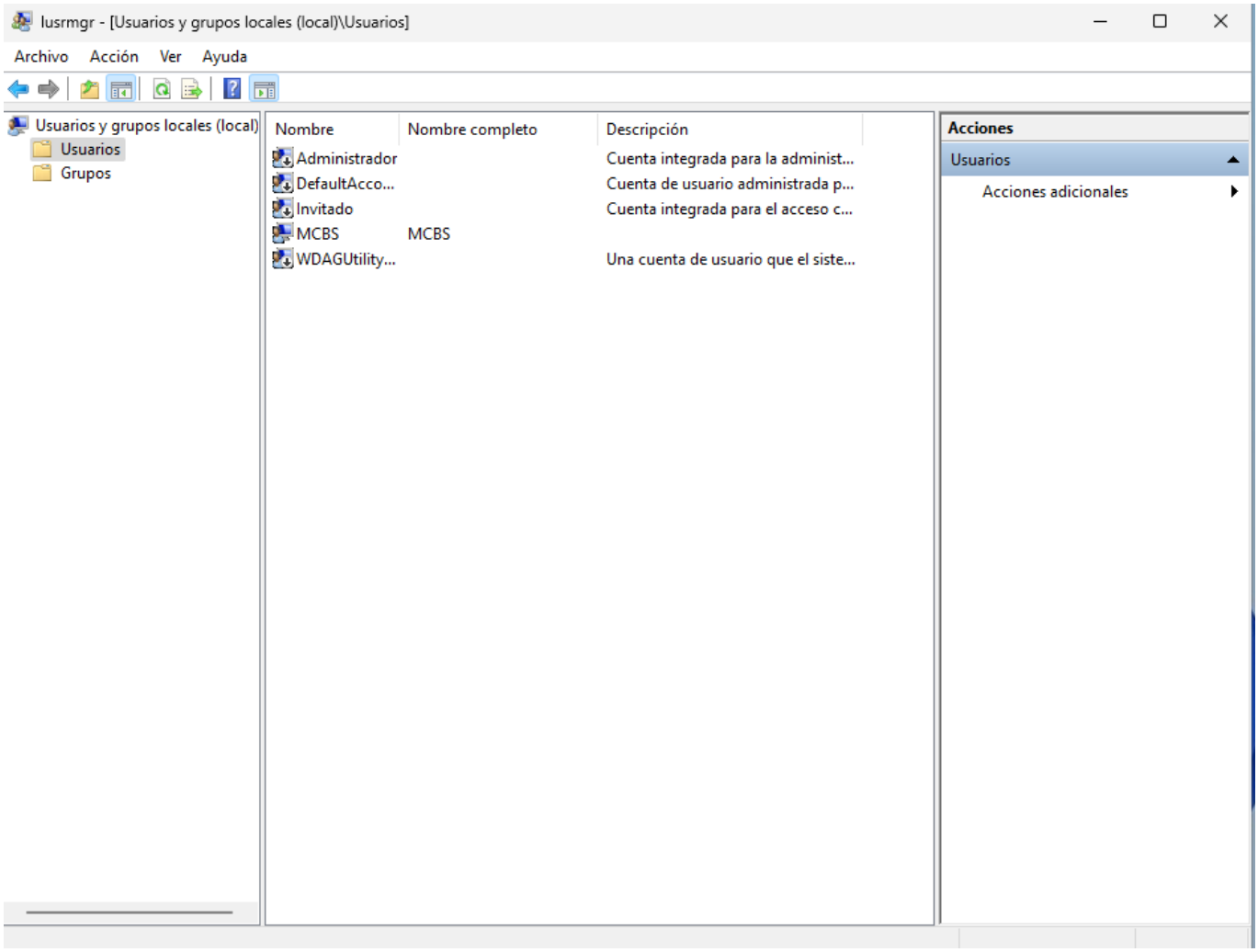
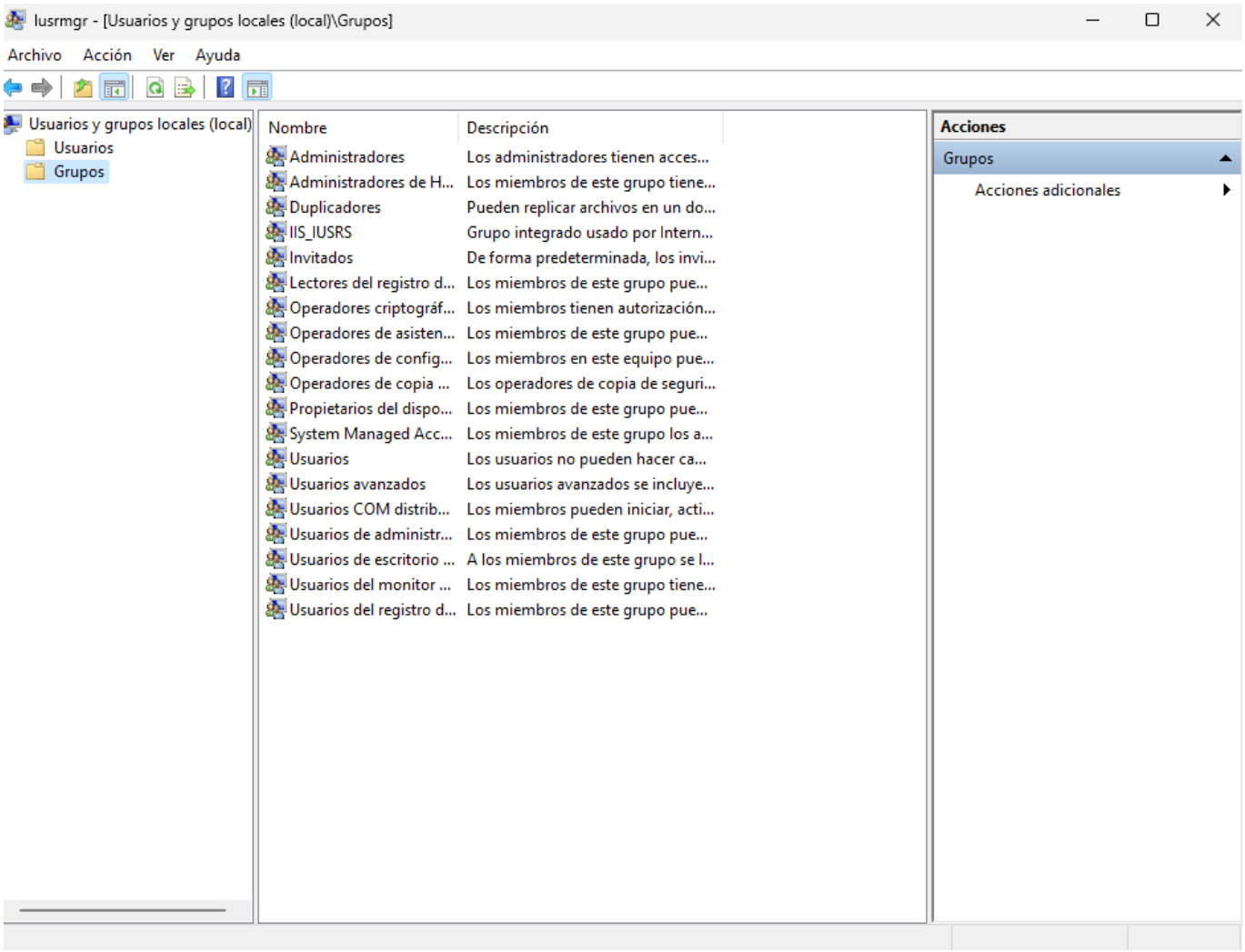
[Fort] Práctica 7: Configuración general de Windows 11 y securización

1. Reinicia el equipo y realiza las siguientes tareas

Lista los usuarios y grupos creados en el sistema de varias formas

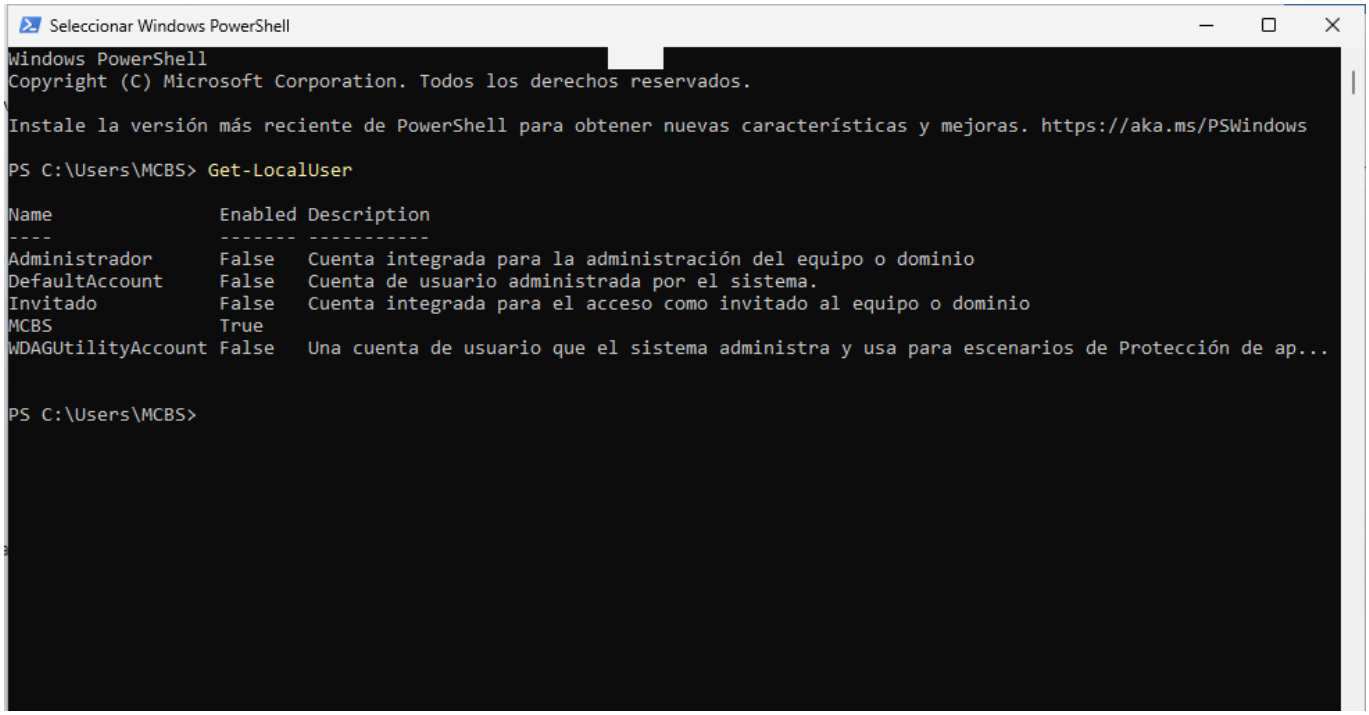
La primera forma de hacerlo es desde la interfaz fráfica, poniendo “ lusrmgr.msc” en la ventana de Windows + R:



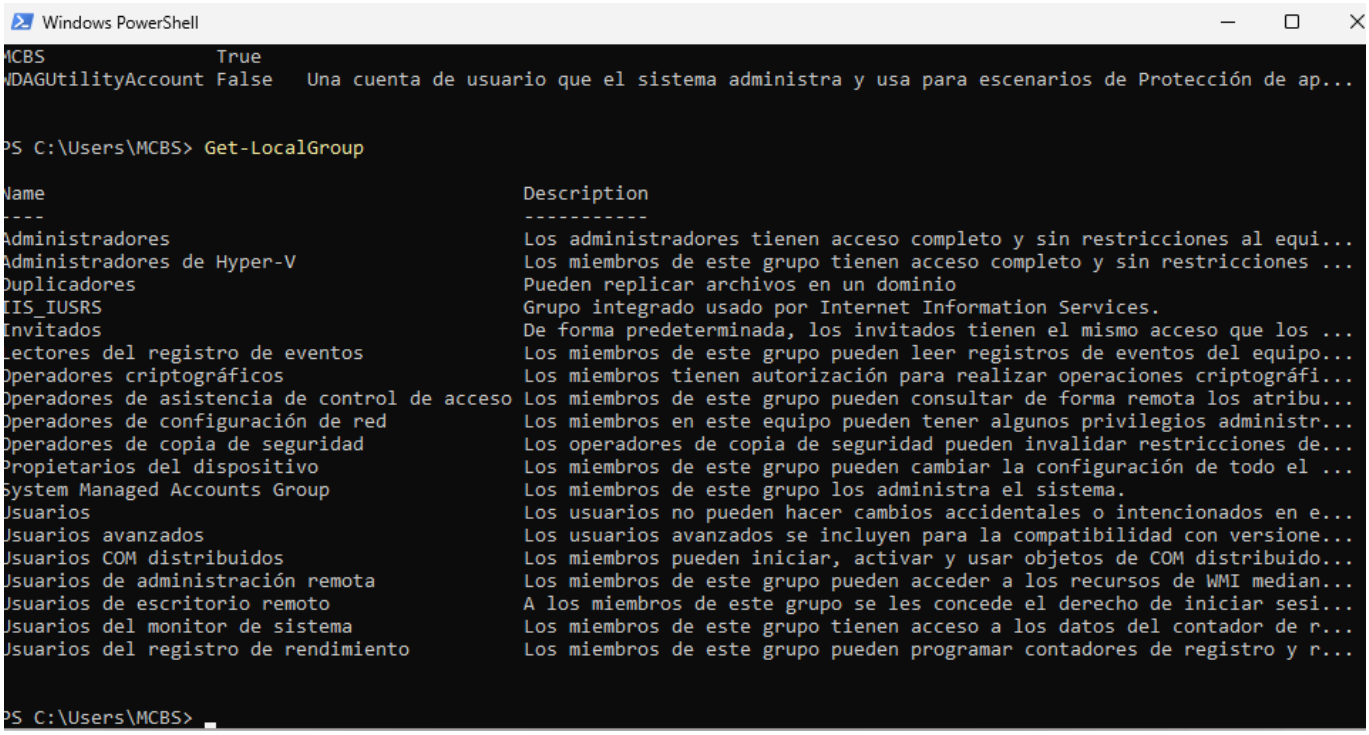


Otra forma es ir a powershell y usar los siguientes comandos para ver los usuarios y grupos:

```
Get-LocalUser
```

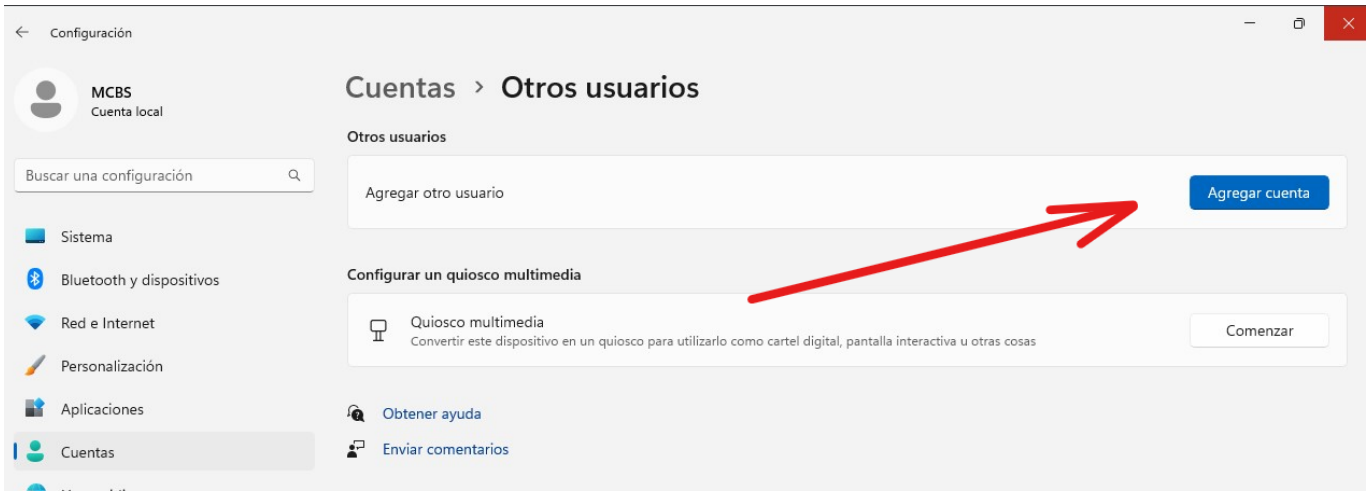


```
Get-LocalGroup
```

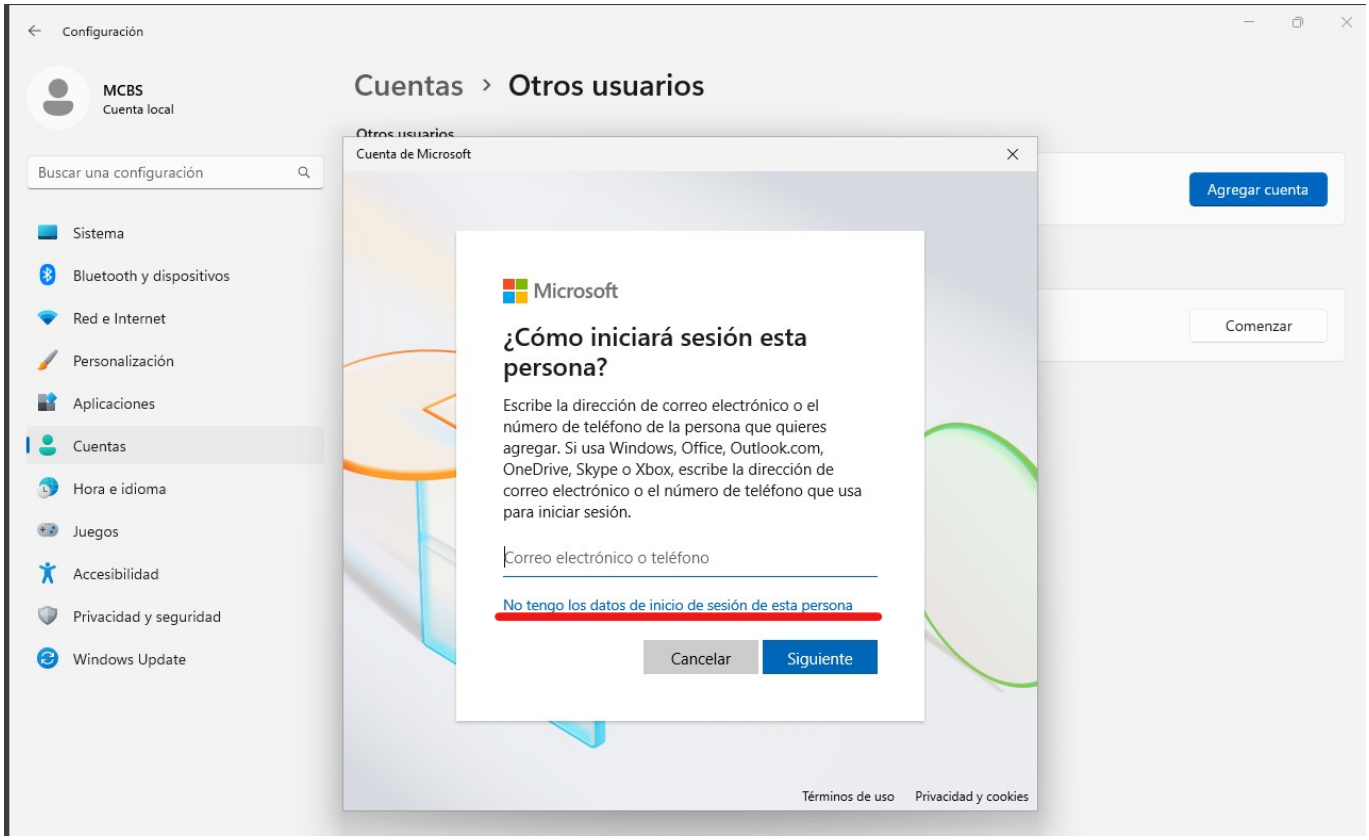


Crea un usuario del grupo usuario de 2 formas distintas

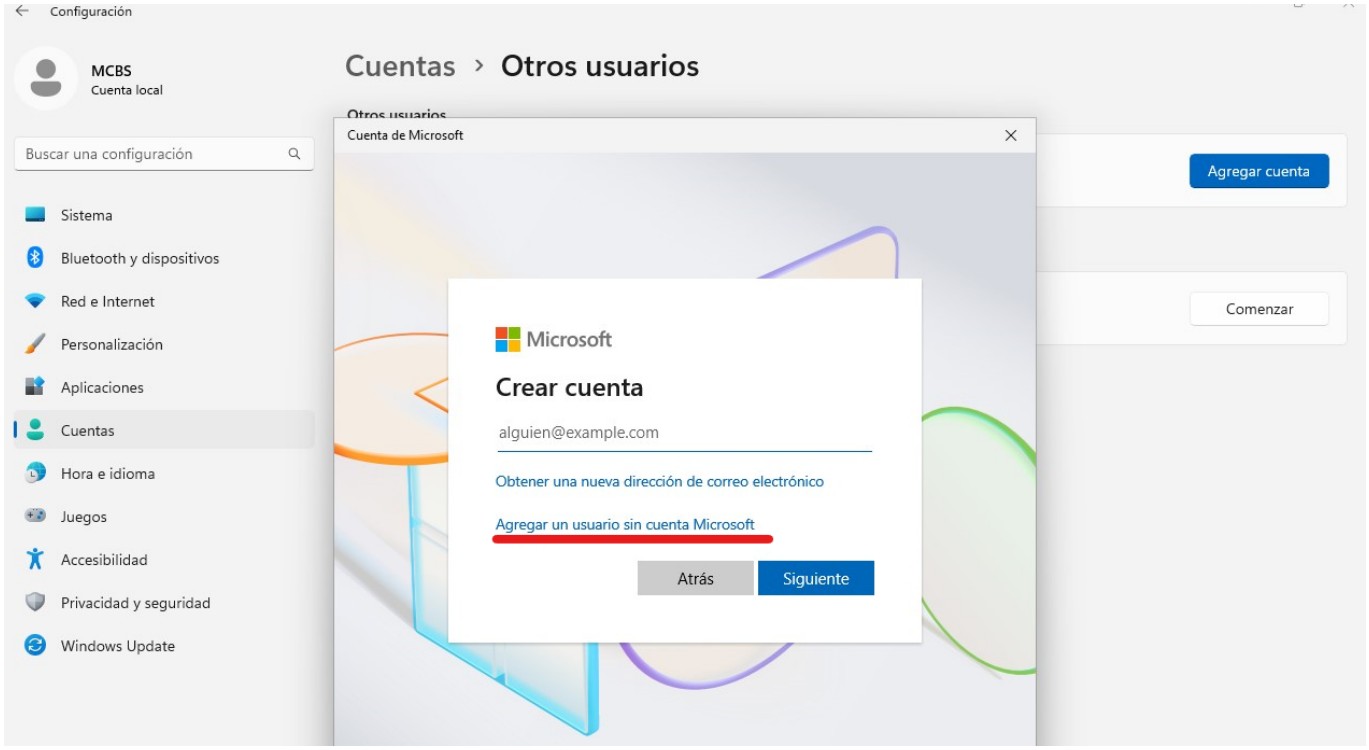
El grupo Usuario es el que se asigna por defecto a un usuario, podemos crear una nueva cuenta de este grupo de varias formas, por un lado se puede hacer desde interfaz gráfica yendo a Configuración/Cuentas/Otros Usuarios y pulsando en agregar cuenta:



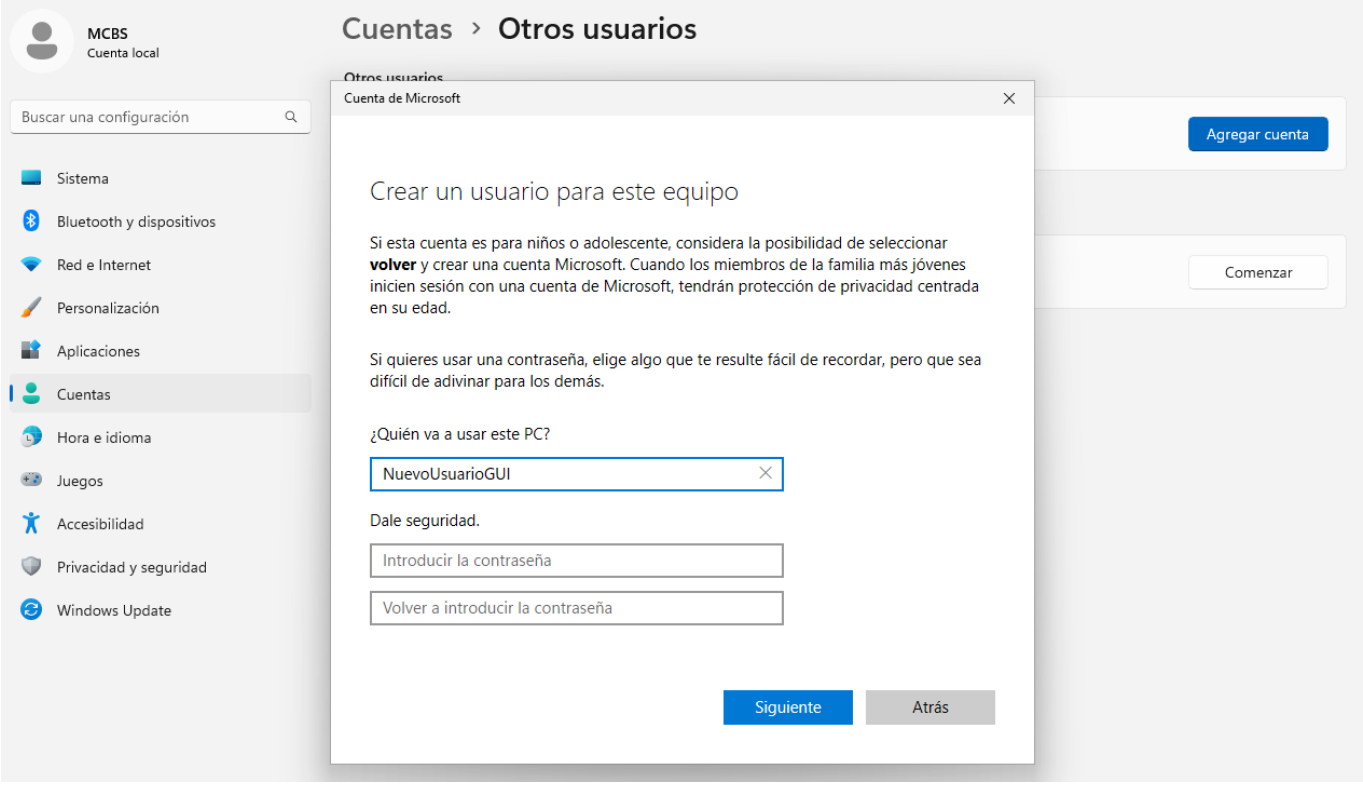
Tras eso, en la ventana que saldrá debemos pulsar en “No tengo los datos de inicio de sesión de esta persona”.



Y en la siguiente ventana presionar en agregar usuario sin cuenta microsoft:

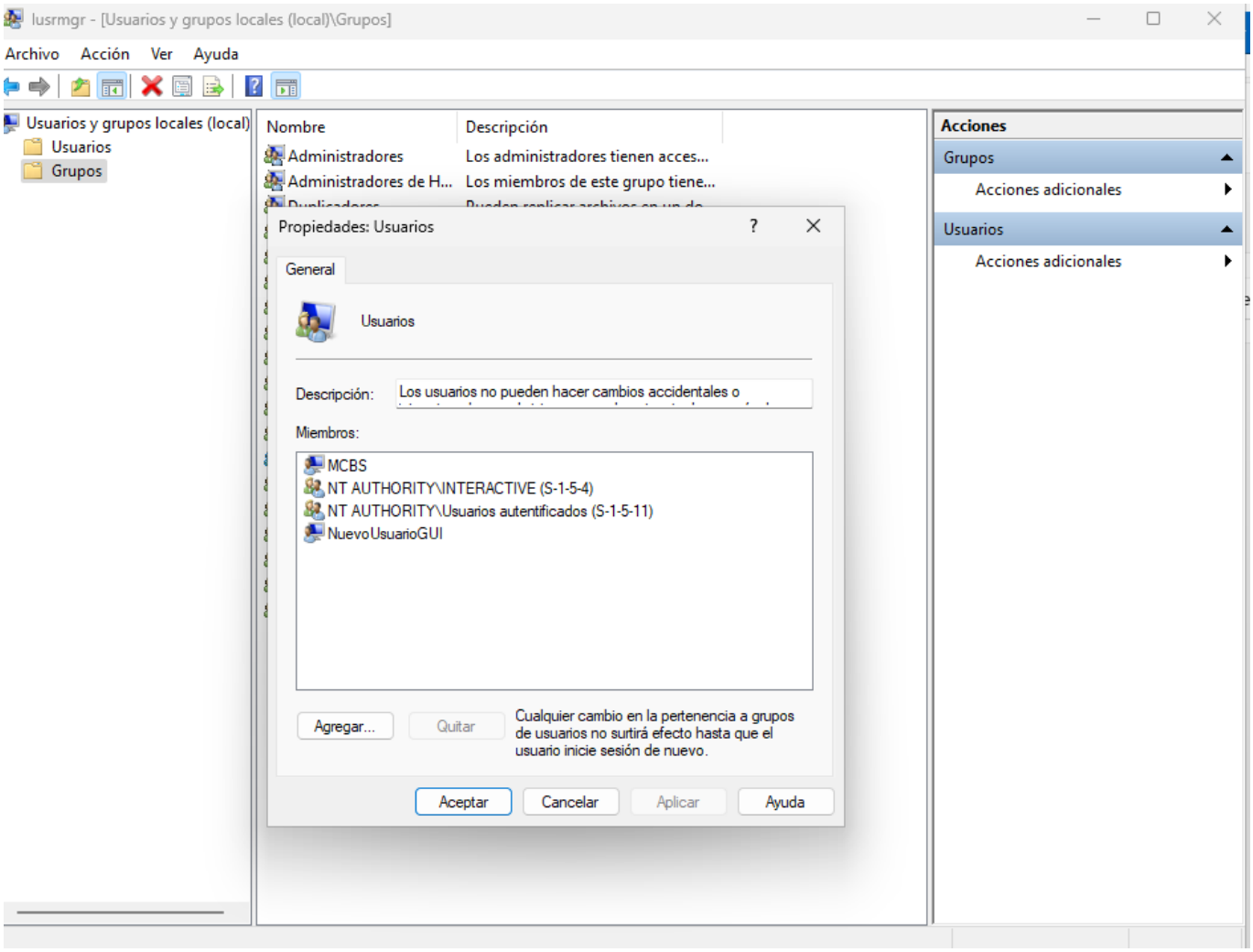


Tras eso nos permitirá crear un nuevo usuario:



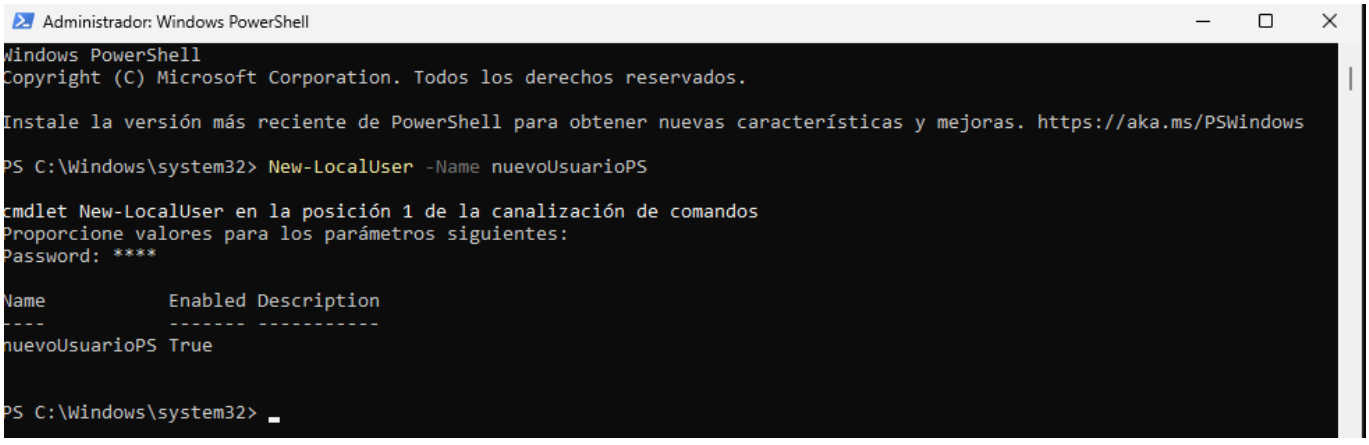
Una vez creado el usuario lo podemos ver en Cuentas/OtrosUsuarios:

Desde Usuarios y Grupos locales podemos observar que el usuario en cuestión se ha añadido de forma automática al grupo Usuarios:



Otra forma de crear usuarios es mediante la utilización de PowerShell como administrador, por ejemplo, podemos usar el comando:

```
New-LocalUser -Name NuevoUsuarioPS
```

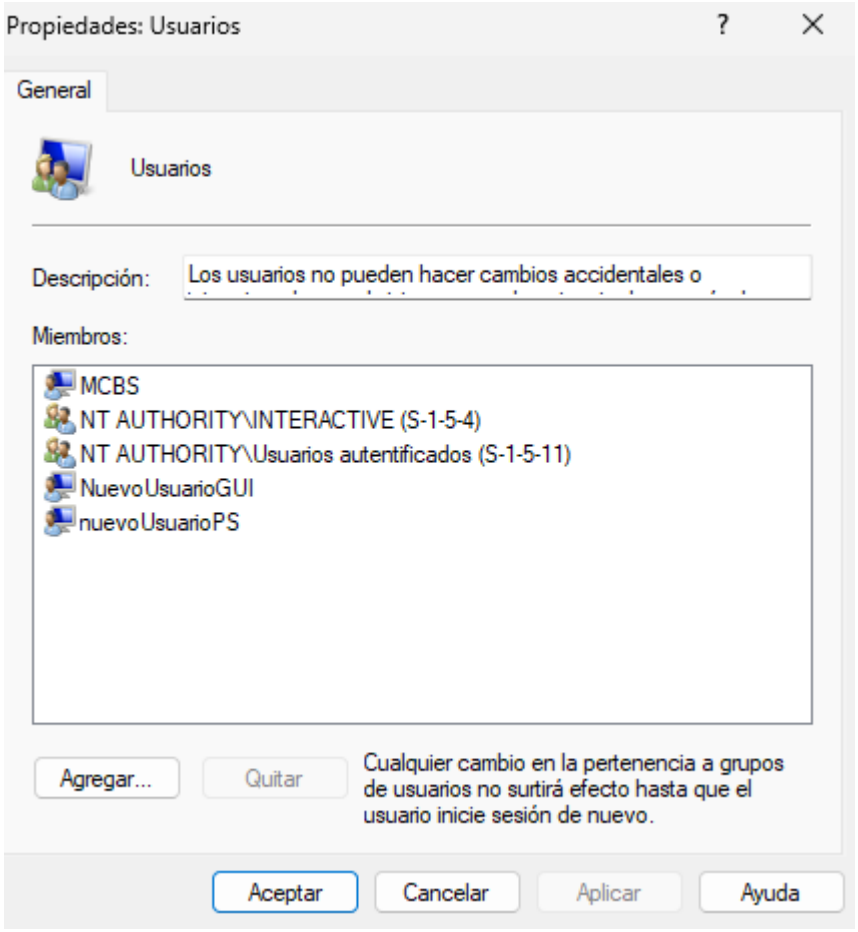


En este caso el usuario no se añade automáticamente al grupo usuarios por lo que lo debemos añadir manualmente con el siguiente comando:

```
Add-LocalGroupMember -Group Usuarios -Member nuevoUsuarioPS
```

```
PS C:\Windows\system32> Add-LocalGroupMember -Group Usuarios -Member nuevoUsuarioPS
PS C:\Windows\system32>
```

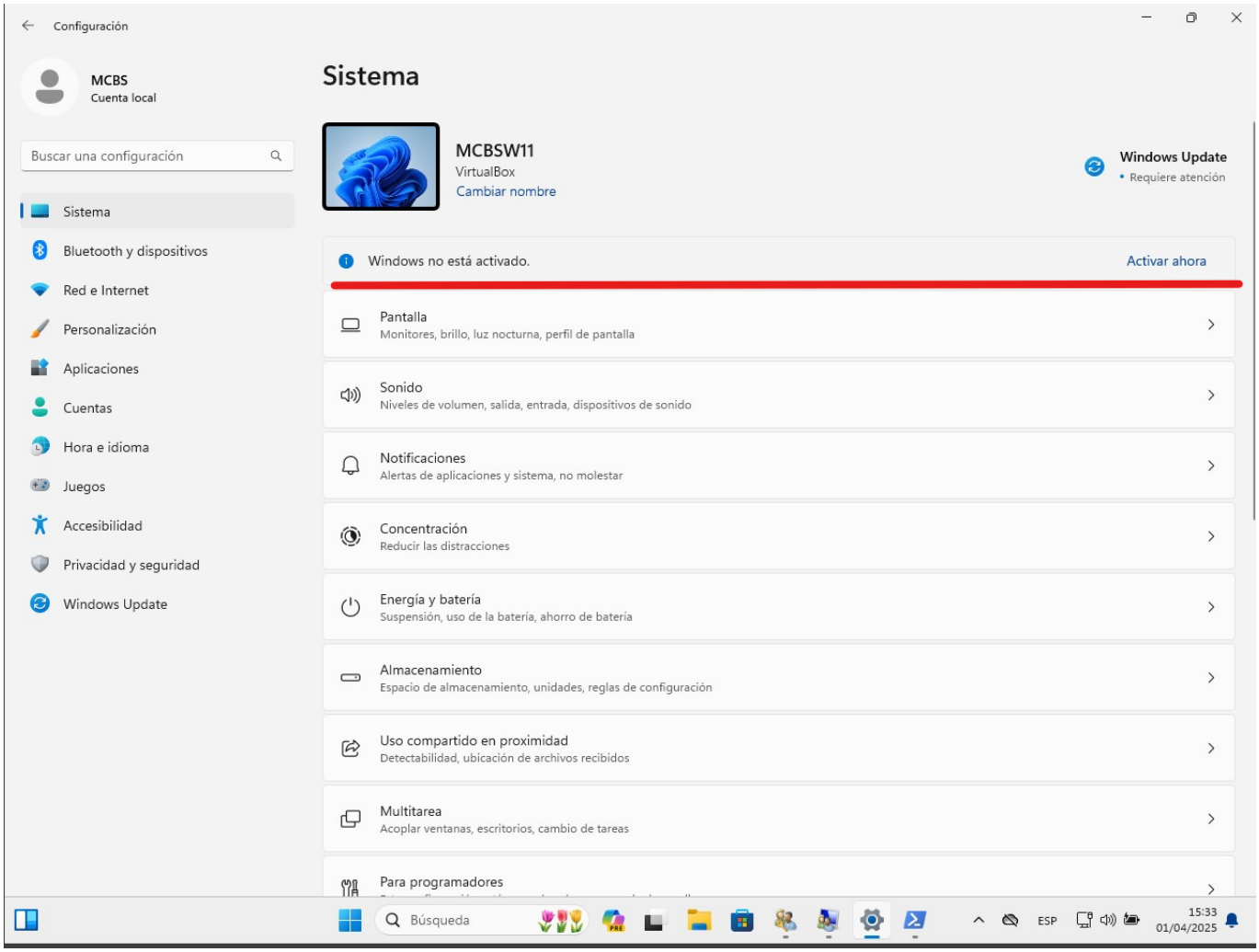
Tras eso podemos confirmar que el usuario está en el grupo desde Usuarios y Grupos locales:



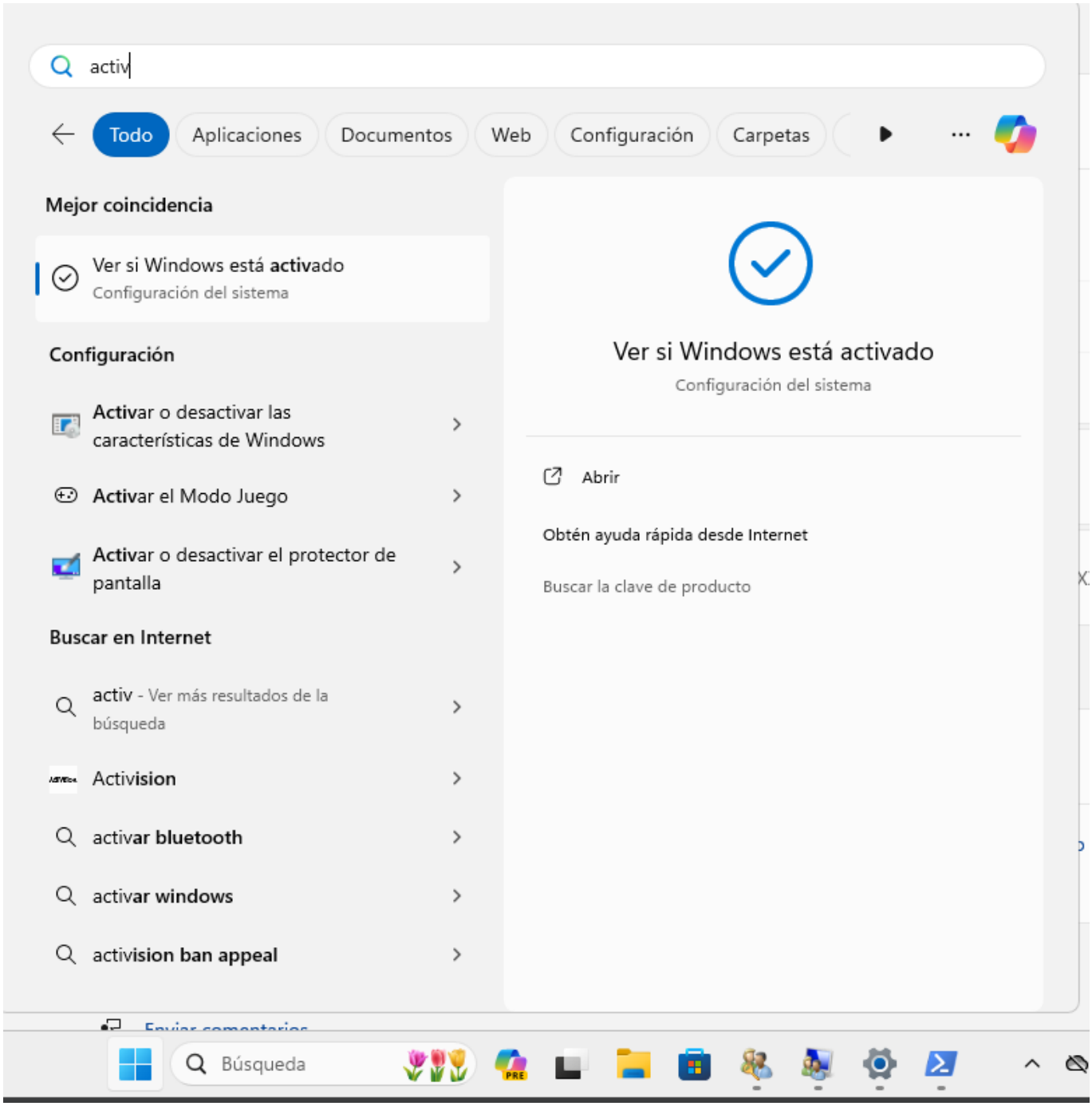
2. Revisa y documenta los siguientes puntos

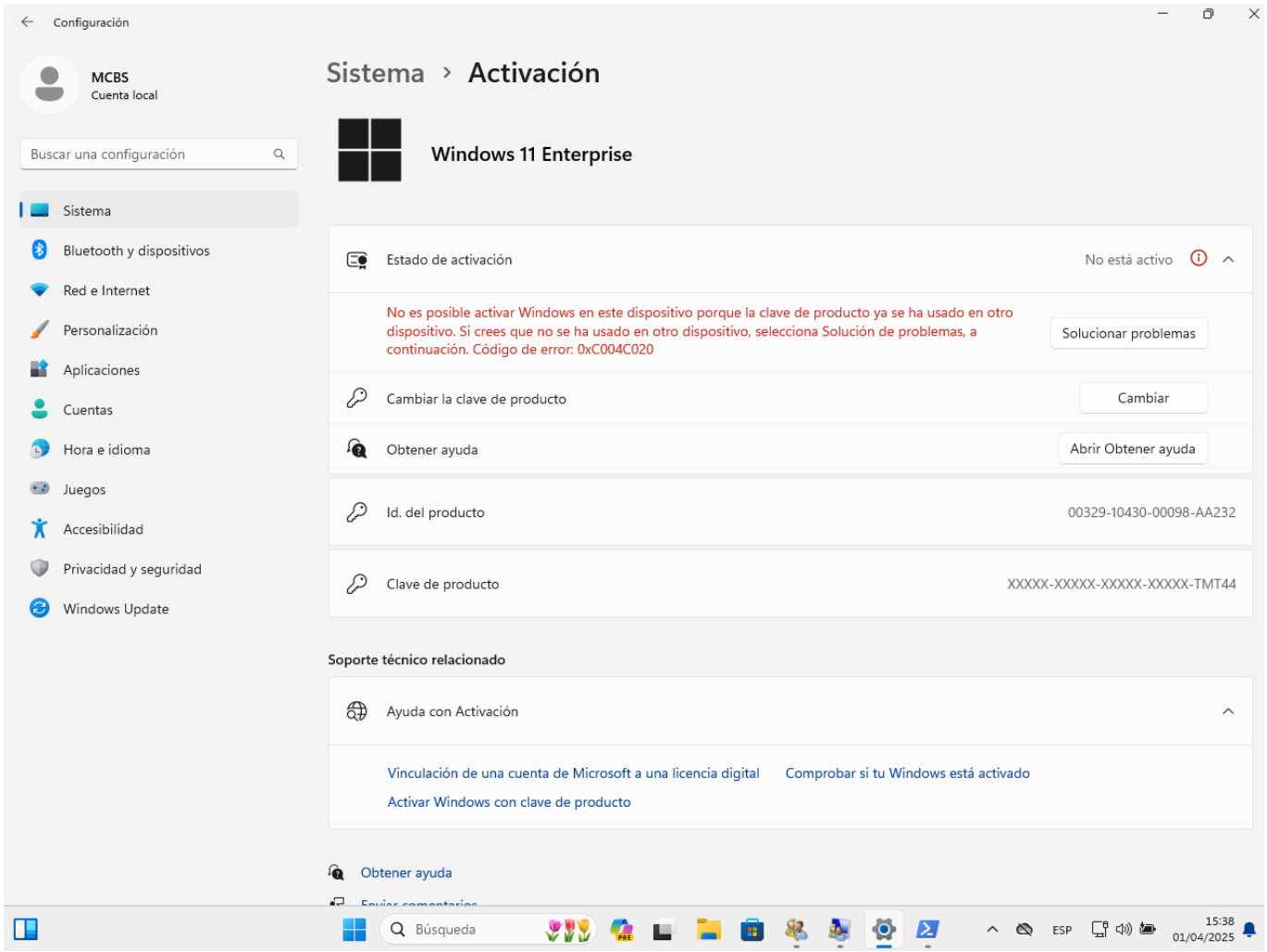
Como podemos saber el estado de la licencia del sistema operativo

Si vamos a Configuración/Sistema podemos obsevar una sección donde indica si windows está activado o no:



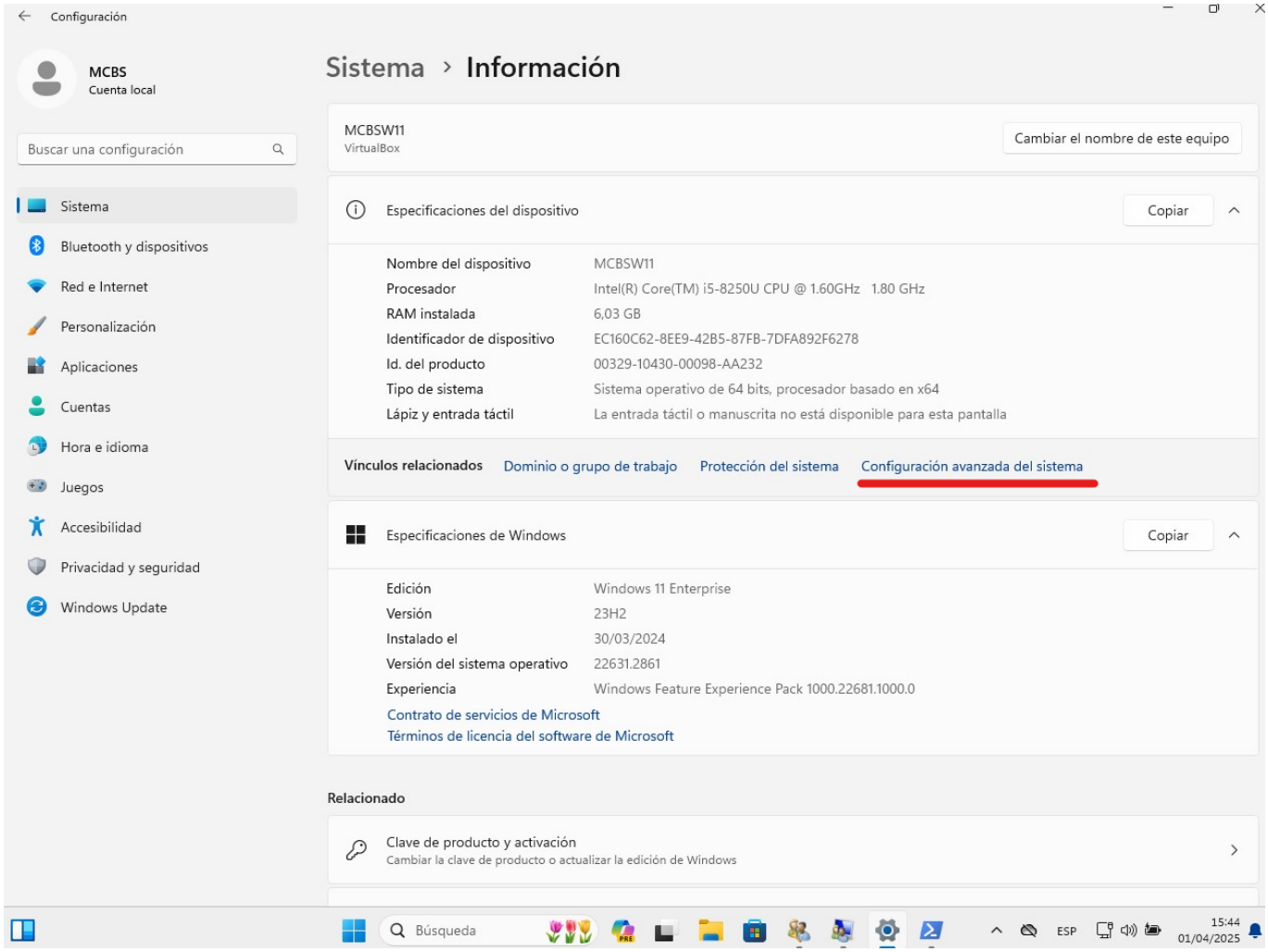
También se puede comprobar escribiendo activación en el menú de inicio y yendo a “Ver si Windows Está Activado”:


activ
Todo
Aplicaciones
Documentos
Web
Configuración
Carpetas
Mejor coincidencia
Ver si Windows está activado
Configuración del sistema
Configuración
Activar o desactivar las características de Windows
Activar el Modo Juego
Activar o desactivar el protector de pantalla
Buscar en Internet
activ - Ver más resultados de la búsqueda
Activision
activar bluetooth
activar windows
activision ban appeal
Ver si Windows está activado
Configuración del sistema
Abrir
Obtén ayuda rápida desde Internet
Buscar la clave de producto
Búsqueda

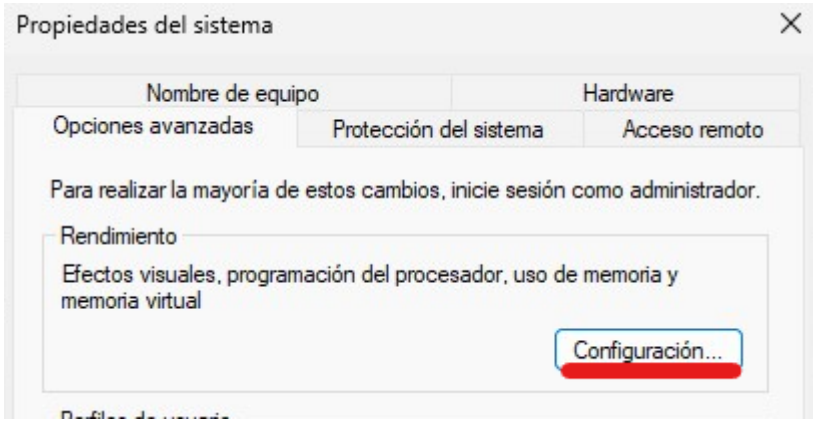


¿Está activo el DEP?¿Dónde podemos verlo?

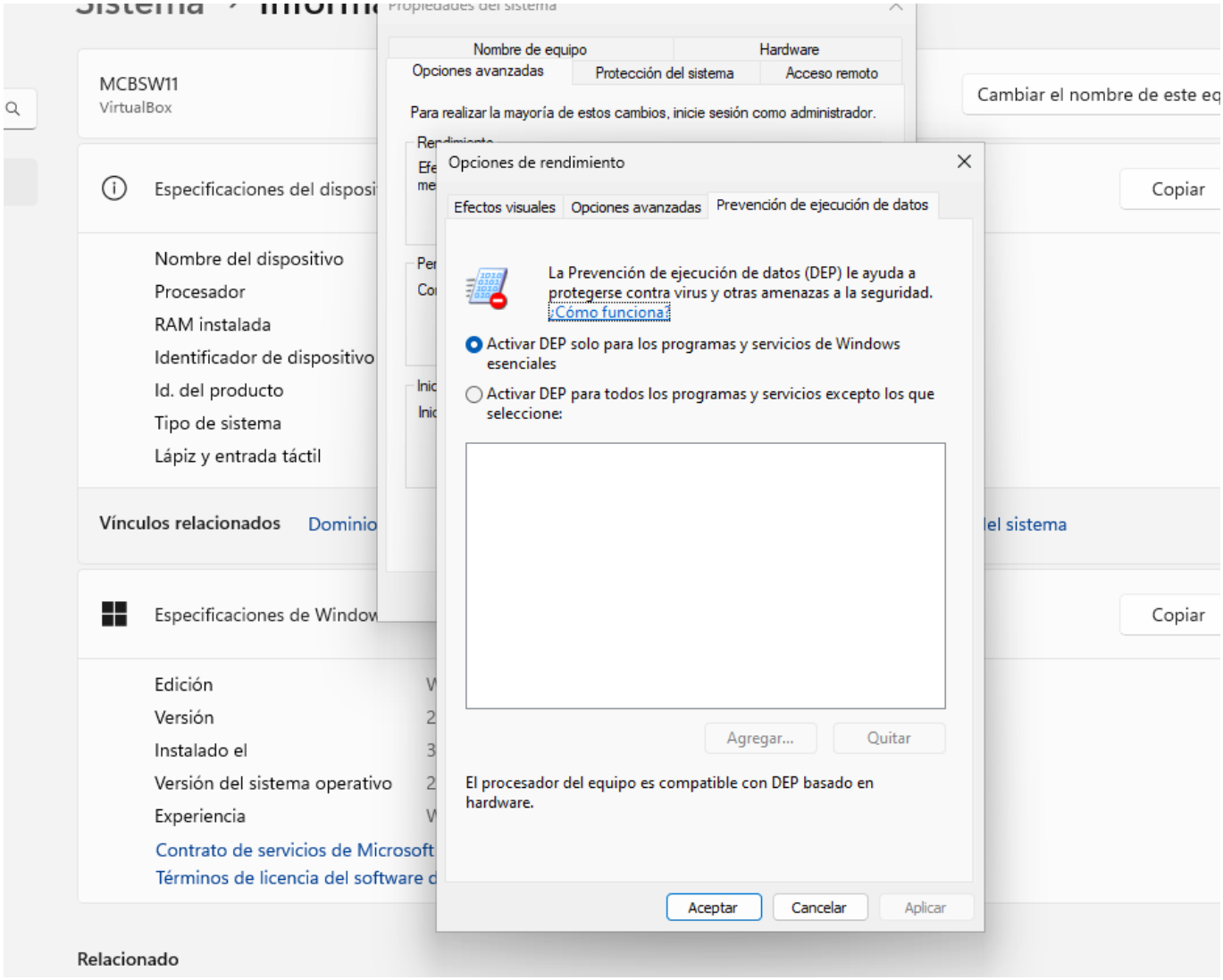
Para revisar si está activo el DEP debemos ir a Configuración/Sistema/Información y ahí presionamos en Configuración Avanzada del Sistema:



En la ventana que aparece presionamos, en la pestaña de opciones avanzadas presionamos en configuración en la sección de rendimiento:



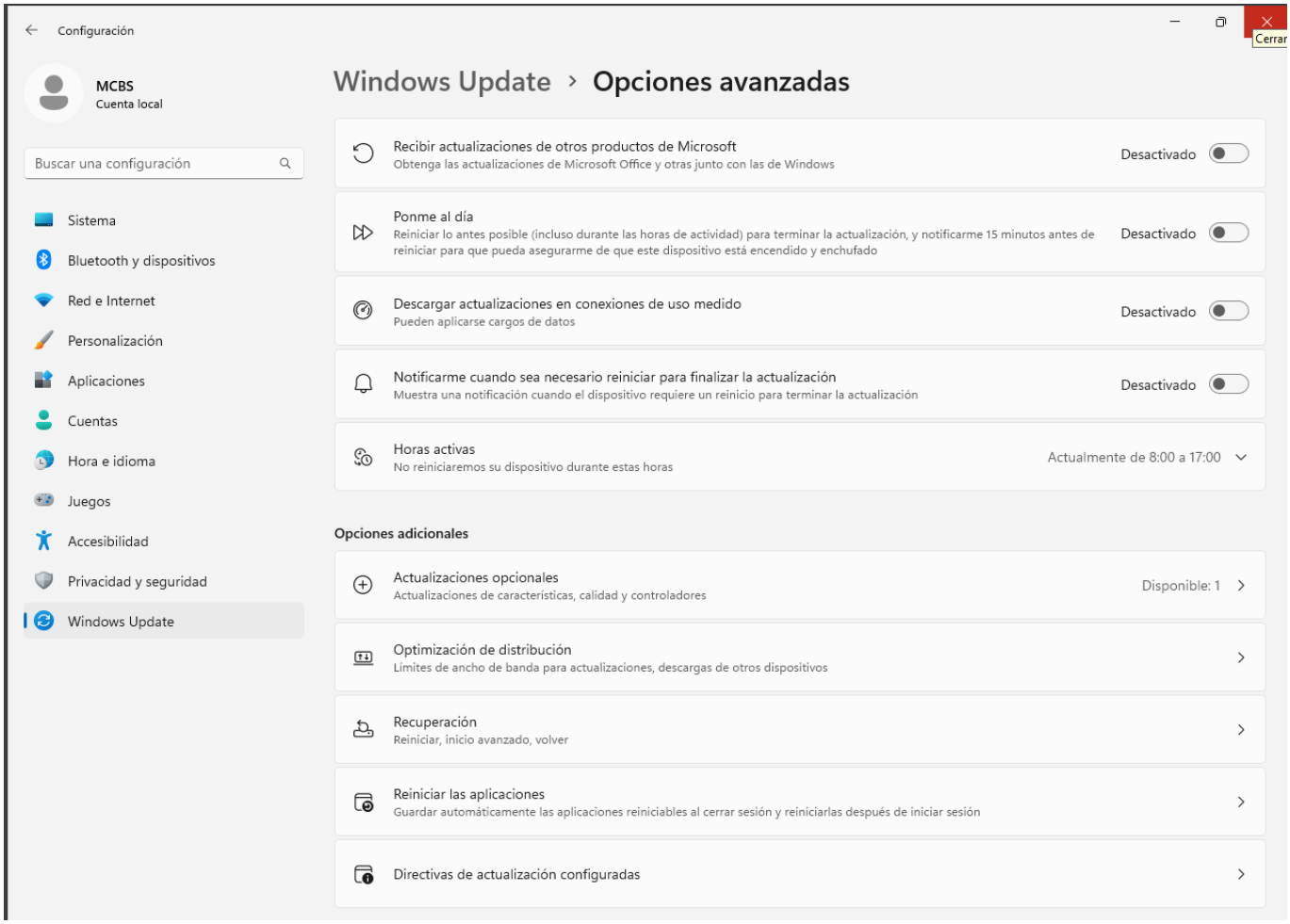
En la ventana que nos sale presionamos en la epstaña de Prevención de Ejecución de Datos y ahí podemos ver si DEP está activado o no y podemos cambiar su estado:



En este caso DEP está activado para todos los programas y servicios esenciales.

¿Cual es la configuración por defecto del sistema de actualizaciones automáticas?

Podemos revisar esta configuración desde Configuración/Windows Update/Opciones Avanzadas:



Identifica y lista los permisos NTFS que tiene el disco C:

Podemos obtener dicho listado de permisos con el comando de PowerShell:

```
.\icacls.exe C:\ /T
```

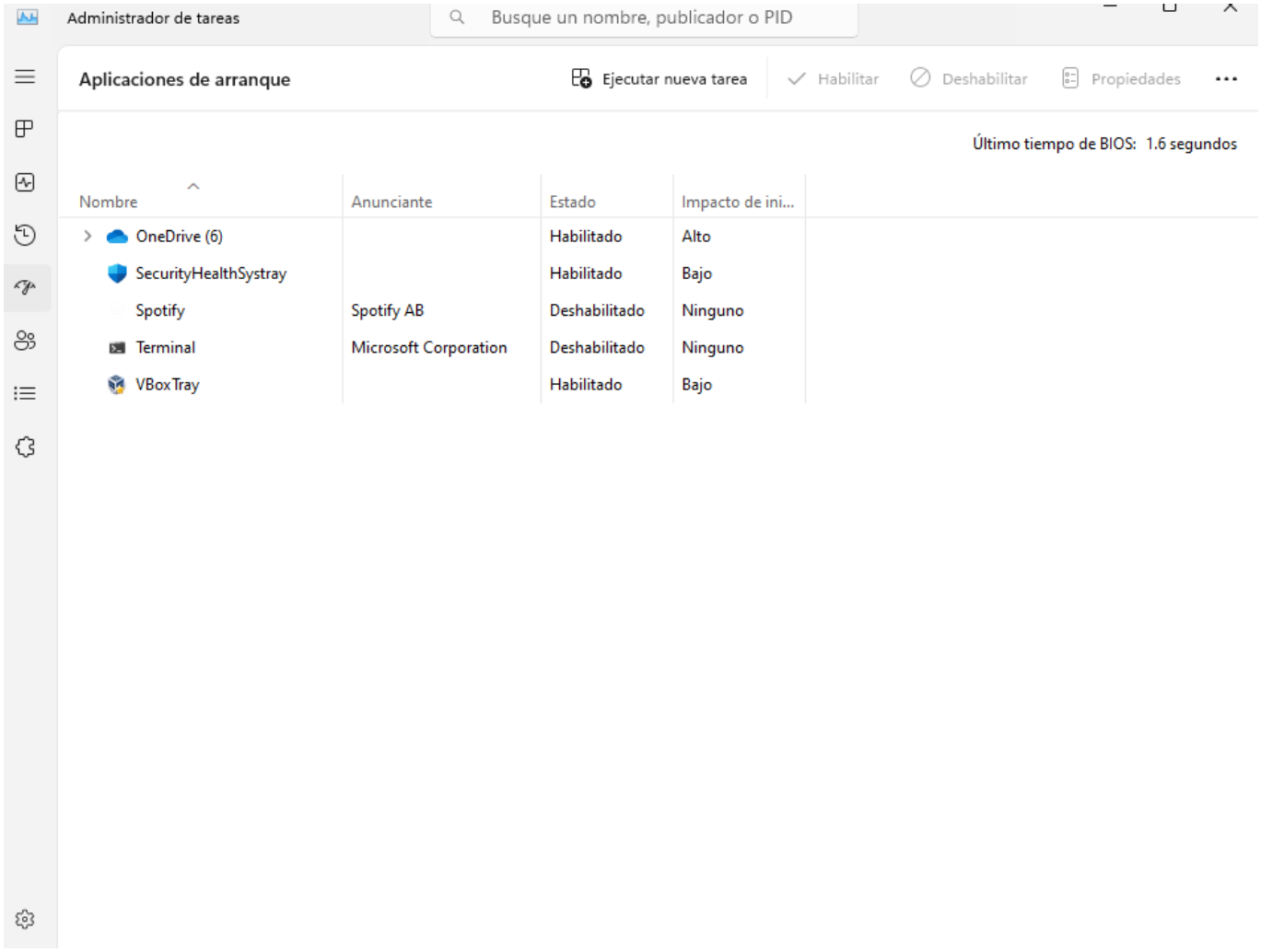
```
PS C:\Windows\system32> .\icacls.exe C:\ /T
C:\ BUILTIN\Administradores:(OI)(CI)(F)
    NT AUTHORITY\SYSTEM:(OI)(CI)(F)
    BUILTIN\Usuarios:(OI)(CI)(RX)
    NT AUTHORITY\Usuarios autentificados:(OI)(CI)(IO)(M)
    NT AUTHORITY\Usuarios autentificados:(AD)
    S-1-15-3-65536-1888954469-739942743-1668119174-2468466756-4239452838-1296943325-355587736-700089176:(S,RD,X,RA)
    Etiqueta obligatoria\Nivel obligatorio alto:(OI)(NP)(IO)(NW)

C:\$Recycle.Bin BUILTIN\Administradores:(F)
                BUILTIN\Administradores:(OI)(CI)(IO)(F)
                NT AUTHORITY\SYSTEM:(F)
                NT AUTHORITY\SYSTEM:(OI)(CI)(IO)(F)
                BUILTIN\Usuarios:(RX,AD,WA)
                Etiqueta obligatoria\Nivel obligatorio bajo:(OI)(CI)(IO)(NW)

C:\$WinREAgent BUILTIN\Administradores:(OI)(CI)(F)
               BUILTIN\Usuarios:(OI)(CI)(RX)
               NT AUTHORITY\SYSTEM:(OI)(CI)(RX)

C:\$WINRE_BACKUP_PARTITION.MARKER BUILTIN\Administradores:(I)(F)
                                  NT AUTHORITY\SYSTEM:(I)(F)
                                  BUILTIN\Usuarios:(I)(RX)
                                  NT AUTHORITY\Usuarios autentificados:(I)(M)
                                  Etiqueta obligatoria\Nivel obligatorio alto:(I)(NW)

C:\Archivos de programa Todos:(DENY)(RD)
                        Todos:(RX)
                        NT AUTHORITY\SYSTEM:(F)
                        BUILTIN\Administradores:(F)

C:\Documents and Settings Todos:(DENY)(RD)
                          Todos:(RX)
                          NT AUTHORITY\SYSTEM:(F)
                          BUILTIN\Administradores:(F)
```

Donde los permisos son:

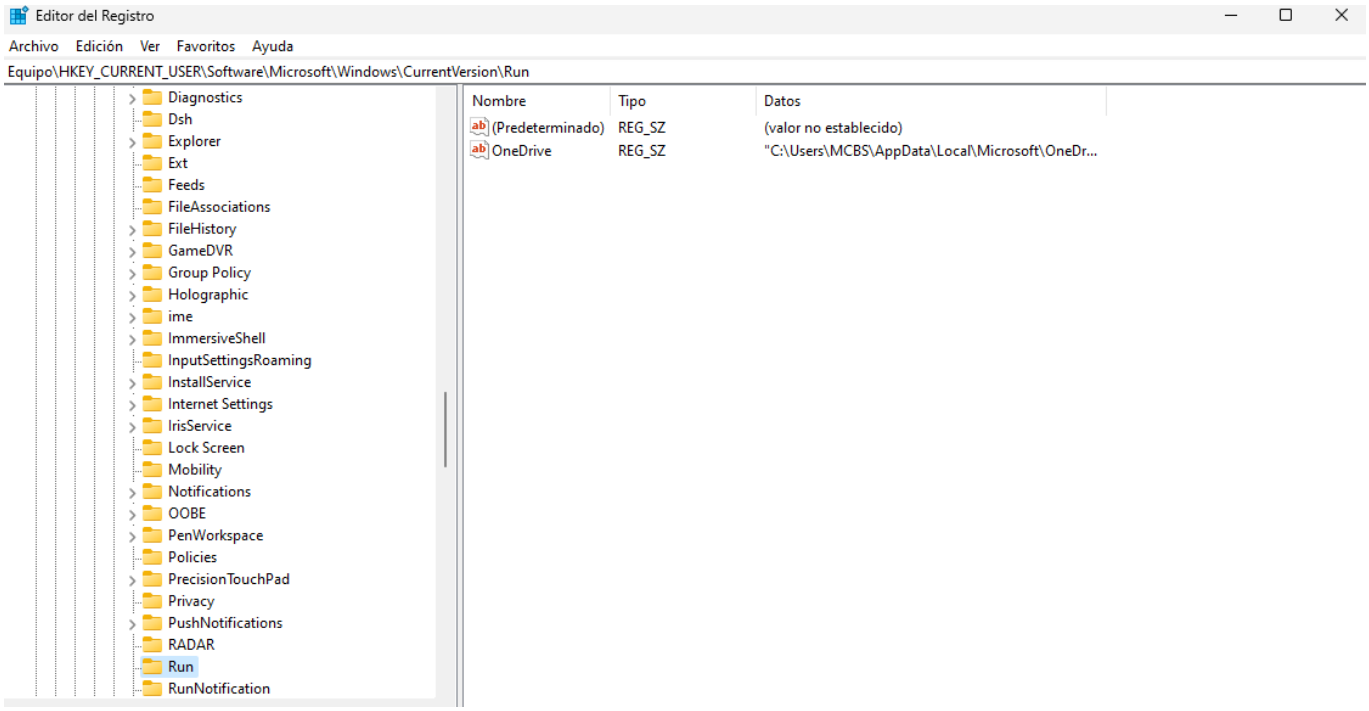
- F: Control total
- RX: Lectura y Ejecución
- I: Permisos heredados de la carpeta superior

Identifica todos los procesos que se inician en el arranque del sistema operativo

Por un lado, podemos indicar que programas se inician en el sistema operativo desde la pestaña Aplicaciones de Arranque del Administrador de Tareas:



También se pueden ver desde el regedit dentro de "HKCU\Software\Microsoft\Windows\CurrentVersion\Run"

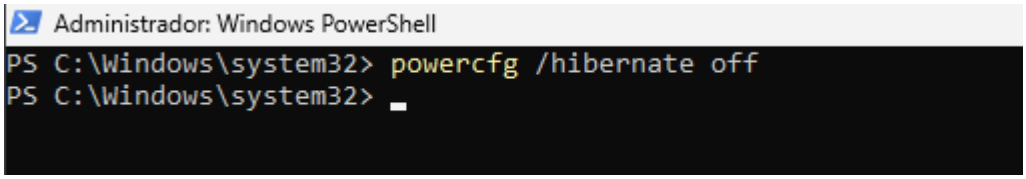


3. Realiza las siguientes tareas

Deshabilitar la gestión de hibernación del equipo

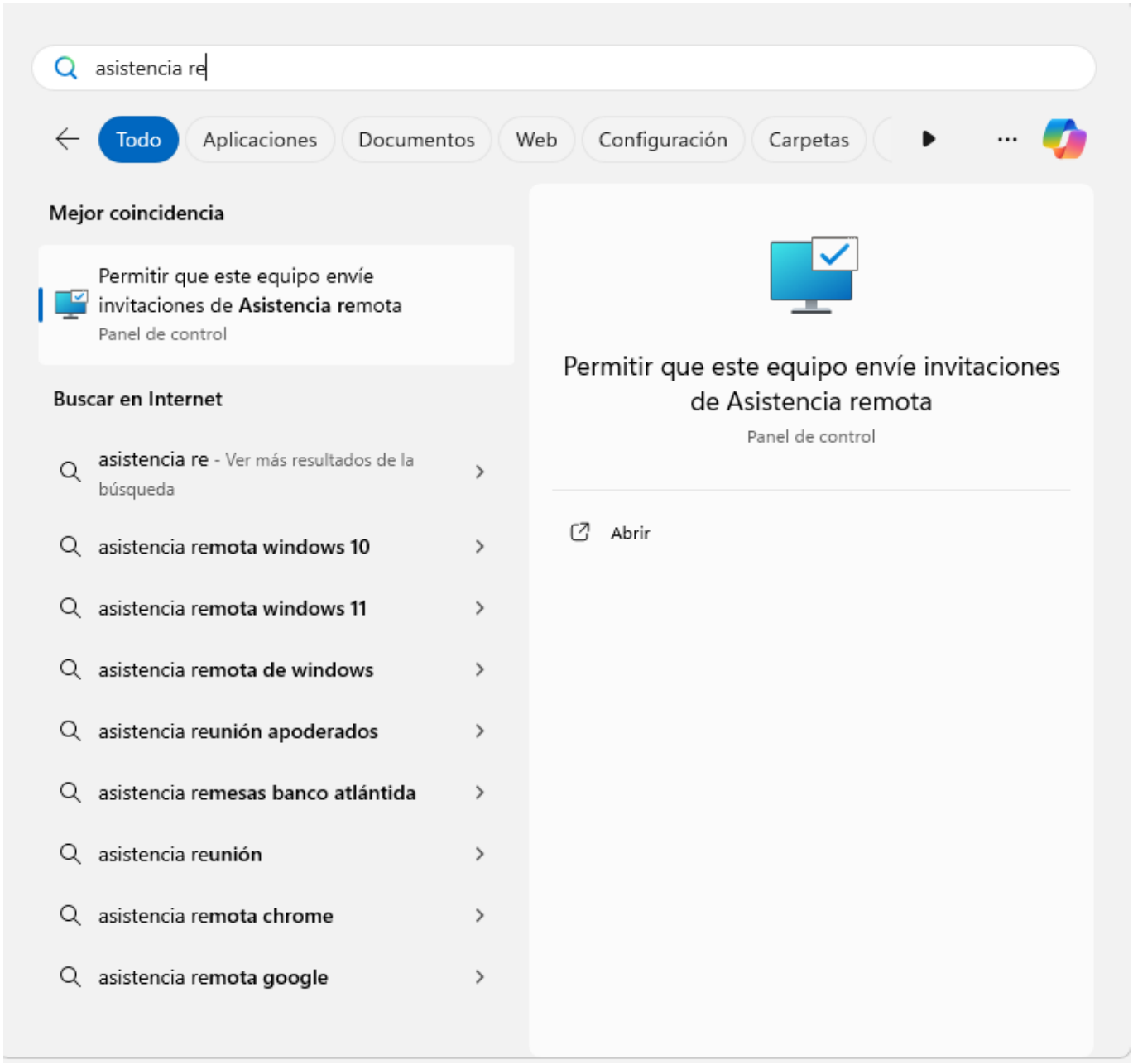
Para deshabilitar la gestión de la hibernación del equipo se usa el siguiente comando:

```
powercfg /hibernate off
```

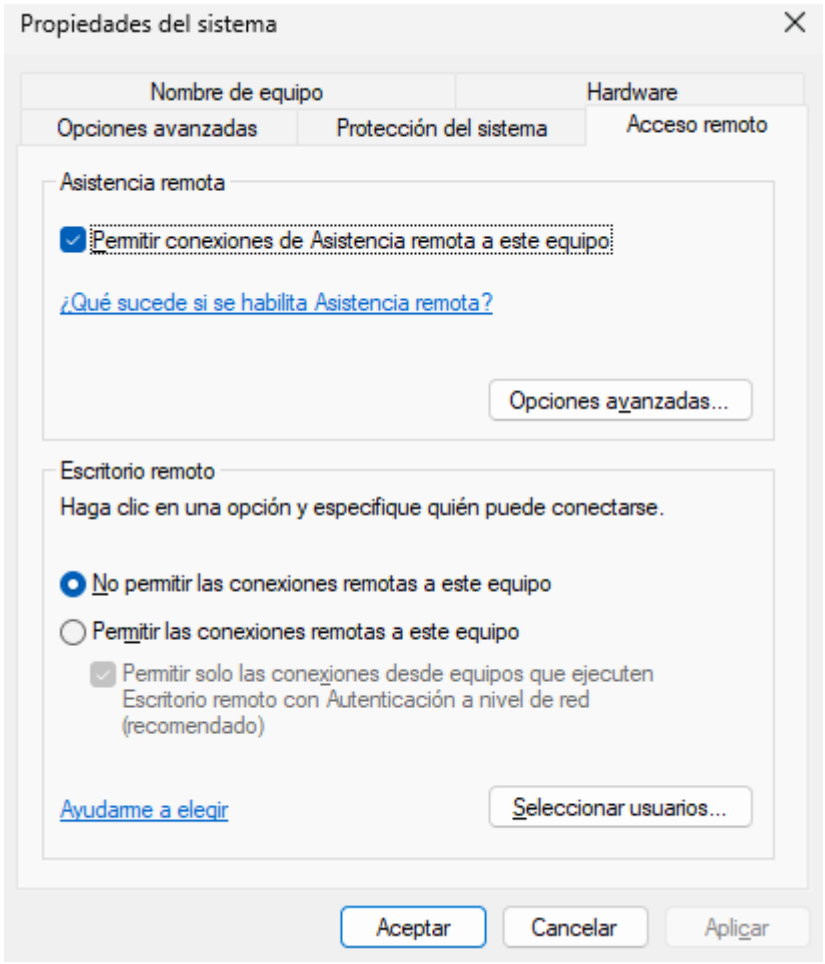


Deshabilita las conexiones de asistencia remota al equipo

Vamos al menú windows y escribimos asistencia remota:

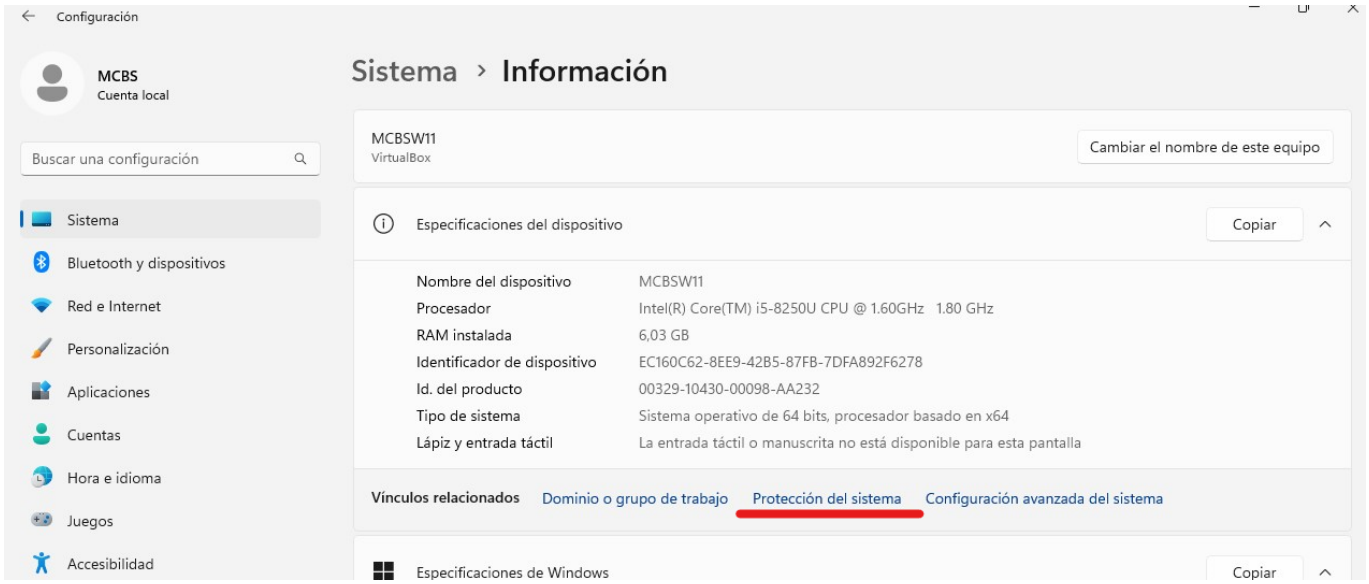


Dentro de la ventana que aparece desmarcamos la casilla de permitir conexiones de asistencia remota a este equipo:

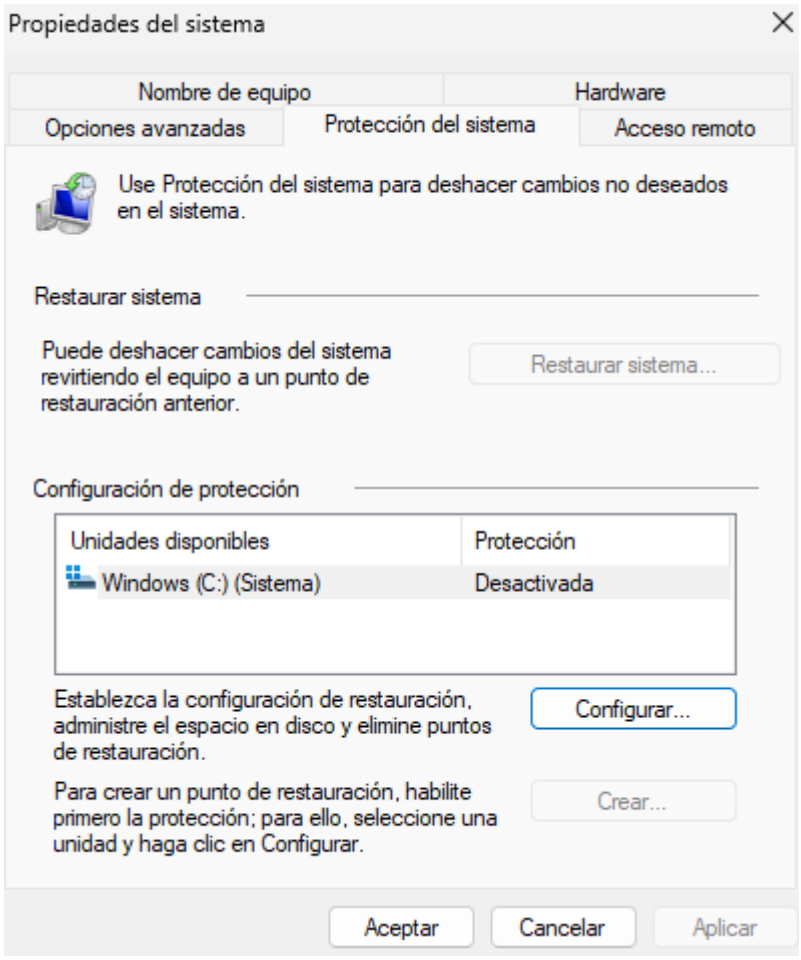


Activa la protección del sistema en la unidad C: (5-10%)

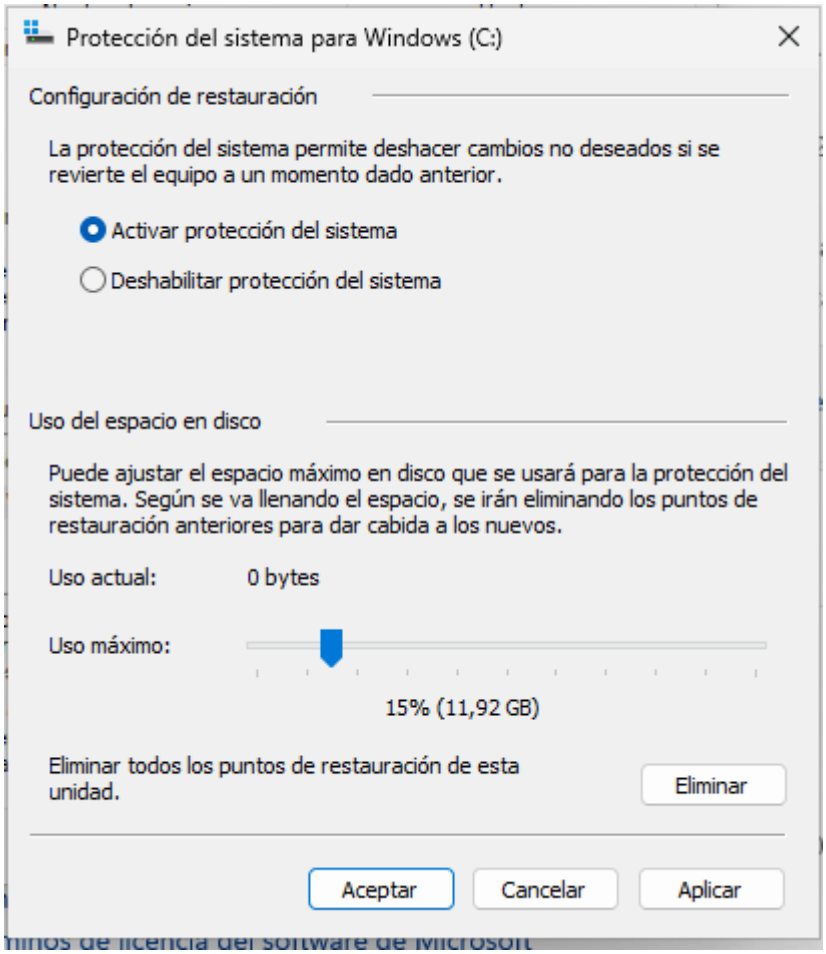
Vamos a Sistema/Información y pinchamos en Protección del sistema:



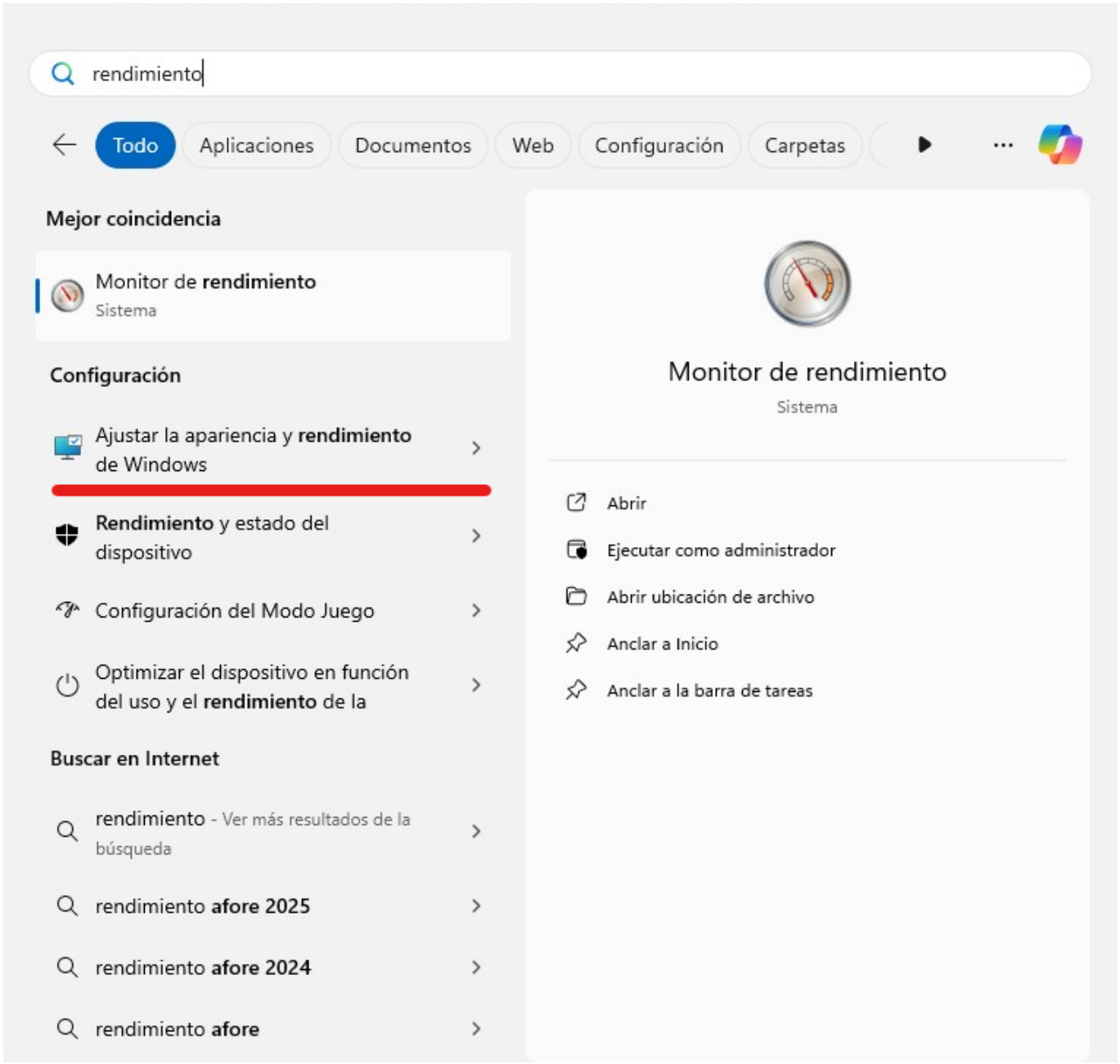
En la ventana que sale presionamos en configurar:



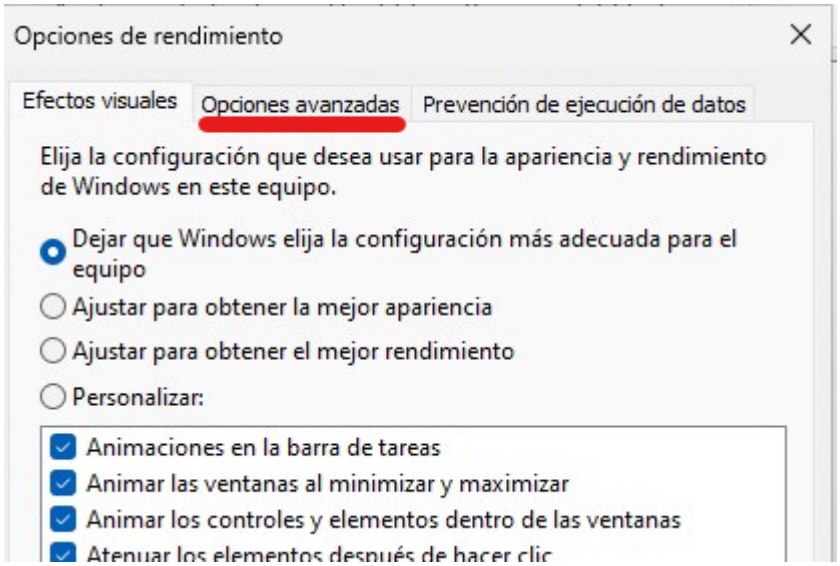
Dentro de configurar activamos la protección del sistema y seleccionamos el uso máximo con el slider:



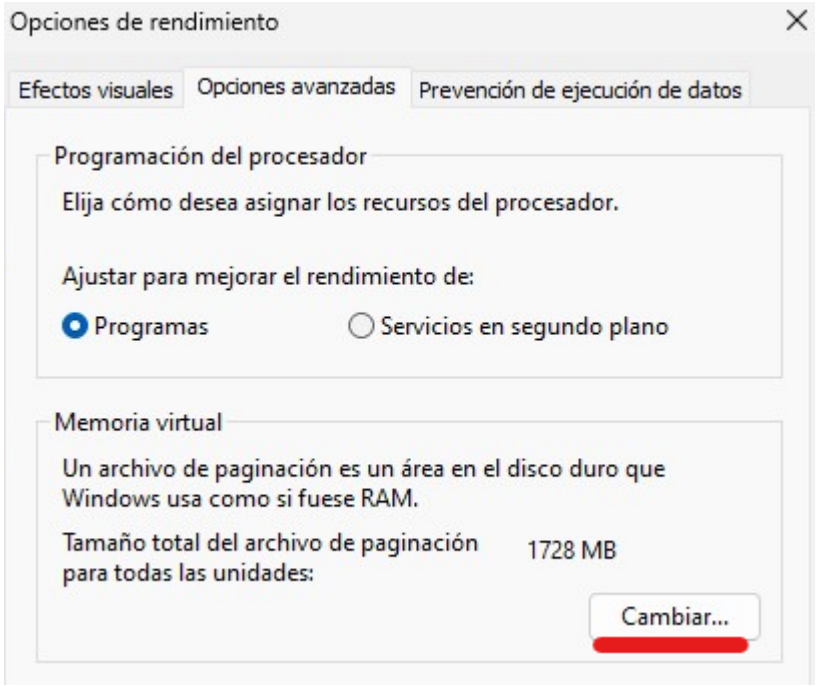
==== Revisa la configuración del archivo de paginación. Confirma que el tamaño sea gestionado por el sistema ==== Para hacer esto escribimos en el menú de inicio rendiminento y seleccionamos “Ajustar apariencia y rendimiento en windows”:



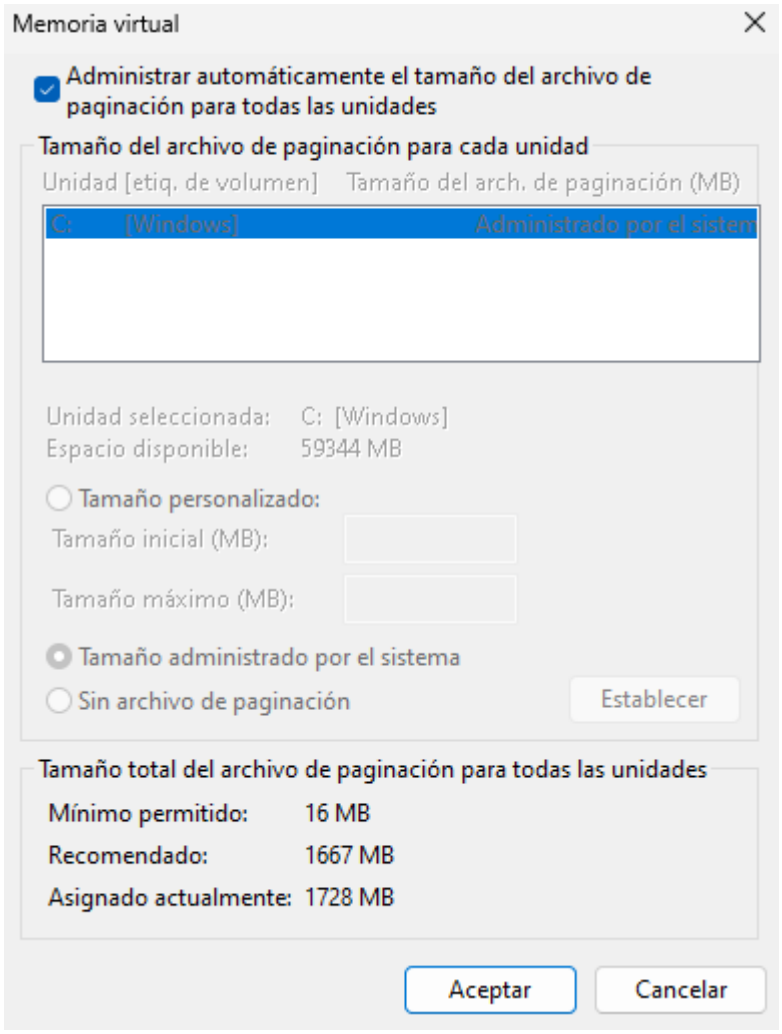
Y en la ventana que aparece seleccionamos la pestaña de Opciones Avanzadas:



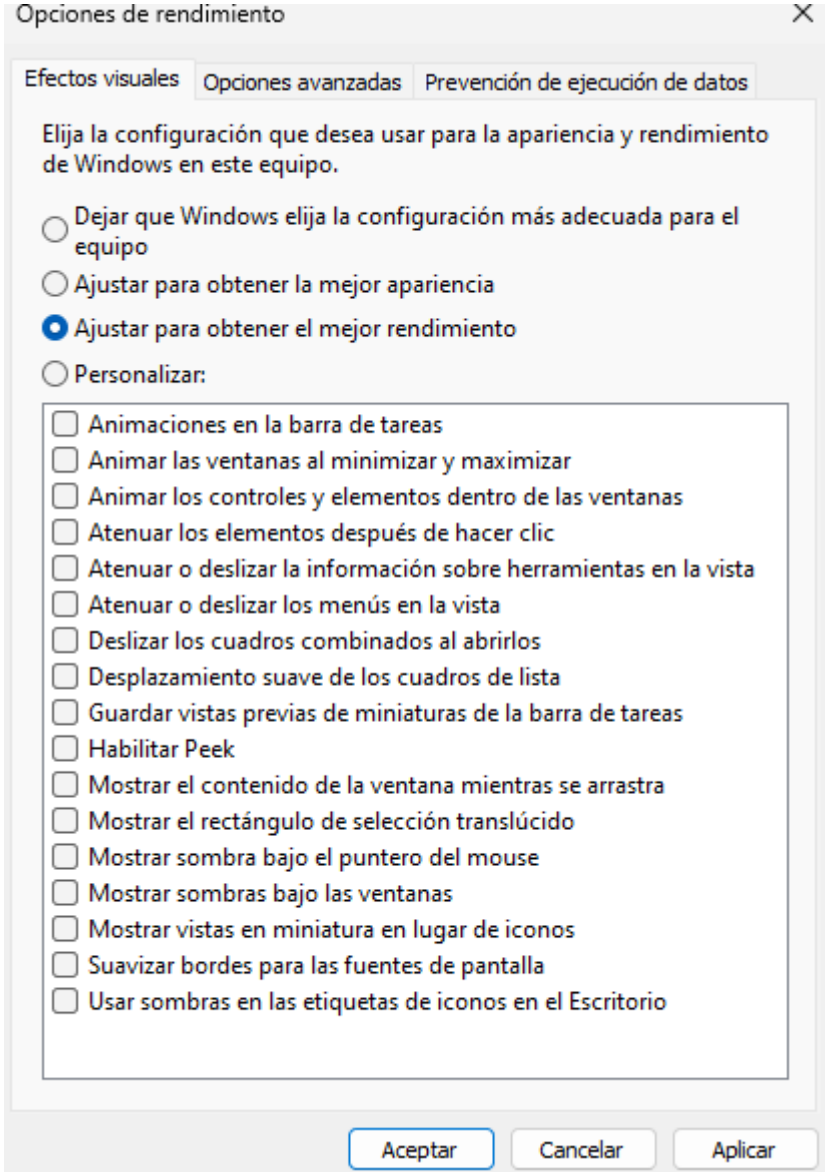
Dentro de esta pestaña pulsamos en el botón cambiar que se encuentra en la sección de Memoria Virtual:



En este caso podemos ver que está gestionado por el sistema:

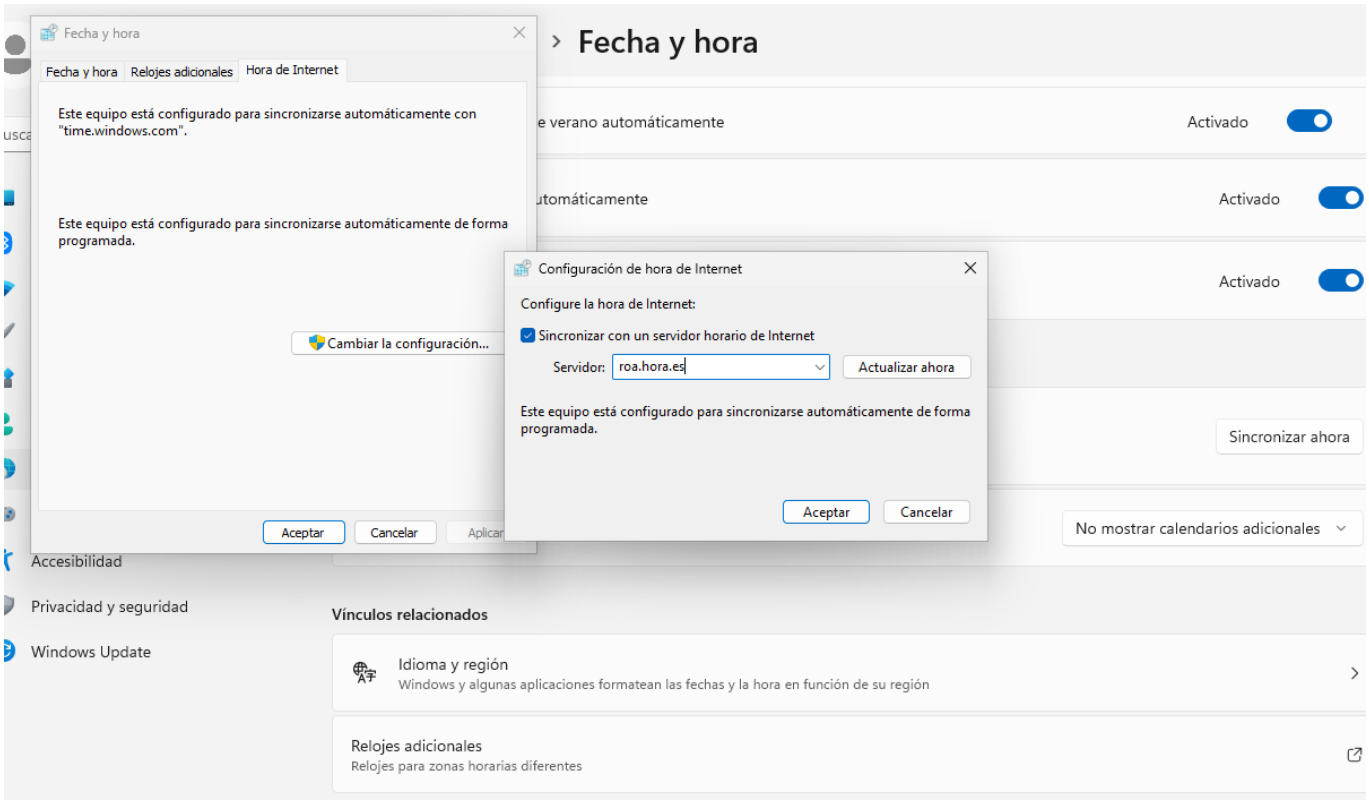


==== Revisa las propiedades del sistema, y dentro de la sección de “Rendimiento” activa la opción de “Ajustar para obtener el mejor rendimiento” ==== En la misma sección que estuvimos en el pasado apartado vamos a la pestaña efectos visuales y seleccionamos Ajustar para obtener el mejor rendimiento:



Cambia el servidor de hora del equipo por un servidor NTP español “roa.hora.es"

Vamos a Ajustar Fecha y hora/Relojes adicionales y enla pestaña de hora de internet le damos a cambiar la configuración y en la ventaba que aparezca ponemos el servidor NTP:



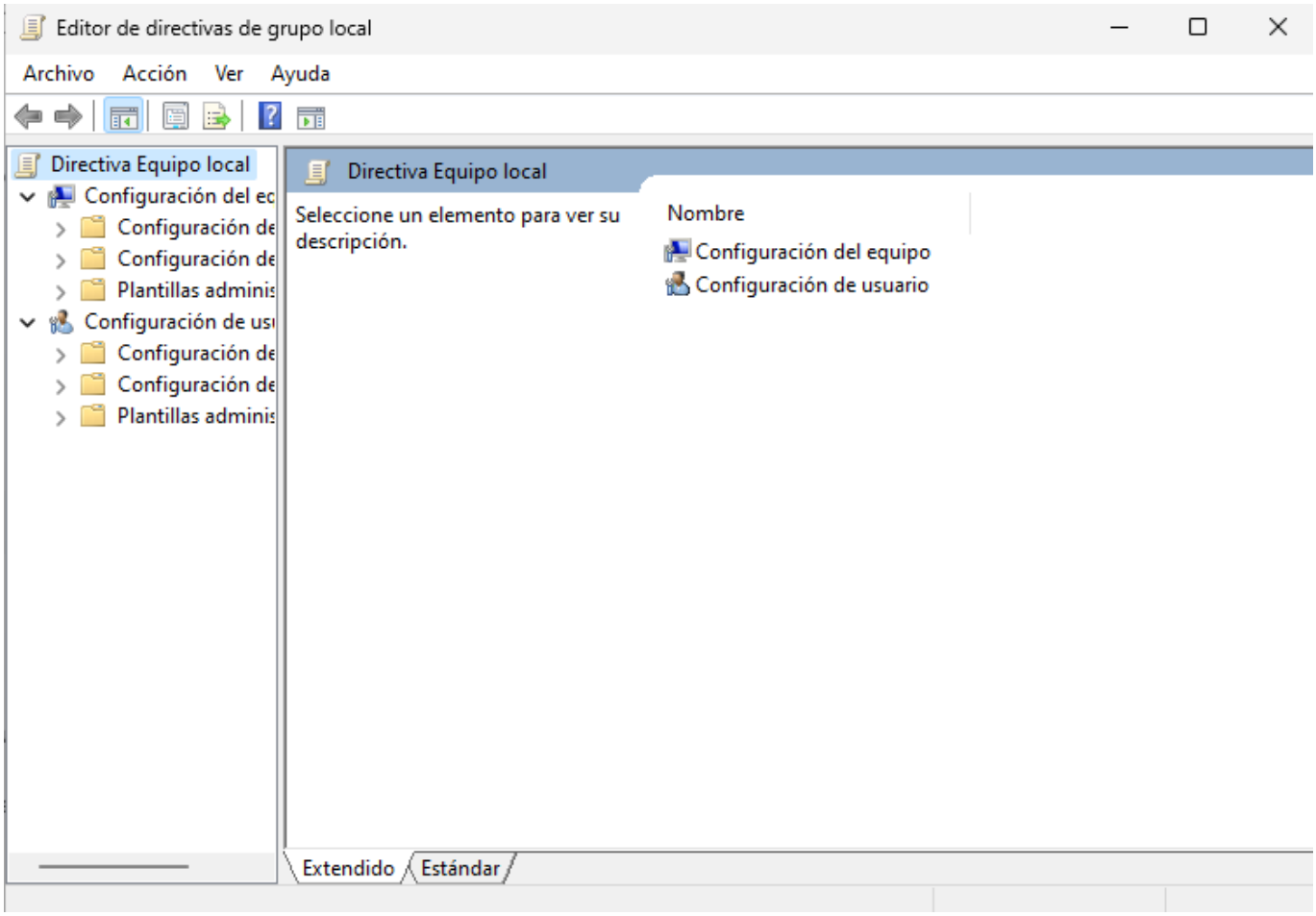
4. Vamos a realizar la configuración de diferentes Directivas de Grupo en Windows 11

a) ¿Qué dos tipos de directivas de grupo locales tenemos? ¿Cuál es la diferencia entreellas?

- Directiva de Configuración Local: Sirve para establecer las configuraciones que seguirán los equipos de los usuarios que pertenezcan al grupo
- Directiva de Seguridad Local: Sirve para definir las restricciones de seguridad de las cuentas de usuario

b) ¿Cómo accedemos a las directivas de grupo locales?

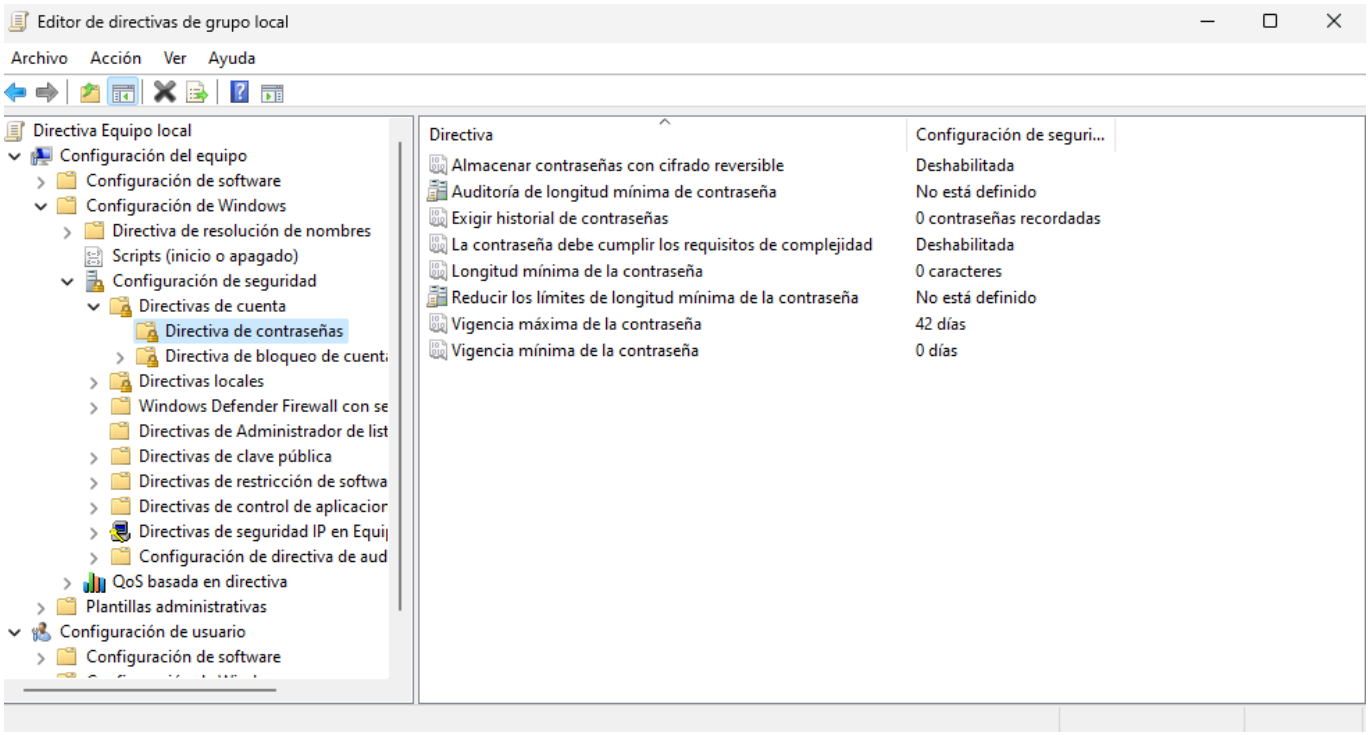
Pulsamos Windows+R y Escribimos gpedit.msc:



c) Revisa las siguientes secciones de las directivas de grupo e identificar que parámetros tenemos que cambiar en cada una de las secciones

Configuración directivas de grupo local I

Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas de cuenta → Directiva de contraseñas

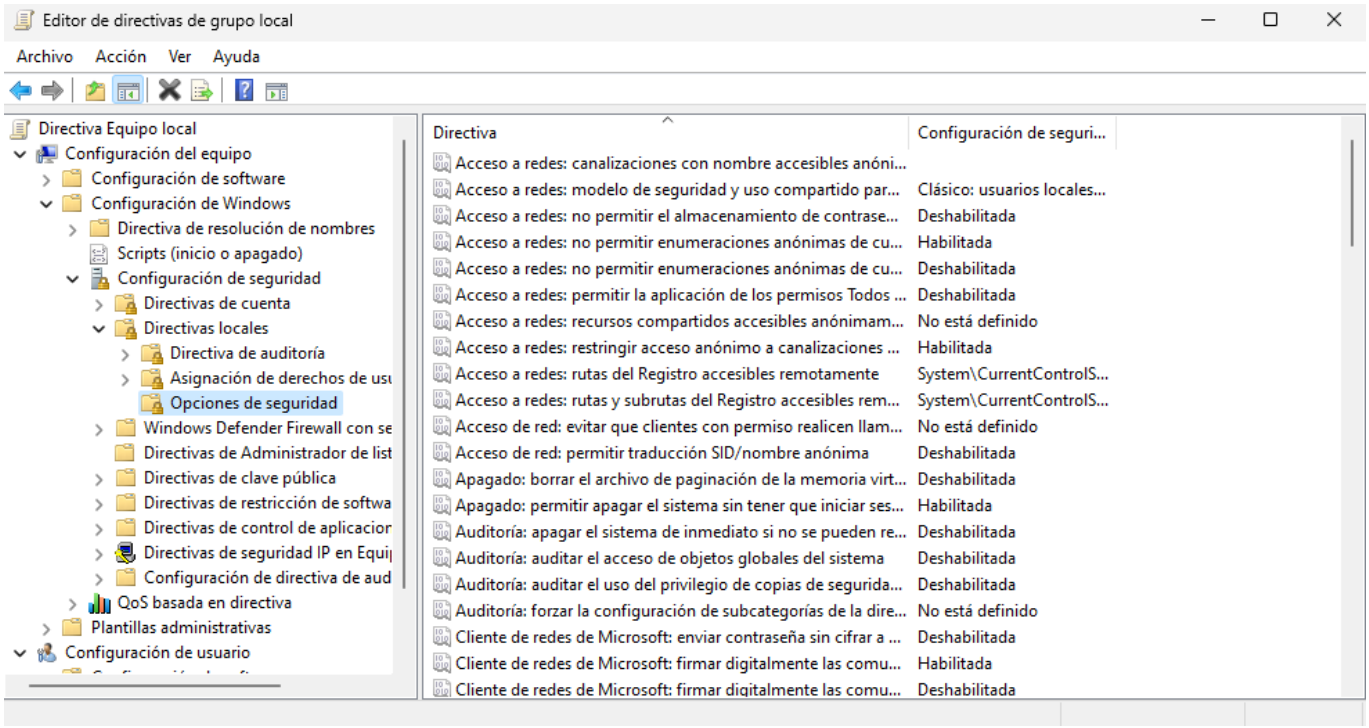


En esta sección podemos encontrar las siguientes directivas:

- Almacenar contraseñas con cifrado reversible: Poco seguro, se recomienda su desactivación ya que hace las contraseñas vulnerables por la forma en la que las almacena
- Longitud mínima de contraseña: Establece que tamaño debe tener la contraseña como mínimo, recomendable para mejorar la complejidad de las contraseñas
- Exigir Historial de contraseñas: Se puede usar para evitar que el usuario repita alguna de las N contraseñas utilizadas, mejorando así algo la seguridad
- La contraseña debe cumplir con los requisitos de complejidad: Permite exigir que la contraseña contenga cierta cantidad de números, mayúsculas, minúsculas y caracteres, para mejorar su complejidad y hacerla más difícil de descifrar.
- Vigencia máxima de la contraseña: Sirve para establecer una fecha de caducidad para la contraseña, pidiendo una contraseña nueva una vez esta ha expirado.
- VIgencia mínima de la contraseña: Evita que la contraseña sea cambiada antes de que pase el tiempo indicado

Configuración de directivas de grupo local II

Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones deSeguridad



- Control de cuentas de Usuario: elevar solo los archivos ejectuables firmados y validados: Se comprueba la firma PKI, permite a la organización controlar las aplicaciones cuya aplicación está permitida.
- Inicio de sesión interactivo: Límite de inactividad del equipo: Bloquea el equipo pasado el tiempo definido de inactividad
- Inicio de sesión interactivo: Pedir al usuario que cambie la contraseña antes de que expire: Muestra una notificación solicitando el cambio de contraseña cierta cantidad de tiempo antes de que esta expire.
- Inicio de sesión interactivo: Umbral de bloqueo de cuenta del equipo: Se definen cuantos intentos de contraseña fallida se permiten antes de bloquear la cuenta.