

A dark blue vertical bar runs down the left side of the page. A blue arrow points to the right from this bar, containing the date.

22-4-2025

TAREA 1:

Iniciándonos en las GPO

Several thin, curved lines in shades of blue and grey originate from the bottom left and sweep upwards and to the right.

Cristóbal Suárez Abad

1º ASIR – IMPLANTACIÓN DE SISTEMAS OPERATIVOS

Índice:

- 0) Introducción.
- 1) Vista General de GPOs:
- 2) Bloquear Pendrives.
- 3) Bloqueo Automático Terminal.
- 4) Bloqueo Inicio Sesión Local.
- 5) Contraseña y Bloqueo de Cuentas.
- 6) Deshabilitar Firewall.
- 7) No Ejecución Aplicaciones Especificadas.
- 8) Comprobación de GPOs.
 - a. Imposible iniciar sesión con una cuenta que no sea alguna de las establecidas en “Bloqueo Inicio Sesión Local”.
 - b. Incapacidad para cambiar el Fondo de Pantalla.
 - c. No se permite el uso de dispositivos de Memoria USB.
 - d. No se puede ejecutar una serie de aplicaciones.

0) Introducción:

Replica las GPO implementadas (6 puntos) en el siguiente enlace:

<https://blog.ragasys.es/administracion-de-directivas-de-grupo-gpo-sobre-ms-windows-server-2016>

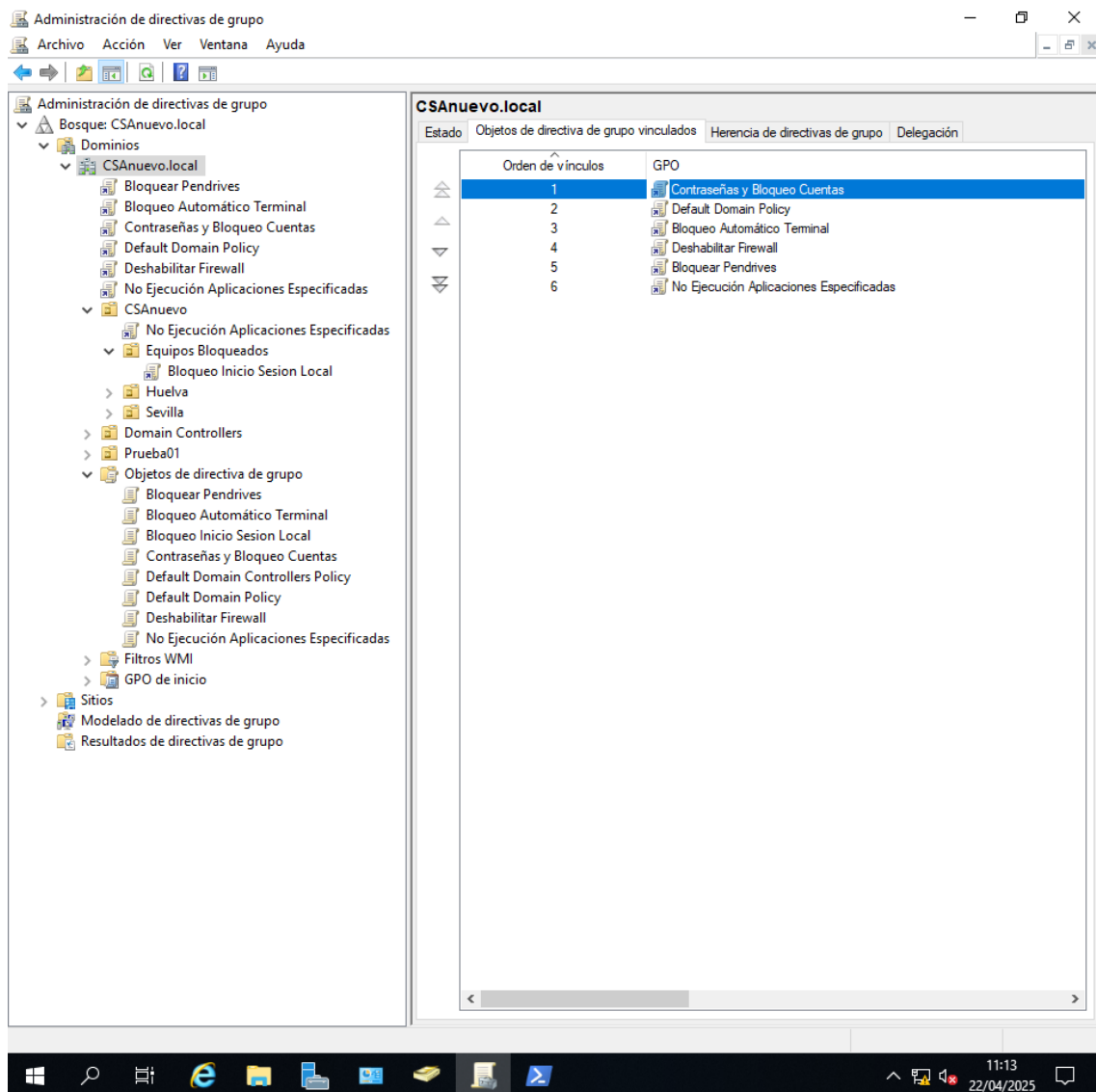
Si consideras oportuno algún cambio en las GPO, indícalo en el documento y justifícalo.

Finalmente, comprueba el funcionamiento de 2 de las GPO en algunos clientes o incluso desde el propio servidor. (3 puntos)

(1 punto) --> Presentación y documentación de la tarea -- En esta tarea no hace falta mucha documentación, simplemente id haciendo capturas de pantalla de cada GPO que vayáis creando y de sus características. Finalmente probad como os indico 2 de ellas y documentadlo.

1) Vista General de GPOs:

Como “Default Domain Policy ya tiene establecido normas sobre las contraseñas y bloqueo de cuentas, debemos establecer la GPO “Contraseñas y Bloqueo de Cuentas” con una prioridad superior a ella. Las GPO “Bloquear Pendrives” y “No Ejecución de Aplicaciones Especificadas” se han vinculado al dominio para que tengan efecto, cosa que en el ejemplo no aparece hecho.



2) Bloquear Pendrives.

Administración de directivas de grupo

Archivo Acción Ver Ventana Ayuda

Administración de directivas de grupo

- Bosque: CSAnuevo.local
 - Domínios
 - CSAnuevo.local
 - Bloqueo Automático Terminal
 - Contraseñas y Bloqueo Cuentas
 - Default Domain Policy
 - Deshabilitar Firewall
 - CSAnuevo
 - No Ejecución Aplicaciones Especificadas
 - Equipos Bloqueados
 - Bloqueo Inicio Sesión Local
 - Huelva
 - Sevilla
 - Domain Controllers
 - Prueba01
 - Objetos de directiva de grupo
 - Bloquear Pendrives**
 - Bloqueo Automático Terminal
 - Bloqueo Inicio Sesión Local
 - Contraseñas y Bloqueo Cuentas
 - Default Domain Controllers Policy
 - Default Domain Policy
 - Deshabilitar Firewall
 - No Ejecución Aplicaciones Especificadas
 - Filtros WMI
 - GPO de inicio
 - Sitios
 - Modelado de directivas de grupo
 - Resultados de directivas de grupo

Bloquear Pendrives

Ámbito Detalles Configuración Delegación Estado

autenticados seguridad)

Configuración del equipo (habilitada)

Directivas

Plantillas administrativas

Definiciones de directiva (archivos ADMX recuperadas del equipo local).

Sistema/Acceso de almacenamiento extraíble

Directiva	Configuración	Comentario
CD y DVD: denegar acceso de ejecución	Habilitado	
CD y DVD: denegar acceso de escritura	Habilitado	
CD y DVD: denegar acceso de lectura	Habilitado	
Discos extraíbles: denegar acceso de ejecución	Habilitado	
Discos extraíbles: denegar acceso de escritura	Habilitado	
Discos extraíbles: denegar acceso de lectura	Habilitado	
Dispositivos WPD: denegar acceso de escritura	Habilitado	
Dispositivos WPD: denegar acceso de lectura	Habilitado	
Todas las clases de almacenamiento extraíble: denegar acceso a todo	Habilitado	
Unidades de disquete: denegar acceso de ejecución	Habilitado	
Unidades de disquete: denegar acceso de escritura	Habilitado	
Unidades de disquete: denegar acceso de lectura	Habilitado	

Configuración del usuario (habilitada)

Configuración no definida.

9:54 22/04/2025

3) Bloqueo Automático Terminal.

Administración de directivas de grupo

Archivo Acción Ver Ventana Ayuda

Administración de directivas de grupo

Bosque: CSAnuevo.local

Dominios

CSAnuevo.local

Bloquear Pendrives

Bloqueo Automático Terminal

Contraseñas y Bloqueo Cuentas

Default Domain Policy

Deshabilitar Firewall

No Ejecución Aplicaciones Especificadas

CSAnuevo

No Ejecución Aplicaciones Especificadas

Equipos Bloqueados

Bloqueo Inicio Sesión Local

Huelva

Sevilla

Domain Controllers

Prueba01

Objetos de directiva de grupo

Bloquear Pendrives

Bloqueo Automático Terminal

Bloqueo Inicio Sesión Local

Contraseñas y Bloqueo Cuentas

Default Domain Controllers Policy

Default Domain Policy

Deshabilitar Firewall

No Ejecución Aplicaciones Especificadas

Filtros WMI

GPO de inicio

Sitios

Modelado de directivas de grupo

Resultados de directivas de grupo

Bloqueo Automático Terminal

Ámbito Detalles Configuración Delegación Estado

Nombre	Permisos válidos	Heredado
CSANUEVO\Administradores de empresas	Editar configuración, eliminar, modificar seguridad	No
CSANUEVO\Admins. del dominio	Editar configuración, eliminar, modificar seguridad	No
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Lectura	No
NT AUTHORITY\SYSTEM	Editar configuración, eliminar, modificar seguridad	No
NT AUTHORITY\Usuarios autenticados	Lectura (de Filtro de seguridad)	No

Configuración del equipo (habilitada)

Configuración no definida.

Configuración del usuario (habilitada)

Directivas

Plantillas administrativas

Definiciones de directiva (archivos ADMX) recuperadas del equipo local.

Panel de control/Personalización

Directiva	Configuración	Comentario
Habilitar protector de pantalla	Habilitado	
Impedir cambiar el fondo de pantalla	Habilitado	
Impedir cambiar el protector de pantalla	Habilitado	
Impedir cambiar el tema	Habilitado	
Proteger el protector de pantalla mediante contraseña	Habilitado	
Tiempo de espera del protector de pantalla	Habilitado	

Número de segundos de espera hasta que se active el protector de pantalla

Segundos: 1200

11:19

22/04/2025

4) Bloqueo Inicio Sesión Local.

Administración de directivas de grupo

ArchivoAcciónVerVentanaAyuda

Administración de directivas de grupo

Bosque: CSAnuevo.local

Domínios

CSAnuevo.local

Bloqueo Automático Terminal

Contraseñas y Bloqueo Cuentas

Default Domain Policy

Deshabilitar Firewall

CSAnuevo

No Ejecución Aplicaciones Especificadas

Equipos Bloqueados

Bloqueo Inicio Sesión Local

Huelva

Sevilla

Domain Controllers

Prueba01

Objetos de directiva de grupo

Bloquear Pendrives

Bloqueo Automático Terminal

Bloqueo Inicio Sesión Local

Contraseñas y Bloqueo Cuentas

Default Domain Controllers Policy

Default Domain Policy

Deshabilitar Firewall

No Ejecución Aplicaciones Especificadas

Filtros WMI

GPO de inicio

Sitios

Modelado de directivas de grupo

Resultados de directivas de grupo

Bloqueo Inicio Sesión Local

ÁmbitoDetallesConfiguraciónDelegaciónEstado

Esta lista solo incluye vínculos en el dominio del GPO.

Filtrado de seguridad

La configuración en este GPO solo se puede aplicar a los grupos, usuarios y equipos siguientes:

Nombre

NT AUTHORITY\Usuarios autenticados

Delegación

Estos grupos y usuarios tienen los permisos especificados para este GPO

Nombre	Permisos válidos	Heredado
CSANUEVO\Administradores de empresas	Editar configuración, eliminar, modificar seguridad	No
CSANUEVO\Admins. del dominio	Editar configuración, eliminar, modificar seguridad	No
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Lectura	No
NT AUTHORITY\SYSTEM	Editar configuración, eliminar, modificar seguridad	No
NT AUTHORITY\Usuarios autenticados	Lectura (de Filtrado de seguridad)	No

Configuración del equipo (habilitada)

Directivas

Configuración de Windows

Configuración de seguridad

Directivas locales/Asignación de derechos de usuario

Directiva	Configuración
Permitir el inicio de sesión local	CSANUEVO\Admins. del dominio, BUILTIN\Administradores

Configuración del usuario (habilitada)

Configuración no definida.

9:55

22/04/2025

5) Contraseña y Bloqueo de Cuentas.

Administración de directivas de grupo

Archivo Acción Ver Ventana Ayuda

Administración de directivas de grupo

Bosque: CSAnuevo.local

- Dominios
 - CSAnuevo.local
 - Bloqueo Automático Terminal
 - Contraseñas y Bloqueo Cuentas
 - Default Domain Policy
 - Deshabilitar Firewall
 - CSAnuevo
 - No Ejecución Aplicaciones Especificadas
 - Equipos Bloqueados
 - Bloqueo Inicio Sesión Local
 - Huelva
 - Sevilla
 - Domain Controllers
 - Prueba01
 - Objetos de directiva de grupo
 - Bloquear Pendrives
 - Bloqueo Automático Terminal
 - Bloqueo Inicio Sesión Local
 - Contraseñas y Bloqueo Cuentas
 - Default Domain Controllers Policy
 - Default Domain Policy
 - Deshabilitar Firewall
 - No Ejecución Aplicaciones Especificadas
 - Filtros WMI
 - GPO de inicio
 - Sitios
 - Modelado de directivas de grupo
 - Resultados de directivas de grupo

Contraseñas y Bloqueo Cuentas

Ámbito Detalles Configuración Delegación Estado

de empresas	modificar seguridad		
CSANUEVO\Admins. del dominio	Editar configuración, eliminar, modificar seguridad	No	
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Lectura	No	
NT AUTHORITY\SYSTEM	Editar configuración, eliminar, modificar seguridad	No	
NT AUTHORITY\Usuarios autenticados	Lectura (de Filtrado de seguridad)	No	

Configuración del equipo (habilitada)

Directivas

Configuración de Windows

Configuración de seguridad

Directivas de cuenta/Directiva de contraseñas

Directiva	Configuración
Almacenar contraseñas usando cifrado reversible	Deshabilitado
Exigir historial de contraseñas	5 contraseñas recordadas
Las contraseñas deben cumplir los requisitos de complejidad	Habilitado
Longitud mínima de la contraseña	7 caracteres
Vigencia máxima de la contraseña	180 días
Vigencia mínima de la contraseña	0 días

Directivas de cuenta/Directiva de bloqueo de cuenta

Directiva	Configuración
Duración del bloqueo de cuenta	25 minutos
Restablecer recuentos de bloqueo de cuenta tras	25 minutos
Umbral de bloqueo de cuenta	10 intentos de inicio de sesión no válidos

Configuración del usuario (habilitada)

Configuración no definida.

9:55 22/04/2025

6) Deshabilitar Firewall.

Administración de directivas de grupo

Archivo Acción Ver Ventana Ayuda

Administración de directivas de grupo

- ▼ Bosque: CSAnuevo.local
 - ▼ Dominios
 - CSAnuevo.local
 - Bloqueo Automático Terminal
 - Contraseñas y Bloqueo Cuentas
 - Default Domain Policy
 - Deshabilitar Firewall
 - ▼ CSAnuevo
 - No Ejecución Aplicaciones Especificadas
 - ▼ Equipos Bloqueados
 - Bloqueo Inicio Sesión Local
 - Huelva
 - Sevilla
 - Domain Controllers
 - Prueba01
 - ▼ Objetos de directiva de grupo
 - Bloquear Pendrives
 - Bloqueo Automático Terminal
 - Bloqueo Inicio Sesión Local
 - Contraseñas y Bloqueo Cuentas
 - Default Domain Controllers Policy
 - Default Domain Policy
 - Deshabilitar Firewall
 - No Ejecución Aplicaciones Especificadas
 - Filtros WMI
 - GPO de inicio
 - Sitios
- Modelado de directivas de grupo
- Resultados de directivas de grupo

Deshabilitar Firewall

Ámbito Detalles Configuración Delegación Estado

Directivas

Configuración de Windows

Configuración de seguridad

Firewall de Windows con seguridad avanzada

Configuración global

Directiva	Configuración
Versión de directivas	2.29
Deshabilitar FTP con estado	No configurado
Deshabilitar PPTP con estado	No configurado
Exención de IPsec	No configurado
IPsec a través de NAT	No configurado
Codificación de clave previamente compartida	No configurado
Tiempo inactivo de SA	No configurado
Comprobación CRL fuerte	No configurado

Configuración de perfil de dominio

Directiva	Configuración
Estado del firewall	Desactivado
Conexiones entrantes	No configurado
Conexiones salientes	No configurado
Aplicar reglas de firewall local	No configurado
Aplicar reglas de seguridad de conexión local	No configurado
Mostrar notificaciones	No configurado
Permitir respuestas de unidifusión	No configurado
Registrar paquetes perdidos	No configurado
Registrar conexiones correctas	No configurado
Ruta de acceso del archivo de registro	No configurado
Tamaño máximo del archivo de registro (KB)	No configurado

Configuración de seguridad de conexión

Plantillas administrativas

Definiciones de directiva (archivos ADMX) recuperadas del equipo local.

Red/Conexiones de red/Firewall de Windows Defender/Perfil de dominio

9:57 22/04/2025

Administración de directivas de grupo

ArchivoAcciónVerVentanaAyuda

Administración de directivas de grupo

Bosque: CSAnuevo.local

Dominios

CSAnuevo.local

Bloqueo Automático Terminal

Contraseñas y Bloqueo Cuentas

Default Domain Policy

Deshabilitar Firewall

CSAnuevo

No Ejecución Aplicaciones Especificadas

Equipos Bloqueados

Bloqueo Inicio Sesión Local

Huelva

Sevilla

Domain Controllers

Prueba01

Objetos de directiva de grupo

Bloquear Pendrives

Bloqueo Automático Terminal

Bloqueo Inicio Sesión Local

Contraseñas y Bloqueo Cuentas

Default Domain Controllers Policy

Default Domain Policy

Deshabilitar Firewall

No Ejecución Aplicaciones Especificadas

Filtros WMI

GPO de inicio

Sitios

Modelado de directivas de grupo

Resultados de directivas de grupo

Deshabilitar Firewall

Ámbito

Detalles

Configuración

Delegación

Estado

Coordinación de clave previamente compartida

No configurado

Tiempo inactivo de SA

No configurado

Comprobación CRL fuerte

No configurado

Configuración de perfil de dominio

Directiva	Configuración
Estado del firewall	Desactivado
Conexiones entrantes	No configurado
Conexiones salientes	No configurado
Aplicar reglas de firewall local	No configurado
Aplicar reglas de seguridad de conexión local	No configurado
Mostrar notificaciones	No configurado
Permitir respuestas de unidifusión	No configurado
Registrar paquetes perdidos	No configurado
Registrar conexiones correctas	No configurado
Ruta de acceso del archivo de registro	No configurado
Tamaño máximo del archivo de registro (KB)	No configurado

Configuración de seguridad de conexión

Plantillas administrativas

Definiciones de directiva (archivos ADMX) recuperadas del equipo local.

Red/Conexiones de red/Firewall de Windows Defender/Perfil de dominio

Directiva	Configuración	Comentario
Firewall de Windows Defender: proteger todas las conexiones de red	Deshabilitado	

Red/Conexiones de red/Firewall de Windows Defender/Perfil estándar

Directiva	Configuración	Comentario
Firewall de Windows Defender: proteger todas las conexiones de red	Deshabilitado	

Configuración del usuario (habilitada)

Configuración no definida.

Windows

9:57

22/04/2025

7) No Ejecución Aplicaciones Especificadas.

Administración de directivas de grupo

Archivo Acción Ver Ventana Ayuda

Administración de directivas de grupo

- Bosque: CSAnuevo.local
 - Dominios
 - CSAnuevo.local
 - Bloqueo Automático Terminal
 - Contraseñas y Bloqueo Cuentas
 - Default Domain Policy
 - Deshabilitar Firewall
 - CSAnuevo
 - No Ejecución Aplicaciones Especificadas
 - Equipos Bloqueados
 - Bloqueo Inicio Sesión Local
 - Huelva
 - Sevilla
 - Domain Controllers
 - Prueba01
 - Objetos de directiva de grupo
 - Bloquear Pendrives
 - Bloqueo Automático Terminal
 - Bloqueo Inicio Sesión Local
 - Contraseñas y Bloqueo Cuentas
 - Default Domain Controllers Policy
 - Default Domain Policy
 - Deshabilitar Firewall
 - No Ejecución Aplicaciones Especificadas
 - Filtros WMI
 - GPO de inicio
 - Sitios
 - Modelado de directivas de grupo
 - Resultados de directivas de grupo

No Ejecución Aplicaciones Especificadas

Ámbito Detalles Configuración Delegación Estado

NT AUTHORITY\Usuarios autenticados

Delegación

Estos grupos y usuarios tienen los permisos especificados para este GPO

Nombre	Permisos válidos	Heredado
CSANUEVO\Administradores de empresas	Editar configuración, eliminar, modificar seguridad	No
CSANUEVO\Admins. del dominio	Editar configuración, eliminar, modificar seguridad	No
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Lectura	No
NT AUTHORITY\SYSTEM	Editar configuración, eliminar, modificar seguridad	No
NT AUTHORITY\Usuarios autenticados	Lectura (de Filtro de seguridad)	No

Configuración del equipo (habilitada)

Configuración no definida.

Configuración del usuario (habilitada)

Directivas

Plantillas administrativas

Definiciones de directiva (archivos ADMX) recuperadas del equipo local.

Sistema

Directiva	Configuración	Comentario
No ejecutar aplicaciones de Windows especificadas	Habilitado	

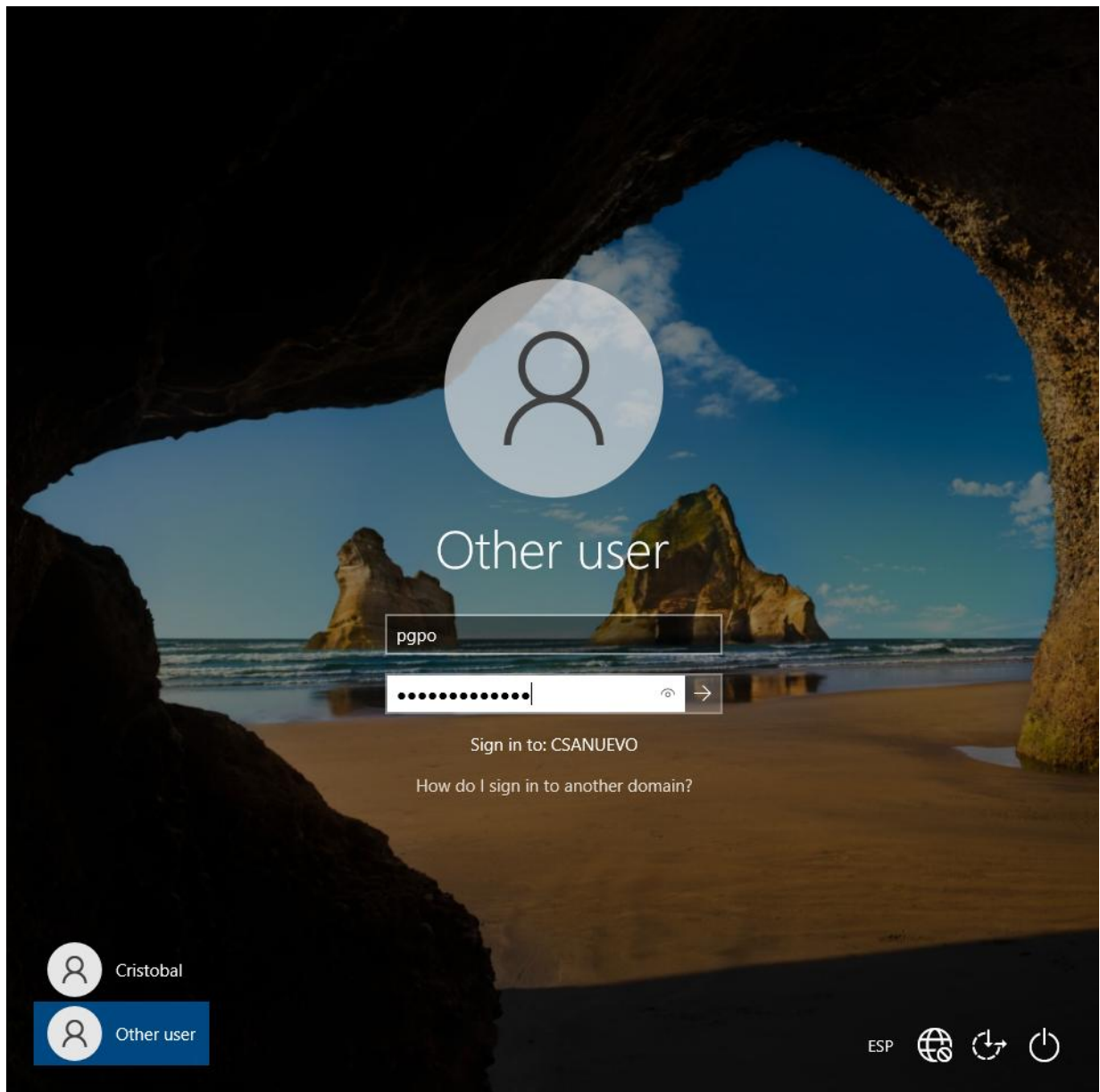
Lista de aplicaciones no permitidas

- emule.exe
- ares.exe
- utorrent.exe
- dropbox.exe

9:57 22/04/2025

8) Comprobación de GPOs.

- a. Imposible iniciar sesión con una cuenta que no sea alguna de las establecidas en “Bloqueo Inicio Sesión Local”.



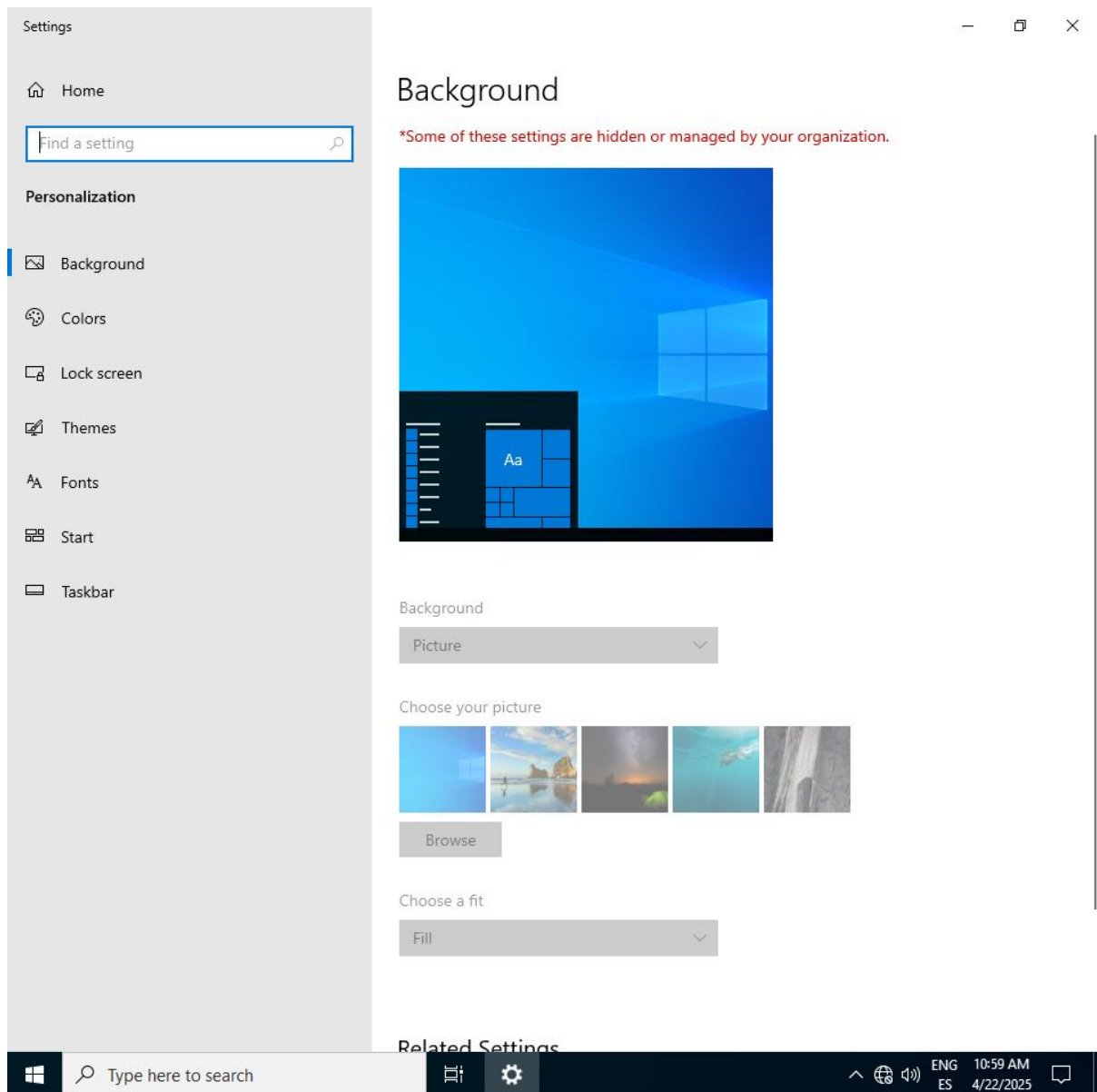


Other user

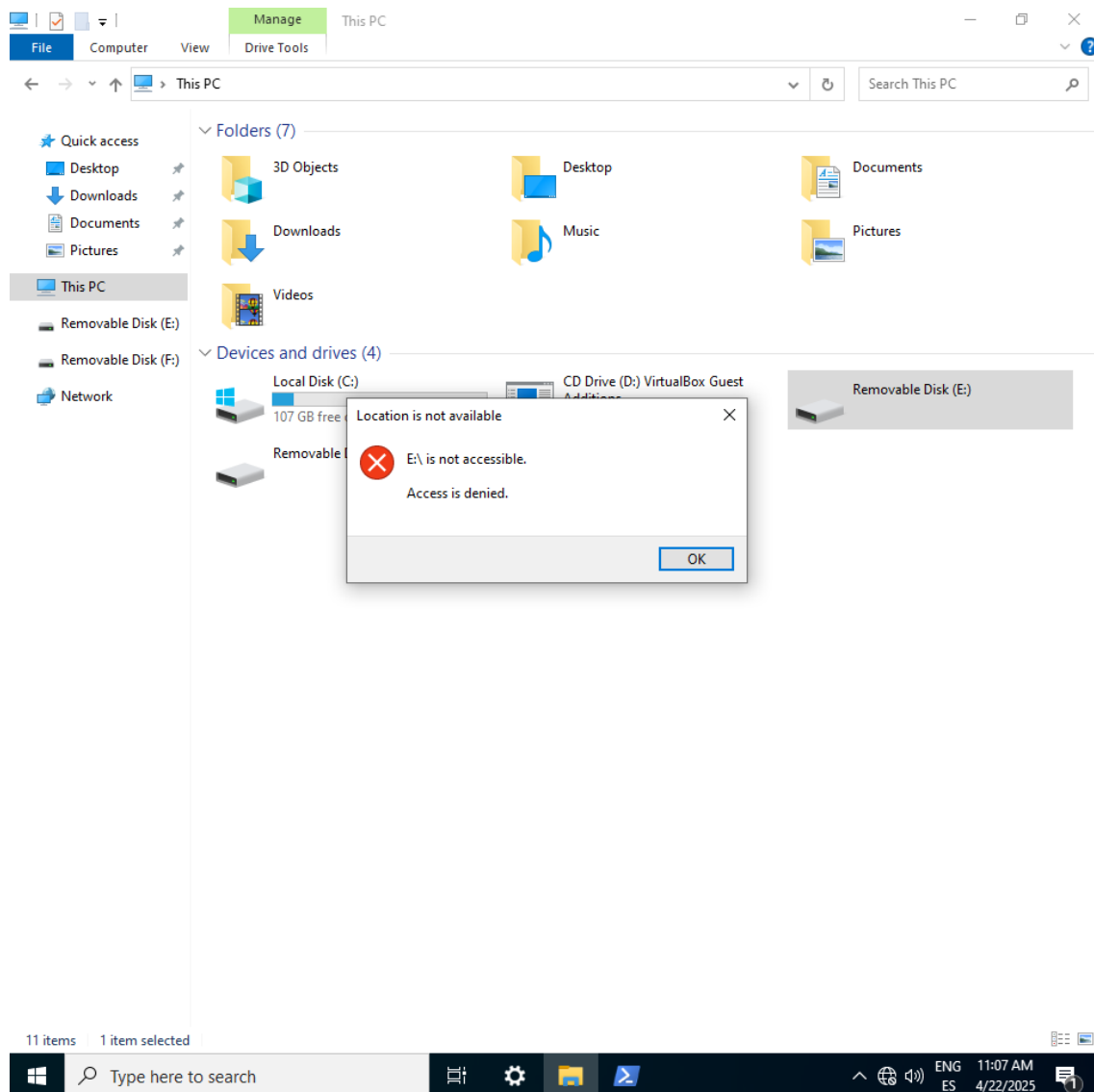
The sign-in method you're trying to use isn't allowed. For more info, contact your network administrator.

OK

b. Incapacidad para cambiar el Fondo de Pantalla.



c. No se permite el uso de dispositivos de Memoria USB.



d. No se puede ejecutar una serie de aplicaciones.

