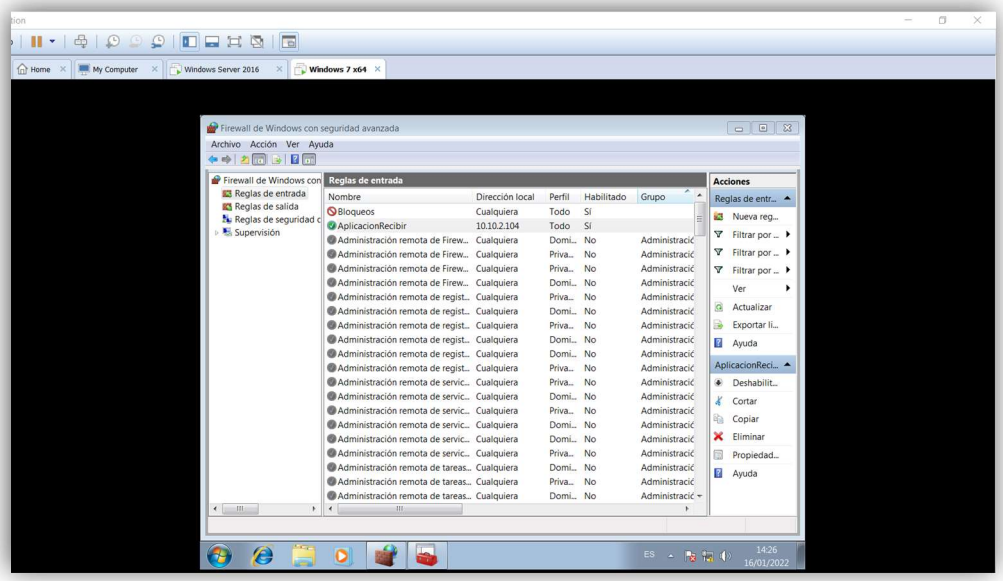


6.2 Configuración del Firewall de Windows

En la práctica nos indica que debemos bloquear todas las conexiones al equipo, a excepción de una aplicación que recibirá peticiones al puerto TCP desde la IP Local 10.10.2.104.

Para ello accedemos al panel de control con una cuenta de administrador local y en el firewall de Windows entramos en la configuración avanzada del cortafuegos.
Creamos una nueva regla de entrada personalizada con el asistente.
Aquí podemos ver cómo queda finalmente la configuración de las reglas de entrada del cortafuegos

Asignatura	Datos del alumno	Fecha
Seguridad en Sistemas Operativos	Apellidos: Mehrez Garcia	16-01-2022
	Nombre: Amir Fernando Mamdouh	



7 Resumen y referencias

En esta actividad se han puesto en práctica los conocimientos adquiridos en la asignatura de Seguridad en Sistemas Operativos. En particular se han utilizado para su desarrollo los apuntes y transparencias relativos a Seguridad en Sistemas Operativos Windows tanto a nivel de Equipo de usuario como de servidor, así como las referenciadas a PowerShell y políticas de dominio.
También se han utilizado los recursos disponibles en la web de soporte técnico de Microsoft y otros documentos en soporte digital.

Principales Referencias:

Prueba Windows Server 2016 en Microsoft Evaluation Software ¿Qué es Active Directory? ¿Cómo funciona? | Quest about While - PowerShell | Microsoft Docs

https://powertoe.wordpress.com/2009/12/14/powershell-part-4-arrays-and-for loops/

Operadores de Comparación con PowerShell Scripting - (salyseo.com) Powershell: Everything you wanted to know about arrays (powershellexplained.com)

active directory - New-ADUser -Path syntax? - Server Fault

New-ADUser (ActiveDirectory) | Microsoft Docs

Get-ADDomain (ActiveDirectory) | Microsoft Docs

PowerShell Array Guide: How to Use and Create (varonis.com)

New-ADGroup (ActiveDirectory) | Microsoft Docs

PowerShell Concatenate String | Different Examples of Concatenate String (educba.com)

Asignatura	Datos del alumno	Fecha
Seguridad en Sistemas Operativos	Apellidos: Mehrez Garcia	16-01-2022
	Nombre: Amir Fernando Mamdouh	

Adding User In Active Directory gives Error Directory Object not found powershell (microsoft.com)

New-ADUser error (microsoft.com)

Powershell Add Users Error - Spiceworks

GPO from Group Policy Objects

AEG: How to Create and Link a GPO in Active Directory :: AEG: How to Create and Link a GPO in Active Directory :: GlobalSign Support

Deploy Desktop Background Wallpaper using Group Policy (prajwaldesai.com)

Minimum Password Length auditing and enforcement on certain versions of Windows (microsoft.com)

Applocker :%SYSTEM32% xxx123yyy.DLL was prevented from running. (microsoft.com)

Firewall :How to Create Advanced Firewall Rules in the Windows Firewall (howtogeek.com)

8 Hoja de control

Para el presente trabajo se contó con la colaboración de los siguientes integrantes y en base a ello se procedió a llenar el cuadro:

- Espiritu Zarate, Danny Jonathan
- Mehrez Garcia, Amir Fernando Mamdouh

	Sí	**No**	**A veces**
Todos los miembros se han integrado al trabajo del grupo	X		
Todos los miembros participan activamente	X		
Todos los miembros respetan otras ideas aportadas	X		
Todos los miembros participan en la elaboración del informe	X		
Me he preocupado por realizar un trabajo cooperativo con mis compañeros	X		
Señala si consideras que algún aspecto del trabajo en grupo no ha sido adecuado		X	