

# Memoria Laboratorios FORT

## Laboratorio 7: EJERCICIOS DE SECURIZACIÓN DE WINDOWS 11

Marcos Villar Avión

María Andrea Ugarte Valencia

# 1 - Reinicia el equipo y realiza las siguientes tareas:

- Lista los usuarios y grupos que ha creado el sistema operativo por defecto. Indica dos maneras distintas.
- Crea un usuario que pertenezca al grupo Usuarios. Indica dos formas distintas.

## 1.1 - Listado de usuarios y grupos

Gracias al comando **net user** podemos ver los usuarios del sistema:

```
net user
```

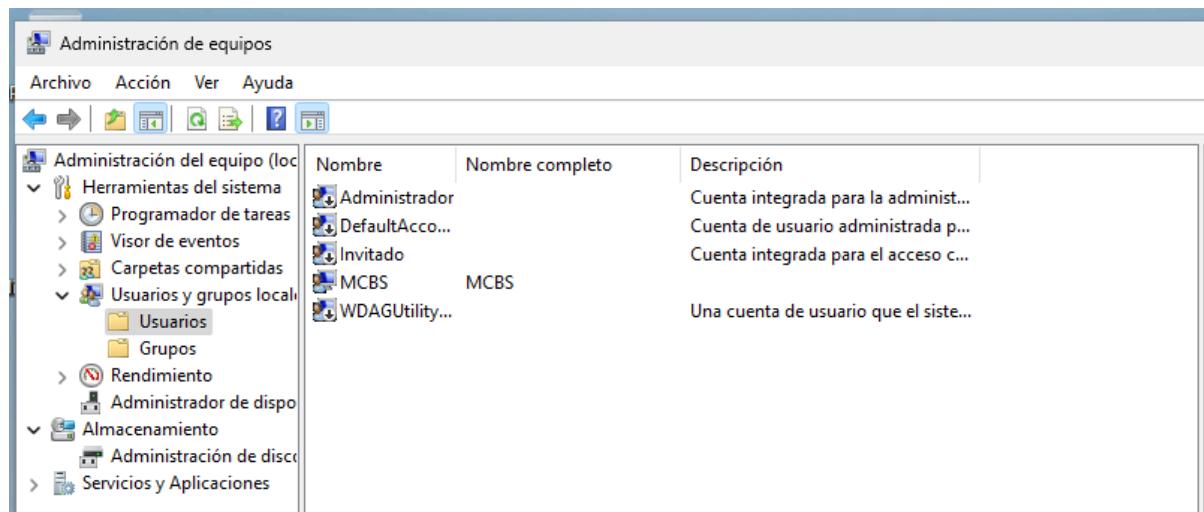
```
C:\Users\MCBS>net user

Cuentas de usuario de \\MCBSW11

-----
Administrador          DefaultAccount      Invitado
MCBS                  WDAGUtilityAccount

Se ha completado el comando correctamente.
```

Otra forma de ver a los usuarios del sistema es usando el GUI. Para ello, iremos a la administración de equipos y haremos click en el apartado del usuario. Podemos ver como se muestran los 5 usuarios que hemos listado anteriormente.



Para visualizar los grupos que el propio sistema ha creado podemos emplear el siguiente comando que listará cada uno de los siguientes grupos

```
net localgroup
```

```
c:\ Seleccionar Símbolo del sistema

C:\Users\MCBS>net localgroup

Alias para \\MCBSW11

-----
*Administradores
*Administradores de Hyper-V
*Duplicadores
*IIS_IUSRS
*Invitados
*Lectores del registro de eventos
*Operadores criptográficos
*Operadores de asistencia de control de acceso
*Operadores de configuración de red
*Operadores de copia de seguridad
*Propietarios del dispositivo
*System Managed Accounts Group
*Usuarios
*Usuarios avanzados
*Usuarios COM distribuidos
*Usuarios de administración remota
*Usuarios de escritorio remoto
*Usuarios del monitor de sistema
*Usuarios del registro de rendimiento
Se ha completado el comando correctamente.
```

Otra forma de listar los grupos es mediante la GUI, como se ha hecho anteriormente a través del **administración de equipos**

Administración de equipos

Archivo Acción Ver Ayuda

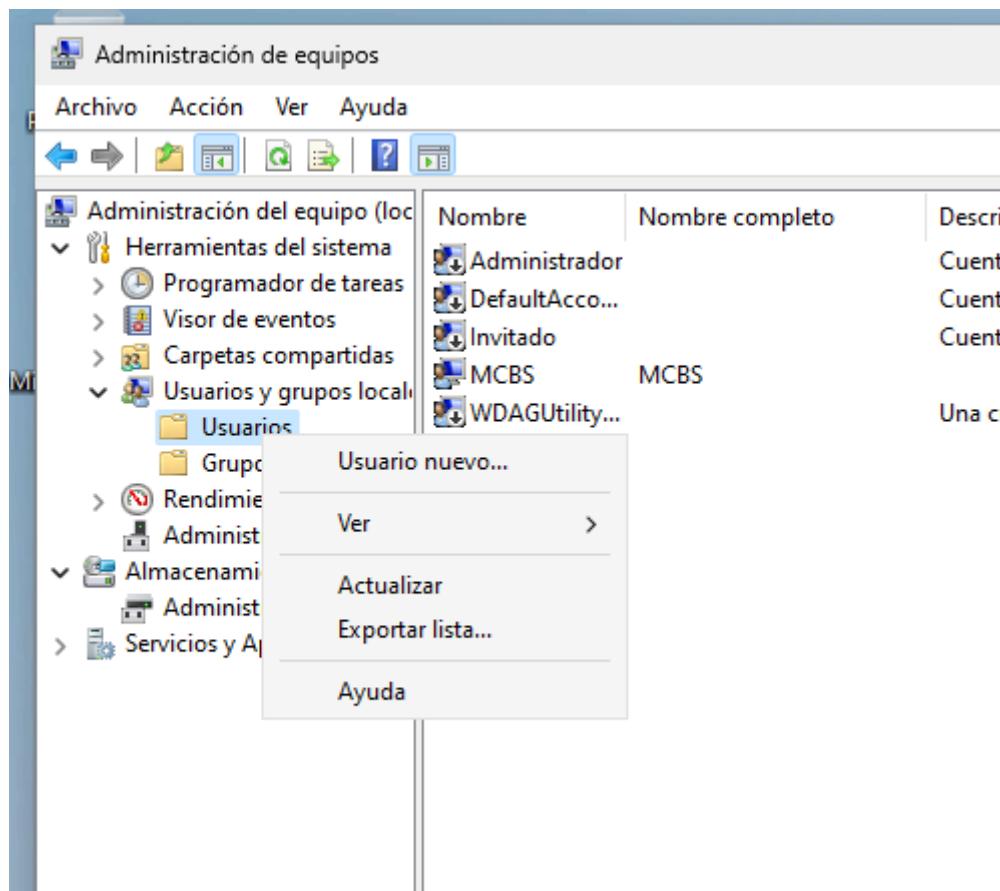
Administración del equipo (loc)

- ↳ Herramientas del sistema
  - > Programador de tareas
  - > Visor de eventos
  - > Carpetas compartidas
- ↳ Usuarios y grupos locales
  - ↳ Usuarios
  - ↳ Grupos
- > Rendimiento
- ↳ Administrador de dispositivos
- ↳ Almacenamiento
  - ↳ Administración de discos
- ↳ Servicios y Aplicaciones

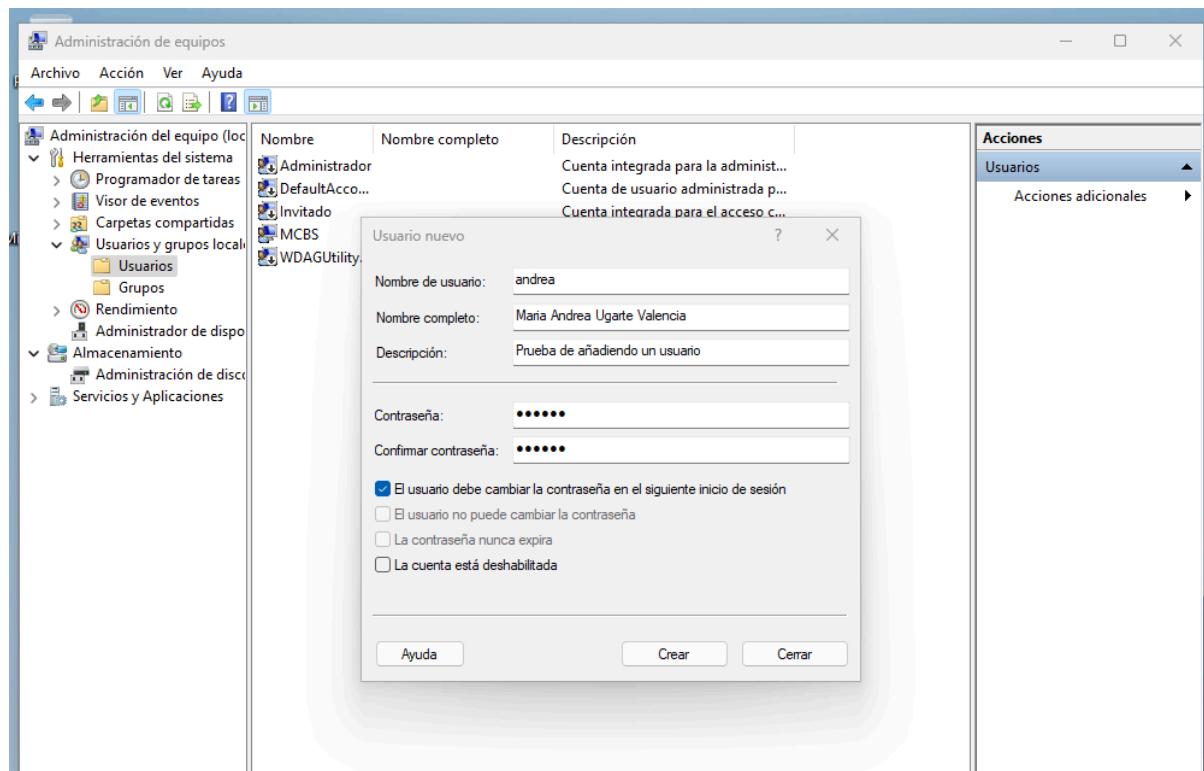
Nombre	Descripción
Administradores	Los administradores tienen acceso...
Administradores de H...	Los miembros de este grupo tienen...
Duplicadores	Pueden replicar archivos en un directorio...
IIS_IUSRS	Grupo integrado usado por Internet...
Invitados	De forma predeterminada, los invitados...
Lectores del registro d...	Los miembros de este grupo pueden...
Operadores criptográficos	Los miembros tienen autorización para...
Operadores de asistencia	Los miembros de este grupo pueden...
Operadores de configuración	Los miembros en este equipo pueden...
Operadores de copia de seguridad	Los operadores de copia de seguridad...
Propietarios del dispositivo	Los miembros de este grupo pueden...
System Managed Accounts	Los miembros de este grupo los administran...
Usuarios	Los usuarios no pueden hacer cambios...
Usuarios avanzados	Los usuarios avanzados se incluyen...
Usuarios COM distribuidos	Los miembros pueden iniciar, activar...
Usuarios de administración	Los miembros de este grupo pueden...
Usuarios de escritorio remoto	A los miembros de este grupo se les...
Usuarios del monitor de actividad	Los miembros de este grupo tienen...
Usuarios del registro de auditoría	Los miembros de este grupo pueden...

## 1.2 - Creación de un usuario

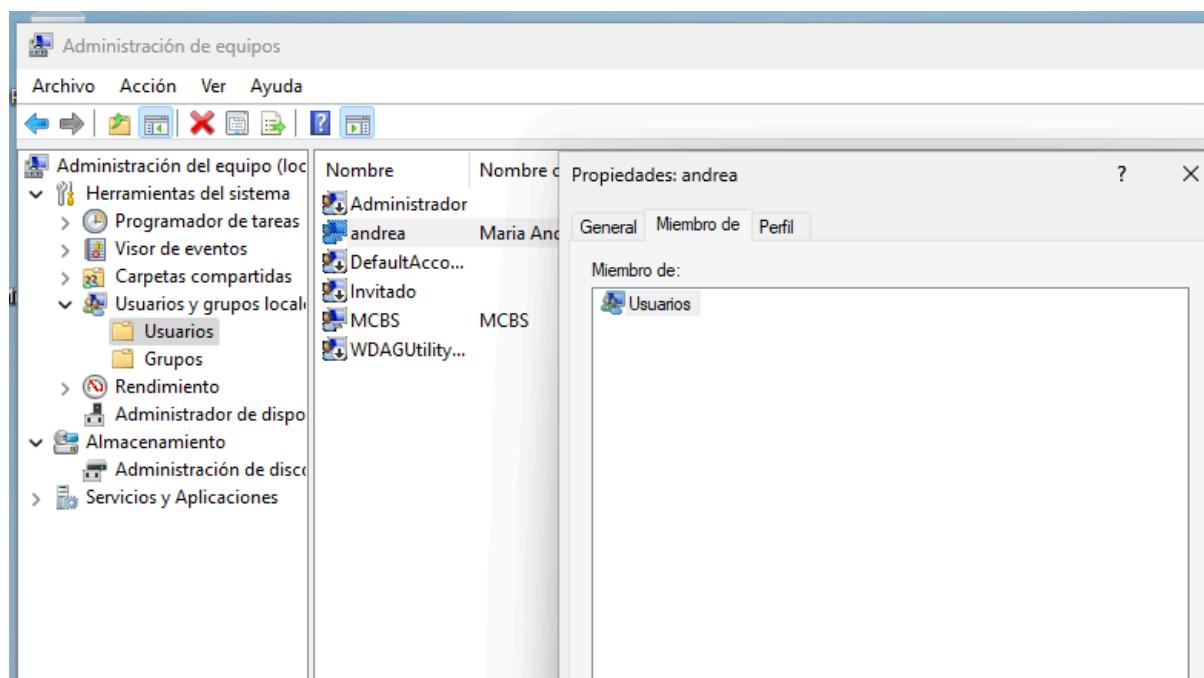
Para la creación del usuario podemos emplear tanto el CLI como a través de la GUI. Para ello, primeramente, vamos a emplear el **administración de equipos** y haciendo click derecho en la sección de usuarios, podemos crear uno



Posteriormente añadiremos toda la información necesaria:



Y podemos confirmar que el usuario **andrea** está en el grupo usuarios gracias a ver las propiedades de esta cuenta de la siguiente forma:



Otra forma sería mediante la CLI a través de un comando:

**net user /add marcos marcos**

```
Administrator: Símbolo del sistema
Microsoft Windows [Versión 10.0.22631.2861]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Windows\System32>net user /add marcos marcos
Se ha completado el comando correctamente.

C:\Windows\System32>net user

Cuentas de usuario de \\MCBSW11

-----
Administrador           andrea           DefaultAccount
Invitado                marcos            MCBS
WDAGUtilityAccount
Se ha completado el comando correctamente.
```

Se puede verificar que el usuario se ha creado correctamente. Ahora podríamos mostrar información del usuario con el siguiente comando:

**net user marcos**

```
C:\Windows\System32>net user marcos
Nombre de usuario          marcos
Nombre completo
Comentario
Comentario del usuario
Código de país o región    000 (Predeterminado por el equipo)
Cuenta activa              Sí
La cuenta expira          Nunca

Último cambio de contraseña 02/04/2024 15:28:51
La contraseña expira       14/05/2024 15:28:51
Cambio de contraseña        02/04/2024 15:28:51
Contraseña requerida       Sí
El usuario puede cambiar la contraseña  Sí

Estaciones de trabajo autorizadas  Todas
Script de inicio de sesión
Perfil de usuario
Directorio principal
Última sesión iniciada       Nunca

Horas de inicio de sesión autorizadas  Todas

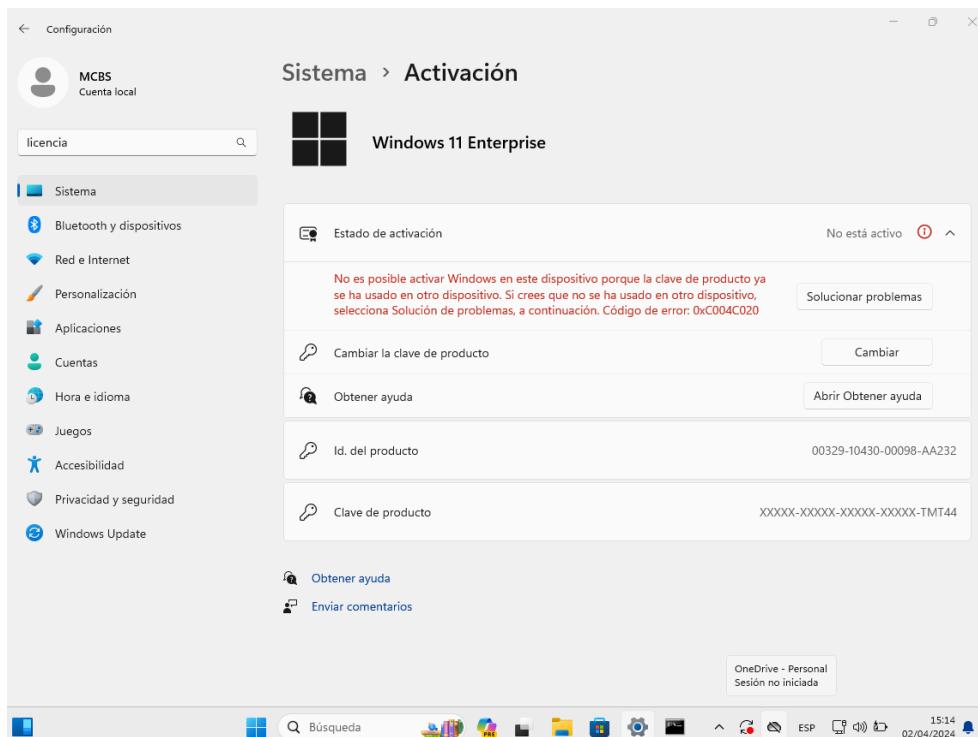
Miembros del grupo local      *Usuarios
Miembros del grupo global     *Ninguno
Se ha completado el comando correctamente.
```

Se verifica así que el usuario ya está en el grupo **Usuarios**

## 2 - Revisa y documenta los siguientes puntos de configuración:

### **1. ¿Cómo podemos saber el estado de la licencia del sistema operativo?**

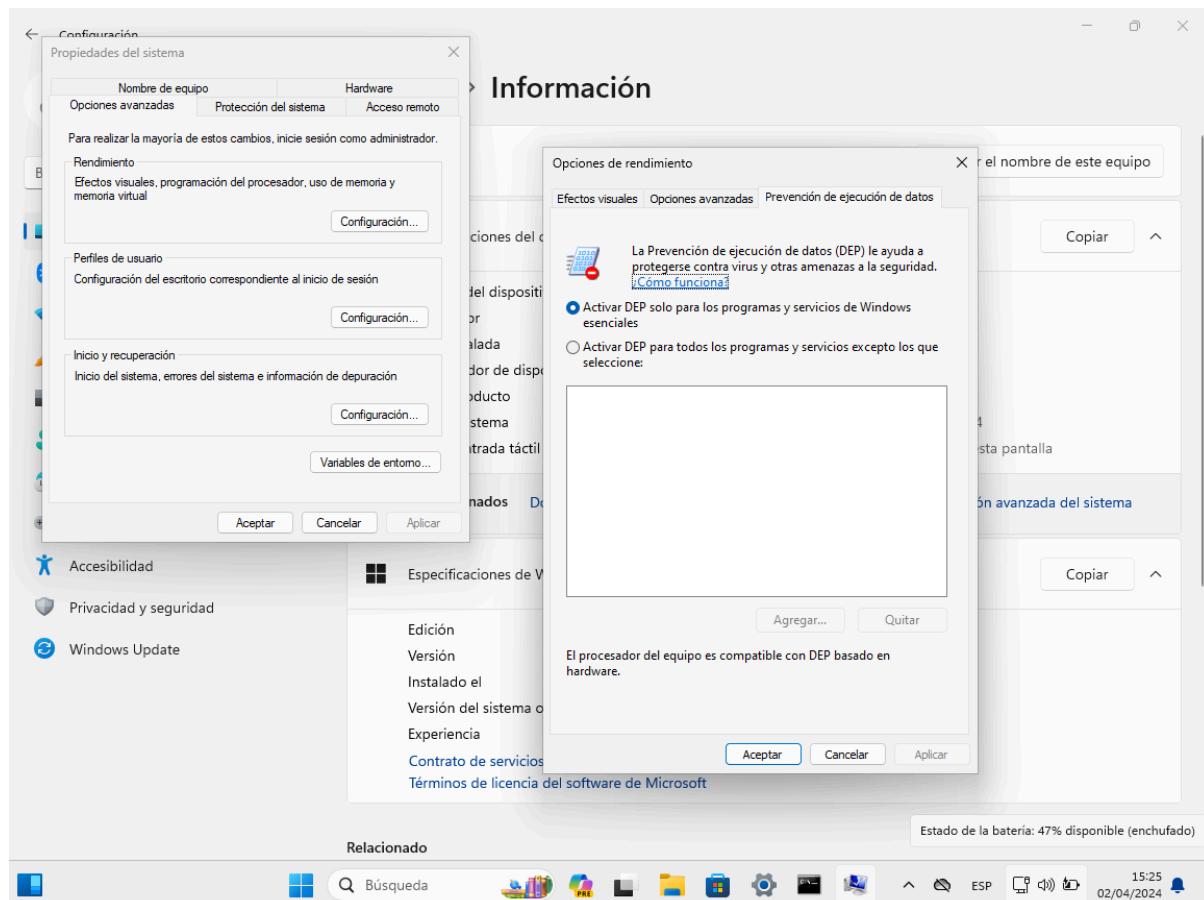
Para saber el estado de la licencia del sistema operativo nos vamos a Inicio y después a **Configuración > Sistema > Activación**:



Nuestra licencia no está activa.

### **2. ¿Está activo el DEP? ¿Dónde podemos verlo?**

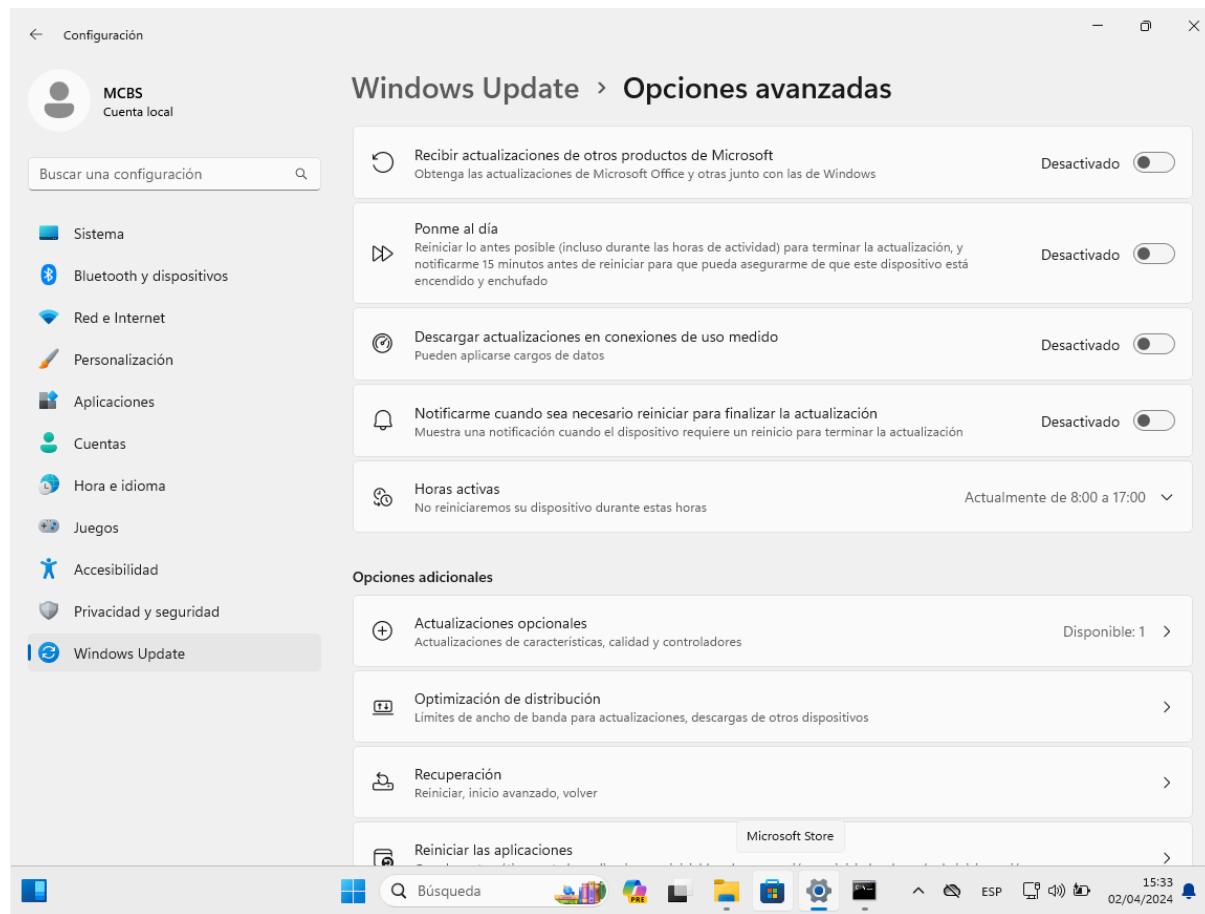
En la siguiente imagen podemos ver que DEP está activo solo para los programas y servicios de Windows esenciales.



Hemos llegado allí en **Configuración > Sistema > Información > Configuración avanzada del sistema**. Una vez allí le damos a **Configuración...** del apartado **Rendimiento** y vamos a **Prevención de ejecución de datos**.

### 3. ¿Cuál es la configuración por defecto del sistema de Actualizaciones automáticas?

Para ver esto nos vamos a **Configuración > Windows Update > Opciones avanzadas**



Podemos ver que las horas activas son de 8:00 a 17:00 (horas en las que no se reiniciará el equipo) y que el resto de opciones están desactivadas.

#### 4. ¿Identificar y listar los permisos NTFS que tiene el disco C?:

Para poder ver los permisos hemos ido al explorador de archivos, hemos hecho click derecho en la **Unidad C:** y hemos seleccionado **Propiedades**. En el apartado **Seguridad** se pueden ver los permisos NTFS.

**Propiedades: Windows (C:)**

Seguridad			Compartir		
General			Herramientas		
Seguridad			Hardware		
Versiones anteriores			Cuota		
Nombre de objeto: C:\					
Nombres de grupos o usuarios:					
<input checked="" type="checkbox"/> Cuenta desconocida (S-1-5-3-65536-1888954469-739942 <input checked="" type="checkbox"/> Usuarios autenticados <input checked="" type="checkbox"/> SYSTEM <input checked="" type="checkbox"/> Administradores (MCBSW11\Administradores)					
Para cambiar los permisos, haga clic en Editar. <input type="button" value="Editar..."/>					
Permisos de Cuenta desconocida (S-1-5-3-65536-1888954469-739942 Control total: Permitir Denegar Modificar Lectura y ejecución Mostrar el contenido de la carpeta Lectura Escritura Permisos especiales					
Para especificar permisos especiales o configuraciones avanzadas, haga clic en Opciones avanzadas.					
<input type="button" value="Aceptar"/> <input type="button" value="Cancelar"/> <input type="button" value="Aplicar"/>					

**Propiedades: Windows (C:)**

Seguridad			Compartir		
General			Herramientas		
Seguridad			Hardware		
Versiones anteriores			Cuota		
Nombre de objeto: C:\					
Nombres de grupos o usuarios:					
<input checked="" type="checkbox"/> Cuenta desconocida (S-1-5-3-65536-1888954469-739942 <input checked="" type="checkbox"/> Usuarios autenticados <input checked="" type="checkbox"/> SYSTEM <input checked="" type="checkbox"/> Administradores (MCBSW11\Administradores)					
Para cambiar los permisos, haga clic en Editar. <input type="button" value="Editar..."/>					
Permisos de Usuarios autenticados Control total: Permitir Denegar Modificar Lectura y ejecución Mostrar el contenido de la carpeta Lectura Escritura Permisos especiales					
Para especificar permisos especiales o configuraciones avanzadas, haga clic en Opciones avanzadas.					
<input type="button" value="Aceptar"/> <input type="button" value="Cancelar"/> <input type="button" value="Aplicar"/>					

**Propiedades: Windows (C:)**

Seguridad			Compartir		
General			Herramientas		
Seguridad			Hardware		
Versiones anteriores			Cuota		
Nombre de objeto: C:\					
Nombres de grupos o usuarios:					
<input checked="" type="checkbox"/> SYSTEM <input checked="" type="checkbox"/> Administradores (MCBSW11\Administradores) <input checked="" type="checkbox"/> Usuarios (MCBSW11\Usuarios)					
Para cambiar los permisos, haga clic en Editar. <input type="button" value="Editar..."/>					
Permisos de SYSTEM Control total: Permitir Denegar Modificar Lectura y ejecución Mostrar el contenido de la carpeta Lectura Escritura Permisos especiales					
Para especificar permisos especiales o configuraciones avanzadas, haga clic en Opciones avanzadas.					
<input type="button" value="Aceptar"/> <input type="button" value="Cancelar"/> <input type="button" value="Aplicar"/>					

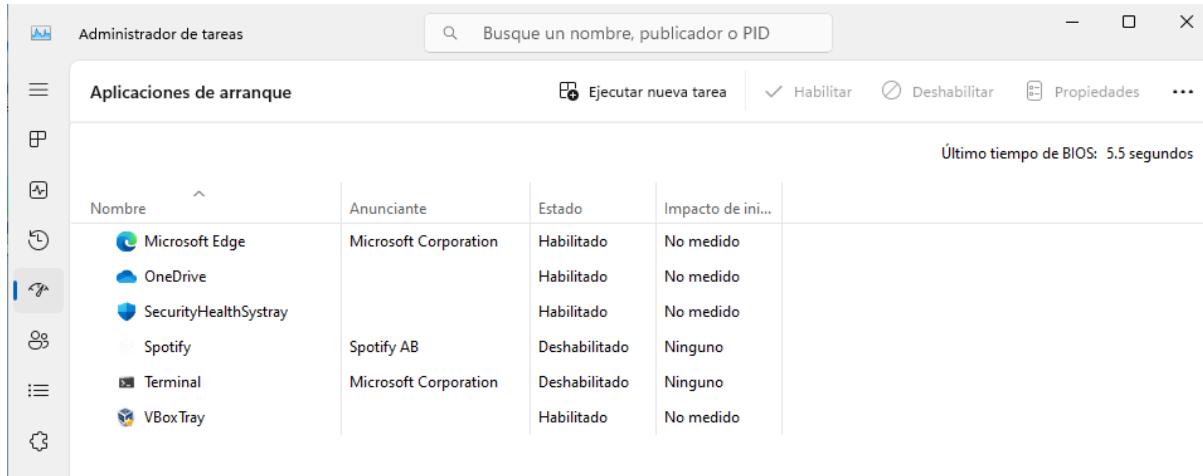
  

**Propiedades: Windows (C:)**

Seguridad			Compartir		
General			Herramientas		
Seguridad			Hardware		
Versiones anteriores			Cuota		
Nombre de objeto: C:\					
Nombres de grupos o usuarios:					
<input checked="" type="checkbox"/> SYSTEM <input checked="" type="checkbox"/> Administradores (MCBSW11\Administradores) <input checked="" type="checkbox"/> Usuarios (MCBSW11\Usuarios)					
Para cambiar los permisos, haga clic en Editar. <input type="button" value="Editar..."/>					
Permisos de Usuarios Control total: Permitir Denegar Modificar Lectura y ejecución Mostrar el contenido de la carpeta Lectura Escritura Permisos especiales					
Para especificar permisos especiales o configuraciones avanzadas, haga clic en Opciones avanzadas.					
<input type="button" value="Aceptar"/> <input type="button" value="Cancelar"/> <input type="button" value="Aplicar"/>					

## 5. ¿Identifica todos los procesos que se arrancan durante el inicio del Sistema Operativo?

En el administrador de tareas podemos ver los programas de arranque:



The screenshot shows the Windows Task Manager window titled "Administrador de tareas". The main pane is labeled "Aplicaciones de arranque" (Startup Applications). At the top right, there are buttons for "Ejecutar nueva tarea" (New Task), "Habilitar" (Enable), "Deshabilitar" (Disable), "Propiedades" (Properties), and a "..." menu. A search bar at the top says "Busque un nombre, publicador o PID". Below the header, a message says "Último tiempo de BIOS: 5.5 segundos". The table lists the following startup items:

Nombre	Anunciante	Estado	Impacto de ini...
Microsoft Edge	Microsoft Corporation	Habilitado	No medido
OneDrive		Habilitado	No medido
SecurityHealthSystray		Habilitado	No medido
Spotify	Spotify AB	Deshabilitado	Ninguno
Terminal	Microsoft Corporation	Deshabilitado	Ninguno
VBoxTray		Habilitado	No medido

Con **net start** se nos muestra una lista de los servicios ejecutándose. Al no haberlos alterado, coinciden con los de arranque.

```
C:\Users\MCBS>net start
Se han iniciado estos servicios de Windows:

    Acceso a datos de usuarios_53a9f
    Administrador de conexiones de acceso remoto
    Administrador de conexiones de Windows
    Administrador de credenciales
    Administrador de cuentas de seguridad
    Administrador de cuentas web
    Administrador de sesión local
    Administrador de usuarios
    Agente de conexión de red
    Agente de eventos de tiempo
    Agente de eventos del sistema
    Aislamiento de claves CNG
    Almacenamiento de datos de usuarios_53a9f
    Aplicación auxiliar de NetBIOS sobre TCP/IP
    Aplicación auxiliar IP
    Asignador de extremos de RPC
    Audio de Windows
    Ayudante para el inicio de sesión de cuenta Microsoft
    Centro de seguridad
    Cliente de directiva de grupo
    Cliente de seguimiento de vínculos distribuidos
    Cliente DHCP
    Cliente DNS
    Cola de impresión
    Compilador de extremo de audio de Windows
    CoreMessaging
    Datos de contactos_53a9f
    Detección de hardware shell
    Detección SSDP
    Energía
    Estación de trabajo
    Experiencias del usuario y telemetría asociadas
    Firewall de Windows Defender
    Host de sistema de diagnóstico
    Identidad de aplicación
    Información de la aplicación
    Iniciador de procesos de servidor DCOM
    Instrumental de administración de Windows
    Llamada a procedimiento remoto (RPC)
    Mostrar el servicio de directivas
    Motor de filtrado de base
    NPSMSvc_53a9f
    Optimización de distribución
```

**tasklist** nos lista todos los procesos, filtramos la salida para que solo nos muestre los de svchost (los de arranque).

```
C:\Users\MCBS>tasklist /FI "IMAGENAME eq svchost.exe"
```

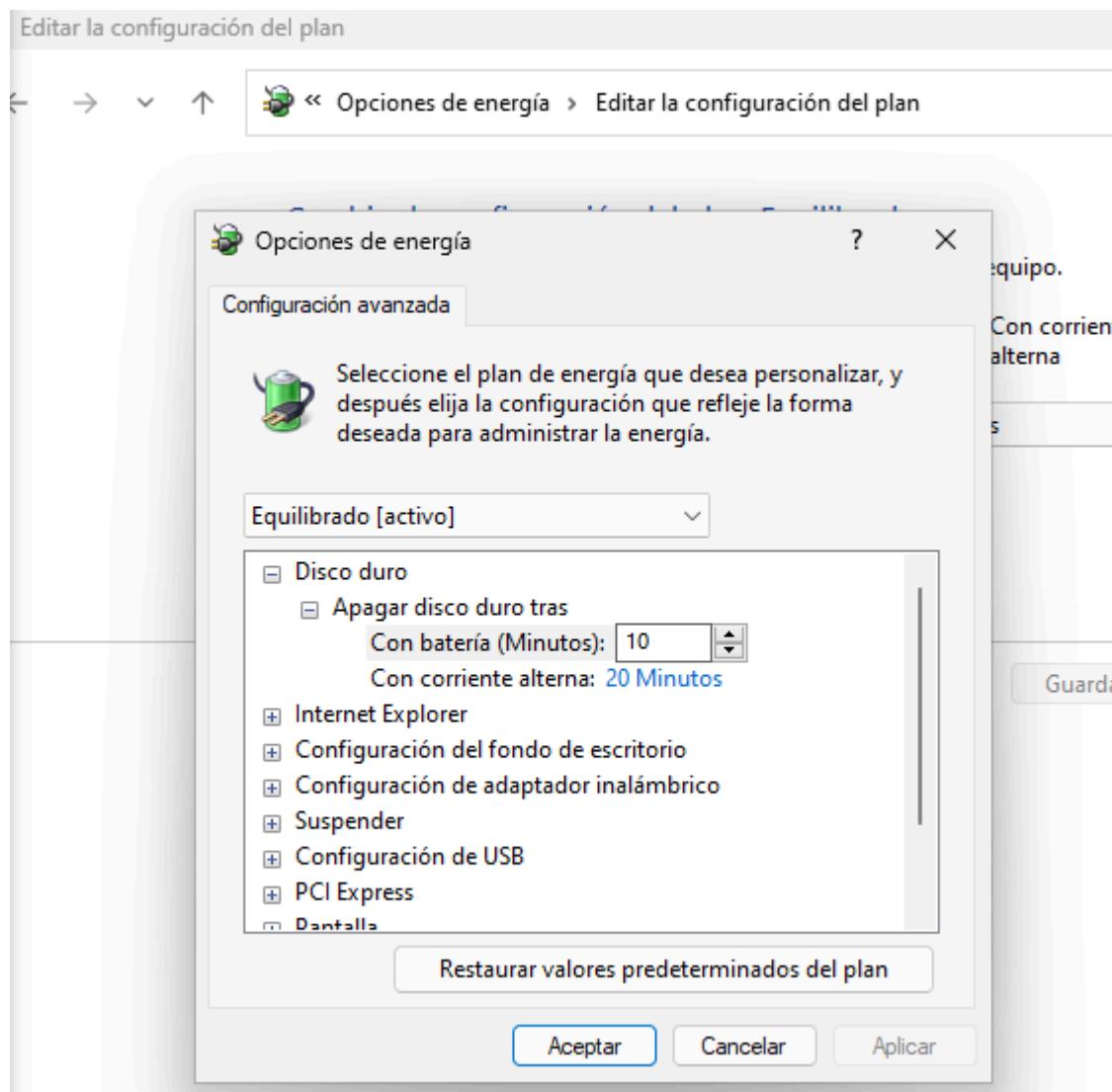
Nombre de imagen	PID	Nombre de sesión	Núm. de ses.	Uso de memoria
svchost.exe	996	Services	0	38.872 KB
svchost.exe	900	Services	0	14.852 KB
svchost.exe	1040	Services	0	8.216 KB
svchost.exe	1216	Services	0	18.856 KB
svchost.exe	1288	Services	0	9.600 KB
svchost.exe	1376	Services	0	15.544 KB
svchost.exe	1416	Services	0	10.064 KB
svchost.exe	1492	Services	0	11.576 KB
svchost.exe	1620	Services	0	5.032 KB
svchost.exe	1632	Services	0	7.168 KB
svchost.exe	1644	Services	0	9.488 KB
svchost.exe	1652	Services	0	6.600 KB
svchost.exe	1660	Services	0	7.208 KB
svchost.exe	1796	Services	0	14.464 KB
svchost.exe	1864	Services	0	49.580 KB
svchost.exe	1924	Services	0	5.676 KB
svchost.exe	1932	Services	0	84.460 KB
svchost.exe	1940	Services	0	7.796 KB
svchost.exe	1508	Services	0	7.580 KB
svchost.exe	2096	Services	0	8.044 KB
svchost.exe	2104	Services	0	8.056 KB
svchost.exe	2148	Services	0	6.928 KB
svchost.exe	2280	Services	0	7.740 KB
svchost.exe	2408	Services	0	7.480 KB
svchost.exe	2556	Services	0	7.212 KB
svchost.exe	2772	Services	0	12.444 KB
svchost.exe	2800	Services	0	6.996 KB
svchost.exe	2900	Services	0	14.036 KB
svchost.exe	2912	Services	0	9.496 KB
svchost.exe	2920	Services	0	9.276 KB
svchost.exe	2984	Services	0	11.488 KB
svchost.exe	3156	Services	0	16.624 KB
svchost.exe	3248	Services	0	7.768 KB
svchost.exe	3332	Services	0	36.724 KB
svchost.exe	3340	Services	0	10.720 KB
svchost.exe	3360	Services	0	5.764 KB
svchost.exe	3380	Services	0	27.816 KB
svchost.exe	3404	Services	0	17.356 KB

### **3 - Realiza las siguientes tareas:**

- Deshabilitar la gestión de Hibernación del equipo.
- Desactiva las conexiones de asistencia remota para el equipo.
- Activa la protección del sistema en la unidad C: (5-10%)
- Revisa la configuración del archivo de paginación. Confirma que el tamaño sea 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”.
- Cambia el servidor de hora del equipo por un servidor NTP español “roa.hora.es”

#### **3.1 - Deshabilitar la gestión de Hibernación del equipo**

Podemos hacer esto de dos formas diferentes. Mediante GUI o CLI. Si vamos al panel de **control > opciones de energía > editar la configuración del plan** y hacemos click en **“Cambiar la configuración avanzada de energía”** podríamos desactivar la hibernación en esta pantalla pero podemos ver como no está accesible esta opción. Por lo tanto, podemos afirmar que el ordenador no tiene el hardware suficiente para ponerse en hibernación



Otra forma sería mediante el siguiente comando:

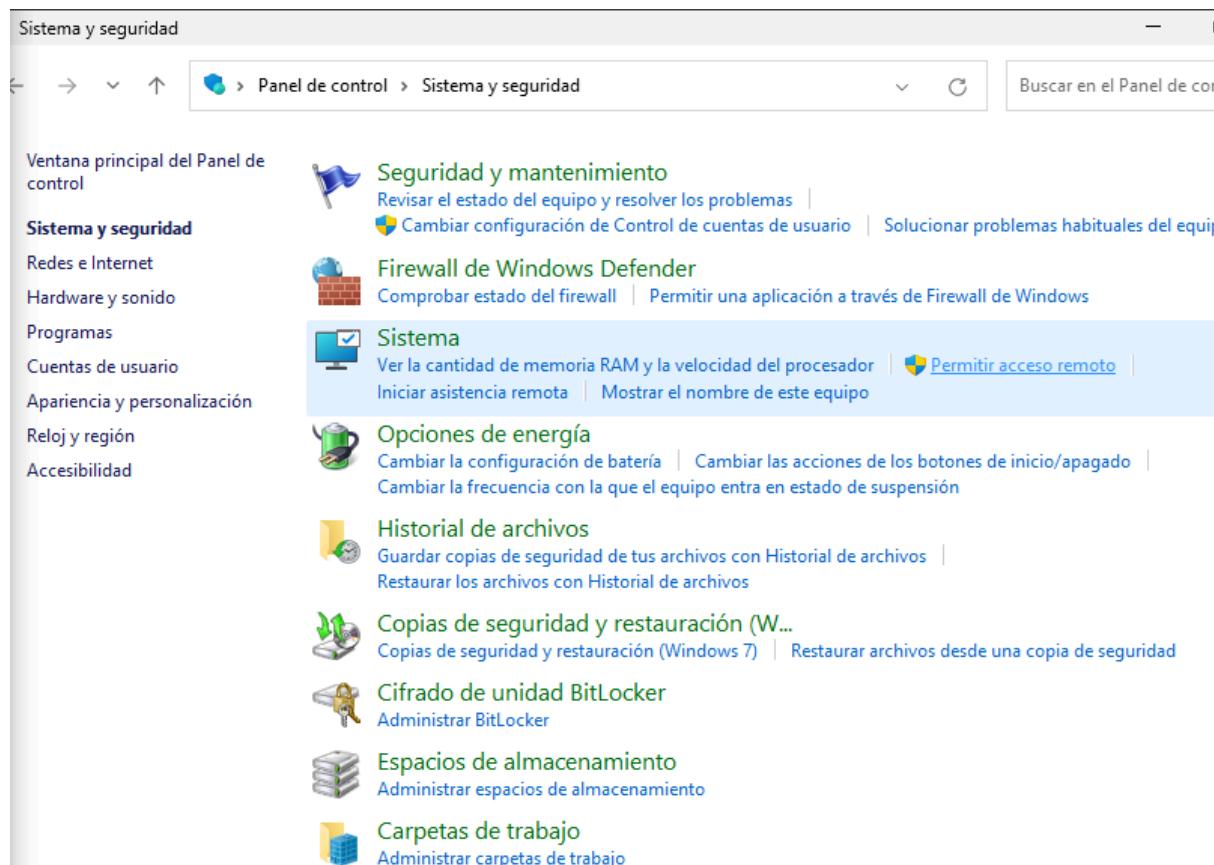
**powercfg.exe /hibernate off**

```
C:\Windows\System32>powercfg.exe /hibernate off  
C:\Windows\System32>powercfg.exe /hibernate on  
Error de hibernación: Solicitud no compatible.  
Los siguientes elementos impiden la hibernación en este sistema.  
    El firmware del sistema no permite la hibernación.
```

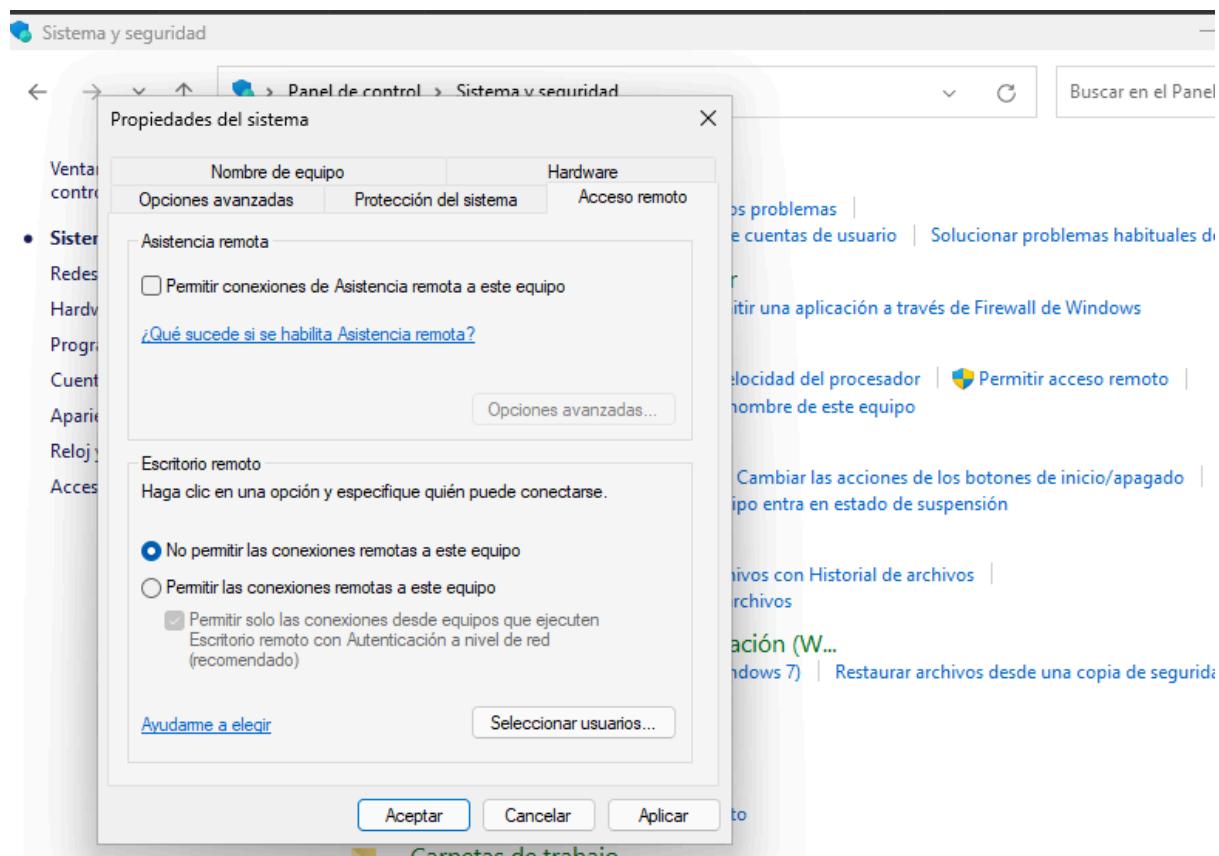
Vemos como si intentamos habilitarlo, nos da un aviso de que no es posible

### 3.2 - Desactiva las conexiones de asistencia remota para el equipo

Para desactivar esta característica iremos al Panel de Control > Sistema y seguridad y en la sección de Sistema podemos ver un apartado de **Permitir acceso remoto**

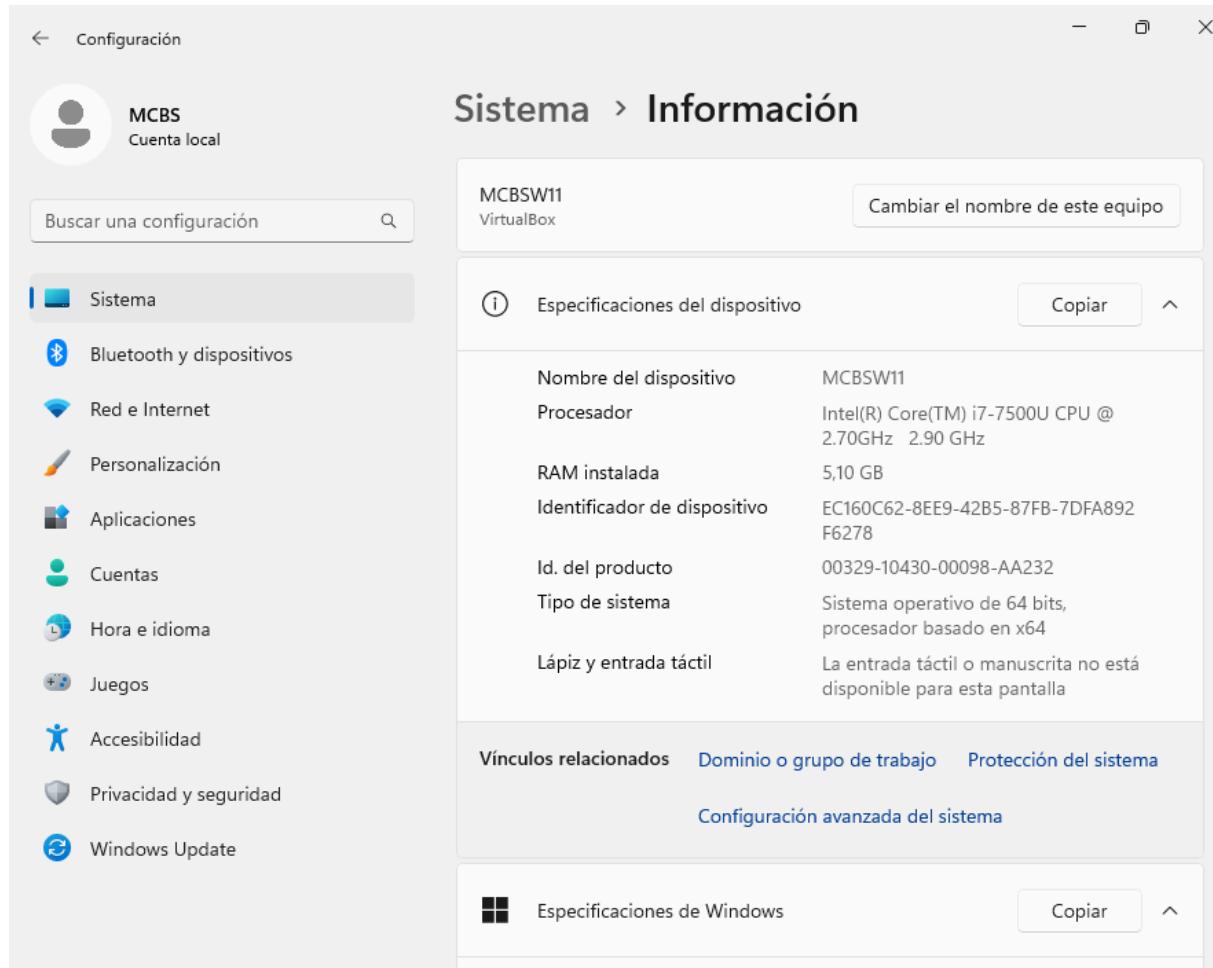


Si hacemos click ahí podemos deshabilitar esta opción

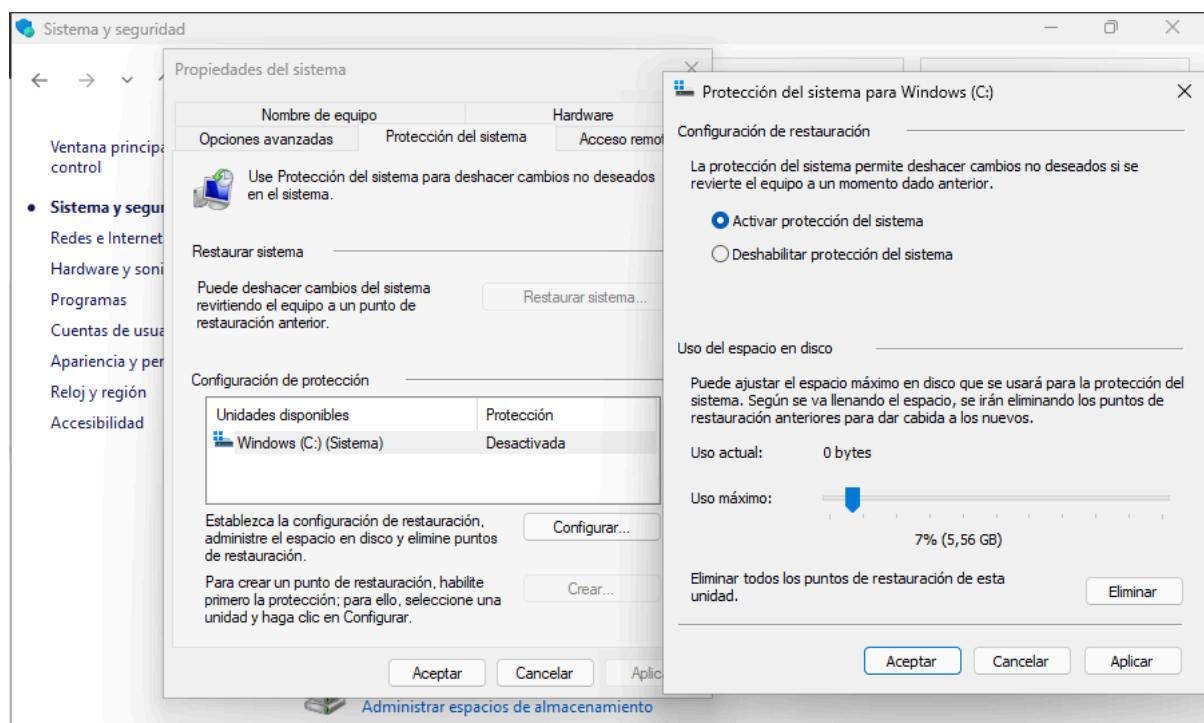


### **3.3 - Activa la protección del sistema en la unidad C: (5-10%)**

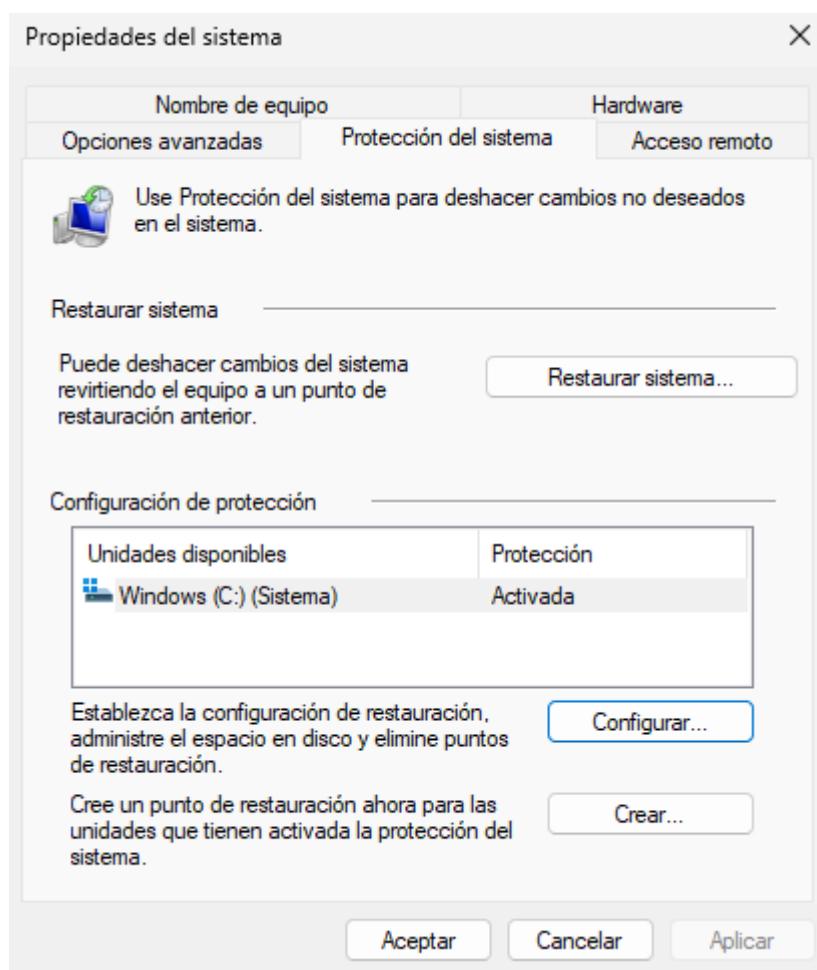
Para activar esta opción iremos al Panel de control > Sistema y seguridad > Sistema > Protección del sistema



Nos saldrá una ventana que nos permitirá configurar esta protección como podemos ver en la siguiente captura



Y vemos como queda activada:

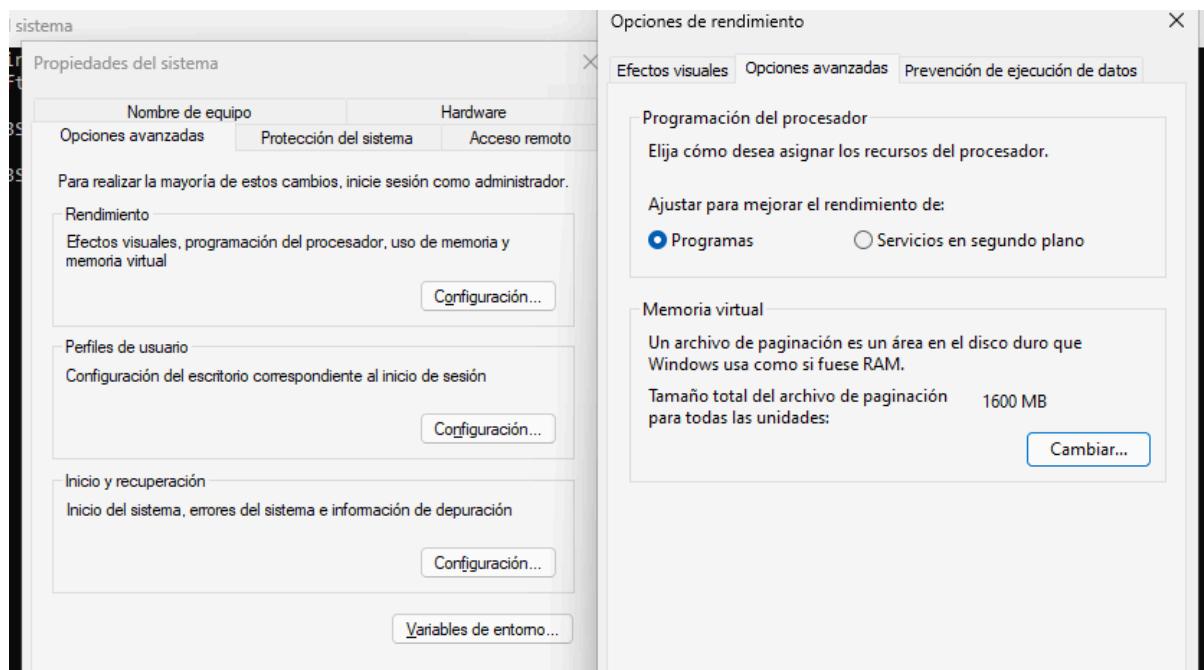


### **3.4 - Revisa la configuración del archivo de paginación. Confirma que el tamaño sea gestionado por el sistema.**

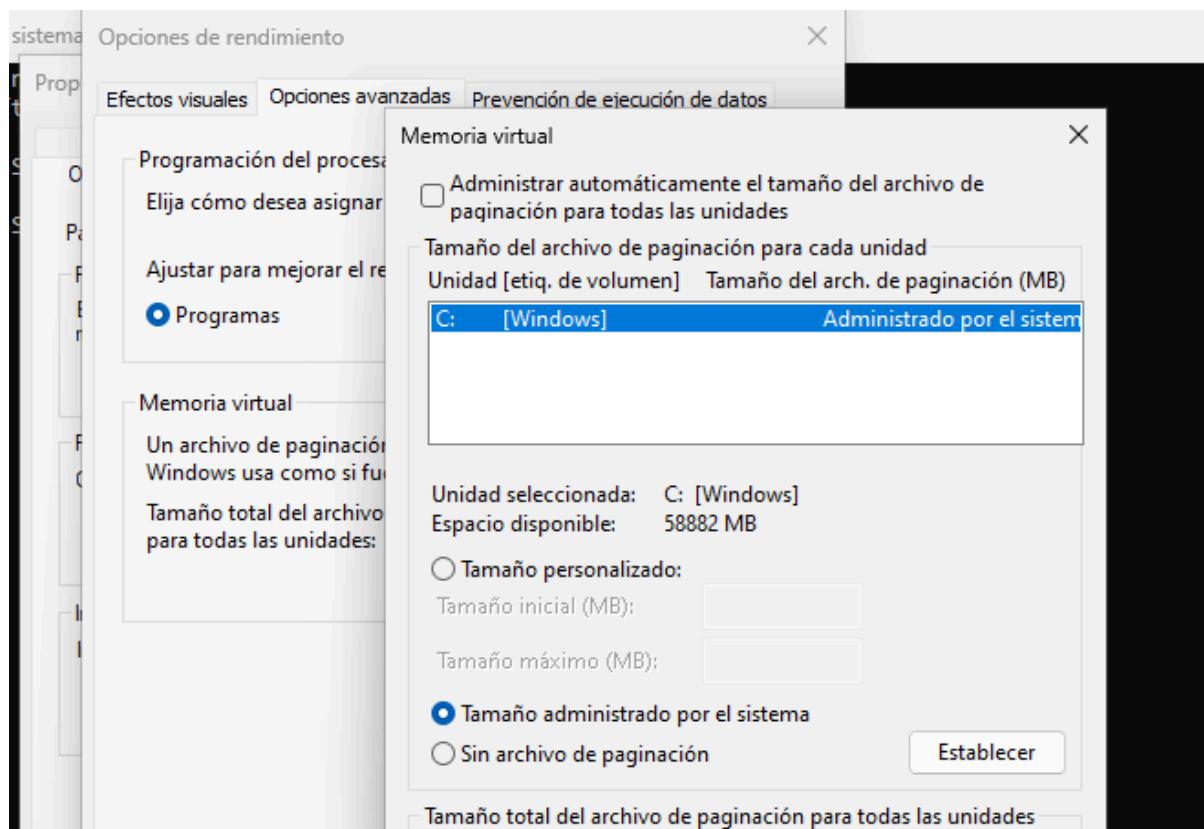
Para ello, ejecutaremos el siguiente comando:

***SystemPropertiesAdvanced.exe***

Vamos a Propiedades del sistema > Rendimiento > Configuración > Memoria Virtual > Cambiar:



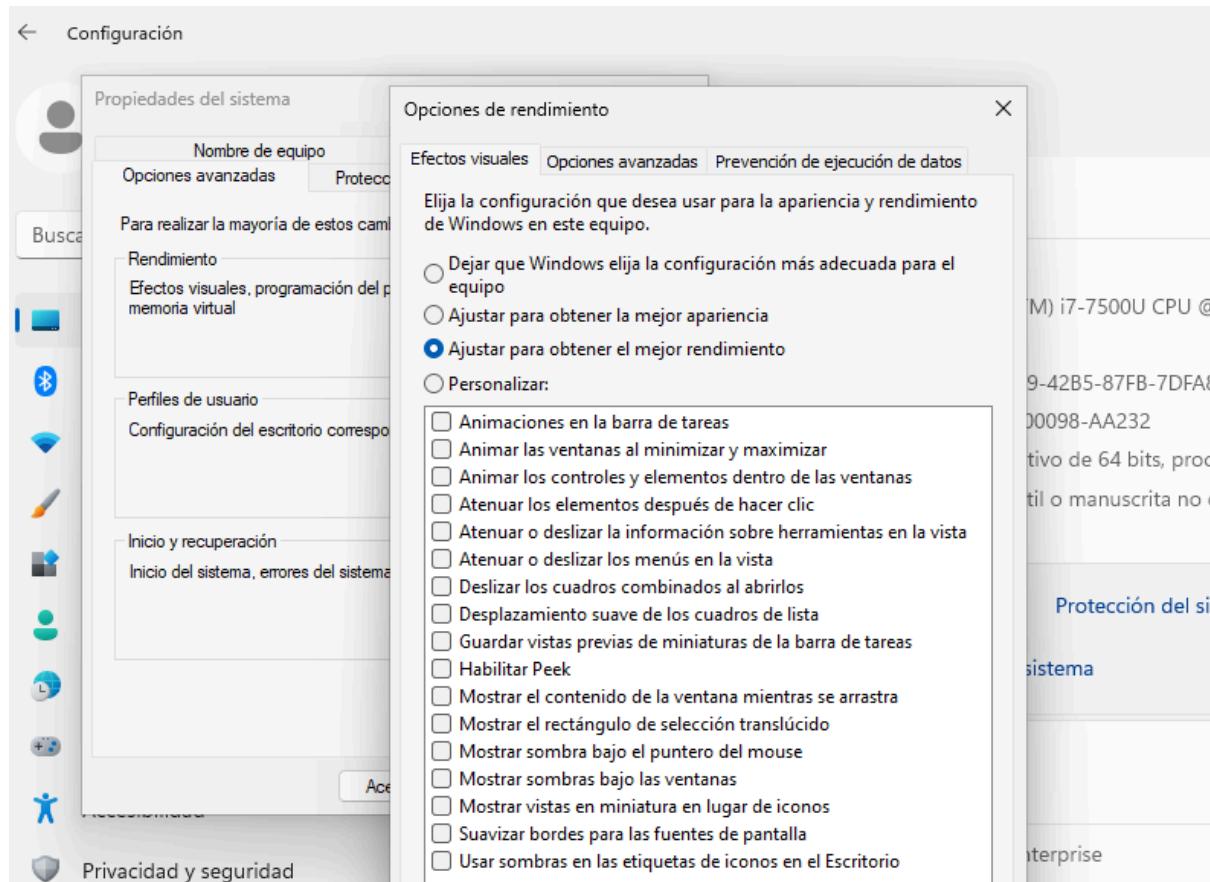
Y



Esto también lo podríamos dejar marcado por defecto ya que tiene el mismo efecto.

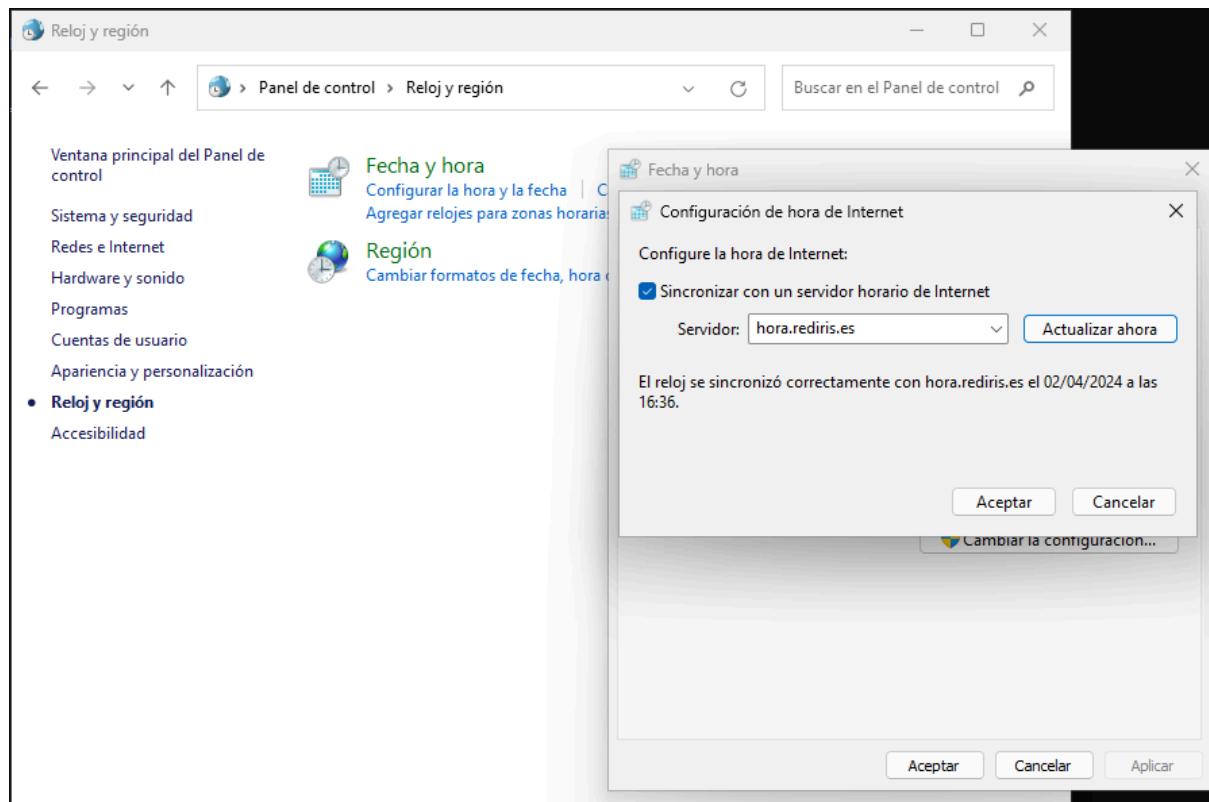
### 3.5 - Revisa las propiedades del sistema, y dentro de la sección de “Rendimiento” activa la opción de “Ajustar para obtener el mejor rendimiento”.

Para habilitar esto iremos a **Configuración > Información > Configuración avanzada del sistema > Opciones Avanzadas > Rendimiento > Ajustar para obtener el mejor rendimiento**



### 3.6 - Cambia el servidor de hora del equipo por un servidor NTP español “roa.hora.es”

Para esto nos vamos a **Panel de control > Reloj y región > Fecha y hora > Configurar la hora y la fecha > Hora de Internet > Cambiar la configuración**. Indicamos el servidor y actualizamos.



# Memoria Laboratorios FORT

## Laboratorio 8: EJERCICIOS DE SECURIZACIÓN DE WINDOWS 11

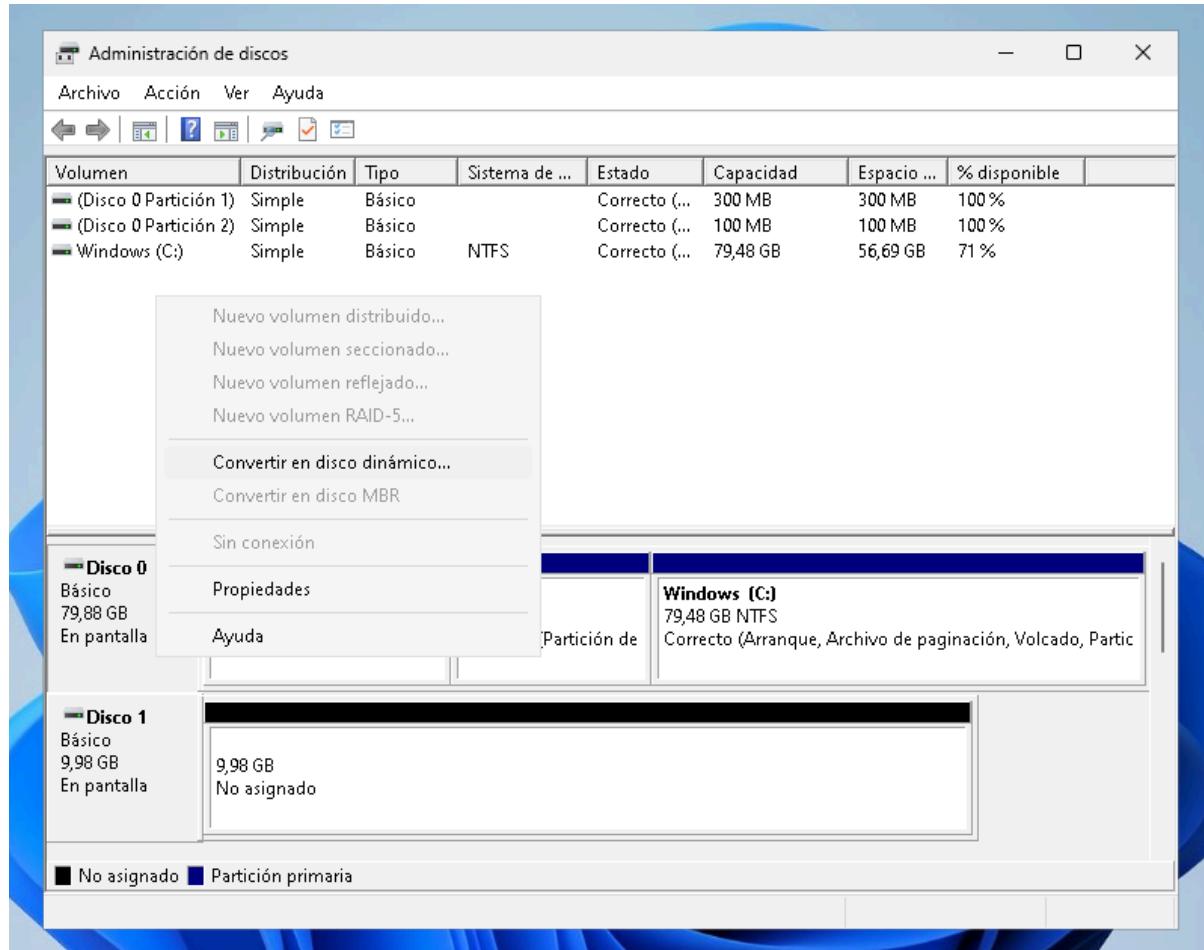
Marcos Villar Avión

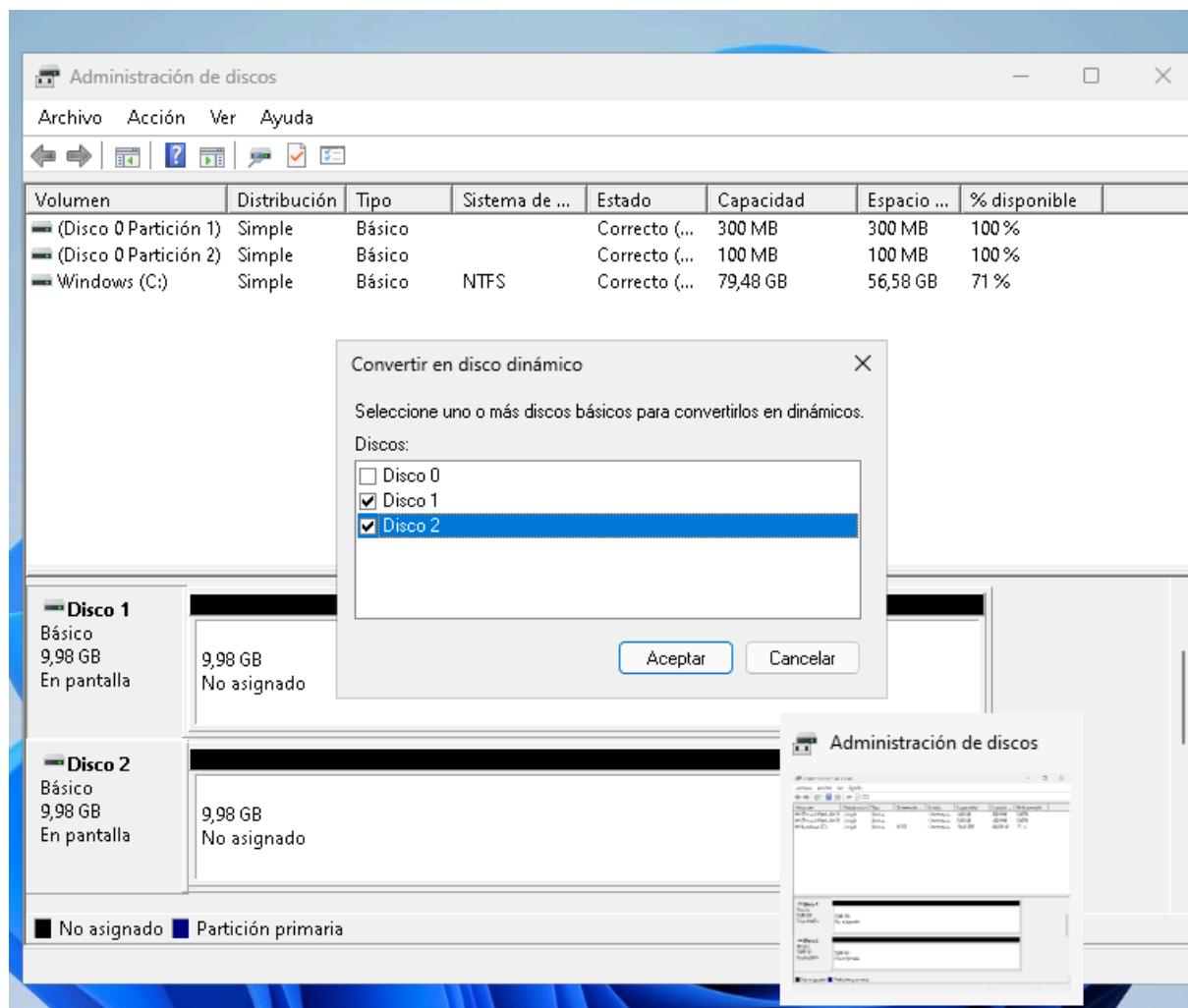
María Andrea Ugarte Valencia

# 1 - Con los dos nuevos discos realiza las siguientes tareas:

## 1.1 - Conviértelos en discos Dinámicos

Para ello, tendremos que ir a Administrador de Discos > seleccionar el disco que queremos ir haciendo click con el botón derecho podemos ver que existe la opción de convertir a dinámico





## 1.2 - ¿Qué diferencia existe entre Discos Básicos y Discos Dinámicos?

Aunque ambos tipo de dispositivos admiten los dos tipos de particiones MBR Y GPT, el disco dinámico admite más tipos de volúmenes:

- volumen simple
- volumen distribuido
- volumen seleccionado
- volúmenes reflejados
- volúmenes RAID-5

Por lo tanto, los discos dinámicos son más versátiles y útiles que los discos básicos.

### 1.3 - ¿Indica que diferencia existe entre MBR y GPT?

Tanto MBR y GPT son tablas de particiones que admite Windows para crear particiones en sus discos duros. MBR es la tabla de particiones más tradicional que soporta los sistemas operativos más antiguos. Por el contrario, GPT es la tabla de particiones más actualizada que permite realizar acciones más adecuadas a las exigencias de hoy en día.

Es por ello que GPT consta de diferentes ventajas frente a MBR:

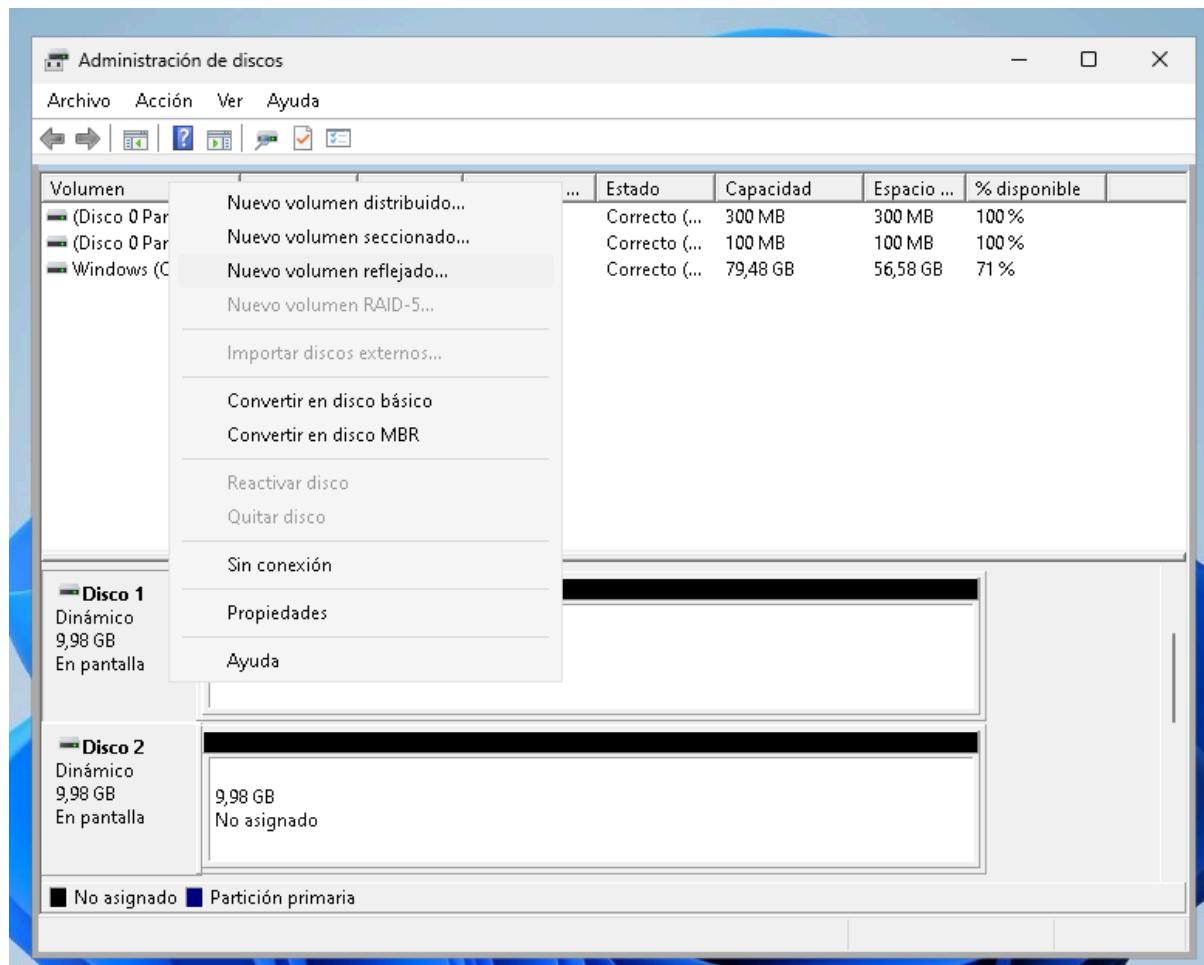
- soporta discos duros más grandes que 2TiB
- Permite crear particiones teóricamente ilimitadas
- Contiene una verificación de redundancia cíclica para comprobar la integridad de sus datos
- Contiene la copia de seguridad del encabezado GPT primario y las entradas de la partición que protege mejor los datos del disco

A pesar de ello, MBR tiene la ventaja clara de que es permitido en sistemas operativos más antiguos

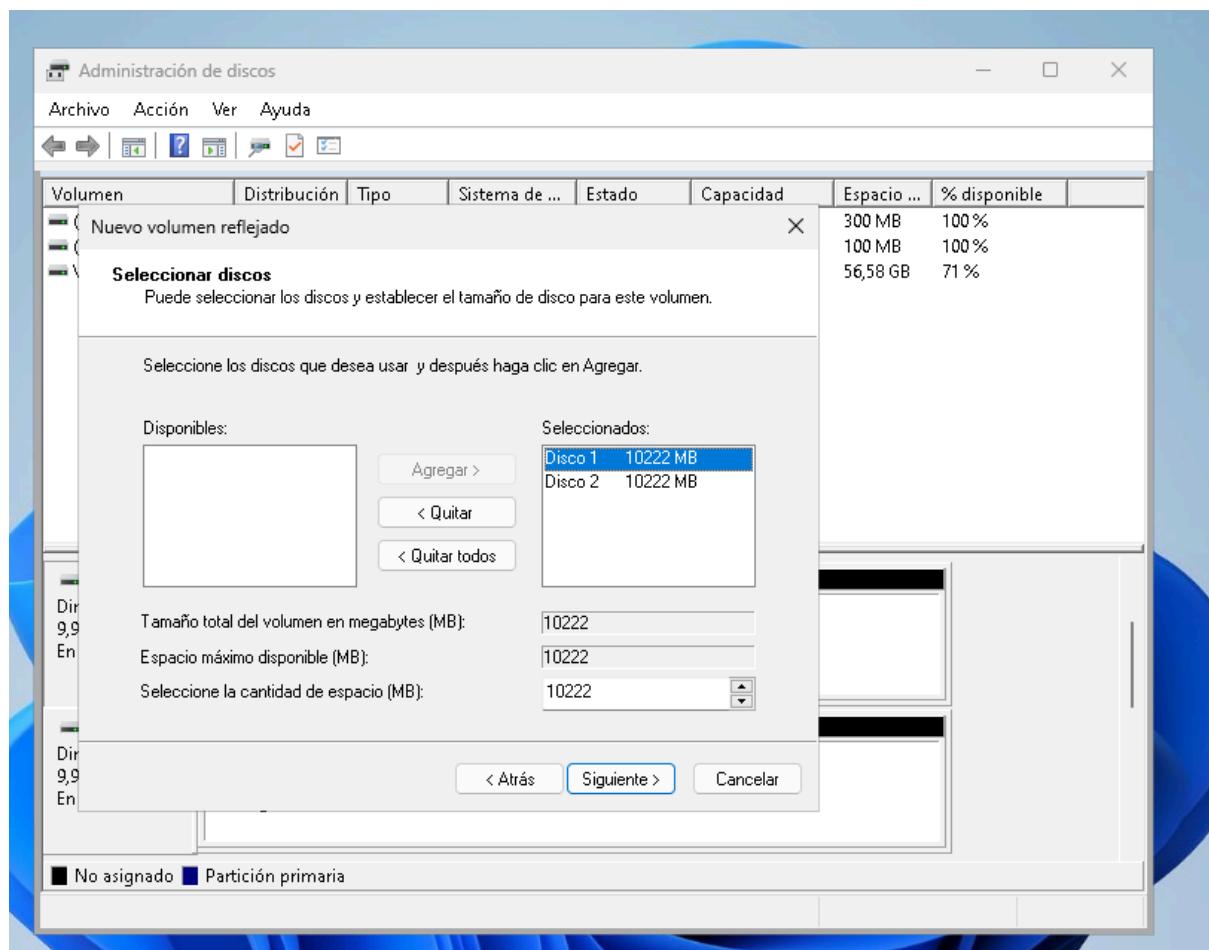
## 1.4 - RAID - 1

### 1.4.1 - ¿Genera un RAID 1?

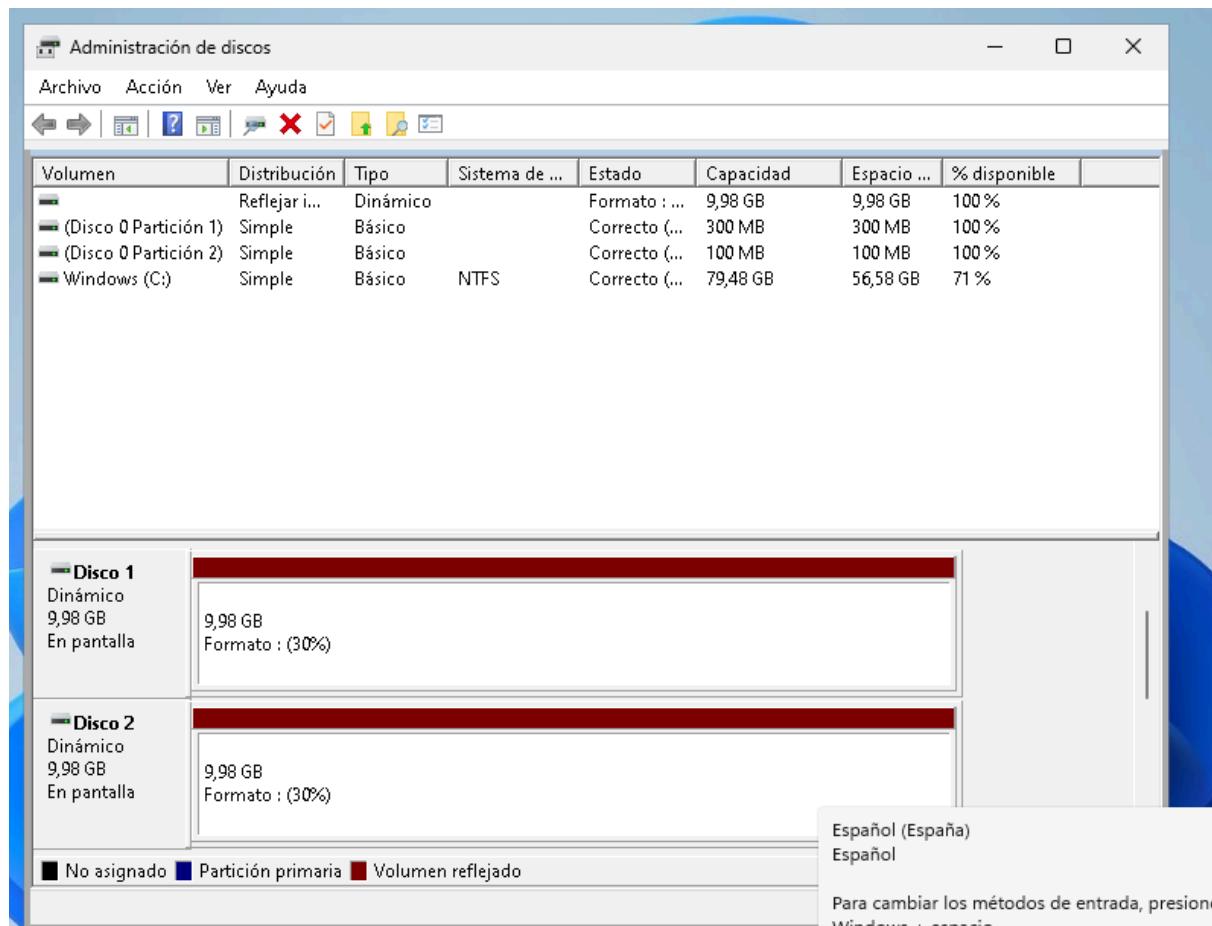
Para ello, vamos al administrador de discos, hacemos click derecho en el volumen que queramos y seleccionamos “Nuevo volumen reflejado” como se ve en la siguiente captura



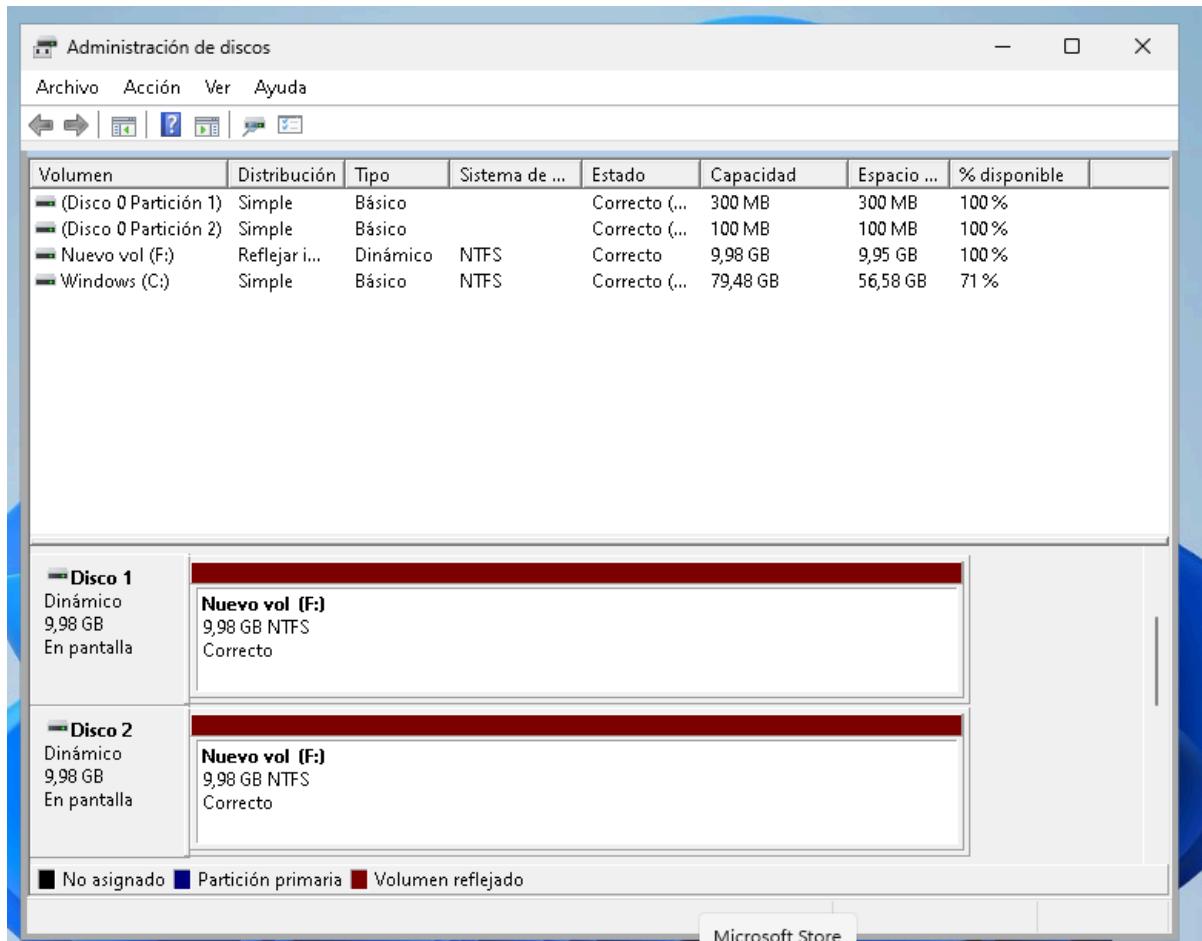
Seleccionamos ambos discos



Seleccionamos todo por defecto y empezará el formateado:



Tras finalizar podremos ver que todo se configuró correctamente

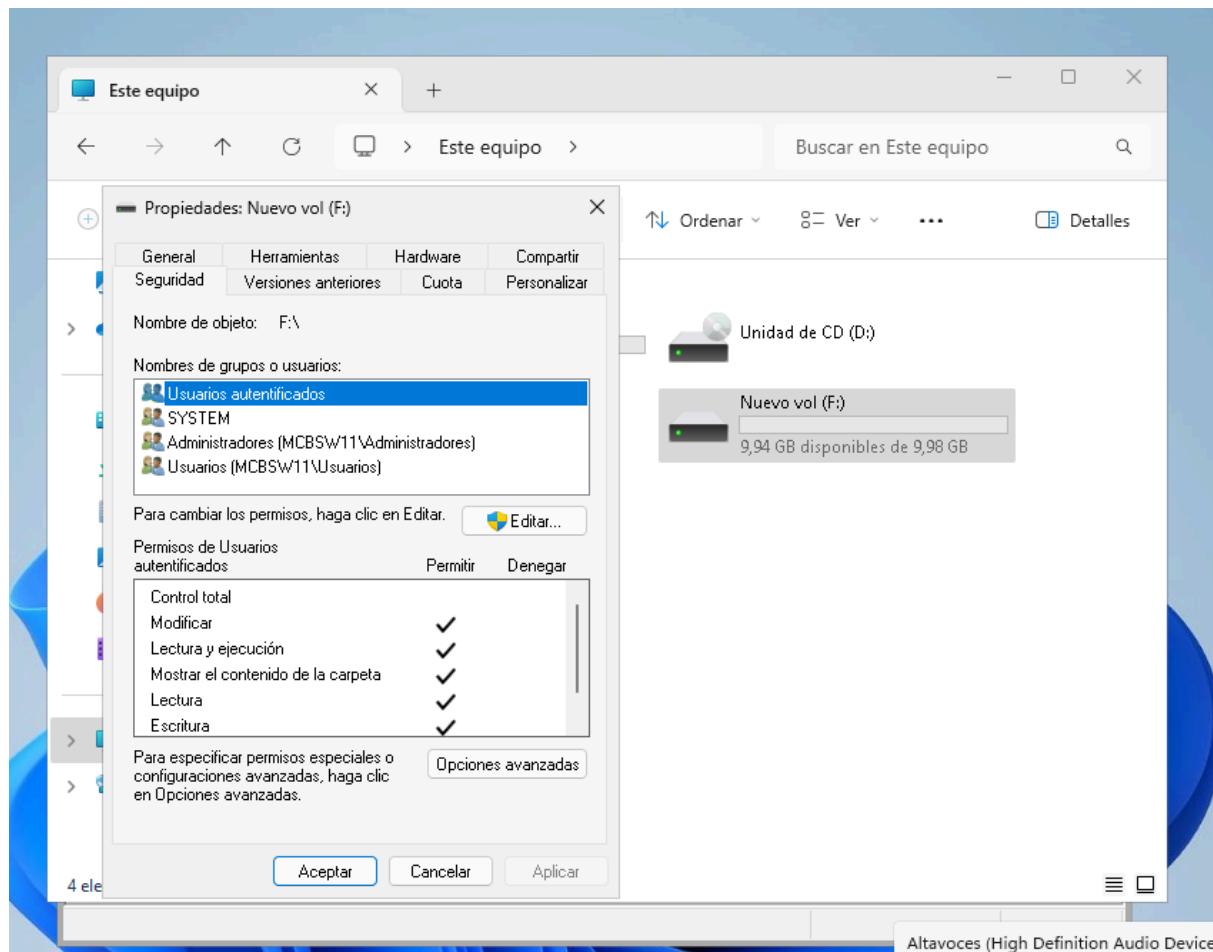


#### 1.4.2 - ¿Cómo ayuda a garantizar la seguridad de los datos?

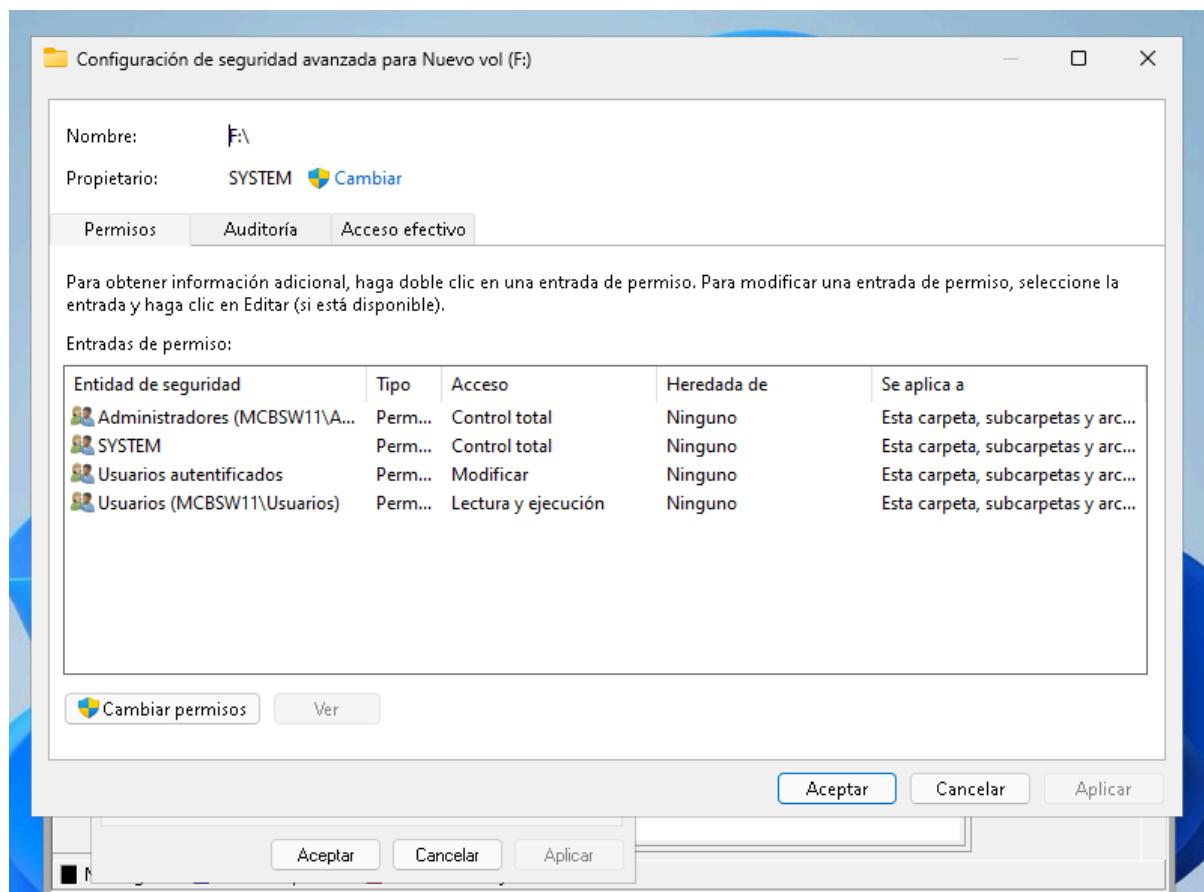
RAID-1 es un tipo de RAID donde se duplica el contenido de un disco a otro. Es por ello que tendríamos redundancia completa de todos los archivos que tendríamos en un disco. Gracias a ello podemos garantizar la seguridad de los datos, puesto que en caso de estropearse un disco, tendríamos el otro completamente funcional y con todos los datos

#### 1.4.3 - ¿Revisa los permisos NTFS de este nuevo volumen?

Para visualizar los diferentes permisos NTFS de este nuevo disco reflejado vamos a ir al **explorador de archivos** y seleccionamos el disco F, accediendo a propiedades de dicho dispositivo y accediendo a la pestaña de seguridad, podremos ver lo que estamos buscando:



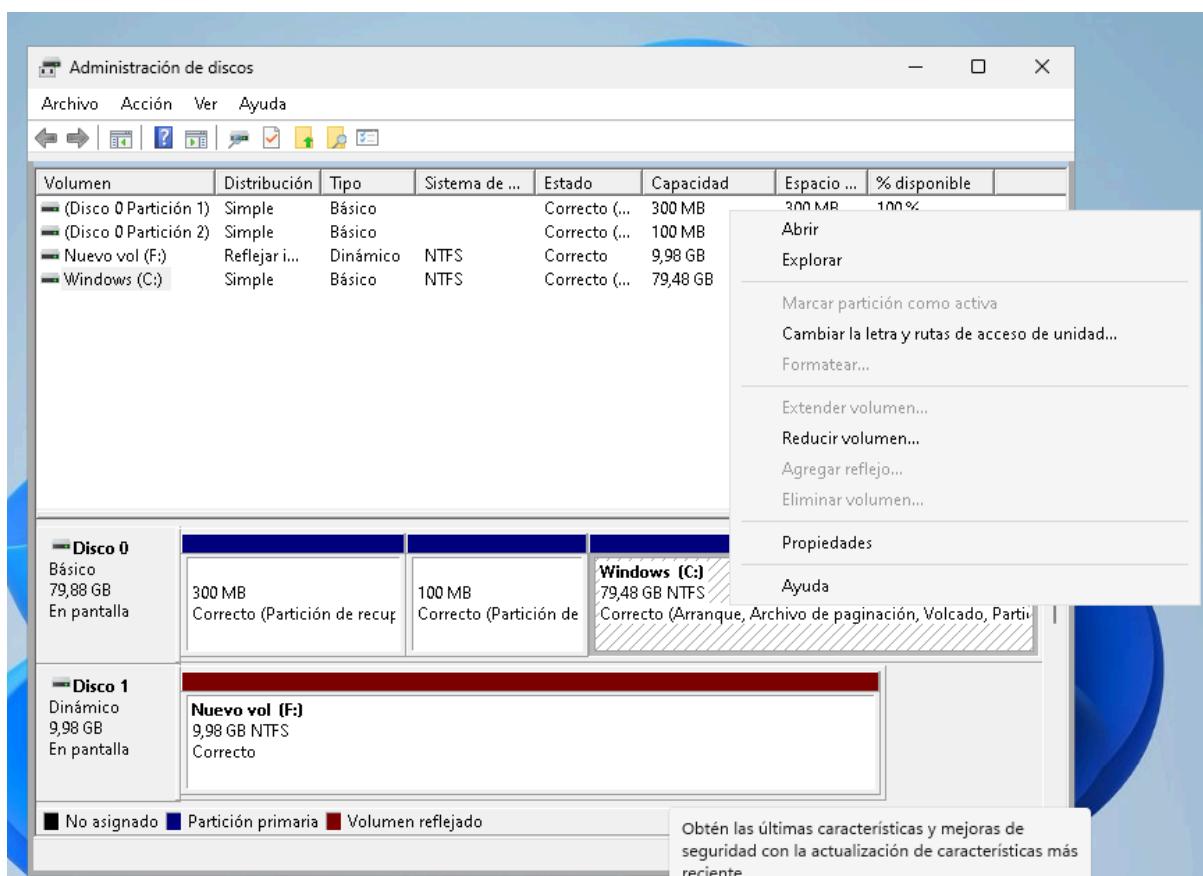
Podemos ver la opciones avanzadas



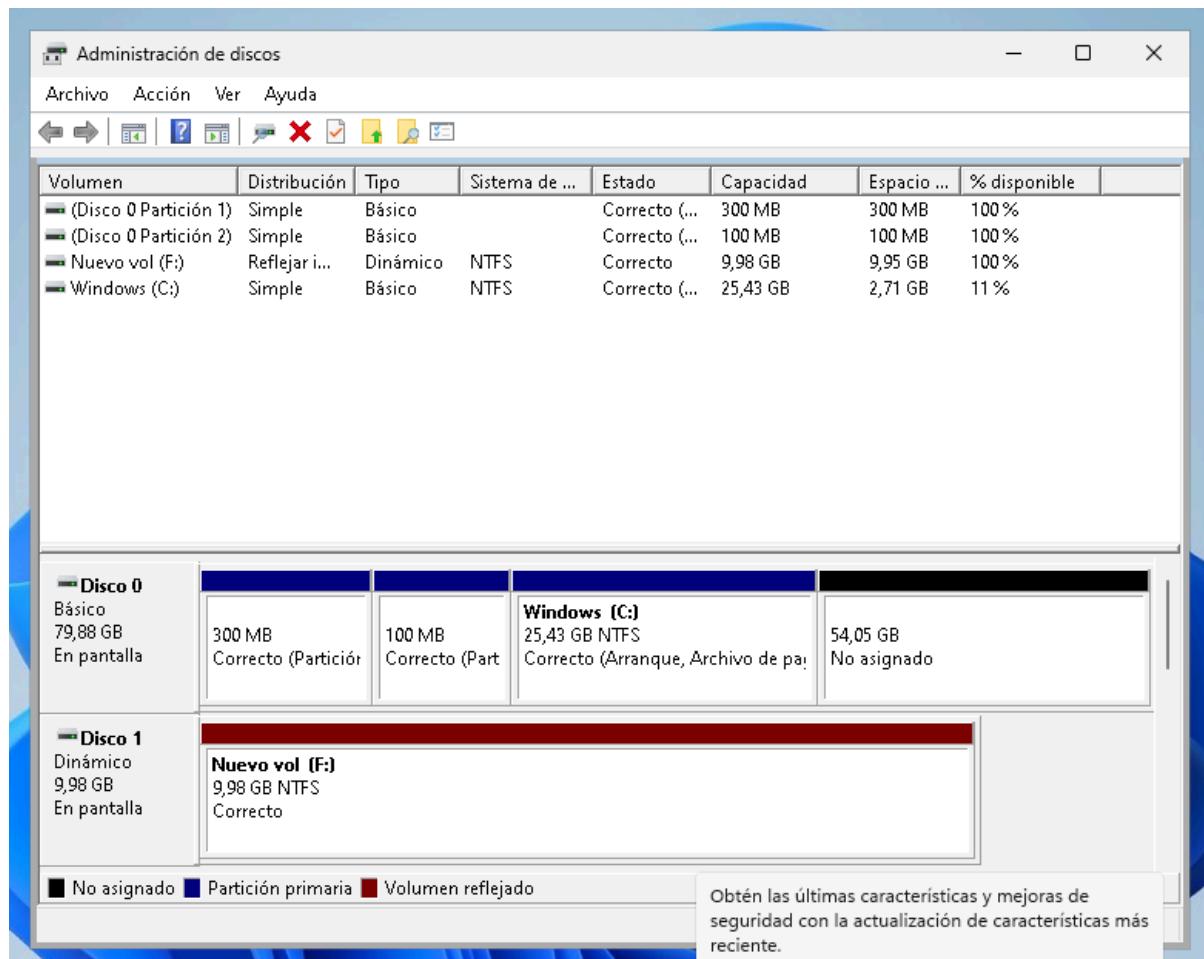
Sobre un RAID no se puede ampliar o modificar el espacio

## 1.5 - ¿Podemos extender o reducir el volumen de sistema que se encuentra como un disco básico? Si es posible indica el procedimiento.

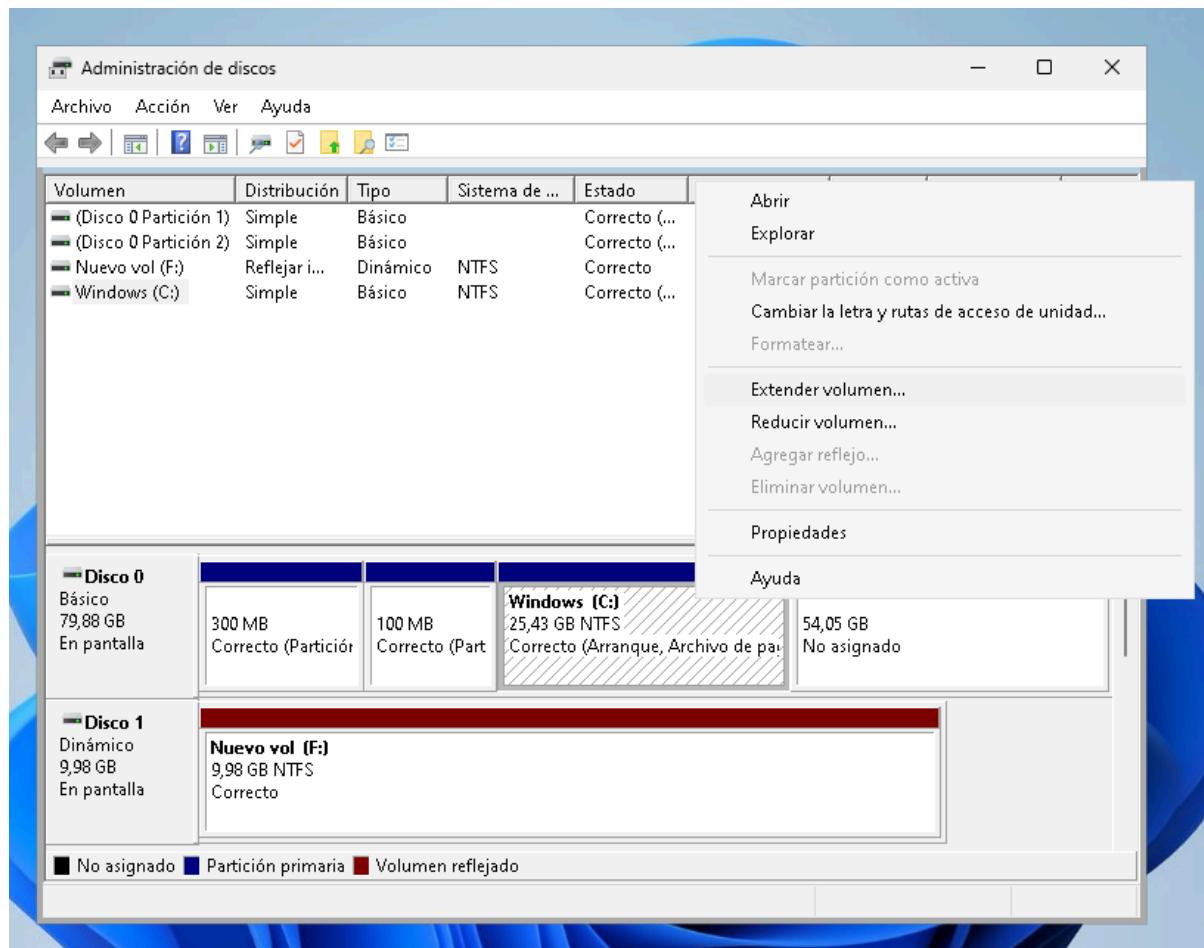
Se podría reducir el volumen del sistema de la siguiente forma: Administrador de Discos > doble click en el disco deseado > “Reducir tamaño”



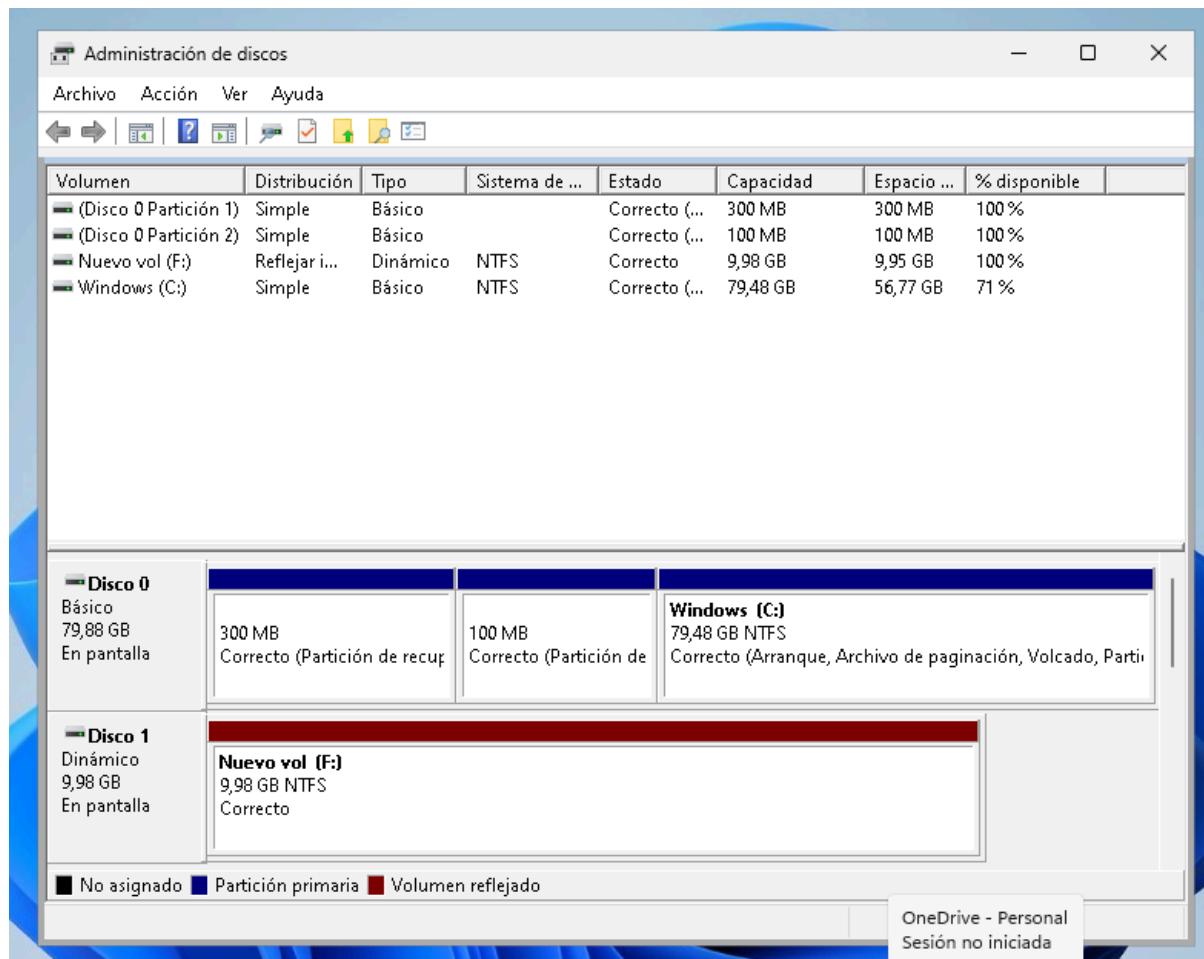
Así quedaría tras aplicar la reducción



Y se podría extender el tamaño del disco haciendo el procedimiento inverso

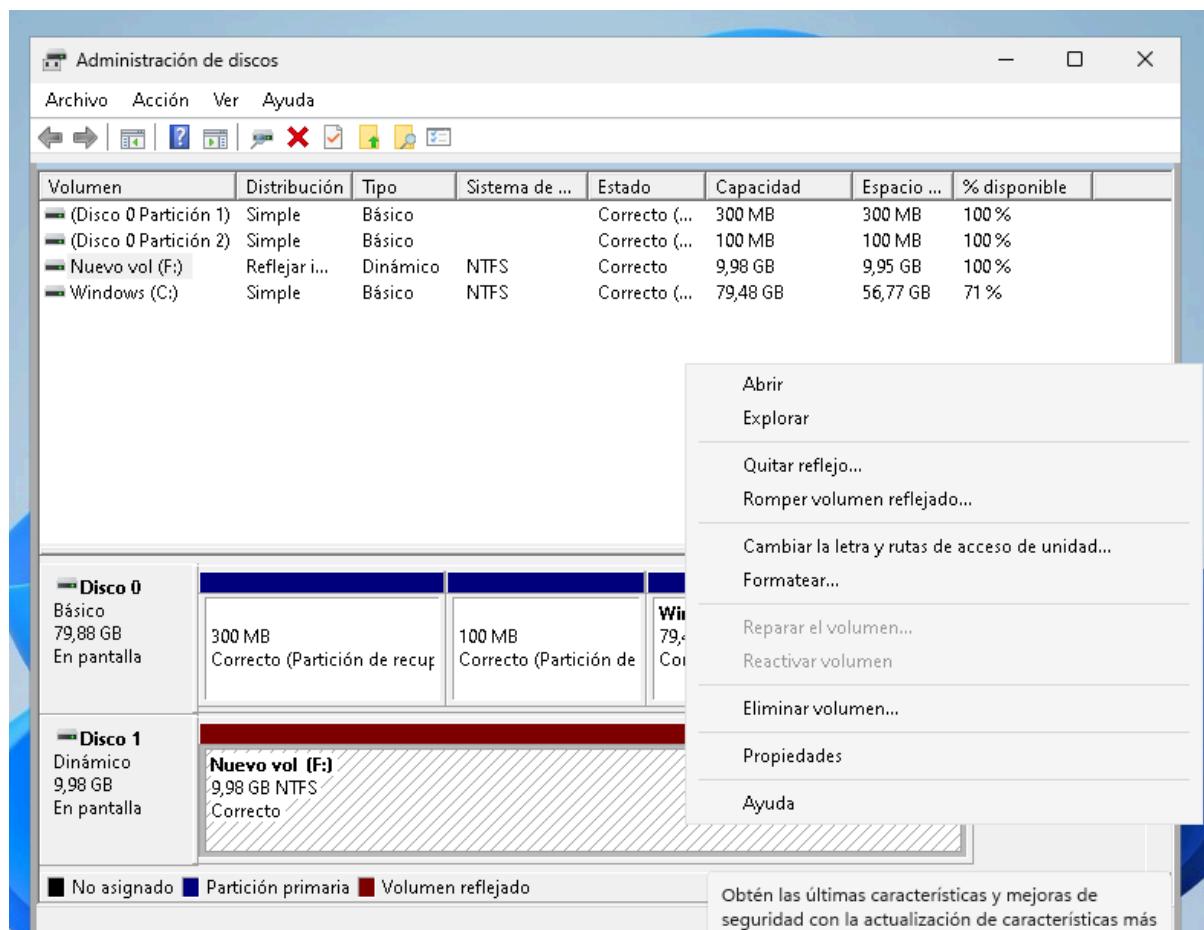


Y quedaría como al principio:



## 1.6 - ¿Podemos extender o reducir el volumen nuevo que hemos creado sobre el RAID 1? Si es posible indica el procedimiento.

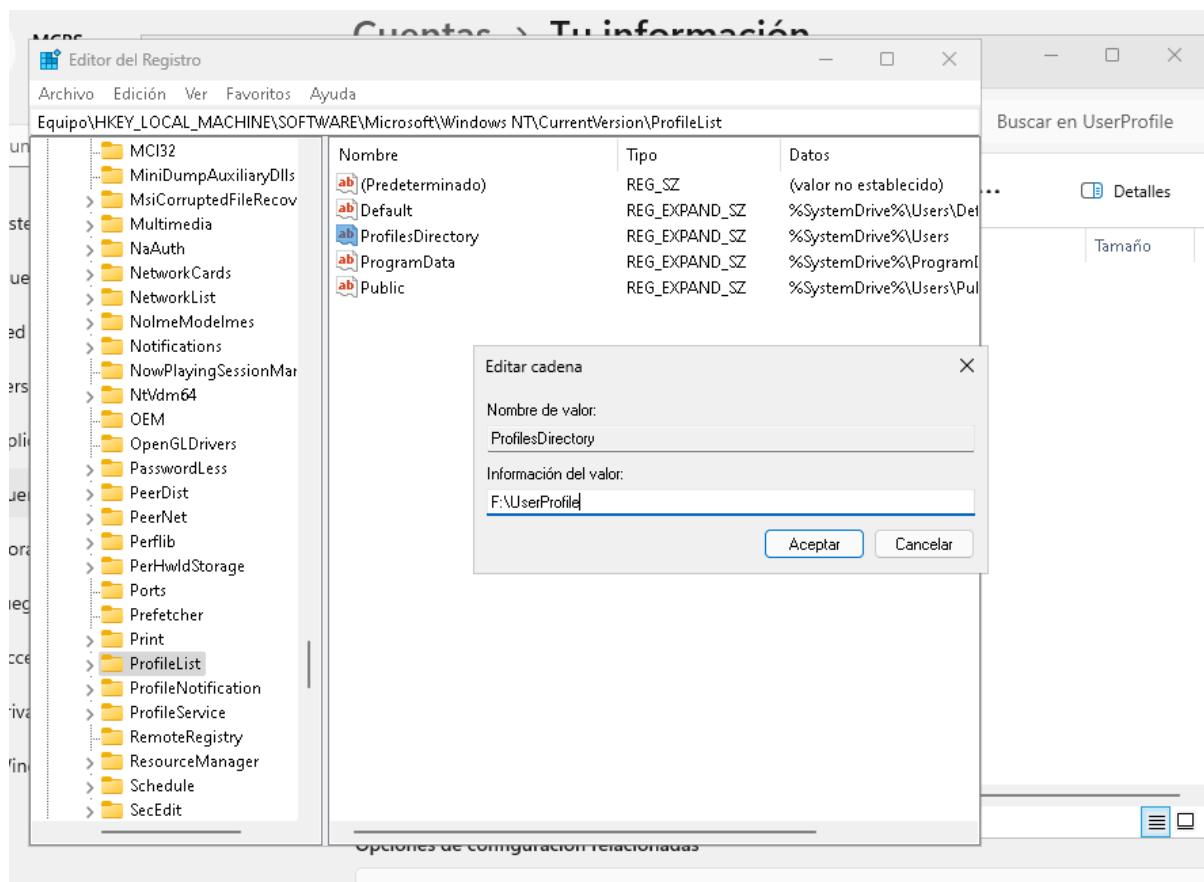
Al estar ante RAID-1 no se puede ni ampliar ni reducir el tamaño del reflejado.



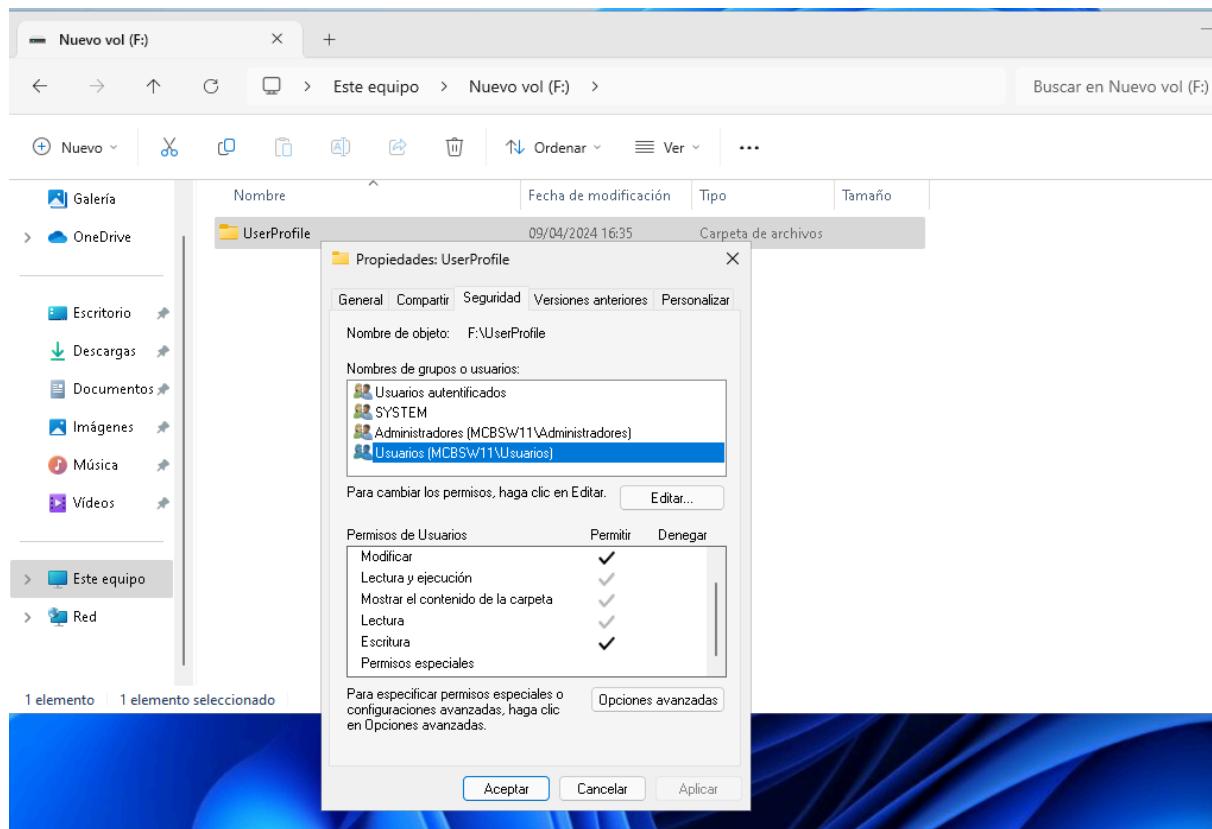
## 2 - Una vez disponemos de la nueva unidad de disco realizaremos las siguientes tareas:

2.1 - Configurar el sistema para que todo usuario nuevo disponga de su carpeta de perfil en el nuevo Disco.  
¿Qué pasos son necesarios realizar para conseguir este objetivo?

Para realizar esto, tendremos que ir al **Editor del Registro** y tendremos que modificar el valor de ProfilesDirectory para que se guarde la información del usuario en el disco reflejado:



A mayores tendremos que añadir el permiso de escritura/modificar como se ve a continuación:

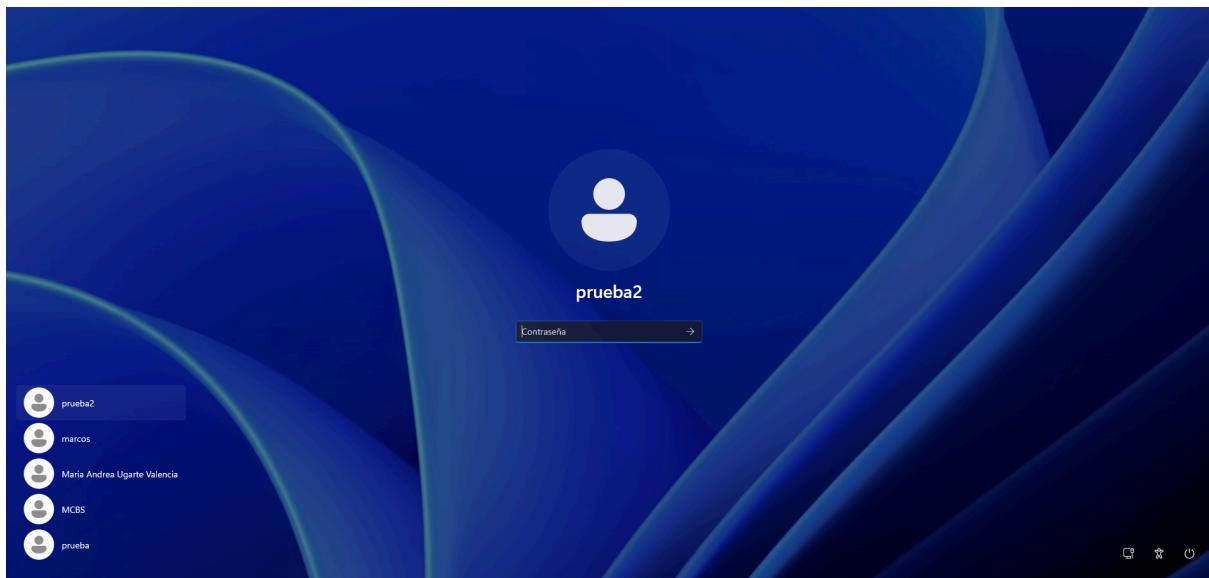


## 2.2 - Crea un nuevo usuario y comprueba que se genera de manera automática la carpeta del perfil.

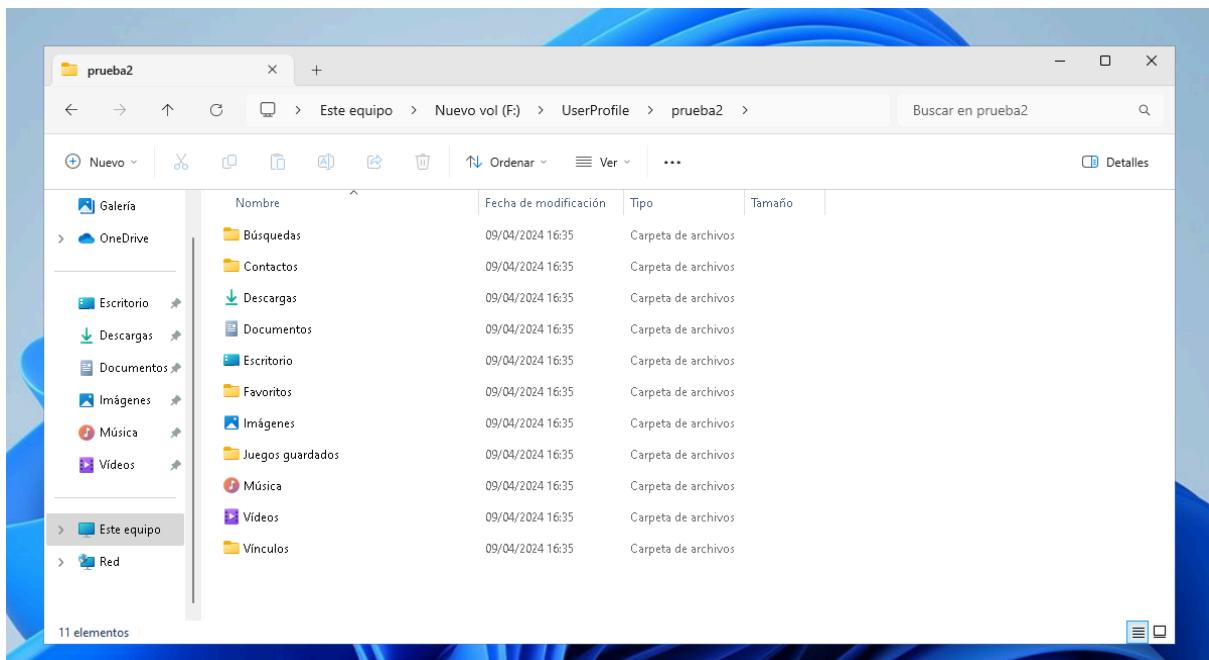
Vamos a crear un usuario **prueba**

```
net user /add prueba prueba
```

Ahora iniciamos sesión con dicho usuario e intentamos crear una carpeta y un archivo en el escritorio



Tras configurar todo, volvemos a iniciar sesión MCBS para ver que efectivamente se creó el directorio del usuario prueba en **F**



Podemos verificar que la carpeta se creó correctamente en el disco reflejado F

### **3 - Vamos a realizar la configuración de diferentes Directivas de Grupo en Windows 11**

#### 3.1 - ¿Qué dos tipos de directivas de grupo locales tenemos? ¿Cuál es la diferencia entre ellas?

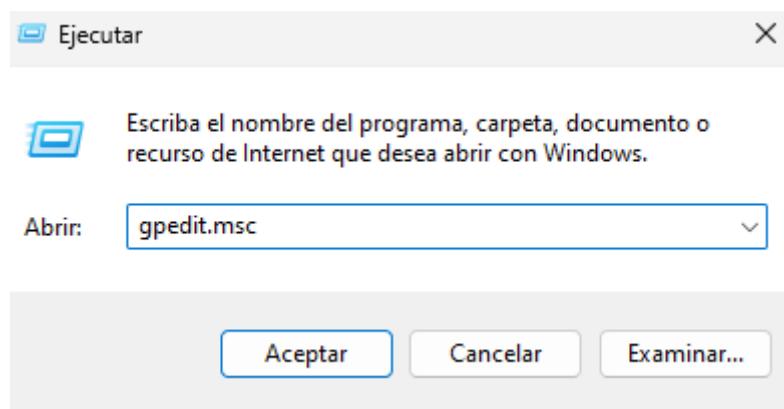
Los dos tipos de directivas de grupos locales de Windows 11 son:

- **Directivas de equipo.**
- **Directivas de usuario.**

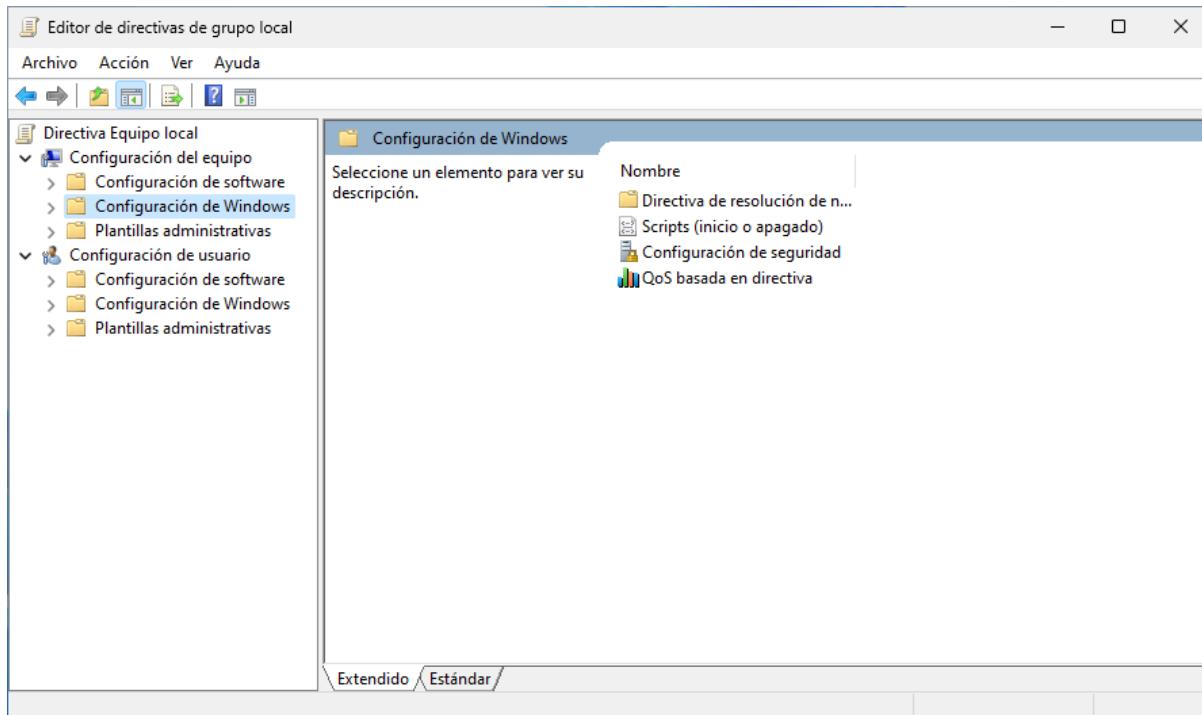
La diferencia entre ellas es que las directivas de equipo afectan a todos los usuarios en un equipo, mientras que las de usuario se aplican solo al usuario al que se asignan.

#### 3.2 - ¿Cómo accedemos a las directivas de grupo locales?

Para acceder a las directivas de grupo locales tenemos que abrir Ejecutar y escribir "gpedit.msc"



Y ya tendremos acceso a las directivas de grupo locales:

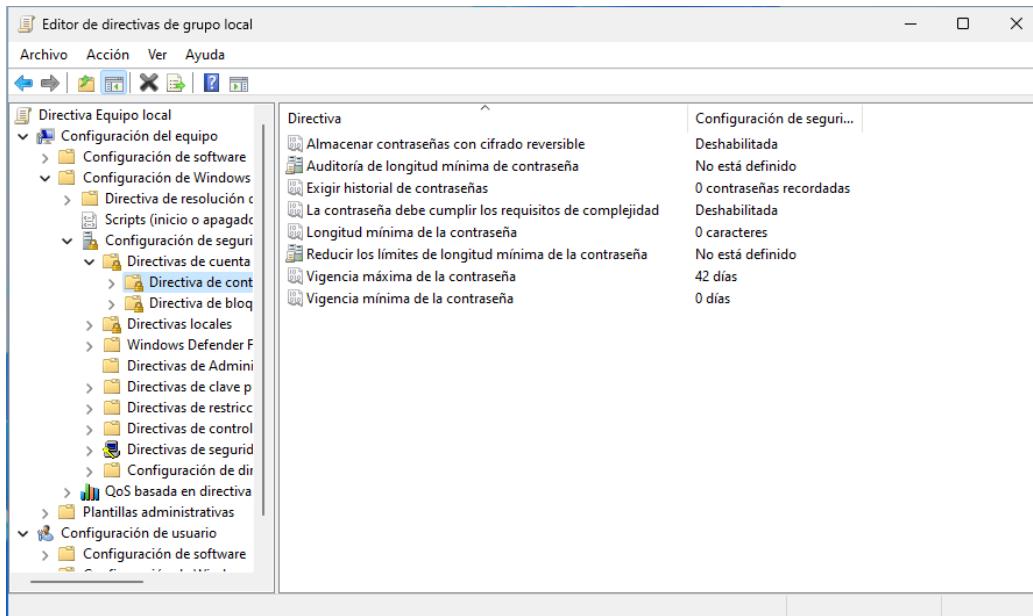


### 3.3 - Revisa las siguientes secciones de las directivas de grupo e identifica qué parámetros tenemos que cambiar en cada una de las secciones

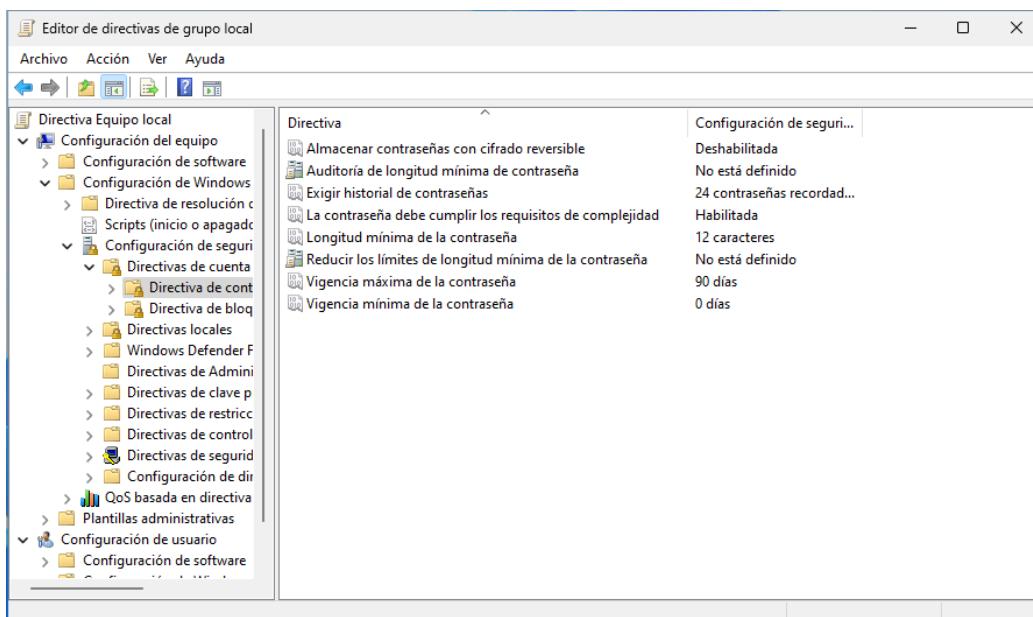
#### 3.3.1 - Configuración directivas de grupo local

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

Si vamos a la sección indicada vemos la siguiente configuración:



Basándonos en los apuntes de la asignatura y en nuestro propio criterio, una configuración adecuada sería:

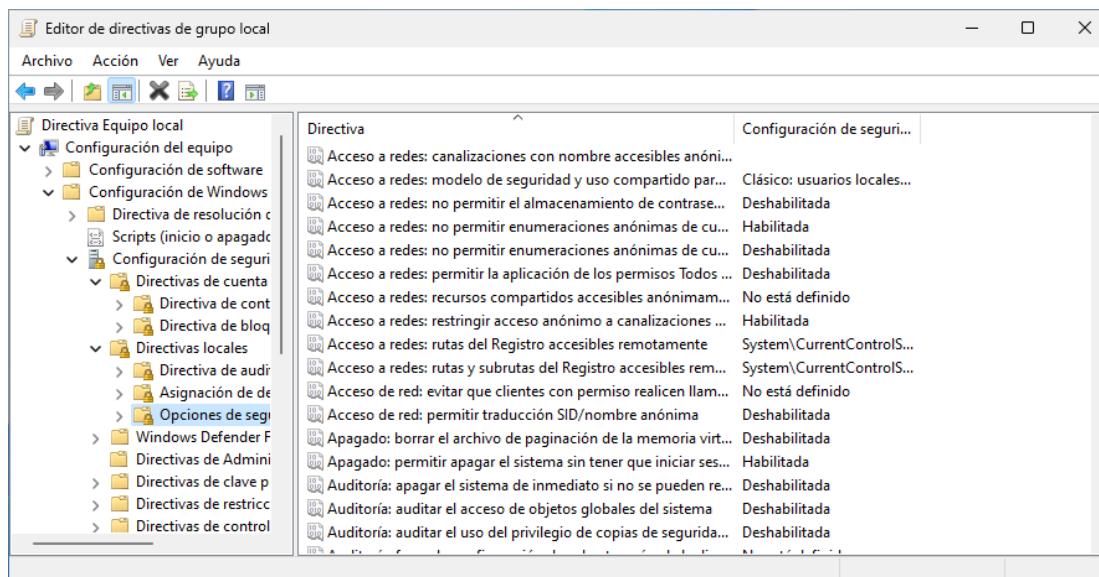


Hemos cambiado los siguientes parámetros:

- **Exigir historial de contraseñas:** Lo hemos cambiado a 24 contraseñas recordadas, para que los usuarios no usen contraseñas antiguas que puedan comprometer su seguridad.
- **La contraseña debe cumplir los requisitos de complejidad:** La hemos habilitado para que las contraseñas puedan resistir a ataques de fuerza bruta o de diccionario.

- **Longitud mínima de la contraseña:** Hemos establecido que la longitud mínima de la contraseña sea de 12 caracteres para dificultar el crackeo de la misma. Por lo tanto, una contraseña de este tipo contando que tenemos letras (mayúsculas y minúsculas), números y símbolos se tardaría 3 mil años
- **Vigencia máxima de la contraseña:** Aunque en los apuntes se indique una vigencia de 30 días, nos parece un tiempo corto para la comodidad del usuario, por lo que lo hemos subido a 90 días, o sea, 3 meses.
- Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de Seguridad

Vamos a la sección y tenemos acceso a la configuración:



En los apuntes se nos dan algunos consejos de configuración que nos parecen correctos como:

- **Seguridad de red: nivel de autenticación de Lan Manager:** Lo modificamos a “Enviar solo respuesta NTLMv2 y rechazar LM y NTLM”, para forzar la utilización de NTLMv2 y evitar las vulnerabilidades de NTLM y LM.
- **Seguridad de red: firmar digitalmente comunicaciones (siempre):** Lo habilitamos para configurar el cifrado TLS en conexiones contra IIS que hagan uso de autenticación NTLM.

Por nuestra parte, también hemos incluído:

- **Inicio de sesión interactivo: límite de inactividad del equipo:** Lo hemos establecido a 900 segundos (15 minutos). Consideramos que

es una buena medida de seguridad que se bloquee el dispositivo tras ese tiempo para evitar que terceros accedan a él en su ausencia.

- **Inicio de sesión interactivo: umbral de bloqueo de cuenta del equipo:** Lo hemos establecido a 5, ya que estaba deshabilitado y consideramos que es una buena medida de seguridad para prevenir ataques de fuerza bruta.
- **Miembro de dominio: duración máxima de contraseña de cuenta de equipo:** Lo hemos modificado de 30 días a 90 días, ya que nos parece lo suficientemente seguro y es una opción mejor para la comodidad del usuario.

# Memoria Laboratorios FORT

## Laboratorio 9: EJERCICIOS DE SECURIZACIÓN DE WINDOWS 11

Marcos Villar Avión

María Andrea Ugarte Valencia

**1 - El primer punto para garantizar es verificar el listado de Interfaces de Red que tenemos en el sistema**

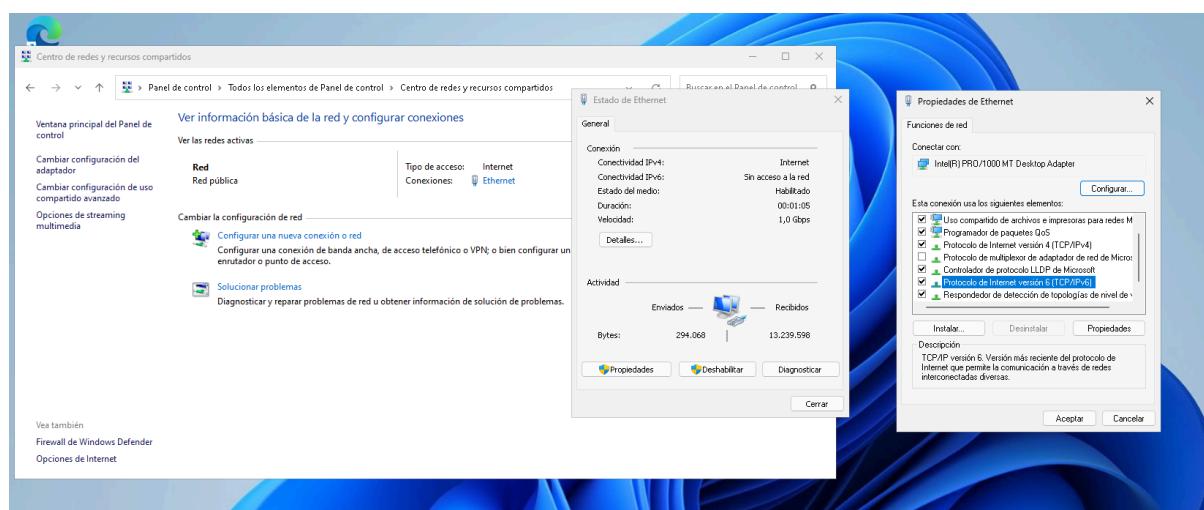
1.1 - Lista todos los interfaces de red que están disponibles en tu sistema

Ejecutando el comando ***ipconfig*** podemos ver todas las interfaces de red disponibles en nuestro sistema:

Se puede visualizar como solo tenemos una interfaz Ethernet

1.2 - Comprueba si tienes IPv6 concedida.

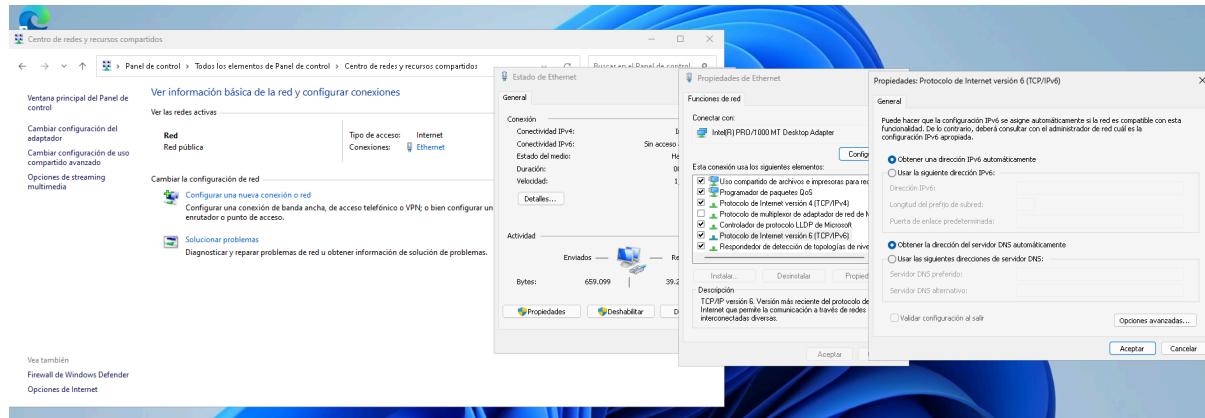
Para ello, iremos al Panel de Control > Centro de redes y recursos compartidos > Seleccionamos la única interfaz > Propiedades



Vemos como sí tenemos IPv6 activado

### 1.3 - ¿Qué tipo de dirección IPv6 es? ¿Cómo la obtienes?

Si hacemos click en las propiedades de la interfaz podemos ver que la dirección de IPv6 se adquiere automáticamente, es decir, mediante el uso de un servidor DHCP.



Vamos a ver ahora que tipo de dirección IPv6 tenemos. Si ejecutamos ahora el comando ***ipconfig /all*** podemos ver tanto nuestra dirección IPv6 como el servidor DHCP.

Como acaba en **fe80::** podemos intuir que se trata de una dirección Link-Local Addresses, es decir, las direcciones de enlace local pueden usarse cuando no hay

disponible un mecanismo externo de configuración de direcciones, tal como DHCP, u otro mecanismo principal de configuración ha fallado.

<b>fe80::/10</b>	<b>Link-Local Addresses</b> These addresses are used on a single link or a non-routed common access network, such as an Ethernet LAN. They do not need to be unique outside of that link.  Link-local addresses may appear as the source or destination of an IPv6 packet. Routers must not forward IPv6 packets if the source or destination contains a link-local address.  Link-local addresses may appear as the source or destination of an IPv6 packet. Routers must not forward IPv6 packets if the source or destination contains a link-local address.	169.254.0.0/16
Example: fe80::200:5aee:fea:20a2		

## 1.4 - Si haces ping al nombre de tu equipo, responde antes la pila IPv6 o la pila IPv4

Podemos verificar este comportamiento haciendo un ping a nuestro propio ordenador:

**ping localhost:**

```
C:\Users\MCBS>ping localhost

Haciendo ping a MCBSW11 [::1] con 32 bytes de datos:
Respuesta desde ::1: tiempo<1m
Respuesta desde ::1: tiempo<1m
Respuesta desde ::1: tiempo<1m

Estadísticas de ping para ::1:
    Paquetes: enviados = 3, recibidos = 3, perdidos = 0
                (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms
Control-C
^C
```

Se visualiza que responde **::1**, qué es la dirección de localhost en IPv6. Por lo tanto podemos concluir que Windows prefiere emplear IPv6 como primera opción.

## 1.5 - Se puede modificar el orden de resolución de IPv6 o IPv4

Para ello, vamos a ejecutar una cmd con línea de comandos y ejecutaremos los siguientes comandos:

***netsh interface ipv6 show prefixpolicies***

```
C:\Windows\System32>netsh interface ipv6 show prefixpolicies
Consultando el estado activo...

Precedencia Etiq. Prefijo
-----
 50      0  ::1/128
 40      1  ::/0
 35      4  ::ffff:0:0/96
 30      2  2002::/16
 5       5  2001::/32
 3       13  fc00::/7
 1       11  fec0::/10
 1       12  3ffe::/16
 1       3   ::/96
```

Vemos que la tercera línea es la dirección que hace el mapeado de IPv6 a IPv4 con lo cual vamos a cambiarle la prioridad:

***netsh interface ipv6 set prefixpolicy ::ffff:0:0/96 50 0***  
***netsh interface ipv6 set prefixpolicy ::1/128 40 1***  
***netsh interface ipv6 set prefixpolicy ::/0 30 2***

```
C:\Windows\System32>netsh interface ipv6 set prefixpolicy ::ffff:0:0/96 50 0
Aceptar

C:\Windows\System32>netsh interface ipv6 set prefixpolicy ::1/128 40 1
Aceptar

C:\Windows\System32>netsh interface ipv6 set prefixpolicy ::/0 30 2
Aceptar

C:\Windows\System32>netsh interface ipv6 show prefixpolicies
Consultando el estado activo...

Precedencia Etiq. Prefijo
----- -----
      50      0 ::ffff:0:0/96
      40      1 ::1/128
      30      2 2002::/16
      30      2 ::/0
       5      5 2001::/32
       3     13 fc00::/7
       1     11 fec0::/10
       1     12 3ffe::/16
       1      3 ::/96
```

Realizado este cambio, podemos realizar un ping a nuestro equipo

```
C:\Windows\System32>ping localhost

Haciendo ping a MCBSW11 [127.0.0.1] con 32 bytes de datos:
Respuesta desde 127.0.0.1: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 127.0.0.1:
  Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
  Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

Y vemos que nos responde IPv4.

Otra forma de hacerlo es mediante el registro:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters\
```

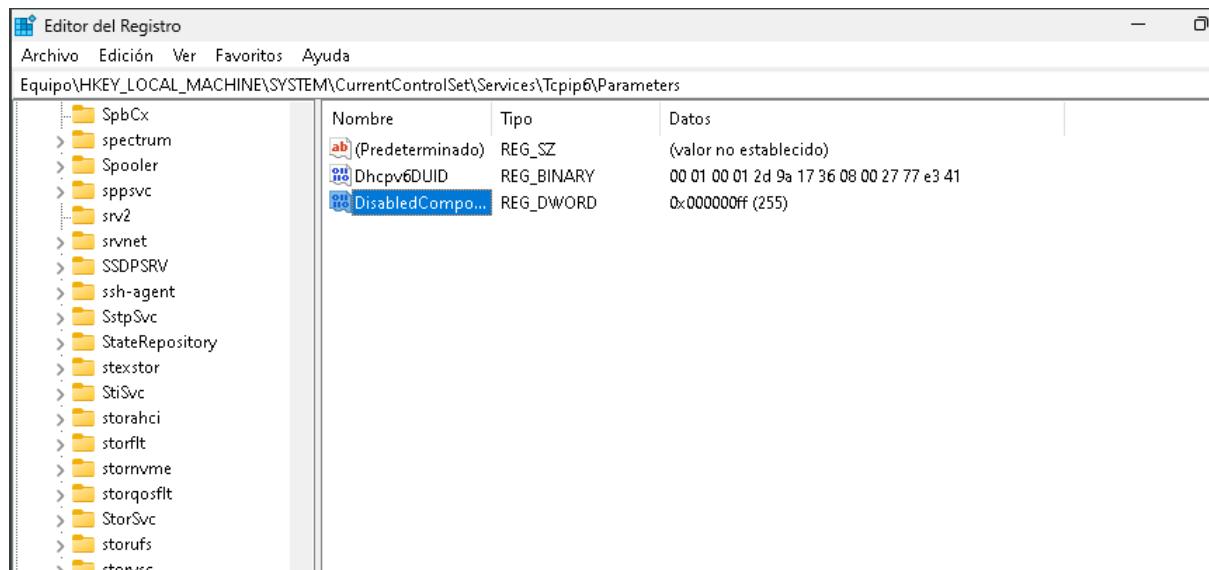
Crearemos un registro llamado DisabledComponents y le asignaremos 0x20 para priorizar IPv4 a IPv6.

## 1.6 - ¿Podemos eliminar la configuración de IPv6 de todas las interfaces?

Para eliminar IPv6 de todas las interfaces tendremos que ir Registro e iremos al siguiente:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters\
```

Crearemos un registro llamado DisabledComponents y le asignaremos 0xFF para deshabilitar IPv6 de todas las interfaces.



## 1.7 - ¿Es posible que al deshabilitar IPv6 se provoque una ralentización del arranque de Windows? ¿Si es así, cómo lo corregimos?

Leyendo la documentación de windows:

*Additionally, system startup will be delayed for five seconds if IPv6 is disabled by incorrectly, setting the DisabledComponents registry setting to a value of 0xffffffff. The correct value should be 0xff. For more information, see Internet Protocol Version 6 (IPv6) Overview.*

Por lo tanto, vamos podemos concluir que no tendremos dicha ralentización ya que nosotros le hemos indicado bien el valor de 0xFF y no 0xffffffff

## **2- Una vez hemos eliminado IPv6 de todas las interfaces:**

2.1 - ¿Qué tipo de perfiles tenemos en una interfaz de Microsoft Windows 11? ¿Qué diferencia tenemos entre ellos?

Podemos tener 3 tipos de perfiles:

- **Red Pública**
  - En este perfil, el equipo está más protegido, ya que se desactivan ciertas funciones de red compartida para protegerlo de amenazas externas.
- **Red Privada**
  - En este perfil, el equipo puede descubrir otros dispositivos en la red y permitir la compartición de archivos e impresoras.
- **Red de Dominio**
  - Este perfil se utiliza en redes corporativas que están conectadas a un dominio de Active Directory.

## 2.2 - ¿Qué perfil es el recomendable para un equipo personal como el que estamos configurando?

El perfil recomendado dependerá de la red a la que estemos conectados. Es decir, si vamos a un aeropuerto o a una cafetería tendremos que ponerlo a red pública para estar más protegidos pero si estamos en nuestra casa podemos configurarlo como red privada.

De todas formas, cuanto más protegidos mejor con lo cual, si tuviéramos que escoger solamente uno, pondremos todas las redes públicas y así siempre estaremos lo máximo protegido posible.

## 2.3 - ¿La configuración del perfil afecta en algo a la seguridad?

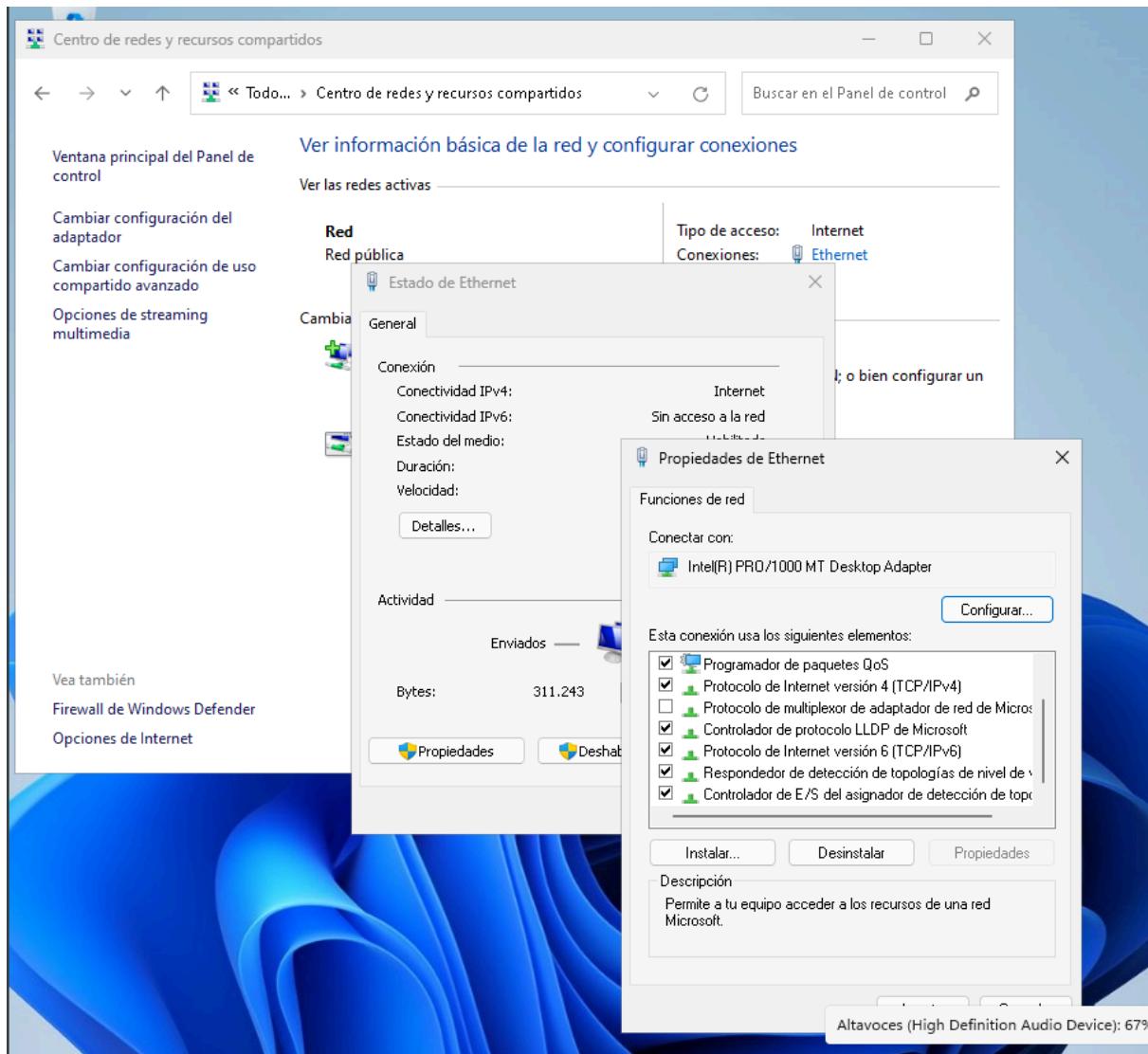
Como se ha indicado anteriormente, dependiendo del perfil se aplican unas medidas de seguridad u otras. Por ejemplo, en redes públicas se configura un nivel de seguridad superior a las redes privadas puesto que se interpreta que en esta última tú tienes más control y confianza.

Es por ello que en redes públicas las funcionalidades de recursos compartidos están deshabilitadas. Mientras que en redes de dominio, es el administrador de la red quien restringe las funcionalidades .

## 2.4 - ¿Qué componentes tiene instalado cada interfaz?

### ¿Es necesario tener instalado todos los componentes en el interfaz? ¿Cuáles podemos eliminar?

Para ver los componentes de una interfaz podemos encontrarlos en: Panel de Control > Centro de redes y recursos compartidos > Seleccionamos la única interfaz > Propiedades



Podemos ver los diferentes elementos que tiene dicha interfaz

- Cliente para redes Microsoft
- Uso compartido de archivos e impresoras para redes Microsoft
- Programador de paquetes QoS
- Protocolo de Internet versión 4 (TCP/IPv4)
- Protocolo de multiplexor de adaptador de red de Microsoft
- Controlador de protocolo LLDP de Microsoft

- Controlador de multiplexor de adaptador de red de Microsoft
- Controlador de protocolo LLDP de Microsoft
- Protocolo de Internet versión 6 (TCP/IPv6)
- Respondedor de detección de topologías de nivel de red
- Controlador de E/S del asignador de detección de topologías de red

En principio, no sería necesario tener todos los componentes instalados

Podriamos eliminar:

- Uso compartido de archivos e impresoras
- Protocolo de multiplexor..
- Protocolo de Internet versión 6
- Controlador de protocolo LLDP

## 2.5 - ¿Hasta qué nivel de la capa OSI nos protege el Firewall de Windows?

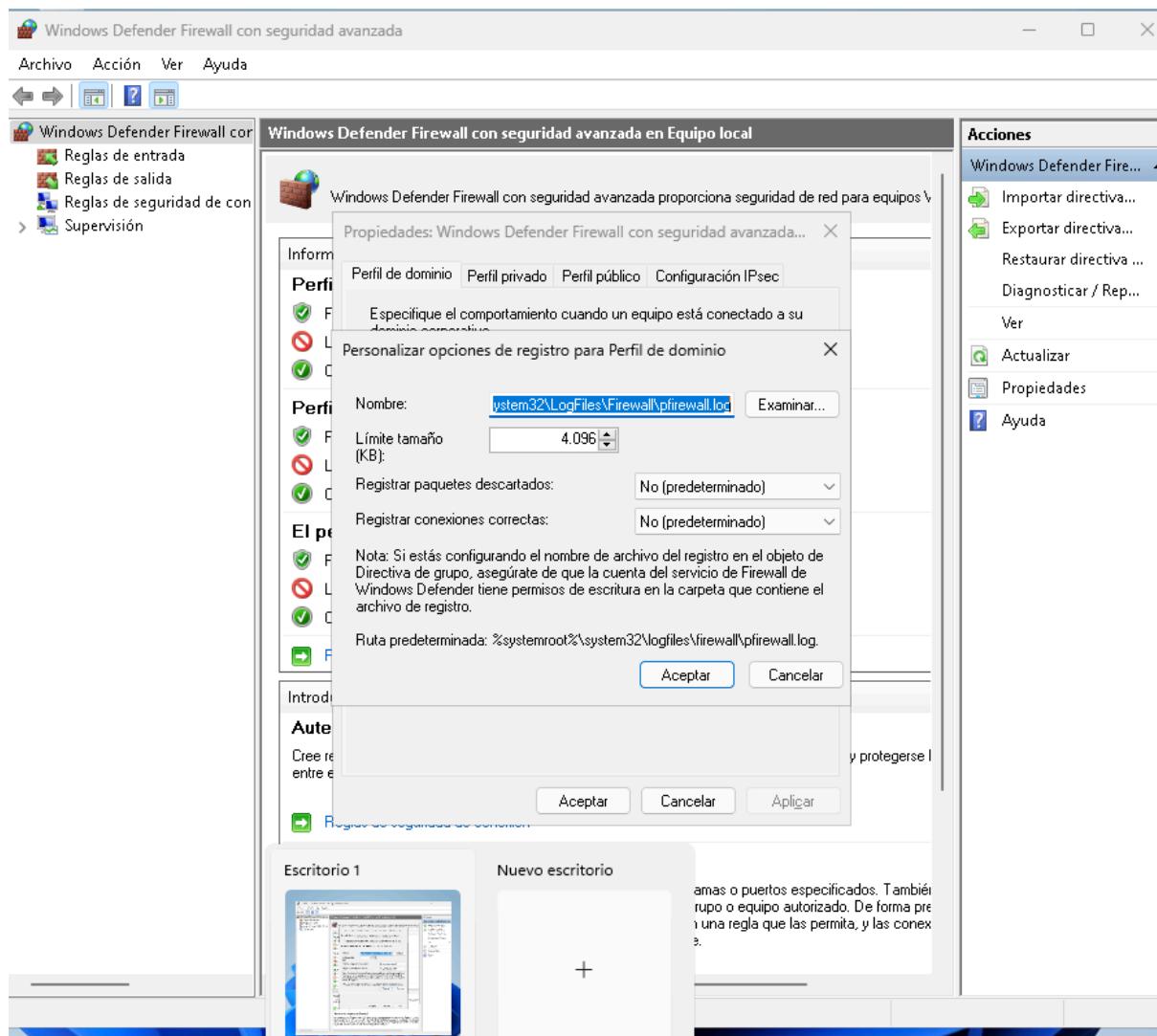
Esta cuestión fue respondida en clase. Se determinó que el Firewall trabaja a nivel 4, es decir, a capa de transporte porque no es capaz de ver el protocolo de aplicación.

## 2.6 - ¿ El Firewall nos permite gestionar tráfico de entrada y tráfico de salida? ¿Cuál es la configuración más restrictiva que podemos aplicar para la configuración actual?

Si, dicho firewall de windows filtra el tráfico entrante y saliente. La configuración más restrictiva que podemos aplicar sería denegar todo menos aquellas aplicaciones específicas que permitamos. Es decir, hacer una whitelist de aplicaciones permitidas.

## 2.7 - ¿Existe un sistema de log´s? ¿En qué carpetas se encuentran, como podemos hacer un debug de las reglas que aplicamos?

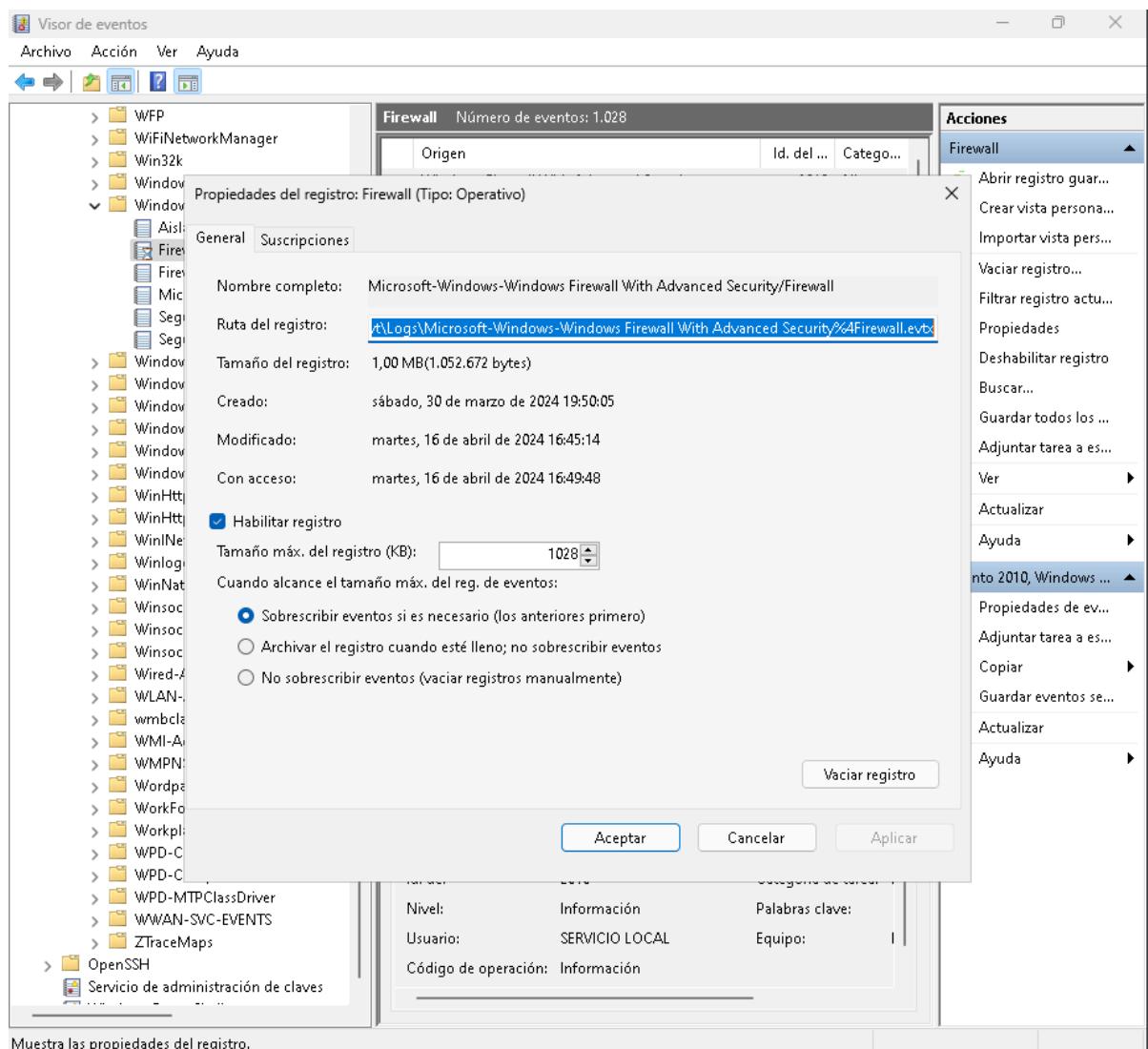
Para ver donde esta el log:



%systemroot%\system32\LogFiles\Firewall\pfirewall.log

Para hacer el debug:

Registros de aplicaciones y servicios -> Microsoft -> Windows -> Windows Firewall With Advanced Security



También lo podríamos hacer con:

Windows Defender Firewall con seguridad avanzada

Archivo Acción Ver Ayuda

Reglas de entrada  
Reglas de salida  
Reglas de seguridad de conexión  
Supervisión

Reglas de salida					Acciones
Nombre	Grupo	Perfil	Habilitado		
@[Microsoft.XboxGamingOverlay_2.622...]	@{Microsoft.XboxGamingOverlay_2.622...}	Todo	Sí		
Spotify Music	{78E1CD88-49E3-476E-B926-...}	Todo	Sí		
Spotify Music	{78E1CD88-49E3-476E-B926-...}	Todo	Sí		
Cliente de sincronización de administración...	Administración de dispositivos...	Todo	Sí		
Instalador del certificado de administración...	Administración de dispositivos...	Todo	Sí		
Servicio de inscripción de administración...	Administración de dispositivos...	Todo	Sí		
Servicio de inscripción de dispositivos de...	Administración de dispositivos...	Todo	Sí		
Administración de tarjetas inteligentes vi...	Administración de tarjetas i...	Privado	No		
Administración de tarjetas inteligentes vi...	Administración de tarjetas i...	Domiciliario	No		
Agregar una cuenta profesional o educativa...	Agregar una cuenta profesiona...	Todo	Sí		
Agregar una cuenta profesional o educativa...	Agregar una cuenta profesiona...	Todo	Sí		
Agregar una cuenta profesional o educativa...	Agregar una cuenta profesiona...	Todo	Sí		
Asistencia remota (PNRP de salida)	Asistencia remota	Público	No		
Asistencia remota (PNRP de salida)	Asistencia remota	Domiciliario	Sí		
Asistencia remota (SSDP-TCP de salida)	Asistencia remota	Domiciliario	Sí		
Asistencia remota (SSDP-UDP de salida)	Asistencia remota	Domiciliario	Sí		
Asistencia remota (TCP de salida)	Asistencia remota	Domiciliario	Sí		
Asistencia remota (TCP de salida)	Asistencia remota	Público	No		
Asistencia remota (TCP de servidor de RA...)	Asistencia remota	Domiciliario	Sí		
Cliente de caché hospedada de BranchCache...	BranchCache: cliente de cac...	Todo	No		
Detección del mismo nivel de BranchCache...	BranchCache: detección del...	Todo	No		
Recuperación de contenido de BranchCache...	BranchCache: recuperación ...	Todo	No		
Servidor de caché hospedada de BranchCac...	BranchCache: servidor de ca...	Todo	No		
Calculadora de Windows	Calculadora de Windows	Todo	Sí		
Cámara de Windows	Cámara de Windows	Todo	Sí		
Características de la familia de Microsoft	Características de la familia ...	Todo	Sí		
Centro de opiniones	Centro de opiniones	Todo	Sí		
Archivos e impresoras compartidos (netw...	Compartir archivos e impres...	Domiciliario	No		

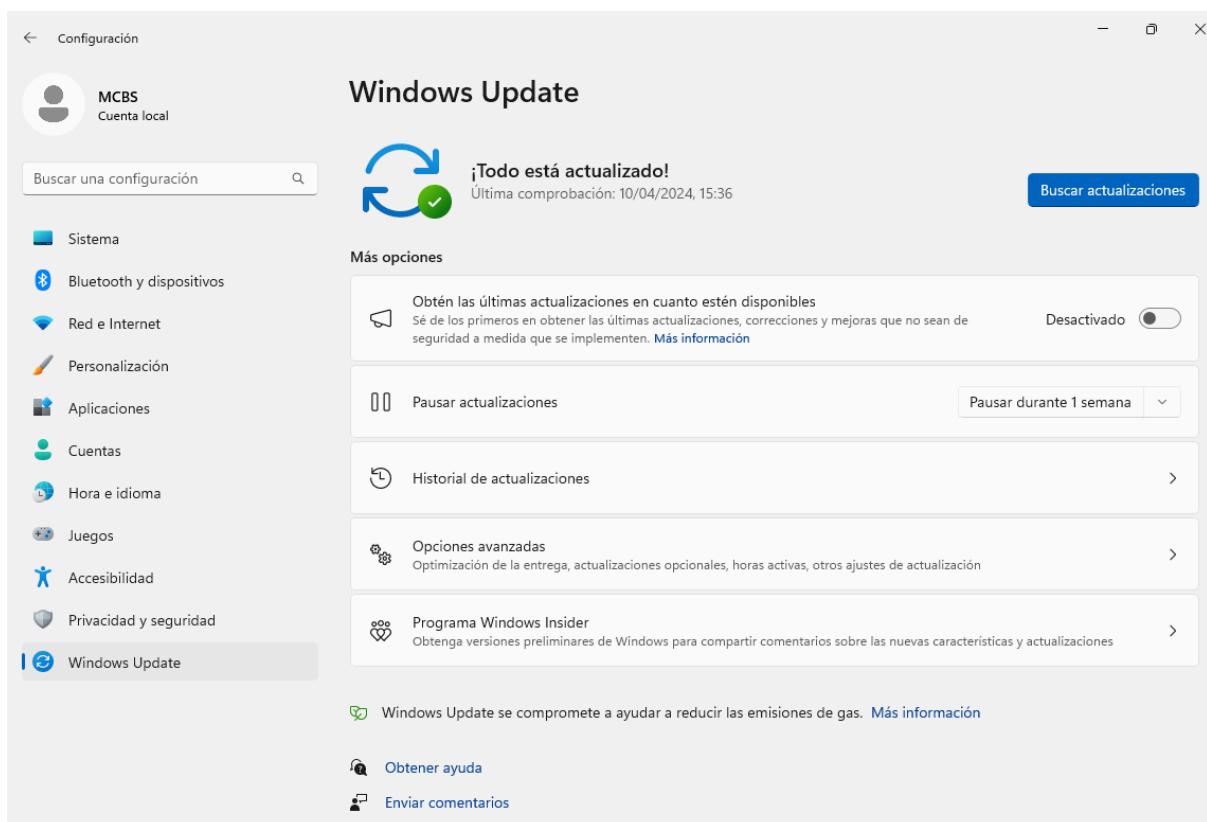
### 3 - Comenzaremos con el sistema de actualización de Microsoft.

3.1 - ¿Windows Update está activado por defecto?

¿Cómo podemos acceder a él y comprobar que está funcionando?

Sí, Windows Update está activado por defecto.

Si nos vamos a **Inicio > Configuración > Windows Update** podemos acceder a Windows Update y vemos como efectivamente está funcionando.



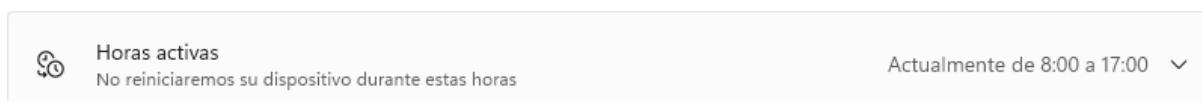
3.2 - ¿Explica brevemente el procedimiento por defecto para instalar las actualizaciones? ¿Podemos controlar cuando y quien instala las actualizaciones?

Windows Update descarga automáticamente las actualizaciones disponibles en segundo plano de forma periódica. Las actualizaciones se descargan en función de la configuración de Windows Update. Una vez completado, Windows verifica que las actualizaciones se hayan aplicado correctamente.

Podemos controlar cuando se controlan las actualizaciones. Windows Update nos permite pausar las actualizaciones:



Y en **Opciones avanzadas** nos permite asignar horas activas en las que no se reiniciará el dispositivo:



En entornos corporativos se puede controlar quién instala las actualizaciones con:

- **WSUS**, para la gestión de actualizaciones de sistemas cliente
- **SCE y SCCM**, para agrupar sistemas en gruposcolecciones para la gestión efectiva de actualizaciones.

### 3.3 - ¿Es posible instalar parches de seguridad de otro software que no sea el sistema operativo? Si es posible ¿esta opción está activada por defecto y que otro software nos actualizará?

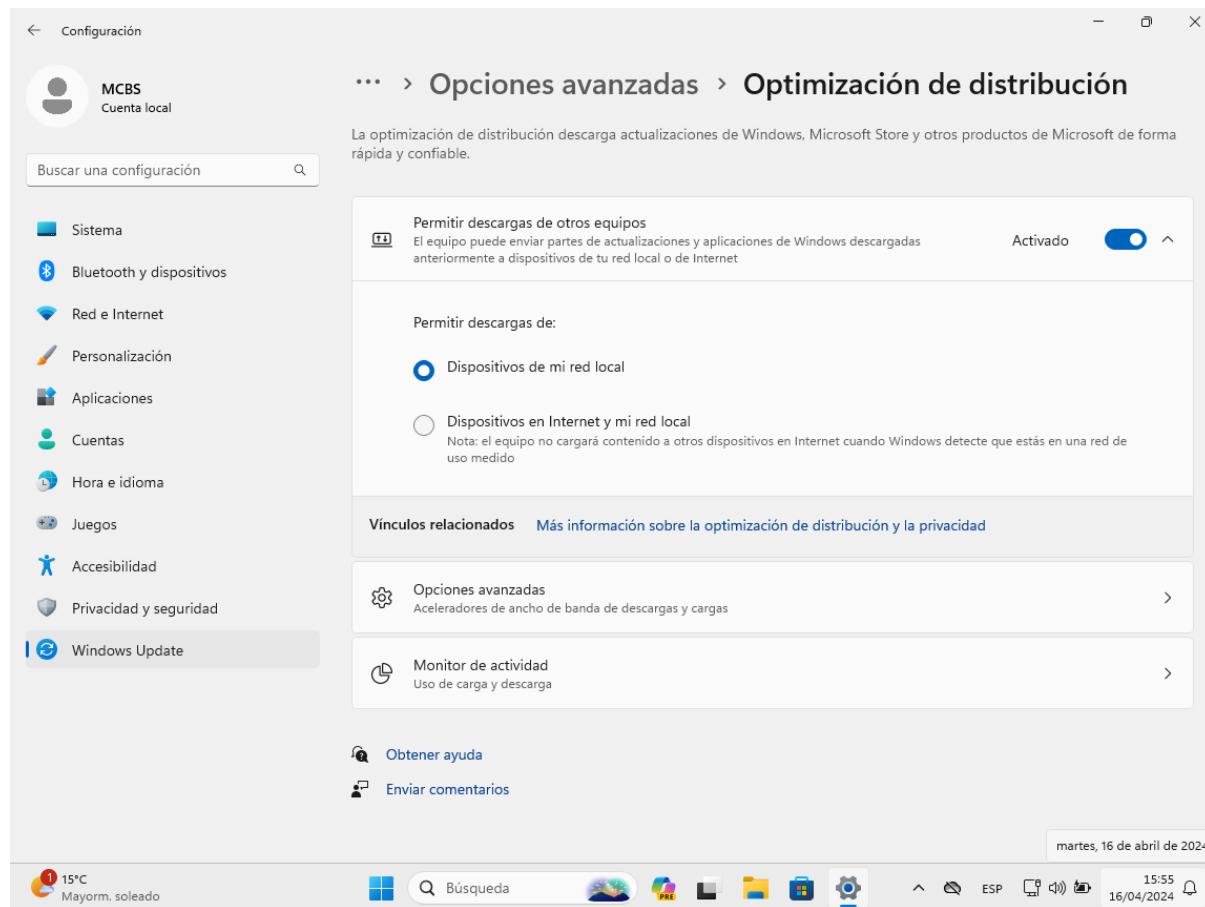
Sí que es posible instalar parches de seguridad de otro software que no sea el sistema operativo. Accedemos a esta opción en **Configuración > Windows Update > Opciones avanzadas** y nos vamos al apartado de **Recibir actualizaciones de otros productos de Microsoft**. No está activada por defecto.



3.4 - Windows Update dispone de la opción de descargar actualizaciones desde otros equipos, ¿en qué caso puede estar bien esta opción? ¿Qué opciones podemos configurar para controlar este tipo de actualización? ¿Al utilizar esta opción tenemos una mayor exposición a un posible fallo de seguridad?

Esa opción puede estar bien en situaciones donde no tenemos acceso físico al dispositivo, como en entornos empresariales con dispositivos distribuidos en diferentes ubicaciones geográficas.

Si vamos a **Inicio > Configuración > Windows Update > Opciones avanzadas > Optimización de distribución** podemos acceder a las opciones de configuración de esta función.



Vemos que podemos permitir las descargas de otros equipos de nuestra red local o de Internet, opciones avanzadas para gestionar el ancho de banda y tenemos un monitor de actividad.

Sí que tenemos mayor exposición a un posible fallo de seguridad al permitir que los dispositivos descarguen actualizaciones de otros dispositivos, ya que las actualizaciones podrían ser comprometidas si un dispositivo en la red está comprometido. Por lo tanto, la descarga de actualizaciones debe hacerse desde fuentes confiables en una red segura.

### 3.5 - ¿Podemos configurar a través de directivas de grupo el comportamiento de Windows Update?

En empresas, se puede usar directivas de grupo a través de la consola de administración de directiva de grupo (GPMC) para controlar el funcionamiento de Windows Update. Nosotros, al no estar en un entorno corporativo, no podemos.

### 3.6 - Hemos visto que determinado software de terceras empresas se actualiza con Windows Update, el resto de software que tenemos instalado como podemos inventariarlo y auditarlo. Investiga e infórmanos de alguna aplicación que nos permita auditar el software instalado y que nos permita la actualización de este.

Podemos inventariar y auditar el software instalado con aplicaciones como **PDQ Deploy & Inventory**, una herramienta que permite realizar inventarios y auditorías de software además de ayudar a los desarrolladores a implementar parches y actualizaciones de software simultáneamente en varios PC con Windows.

## **4 - Pasamos a configurar la UAC**

### **4.1 - ¿Qué es la UAC?**

La UAC (User Account Control) es un sistema de protección contra acciones potencialmente peligrosas.



### **4.2 - ¿Cómo ayuda la UAC a proteger al sistema? ¿Cómo ayuda la UAC a proteger al usuario?**

Para proteger al sistema, la UAC limita los privilegios administrativos en las cuentas de usuario estándar, controla los cambios en el sistema solicitando confirmación del usuario y protege áreas sensibles del sistema.

Para proteger al usuario, la UAC proporciona notificaciones sobre acciones sensibles, lo que aumenta la conciencia del usuario, y reduce el impacto de las vulnerabilidades de software al limitar los privilegios de ejecución de programas.

### **4.3 - ¿Qué niveles de protección dispone la UAC? ¿Sería recomendable modificar el nivel por defecto para incrementar la seguridad? ¿Cuáles serían las ventajas?**

La UAC dispone de 4 niveles de protección:

- Notificarme siempre.

- Notificarme solamente cuando una aplicación intente realizar cambios en el equipo.
- Notificarme solo cuando una aplicación intente realizar cambios en el equipo (no atenuar el escritorio).
- No notificarme nunca.

Aumentar el nivel de protección por defecto de la UAC puede ser recomendable en entornos donde la seguridad es una prioridad absoluta, como entornos corporativos. Al aumentar el nivel de protección, se requiere la confirmación del usuario para más acciones, lo que aporta ventajas como ayudar a prevenir cambios no autorizados en el sistema y a mitigar el riesgo de ataques maliciosos. Sin embargo, puede ser intrusivo para el usuario y empeorar su experiencia.

#### 4.4 - ¿Es posible customizar la seguridad de la UAC de una manera más precisa? Realiza una propuesta.

Sí, podemos aumentar la seguridad de la UAC de una manera más precisa en **Directiva de seguridad local > Directivas locales > Opciones de Seguridad > Control de Cuentas de Usuario**.

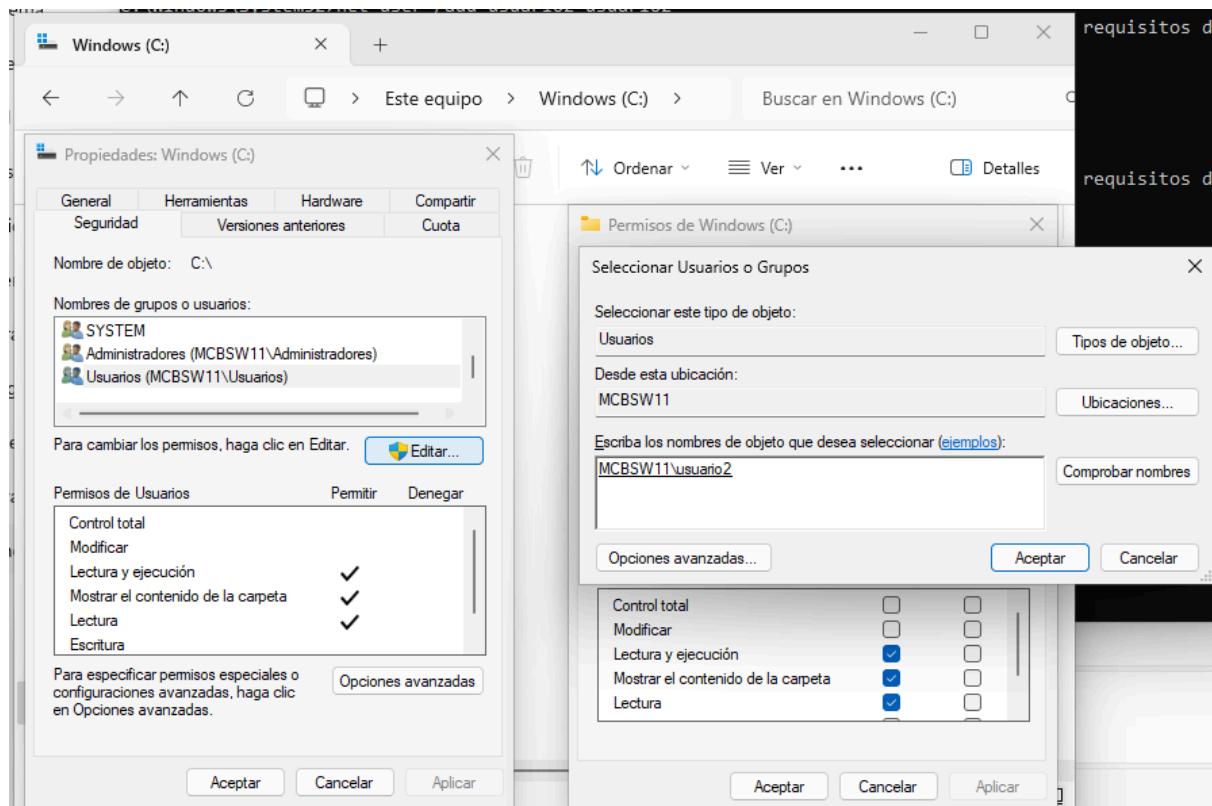
Directiva	Configuración de seguridad...
Auditoría: forzar la configuración de subcategorías de la dire...	No está definido
Cliente de redes de Microsoft: enviar contraseña sin cifrar a ...	Deshabilitada
Cliente de redes de Microsoft: firmar digitalmente las comu...	Habilitada
Cliente de redes de Microsoft: firmar digitalmente las comu...	Deshabilitada
Configuración del sistema: subsistemas opcionales	
Configuración del sistema: usar reglas de certificado en ejec...	Deshabilitada
Consola de recuperación: permitir el inicio de sesión admini...	Deshabilitada
Consola de recuperación: permitir la copia de discos y el ...	Deshabilitada
Control de cuentas de usuario: cambiar al escritorio seguro ...	Habilitada
Control de cuentas de usuario: comportamiento de la petici...	Pedir consentimiento pa...
Control de cuentas de usuario: comportamiento de la petici...	Pedir credenciales
Control de cuentas de usuario: detectar instalaciones de apli...	Habilitada
Control de cuentas de usuario: ejecutar todos los administra...	Habilitada
Control de cuentas de usuario: elevar solo aplicaciones UIAc...	Habilitada
Control de cuentas de usuario: elevar solo los archivos ejec...	Deshabilitada
Control de cuentas de usuario: Modo de aprobación de ad...	No está definido
Control de cuentas de usuario: permitir que las aplicaciones ...	Deshabilitada
Control de cuentas de usuario: virtualizar los errores de escri...	Habilitada
Controlador de dominio: no permitir los cambios de contras...	No está definido
Controlador de dominio: permitir a los operadores de servid...	No está definido
Controlador de dominio: permitir que se vuelva a usar la cu...	No está definido
Controlador de dominio: requisitos de firma de servidor LDAP	No está definido
Controlador de dominio: requisitos del token de enlace de c...	No está definido

Nuestra propuesta para customizarlo de una manera más precisa es:

- **Modo de aprobación de administrador para la cuenta predefinida administrador:** lo habilitamos para un mayor control sobre las acciones administrativas y una mayor protección contra ataques.

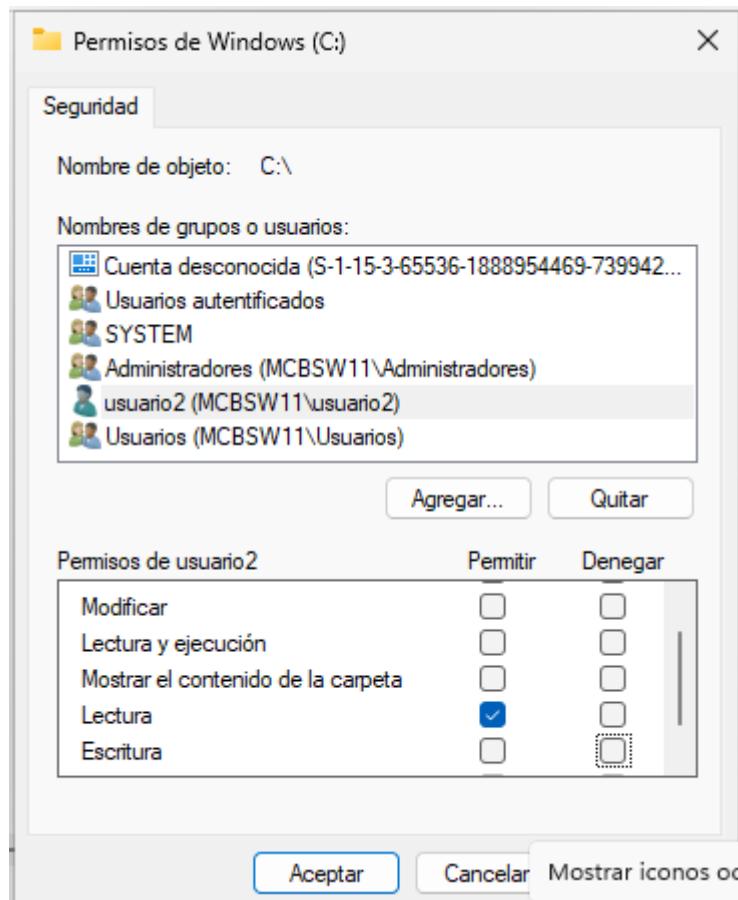
El resto de opciones consideramos que están bien como están y que habilitar más cosas, como elevar sólo los archivos ejecutables firmados y validados, empeoraría la experiencia del usuario.

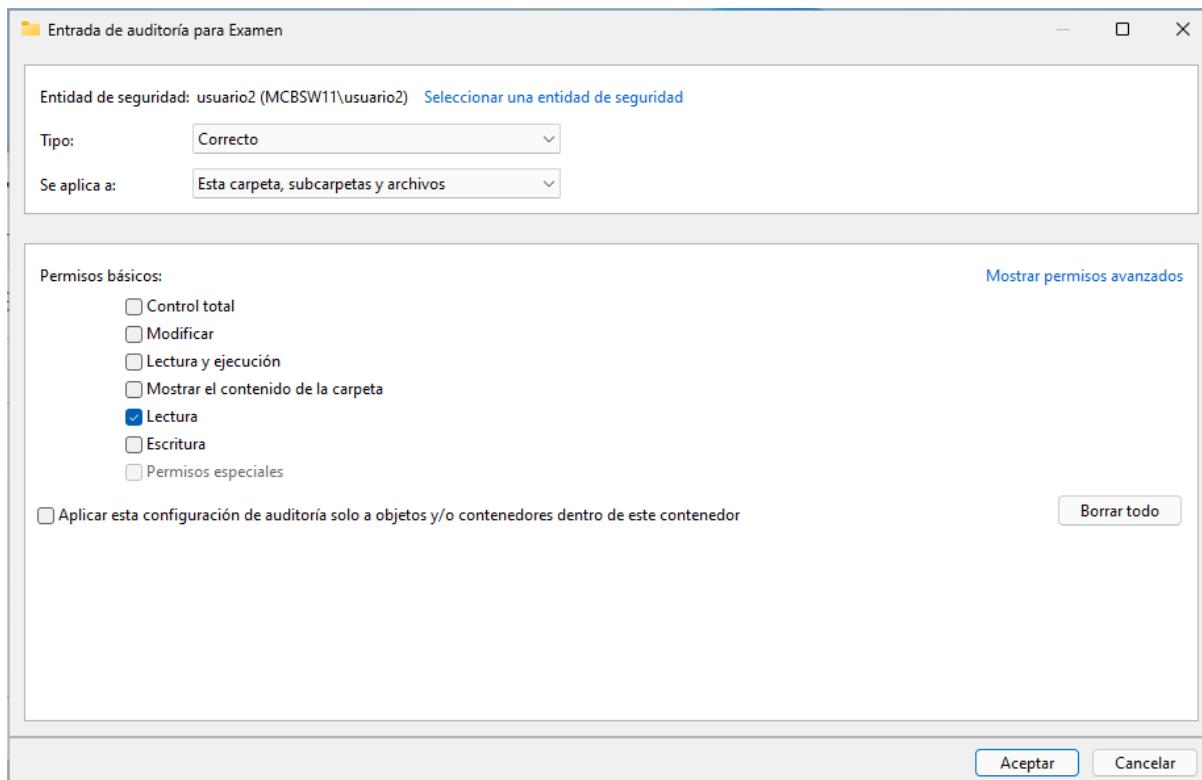
## 5 - Describe como realizas la configuración de los permisos NTFS para un usuario nuevo llamado usuario2 que tienes que crear.



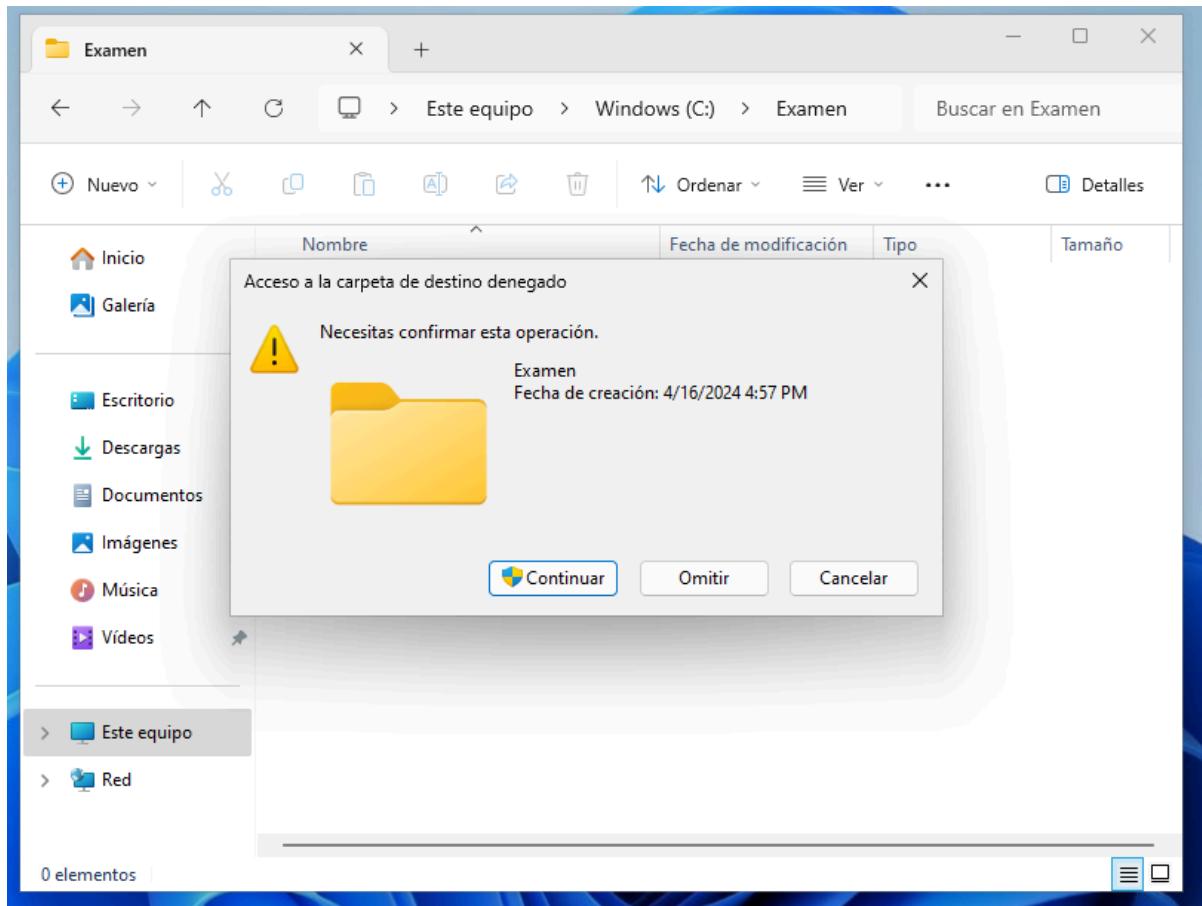
## 5.1 - LECTURA: El usuario2 puede leer el contenido, pero no puede eliminar ninguna carpeta ni crear ninguna carpeta o archivo.

Creamos una política específica para el usuario2 para leer.



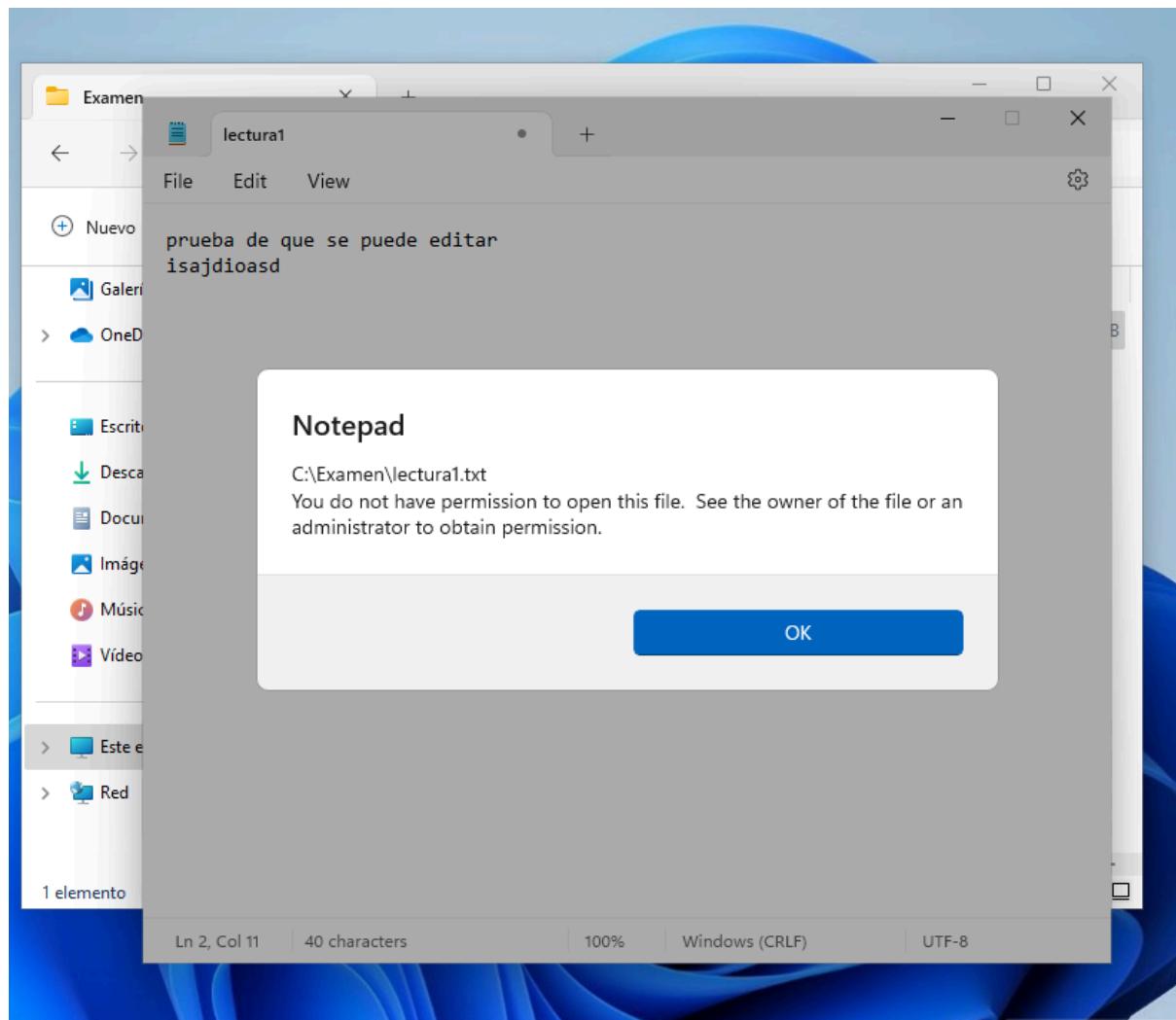


Quitamos también las políticas de usuarios autenticados. Y comprobamos que solo podemos abrir la carpeta, no crear archivos



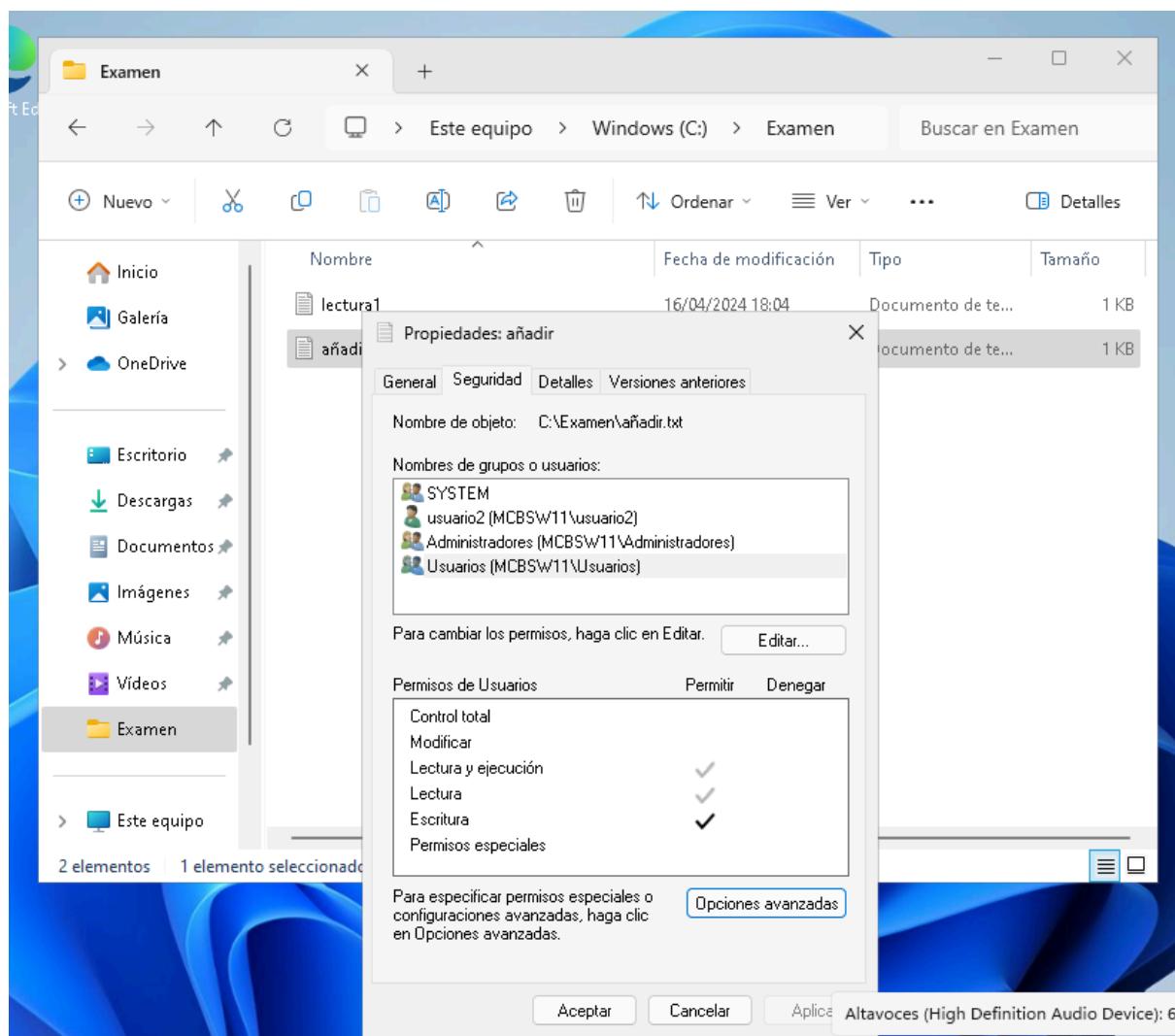
5.2 - SOLOLECTURA: El usuario2 solo puede leer el contenido de la carpeta y del archivo lectura1.txt. No puede modificar, eliminar ni crear nuevas carpetas o archivos.

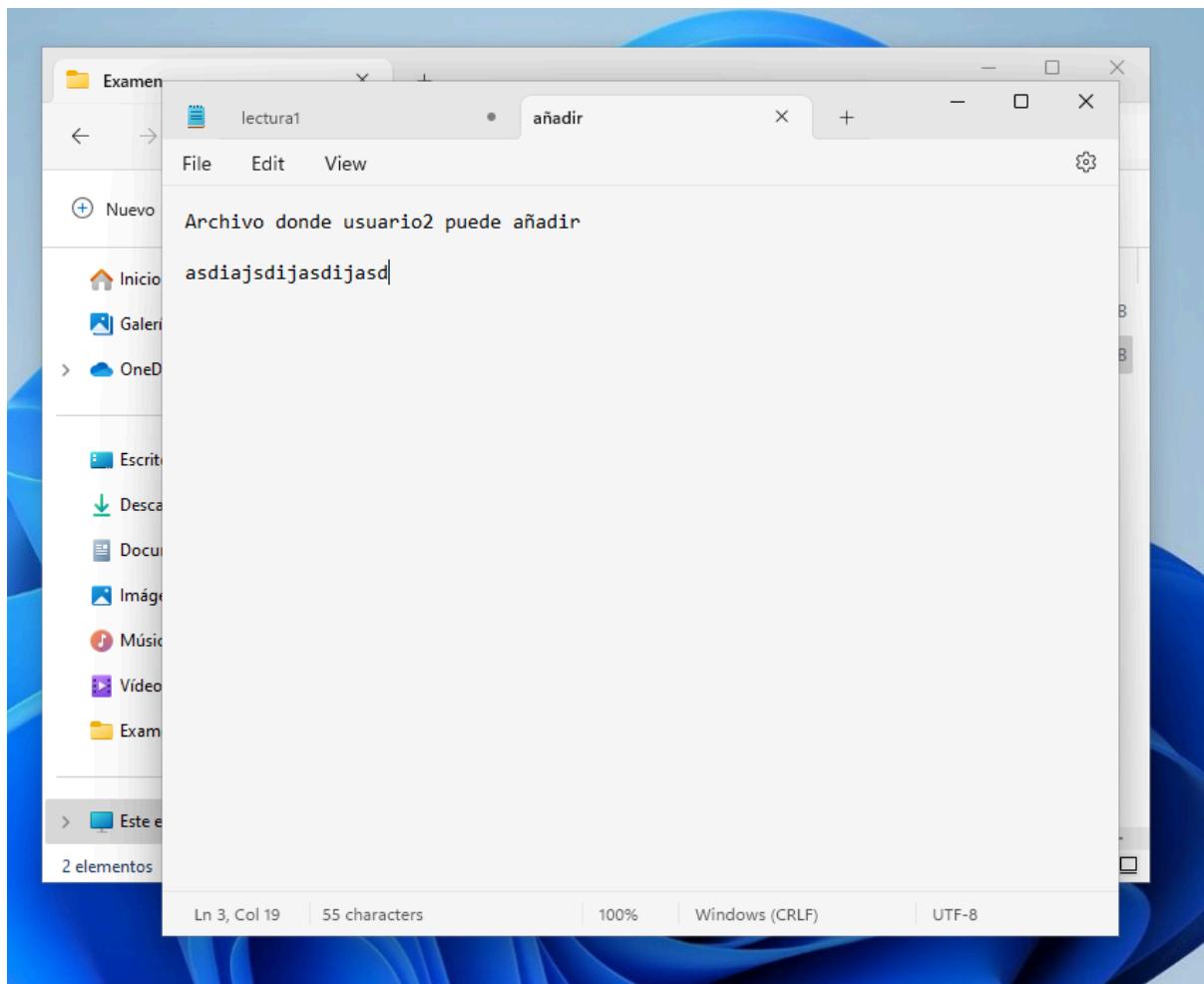
Añadimos el fichero y le asignamos solo permisos de lectura a dicho fichero. Comprobamos que con el usuario 2 solo podemos leer. En la siguiente captura se ve que hemos intentado modificar el archivo pero no hemos podido.



5.3 - LECTURA+AÑADIR: El usuario2 puede leer el contenido de la carpeta y del archivo añadir.txt. No lo puede modificar, pero sí puede crear nuevas carpetas y dentro de estas carpetas puede crear archivos.

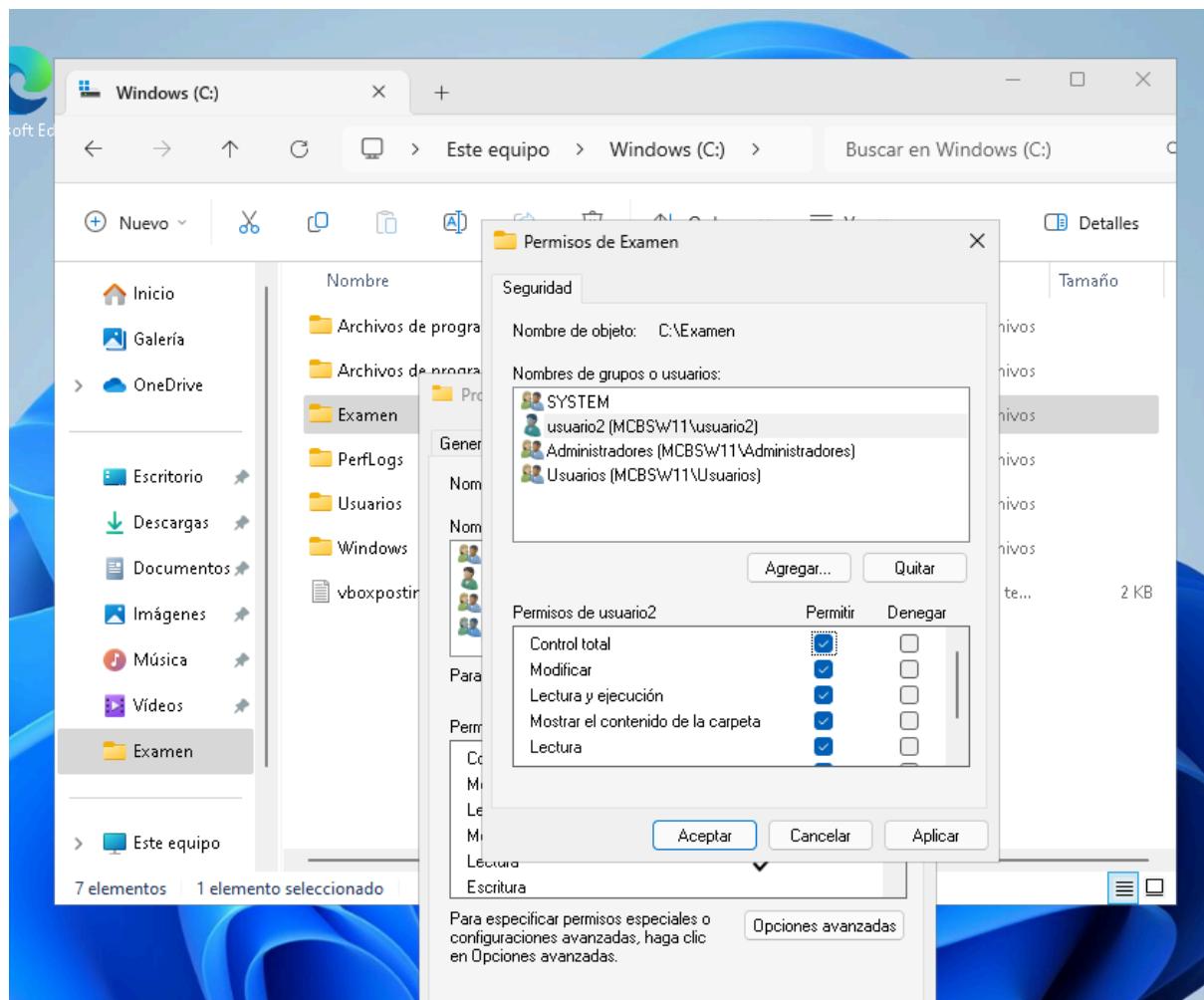
Creamos el fichero y le asignamos el permiso de escritura. Y vemos que podemos editar el fichero con el usuario usuario2.





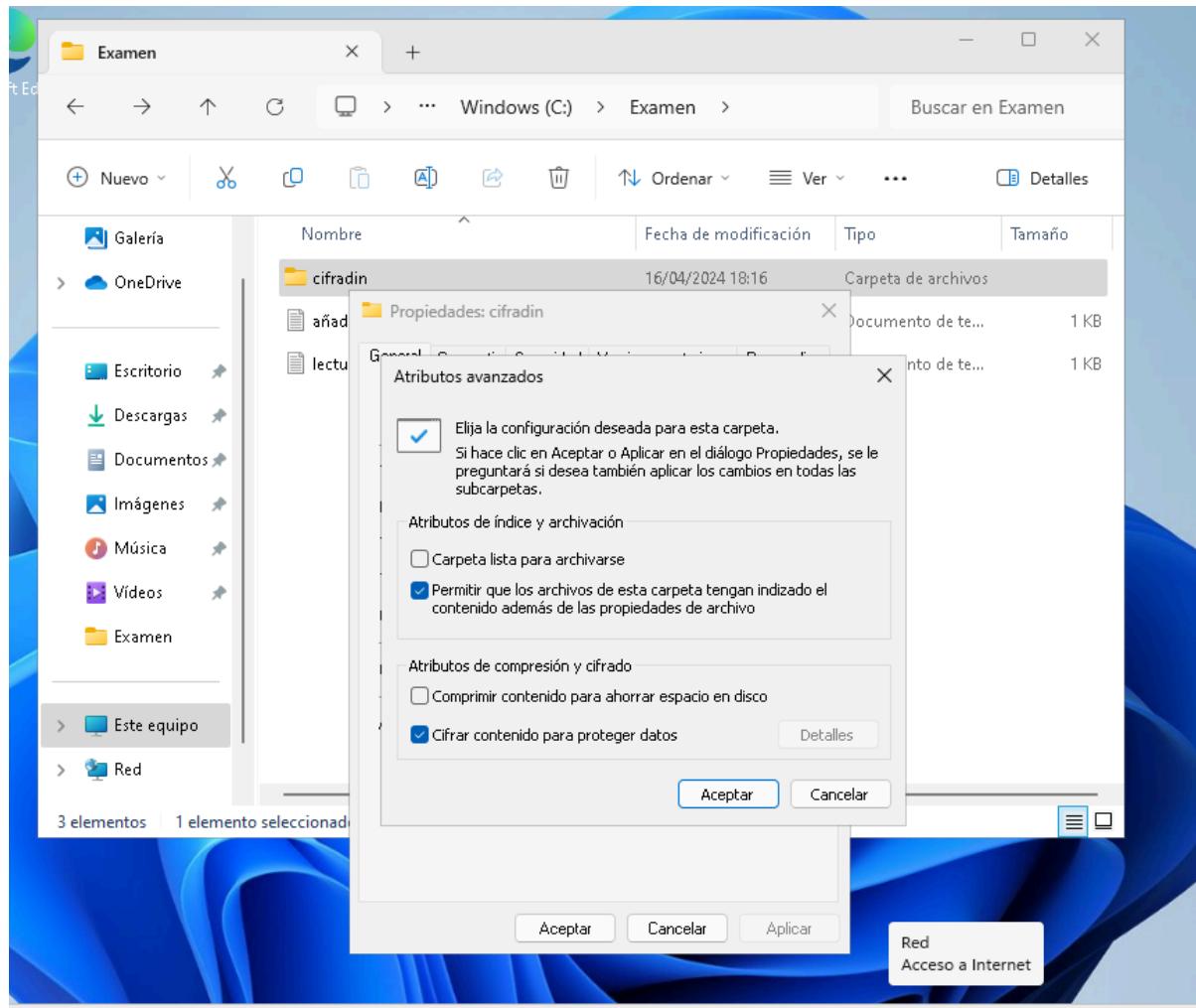
## 5.4 - ACCESOTOTAL: El usuario2 tiene control total sobre la carpeta y componentes

Le asignamos a usuario2 todos los permisos

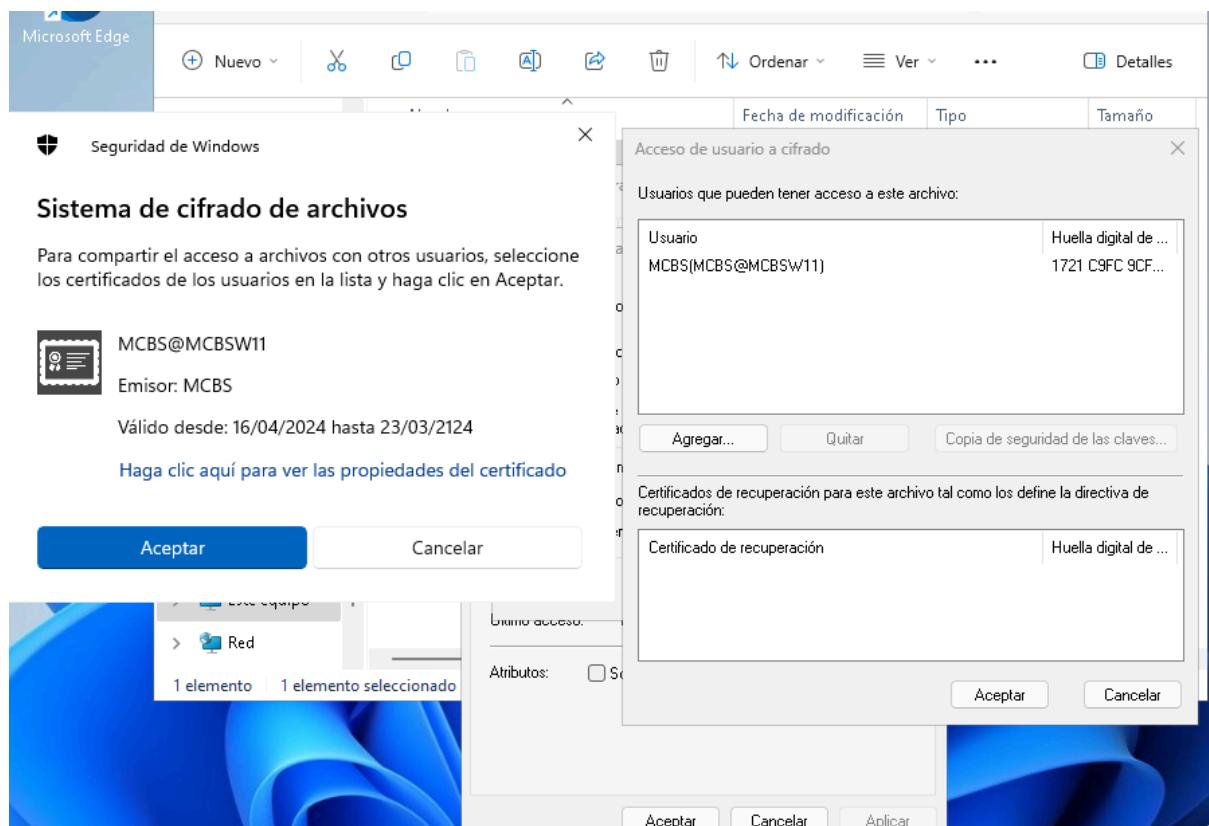


5.5 - CIFRADO: Sólo pueden acceder al contenido de un archivo cifrado los propietarios y los agentes de recuperación por defecto (administradores).

Creamos la carpeta y la ciframos

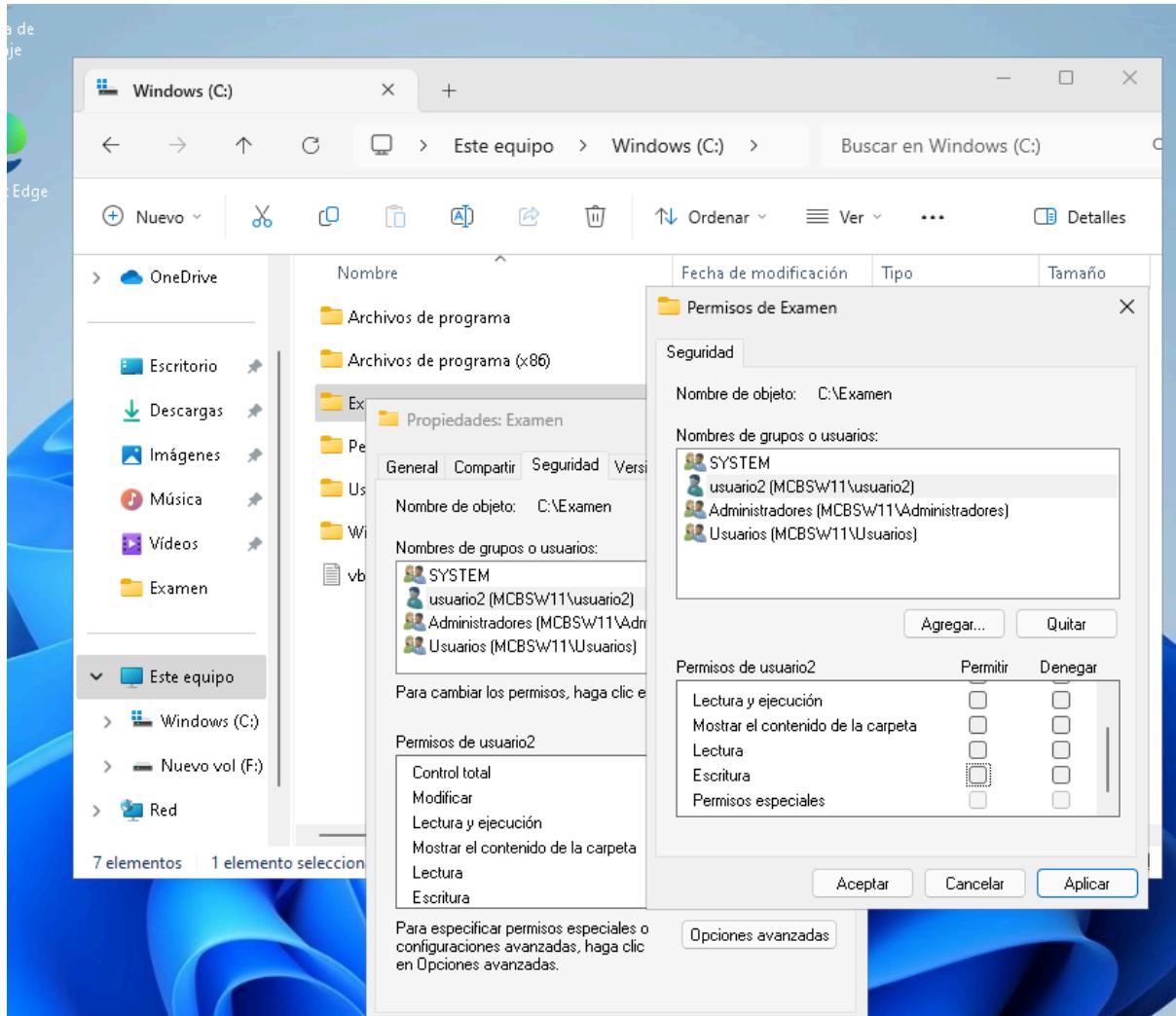


Creamos el archivo, ahora en propiedades del archivo y le añadimos el certificado de los administradores



## 5.6 - PROHIBIDO: El usuario2 no tiene acceso a esta carpeta, tampoco de lectura.

Vamos a quitarle todos los privilegios al usuario2



# Memoria Laboratorios FORT

## Laboratorio 10: EJERCICIOS DE SECURIZACIÓN DE WINDOWS 11

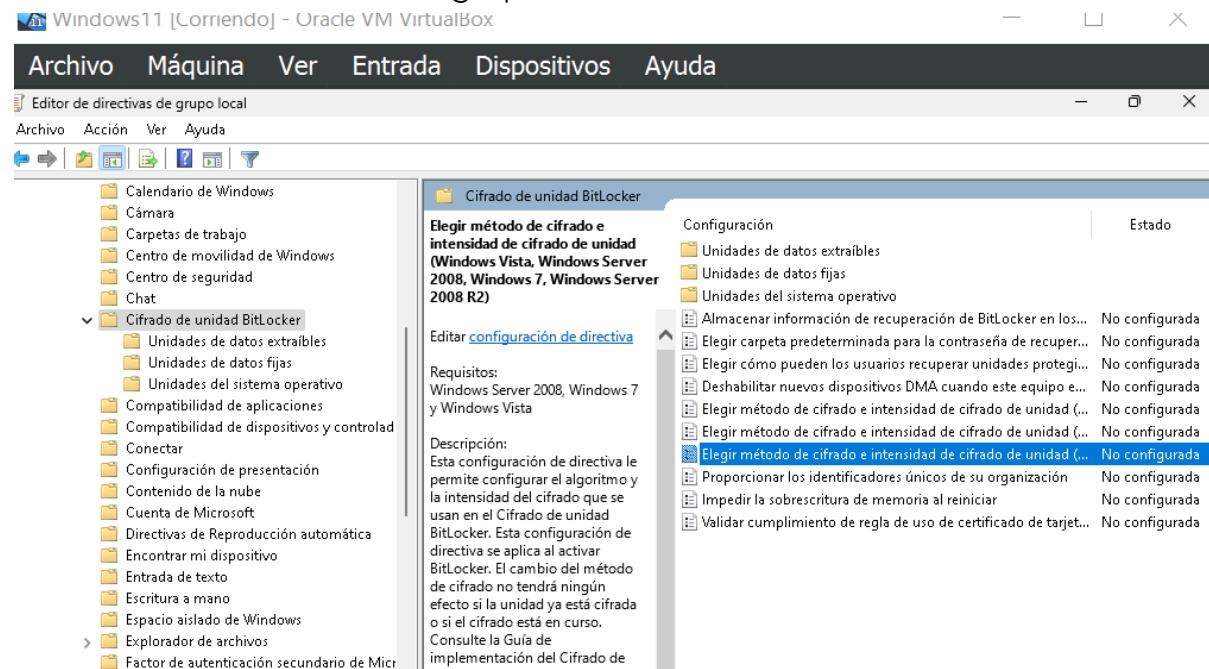
Marcos Villar Avión

María Andrea Ugarte Valencia

# 1 - En este primer punto vamos a proceder con el cifrado de la información, para lo cual utilizaremos la tecnología nativa que nos facilita Microsoft Windows 11 - Bitlocker

1.1 - Revisa las políticas de seguridad relativas a Bitlocker que se encuentran en Configuración del equipo > Plantillas administrativas > Componentes de Windows > Cifrado de unidad BitLocker

Podemos ver las directivas de grupo



Aquí podemos ver el cifrado usado, elegir cómo los usuarios recuperan unidades protegidas...

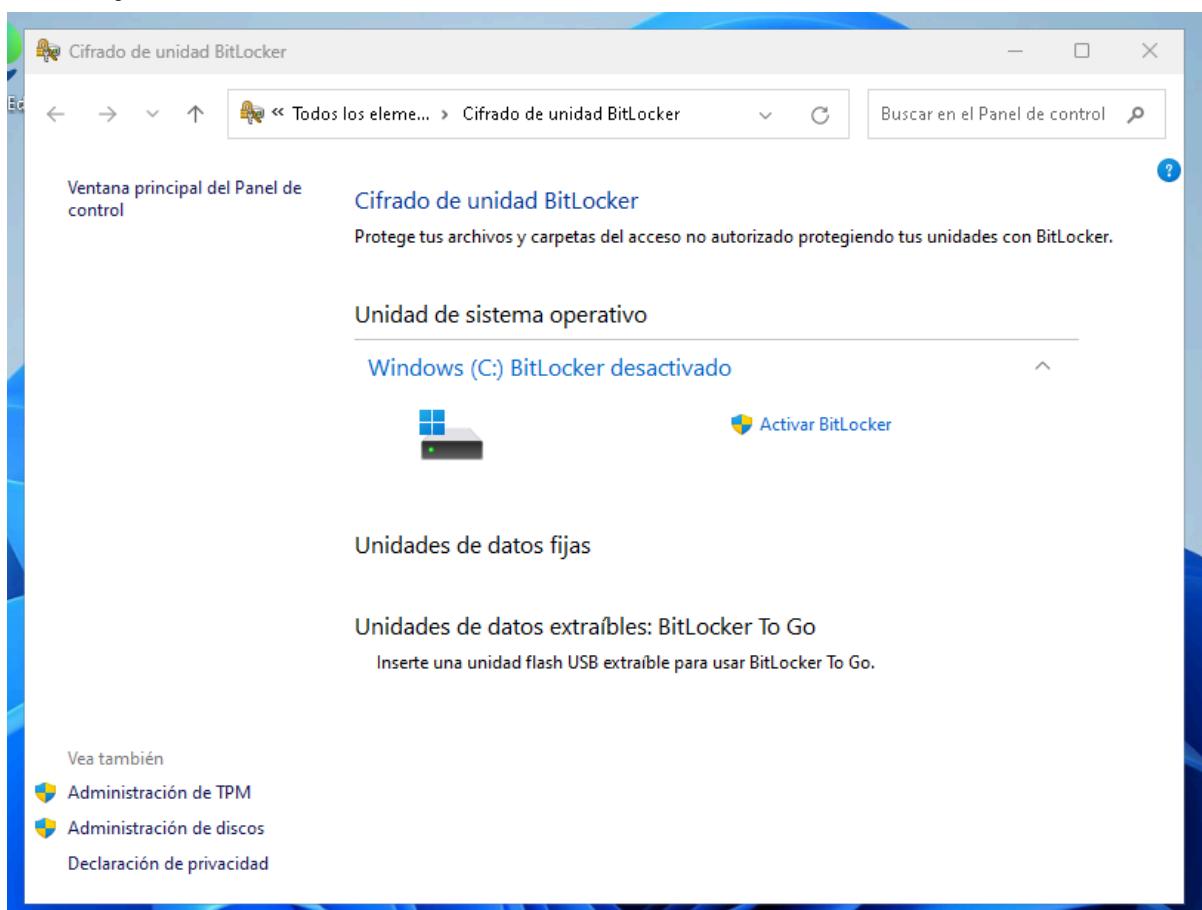
### **1.1.1 - ¿Es necesario realizar algún ajuste para activarlo? ¿Es necesario realizar algún cambio para mejora dicho cifrado?**

No sería necesario realizar ningún ajuste para activar BitLocker, simplemente verificar la compatibilidad del hardware y tener habilitado del TMP

Para mejorar dicho cifrado podemos emplear un algoritmo de cifrado más potente como XTS-AES 256-bits en vez de XTS-AES 128-bit o indicar el modo de rotación de contraseña

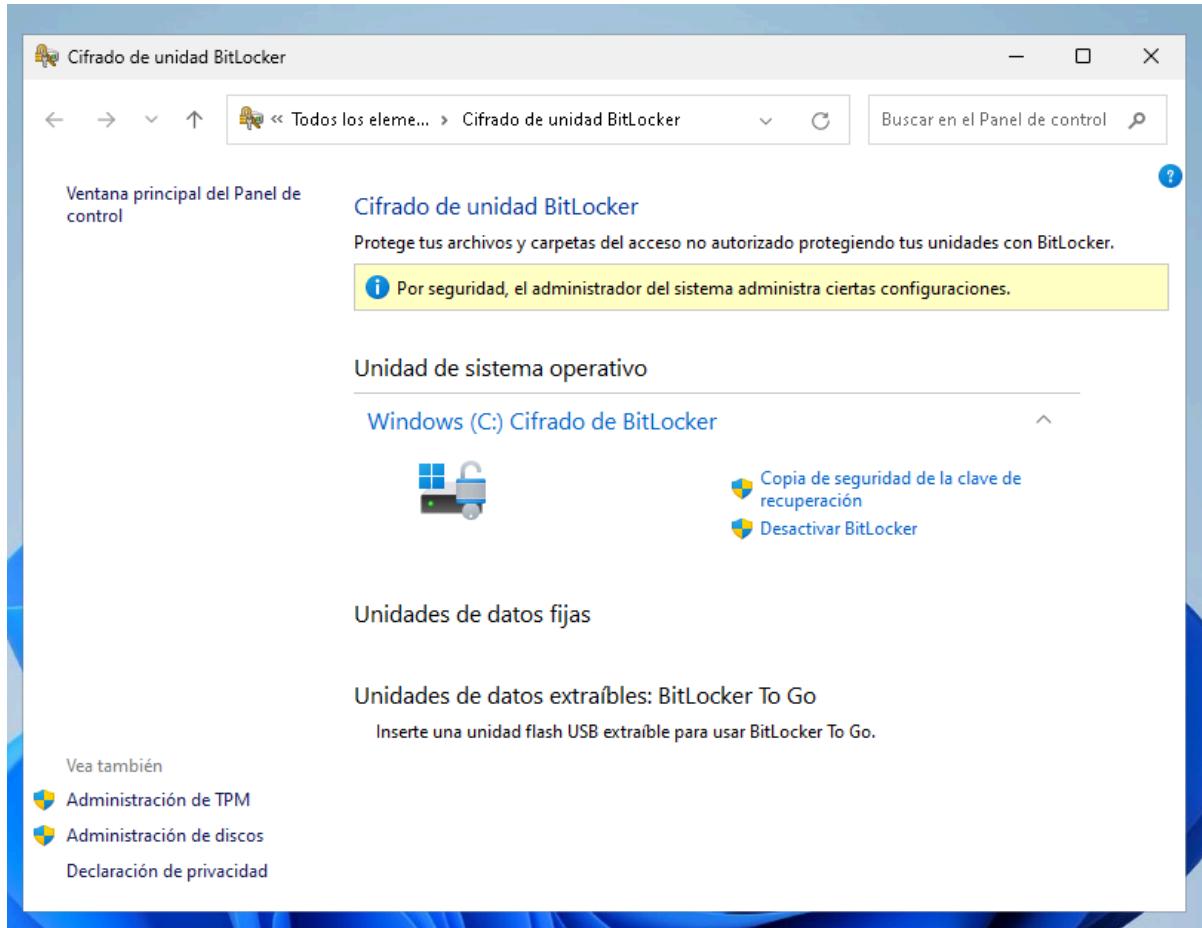
### **1.2 - Realiza la activación del Cifrado de BitLocker sobre la partición del sistema C:**

Para aplicar BitLocker en la unidad C vamos la pantalla de configuración del Cifrado y hacemos click en **Activar BitLocker**



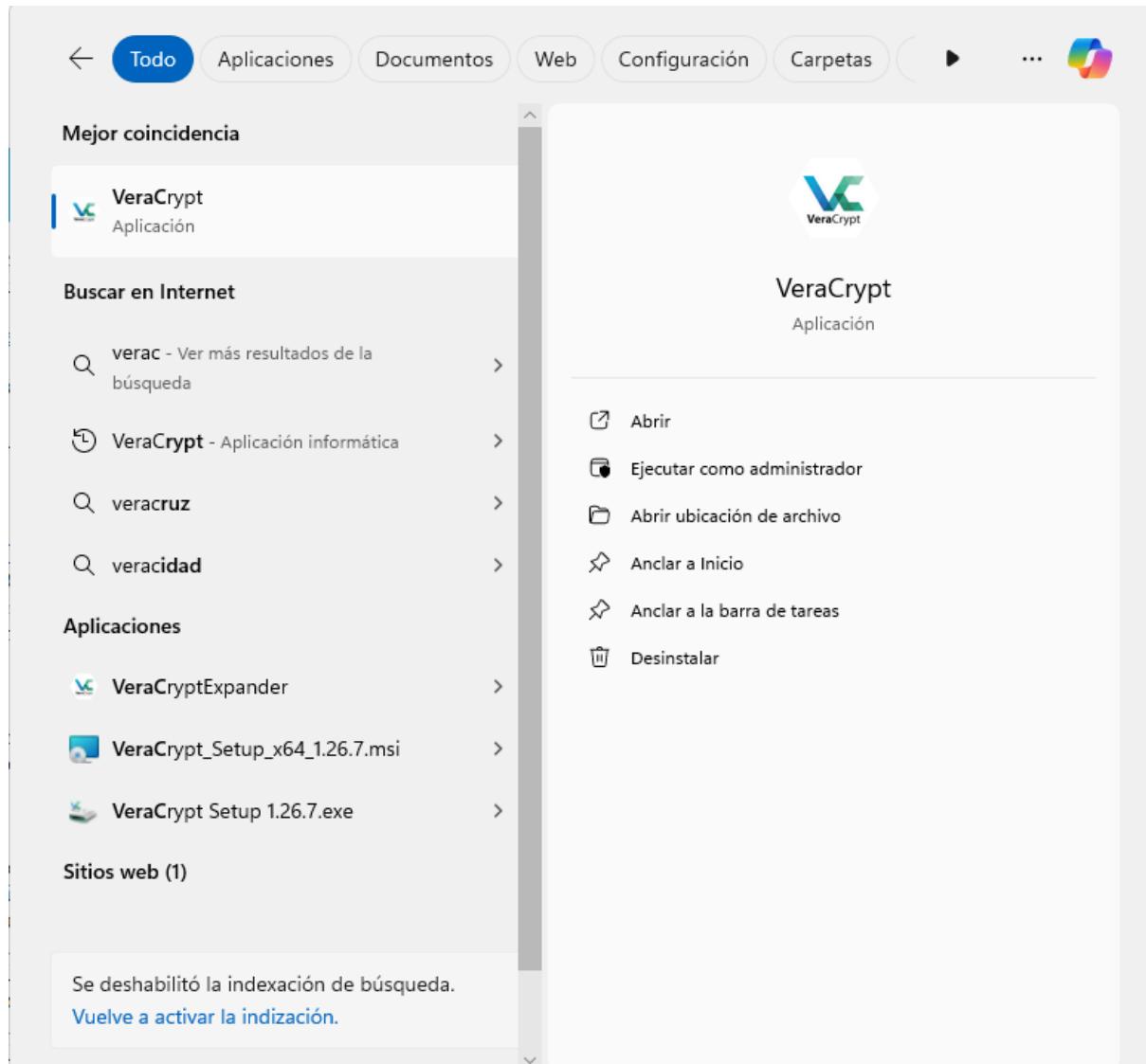
Encriptamos solamente la unidad utilizada y guardamos la clave en la unidad F en un archivo txt (no saque captura de este proceso pero fue todo siguiente > siguiente...)

Tras activar BitLocker en C:\ podemos ver



### **1.3 - Usa Veracrypt para crear un contenedor cifrado para el usuario dentro de su perfil.**

Descargamos e instalamos la aplicación y ya podemos acceder desde la barra del menú



Creamos un contenedor de la siguiente forma:

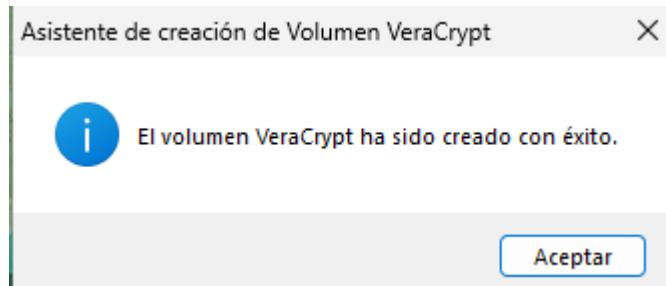




Sabemos que la contraseña no es segura, pero esto es solo una prueba.

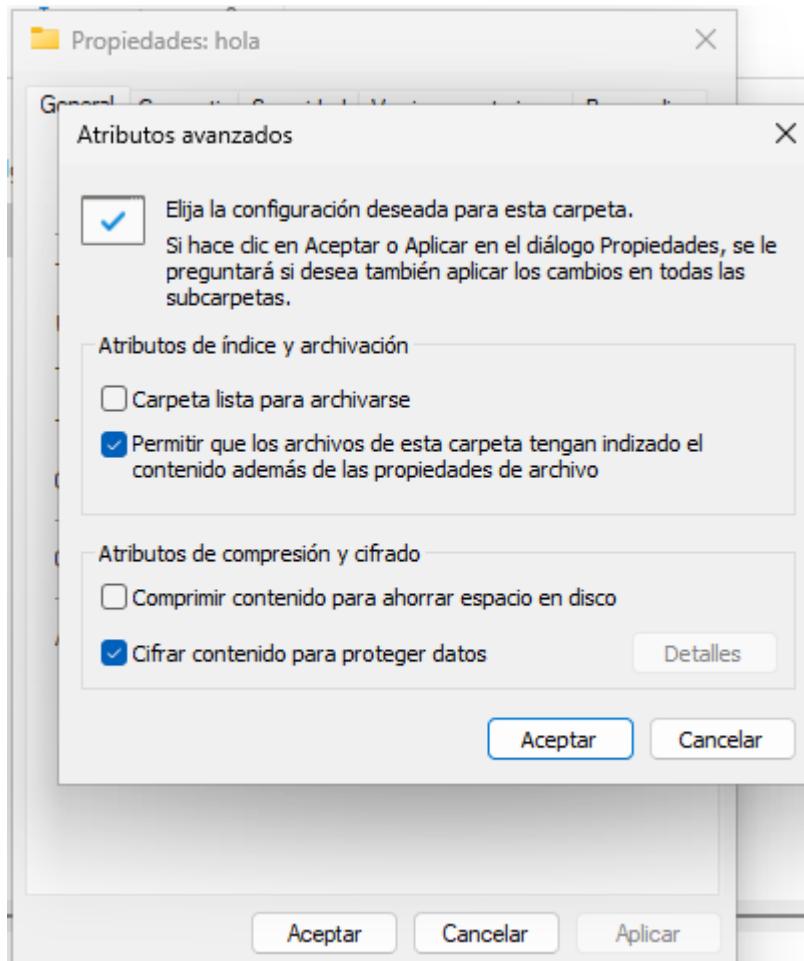
### Establecemos la contraseña



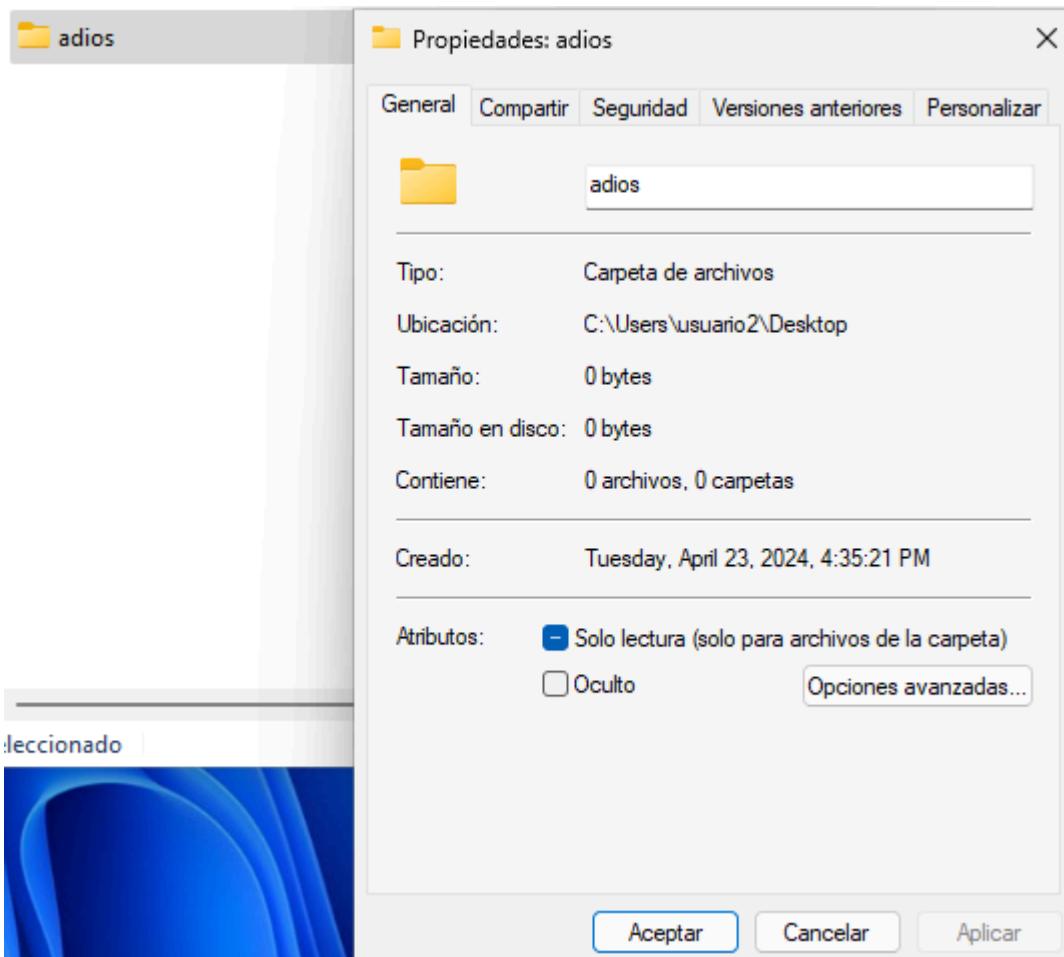


**1.4 - Por último, crea una carpeta con el sistema de cifrado EFS.**

Creamos una carpeta llamada "hola" y la encriptamos yendo a sus propiedades como se ve en la captura anterior.

**¿Puede habilitar este sistema de cifrado un usuario limitado?**

Si que se podría puesto que hemos intentado realizar esto con usuario2 y se ha podido ya que un usuario siempre podría realizar esto en caso de que tenga los privilegios para acceder y modificar esto.



**Podrían acceder varios usuarios al mismo fichero/carpeta compartida. Y cifrada, ¿Cuál sería el procedimiento?**

Si que se podría. Se tendría que tener una carpeta compartida con varios ficheros, y cualquiera con acceso a la carpeta podría realizar el encriptado EFS

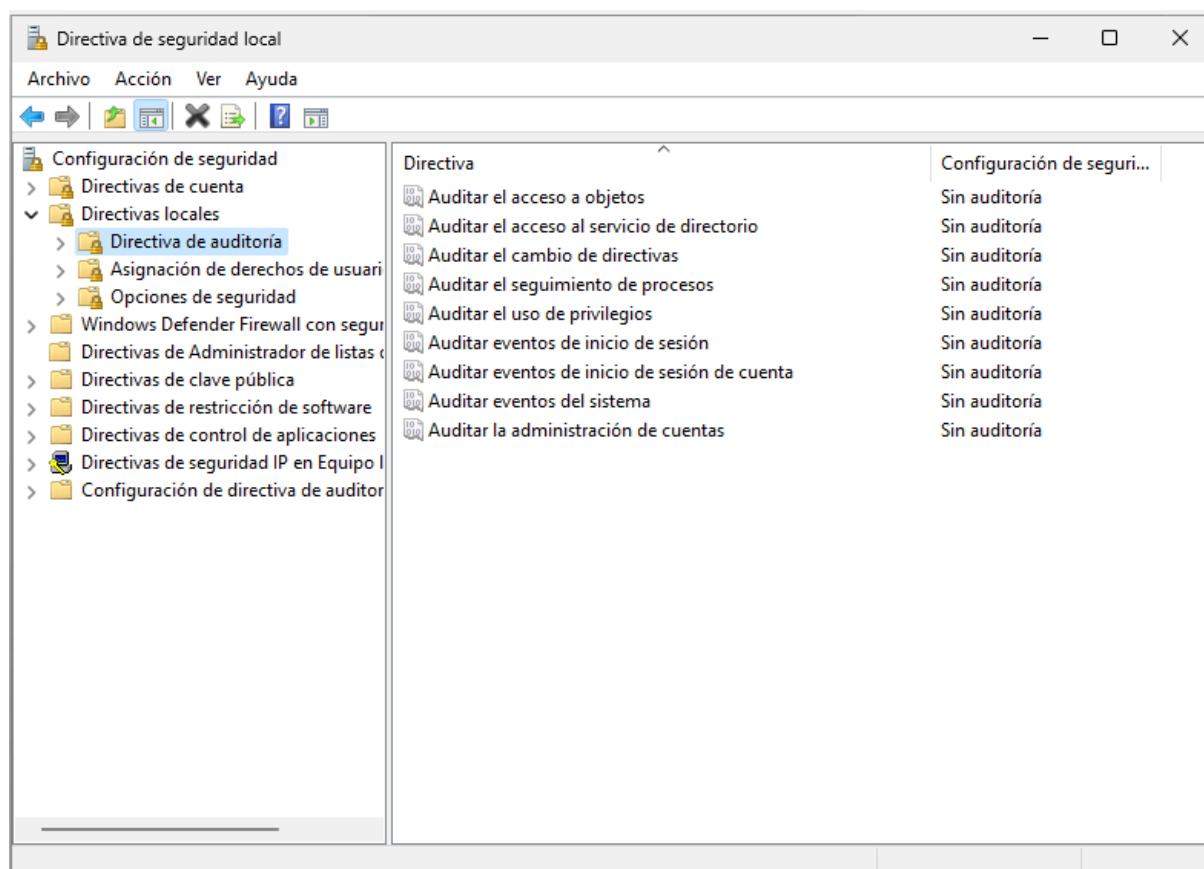
¿Cómo harían el resto de usuarios para acceder a dicha carpeta compartida encriptada?

El usuario que ha encriptado la carpeta tendría que exportar su clave de cifrado y compartirlo con otros usuarios. Esto se hace utilizando la herramienta de administración de certificados en Windows. El usuario que quiera entrar tendrá que importarla y ya podrá ver el contenido de la carpeta

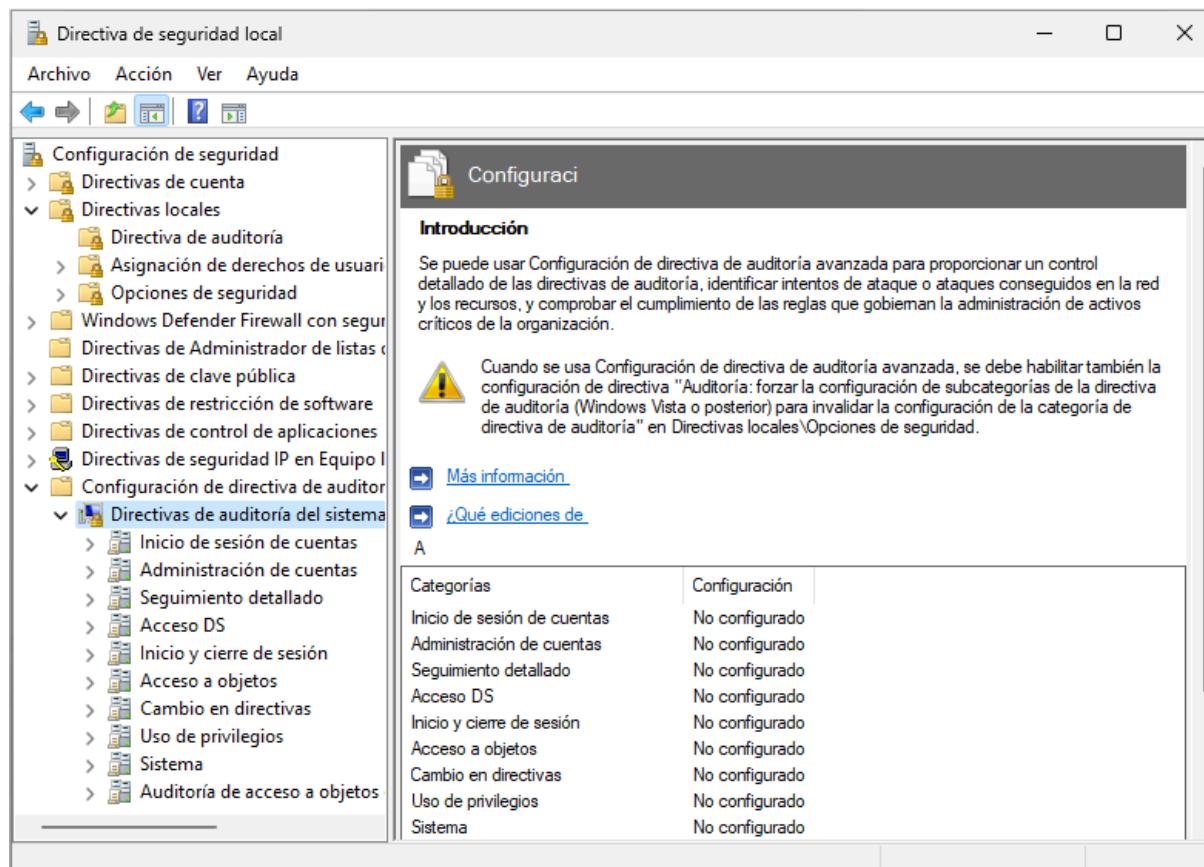
## 2 - Por último, todo buen sistema debe de disponer un sistema de auditoria que garantice realizar un análisis y que nos permita identificar que, quien y como se realizó una acción.

2.1 - Windows 11 dispone de un sistema de auditoria, pero ¿está activado por defecto? Si no estuviera activado ¿Como podríamos activar el sistema de auditoria?

No está activado por defecto el sistema de auditoría. Según los apuntes de la asignatura, Windows dispone de dos categorías de auditoría que podemos activar o bien en: **Directiva de seguridad local > Directivas locales > Directiva de auditoría**



o en **Directiva de seguridad local > Configuración de directiva de auditoría avanzada > Directivas de auditoría del sistema**



The screenshot shows the Windows Local Security Policy snap-in. On the left, the navigation pane lists several security policies: Configuración de seguridad, Directivas de cuenta, Directivas locales, Windows Defender Firewall con seguridad, Directivas de Administrador de listas, Directivas de clave pública, Directivas de restricción de software, Directivas de control de aplicaciones, Directivas de seguridad IP en Equipo, and Configuración de directiva de auditoría. Under 'Configuración de directiva de auditoría', there is a sub-section for 'Directivas de auditoría del sistema' which includes: Inicio de sesión de cuentas, Administración de cuentas, Seguimiento detallado, Acceso DS, Inicio y cierre de sesión, Acceso a objetos, Cambio en directivas, Uso de privilegios, Sistema, and Auditoría de acceso a objetos. The main pane displays the 'Introducción' (Introduction) for advanced audit policy configuration, stating that it provides detailed control over audit policies to identify attack attempts and ensure compliance with critical organization assets. It also notes that enabling this feature requires enabling the 'Auditoría: forzar la configuración de subcategorías de la directiva de auditoría (Windows Vista o posterior)' (Audit: force the configuration of subcategories of the audit policy (Windows Vista or later)) option in the 'Opciones de seguridad' (Security options) section of the 'Directivas locales' (Local policies) node. Below this, there are links for 'Más información' (More information) and '¿Qué ediciones de...' (What editions of...). A table titled 'A' shows the categories and their current configuration status:

Categorías	Configuración
Inicio de sesión de cuentas	No configurado
Administración de cuentas	No configurado
Seguimiento detallado	No configurado
Acceso DS	No configurado
Inicio y cierre de sesión	No configurado
Acceso a objetos	No configurado
Cambio en directivas	No configurado
Uso de privilegios	No configurado
Sistema	No configurado

Estas categorías no se van a aplicar hasta reiniciar el sistema.

## 2.2 - ¿Qué categorías podemos auditar en un sistema operativo Windows 11?

Podemos auditar las siguientes categorías en **Directivas locales > Directiva de auditoría**:

Directiva	Configuración de seguri...
Auditar el acceso a objetos	Sin auditoría
Auditar el acceso al servicio de directorio	Sin auditoría
Auditar el cambio de directivas	Sin auditoría
Auditar el seguimiento de procesos	Sin auditoría
Auditar el uso de privilegios	Sin auditoría
Auditar eventos de inicio de sesión	Sin auditoría
Auditar eventos de inicio de sesión de cuenta	Sin auditoría
Auditar eventos del sistema	Sin auditoría
Auditar la administración de cuentas	Sin auditoría

Y las siguientes en **Configuración de directiva de auditoría avanzada > Directivas de auditoría del sistema**:

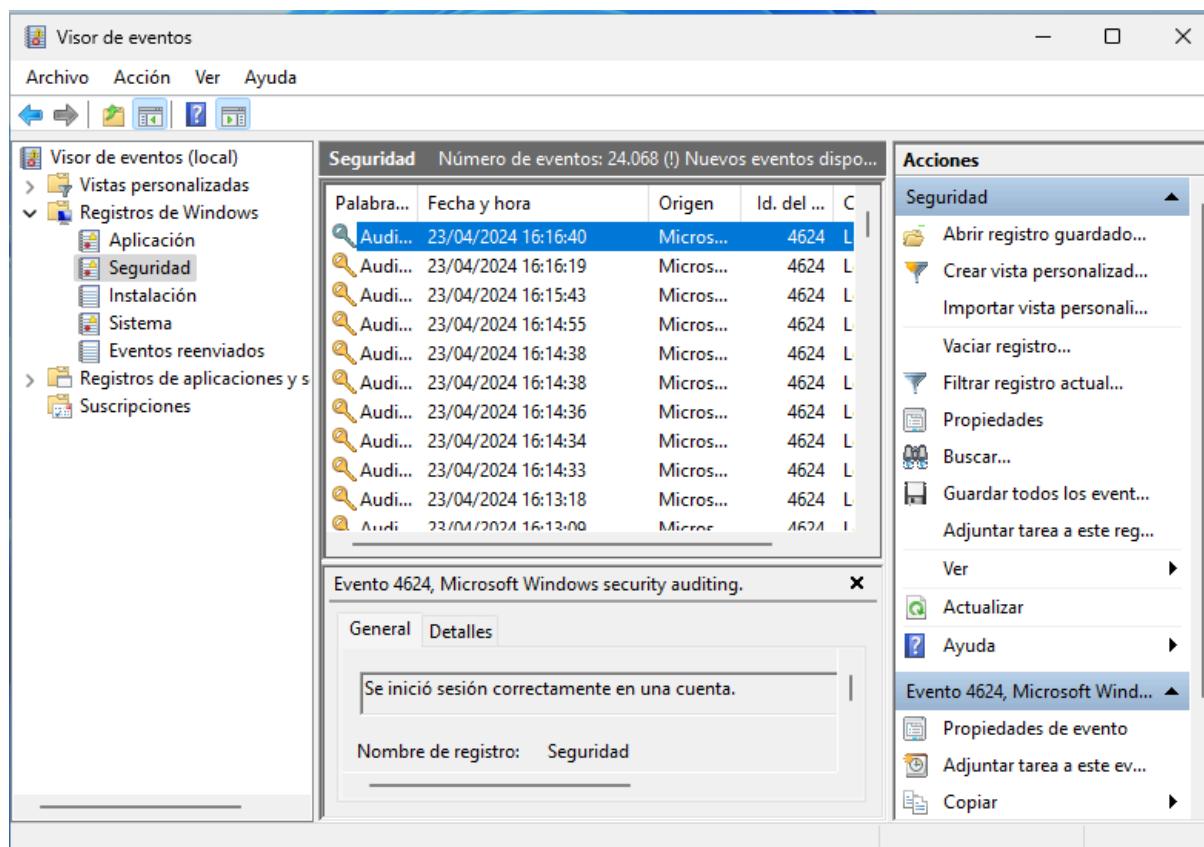
Categorías	Configuración
Inicio de sesión de cuentas	No configurado
Administración de cuentas	No configurado
Seguimiento detallado	No configurado
Acceso DS	No configurado
Inicio y cierre de sesión	No configurado
Acceso a objetos	No configurado
Cambio en directivas	No configurado
Uso de privilegios	No configurado
Sistema	No configurado
Auditoría de acceso a objetos global	No configurado

### **2.3 - ¿Sobre qué tipo de objetos podemos aplicar una auditoría de Windows 11?**

Podemos aplicar una auditoría sobre cualquier tipo de objeto que soporte una SACL, por ejemplo: una directiva de grupo, el comportamiento de una impresora,...

### **2.4 - ¿Cómo podemos observar los resultados de una auditoría?**

Tras reiniciar el equipo, podremos observar los resultados de una auditoría con el visor de eventos. Por ejemplo, hemos configurado la auditoría para el inicio de sesión:



Cabe decir que esta no es la forma más común de realizar una auditoría, normalmente se hace con herramientas como Clara.

# Memoria Laboratorios FORT

## Laboratorio 11: EJERCICIOS DE SECURIZACIÓN DE WINDOWS 11

Marcos Villar Avión

María Andrea Ugarte Valencia

## 1 - ¿Qué dos métodos tenemos de configuración de AppLocker? ¿Cuál consideras que es la mejor opción?

Hay dos formas de configurar AppLocker: a través de **whitelist** o empleando **blacklist**. Es decir, se puede definir una lista de aplicaciones permitidas y el resto será denegada o se puede especificar una lista de aplicaciones no permitidas y el resto serán accesibles en el sistema.

Lógicamente la opción más segura sería emplear whitelist pero como desventaja sería que tendrías que saber con exactitud las aplicaciones empleadas en el ordenador, lo cual puede ser complicado de definir.

## **2 - ¿Por qué es necesario crear las reglas automáticamente para que funcione AppLocker?**

Se necesita crear las reglas automáticamente de permitir para todas las aplicaciones del dispositivo porque todas las aplicaciones que no estén en dichas reglas, serán bloqueadas por AppLocker. Por lo tanto, concluimos que sí que es necesario crear las reglas automáticamente para no bloquear servicios o aplicaciones de primeras.

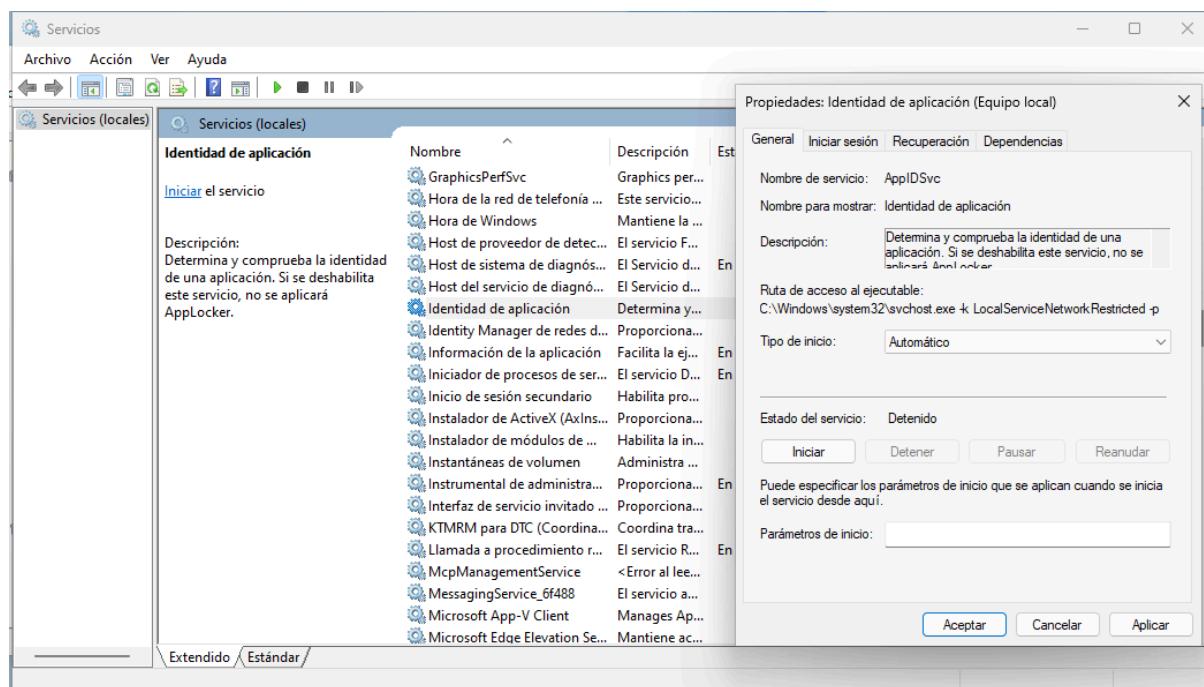
Sin embargo, podemos ver que las realiza por ruta y aunque esto no sea lo recomendable, sí que nos permite que el SO funcione.

### 3 - Instala el siguiente software

## “Notepad++” en tu Windows 11.

**Es necesario bloquear la ejecución de esta aplicación. ¿Qué opciones te muestra AppLocker para identificar la aplicación? ¿Cuál sería la mejor opción?**

Activamos la identidad de aplicación:

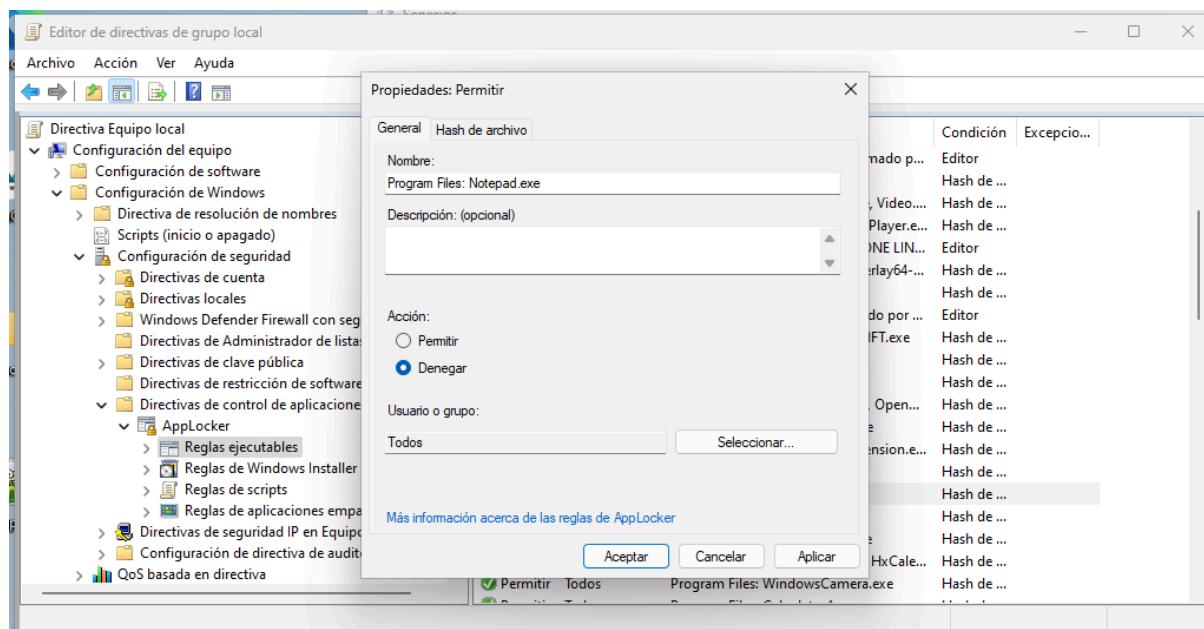


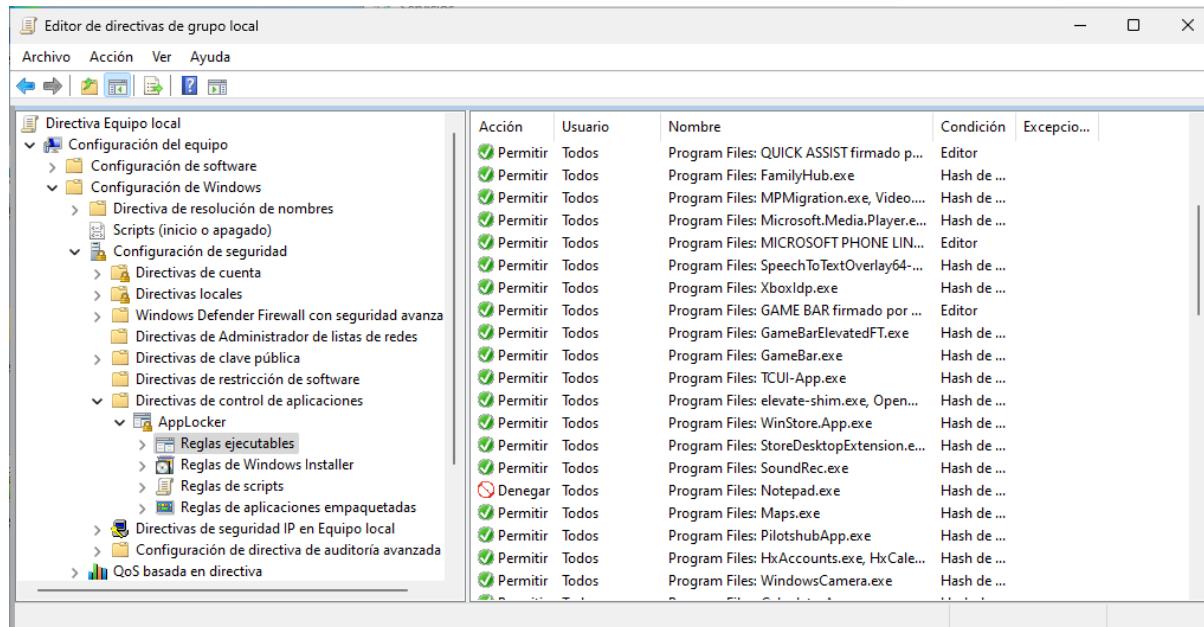
Creamos las reglas, para identificar las aplicaciones podemos o bien usar el hash o el path:



Consideramos que la mejor opción es identificar a las aplicaciones mediante el hash ya que es más preciso porque, por ejemplo, en caso de que cambiase la ubicación de la aplicación aún tendríamos referencia a ella.

Una vez generadas las reglas, denegamos el acceso a Notepad++:





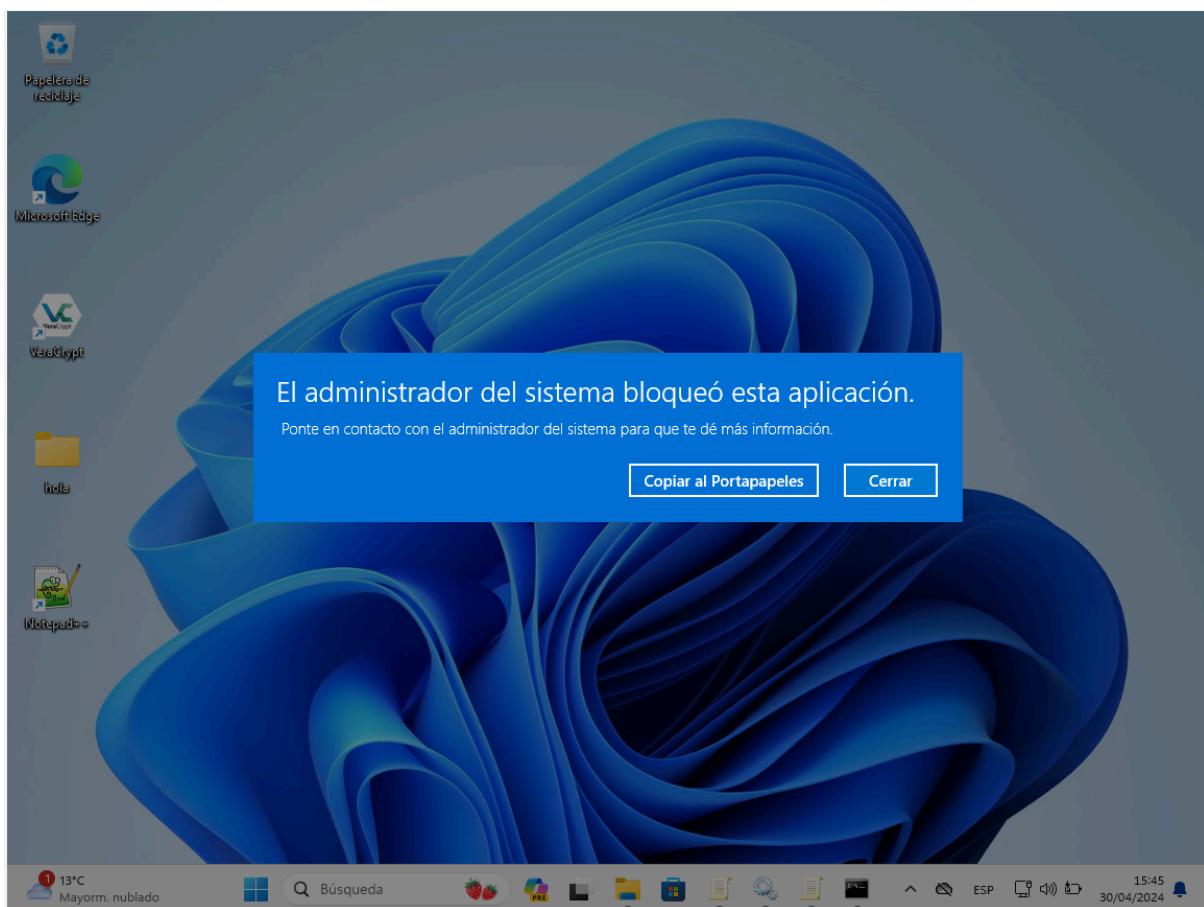
The screenshot shows the Windows Group Policy Editor window titled "Editor de directivas de grupo local". The left pane displays a tree structure of policy settings under "Directiva Equipo local". The right pane is a table listing security rules (Acción, Usuario, Nombre, Condición, Excepcion...) for various programs like QUICK ASSIST, FamilyHub.exe, etc.

Acción	Usuario	Nombre	Condición	Excepcion...
Permitir	Todos	Program Files: QUICK ASSIST firmado p...	Editor	
Permitir	Todos	Program Files: FamilyHub.exe	Hash de ...	
Permitir	Todos	Program Files: MPMigration.exe, Video...	Hash de ...	
Permitir	Todos	Program Files: Microsoft.Media.Player.e...	Hash de ...	
Permitir	Todos	Program Files: MICROSOFT PHONE LIN...	Editor	
Permitir	Todos	Program Files: SpeechToTextOverlay64...	Hash de ...	
Permitir	Todos	Program Files: XboxIdp.exe	Hash de ...	
Permitir	Todos	Program Files: GAME BAR firmado por ...	Editor	
Permitir	Todos	Program Files: GameBarElevatedFT.exe	Hash de ...	
Permitir	Todos	Program Files: GameBar.exe	Hash de ...	
Permitir	Todos	Program Files: TCUI-App.exe	Hash de ...	
Permitir	Todos	Program Files: elevate-shim.exe, Open...	Hash de ...	
Permitir	Todos	Program Files: WinStore.App.exe	Hash de ...	
Permitir	Todos	Program Files: StoreDesktopExtension.e...	Hash de ...	
Permitir	Todos	Program Files: SoundRec.exe	Hash de ...	
Denegar	Todos	Program Files: Notepad.exe	Hash de ...	
Permitir	Todos	Program Files: Maps.exe	Hash de ...	
Permitir	Todos	Program Files: PilothubApp.exe	Hash de ...	
Permitir	Todos	Program Files: HxAccounts.exe, HxCale...	Hash de ...	
Permitir	Todos	Program Files: WindowsCamera.exe	Hash de ...	

Ejecutamos **gpupdate /force**

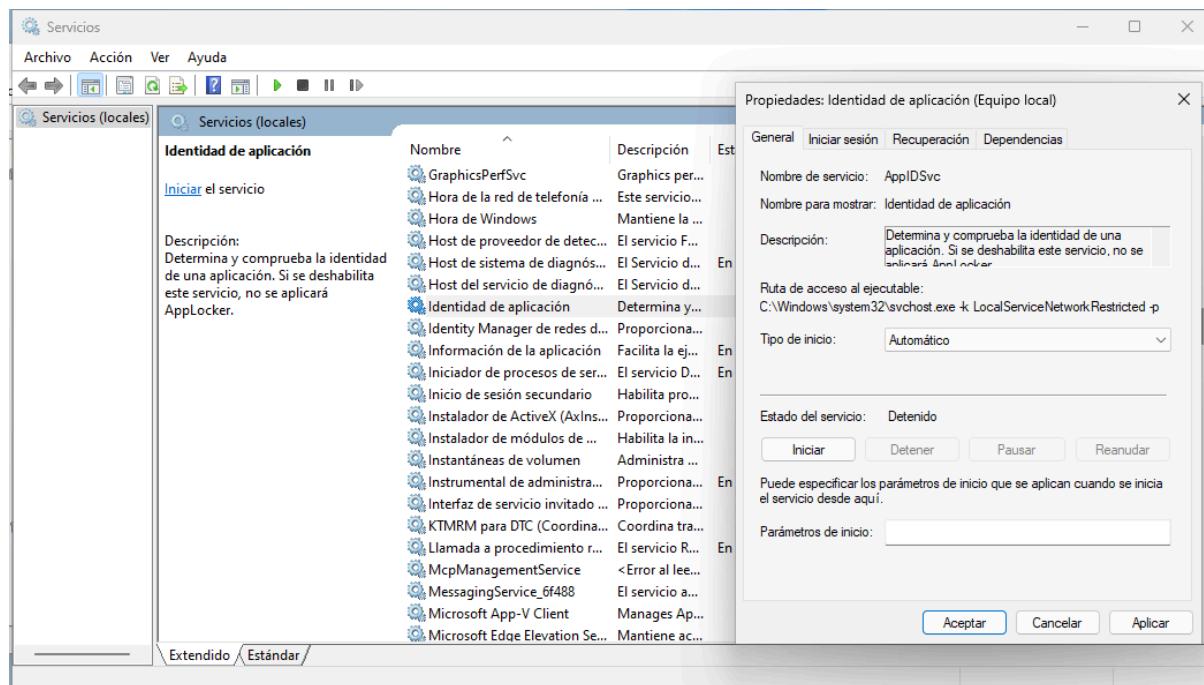
Dicho comando actualiza las directivas del grupo y con el parámetro /force vuelve a aplicar todas las configuraciones de directiva.

y vemos como si intentamos entrar a Notepad++ nos salta este mensaje:



## 4 - ¿Qué servicio es necesario modificar para que funcione el AppLocker? ¿Qué cambios tenemos que realizar?

Como indicamos en el apartado anterior, para que funcione AppLocker es necesario modificar el servicio de **Identidad de Aplicación**. Debemos activarlo:



Además, una vez aplicado los cambios, tenemos que actualizar las políticas de grupos para que se hagan efectivos dichos cambios.

## 5 - El AppLocker se configura a través de las directivas de grupo ¿qué comando tenemos que utilizar para aplicar los cambios que hemos realizado y que el sistema de AppLocker funcione sin la necesidad de reiniciar el equipo?

Con **gpupdate /force** podemos forzar la actualización de las directivas sin reiniciar el equipo.

- **gpupdate** -> comando para actualizar las políticas de grupo
- **/force** vuelve a aplicar todas las configuraciones de directiva

# Memoria Laboratorios FORT

## Laboratorio 12: EJERCICIOS DE SECURIZACIÓN DE WINDOWS 11

Marcos Villar Avión

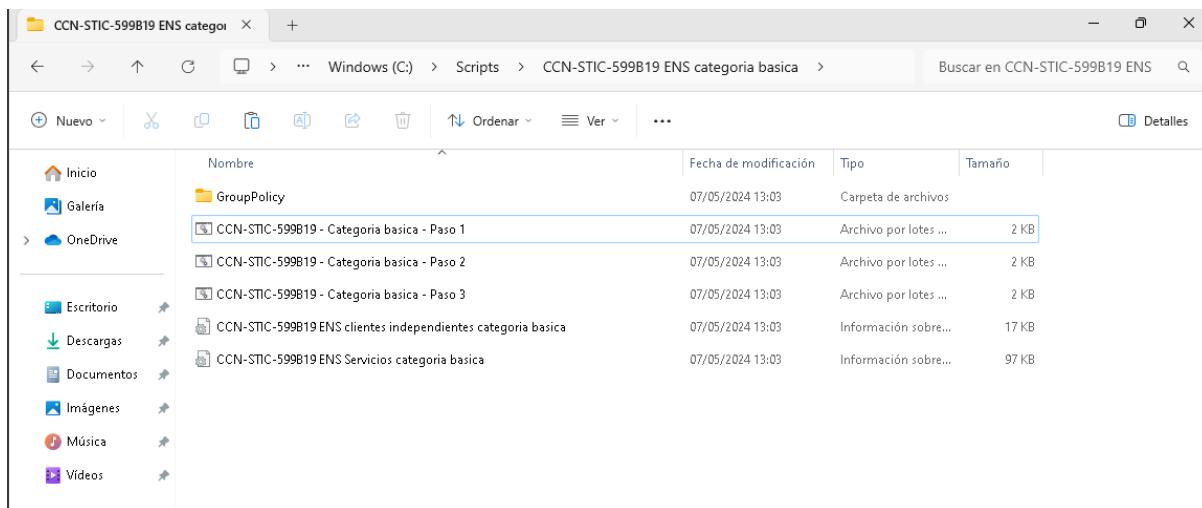
María Andrea Ugarte Valencia

Para un uso normal y no crítico del sistema, el nivel básico es más que suficiente para poder securizar un equipo. Es por ello que nosotros hemos seleccionado dicho nivel para realizar esta práctica.

## **1 - Indica los pasos que seguiste durante el proceso de instalación del script**

Vamos a implementar la medida de seguridad básica del apartado A de: CONFIGURACIÓN SEGURA DE MICROSOFT WINDOWS 10 ENTERPRISE LTSC EN EL ENS COMO CLIENTE INDEPENDIENTE

Vamos a crear una carpeta **Scripts** en C:\ y añadimos el zip que hemos descargado.



Ahora ejecutamos el primer paso.

```
C:\Windows\System32\cmd.exe
-----
CCN-STIC-599B19 ENS Cliente Windows 10 Independiente - Paso 1
    Categoría básica
-----
Este script aplica la plantilla de seguridad.
Antes de ejecutar este script asegúrese que los ficheros
y scripts se encuentran en el directorio "C:\Scripts".
-----
Presione una tecla para continuar . . .
Configurando plantilla de seguridad...
C:\Windows\System32\secedit /configure /quiet /db "c:\scripts\plantilla_windows.sdb" /cfg "c:\scripts\CCN-STIC-599B19 EN
S categoría básica\CCN-STIC-599B19 ENS clientes independientes categoría básica.inf" /overwrite /log "c:\scripts\CCN-STI
C-599B19 ENS categoría básica\plantilla_windows.log"
Plantilla de seguridad configurada.

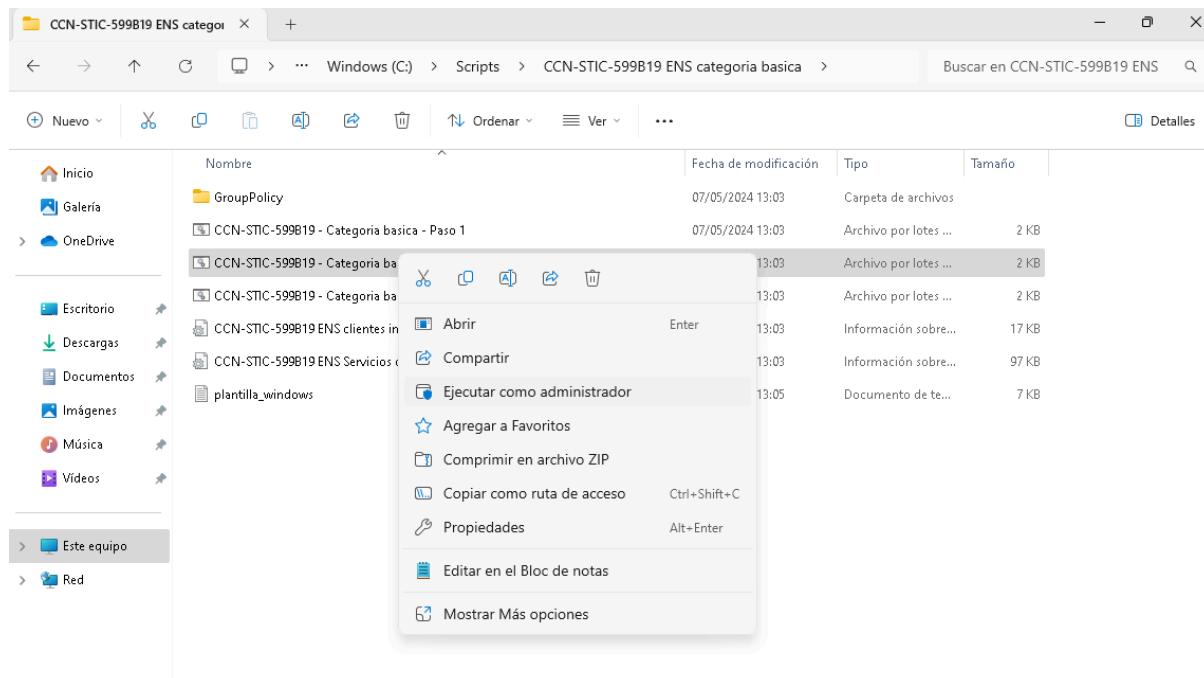
-----
CCN-STIC-599B19 - Paso 1 :     EJECUCIÓN FINALIZADA
-----
Presione una tecla para continuar . . .
```

La ejecución del script genera un log, vamos a analizarlo para verificar que todo fue correctamente.

```
plantilla_windows
Archivo   Editar   Ver
Completado el 45 por ciento (57/83)      Área File Security del proceso
Completado el 46 por ciento (38/83)      Área File Security del proceso
Completado el 48 por ciento (39/83)      Área File Security del proceso
Completado el 49 por ciento (40/83)      Área File Security del proceso
Completado el 50 por ciento (41/83)      Área File Security del proceso
Completado el 51 por ciento (42/83)      Área File Security del proceso
Completado el 53 por ciento (43/83)      Área File Security del proceso
Completado el 54 por ciento (44/83)      Área File Security del proceso
Completado el 55 por ciento (45/83)      Área File Security del proceso
Completado el 56 por ciento (46/83)      Área File Security del proceso
Completado el 57 por ciento (47/83)      Área File Security del proceso
Completado el 59 por ciento (48/83)      Área File Security del proceso
Completado el 60 por ciento (49/83)      Área File Security del proceso
Completado el 61 por ciento (50/83)      Área File Security del proceso
Completado el 61 por ciento (50/83)      Área de servicios del proceso
Completado el 73 por ciento (60/83)      Área de servicios del proceso
Completado el 79 por ciento (65/83)      Área de servicios del proceso
Completado el 79 por ciento (65/83)      Área directivas segur. proc.
Completado el 83 por ciento (68/83)      Área directivas segur. proc.
Completado el 87 por ciento (72/83)      Área directivas segur. proc.
Completado el 91 por ciento (75/83)      Área directivas segur. proc.
Completado el 95 por ciento (78/83)      Área directivas segur. proc.
Completado el 100 por ciento (83/83)     Área directivas segur. proc.

La tarea se ha completado. No se encuentran algunos archivos de la configuración en este sistema, por
lo que la seguridad no puede establecerse ni consultarse. Se puede omitir la advertencia.
```

Como podemos ver, está todo bien.



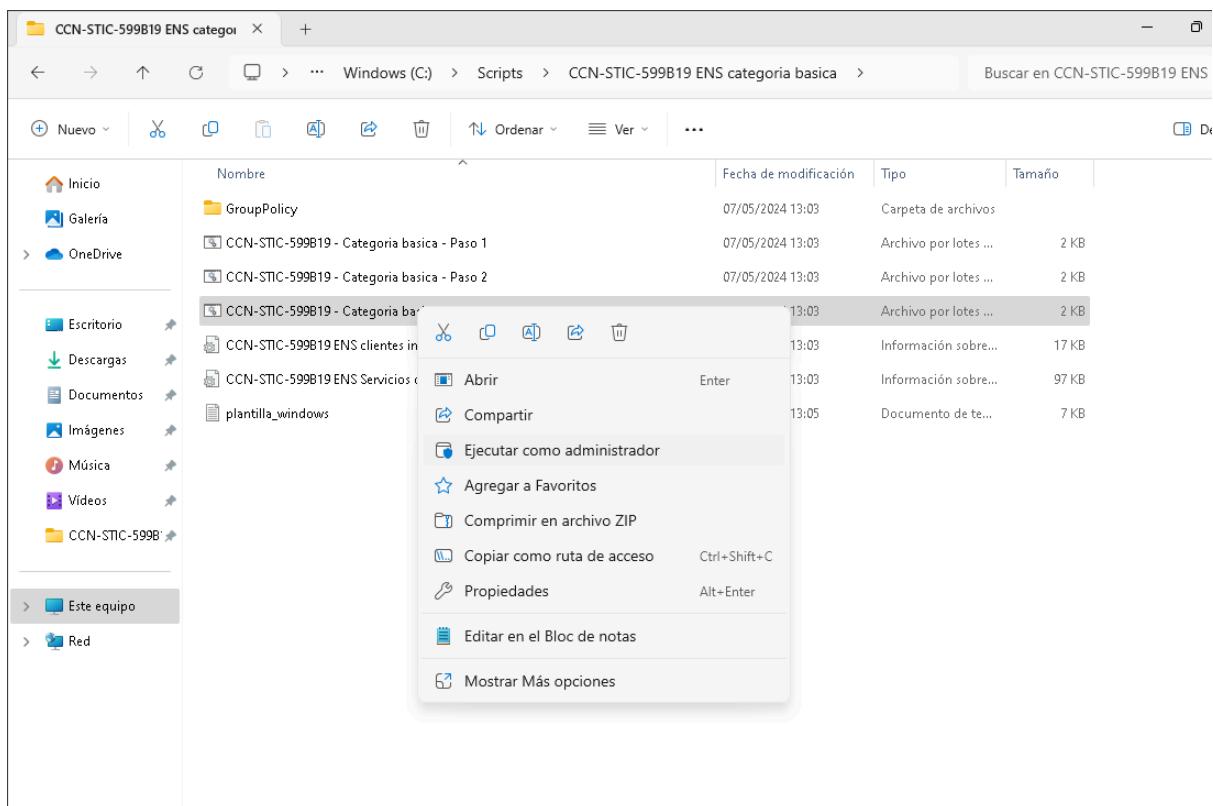
Ejecutamos el segundo paso.

```
C:\Windows\System32\cmd.exe
-----
CCN-STIC-599B19 ENS Cliente Windows 10 Independiente - Paso 2
Categoría basica
-----
Este script copia el objeto de política local a su ubicación
en la carpeta "C:\Windows\System32\groupolicy".
Esta política combina la configuración local de seguridad del
cliente Windows 10 independiente y la establecida para ENS.

Presione una tecla para continuar . . .
C:\Scripts\CCN-STIC-599B19 ENS categoria basica\groupolicy\gpt.ini
C:\Scripts\CCN-STIC-599B19 ENS categoria basica\groupolicy\Machine\comment.cmtx
C:\Scripts\CCN-STIC-599B19 ENS categoria basica\groupolicy\Machine\registry.pol
C:\Scripts\CCN-STIC-599B19 ENS categoria basica\groupolicy\Machine\microsoft\windows nt\SecEdit\GptTmpl.inf
4 archivo(s) copiado(s)

----- CCN-STIC-599B19 - Paso 2 : EJECUCIÓN FINALIZADA -----
Presione una tecla para continuar . . .
```

Posteriormente, ejecutamos el tercer paso.



```
C:\Windows\System32\cmd.exe
CCN-STIC-599B19 ENS Cliente Windows 10 Independiente - Paso 3
Categoría basica

Este script modifica la configuración de inicio de los servicios
requeridos para la seguridad del sistema.

Antes de ejecutar este script asegúrese que los ficheros
y scripts se encuentran en el directorio "C:\Scripts".

Presione una tecla para continuar . . .
Configurando servicios de Windows...

C:\Windows\System32>secedit /configure /quiet /db "c:\scripts\servicios_windows.sdb" /cfg "c:\scripts\CCN-STIC-599B19 ENS
Categoría basica\CCN-STIC-599B19 ENS Servicios categoría basica.inf" /overwrite /log "c:\scripts\CCN-STIC-599B19 ENS c
ategoría basica\servicios_windows.log"

Servicios de Windows configurados.

CCN-STIC-599B19 - Paso 3 :     EJECUCIÓN FINALIZADA
Presione una tecla para continuar . . .
```

Ahora, vemos el fichero ***servicios\_windows.txt***, que es el log de este último paso.

```
plantilla_windows plantilla_windows plantilla_windows servicios_window + - X E
Archivo Editar Ver
+ Completado el 20 por ciento (10/63) Área PRIVILEGE RIGHTS del proceso
Completado el 25 por ciento (15/63) Área Group Membership del proceso
Completado el 49 por ciento (30/63) Área Group Membership del proceso
Completado el 49 por ciento (30/63) Área Registry Keys del proceso
Completado el 49 por ciento (30/63) Área File Security del proceso
Completado el 49 por ciento (30/63) Área de servicios del proceso
Completado el 50 por ciento (31/63) Área de servicios del proceso
Completado el 52 por ciento (32/63) Área de servicios del proceso
Completado el 53 por ciento (33/63) Área de servicios del proceso
Completado el 55 por ciento (34/63) Área de servicios del proceso
Completado el 57 por ciento (35/63) Área de servicios del proceso
Completado el 58 por ciento (36/63) Área de servicios del proceso
Completado el 60 por ciento (37/63) Área de servicios del proceso
Completado el 61 por ciento (38/63) Área de servicios del proceso
Completado el 63 por ciento (39/63) Área de servicios del proceso
Completado el 65 por ciento (40/63) Área de servicios del proceso
Completado el 73 por ciento (45/63) Área directivas segur. proc.
Completado el 73 por ciento (45/63) Área directivas segur. proc.
Completado el 77 por ciento (48/63) Área directivas segur. proc.
Completado el 84 por ciento (52/63) Área directivas segur. proc.
Completado el 88 por ciento (55/63) Área directivas segur. proc.
Completado el 93 por ciento (58/63) Área directivas segur. proc.
Completado el 100 por ciento (63/63) Área directivas segur. proc.

La tarea se ha completado. Han aparecido advertencias acerca de algunos atributos durante esta operación. Se puede omitir la advertencia.

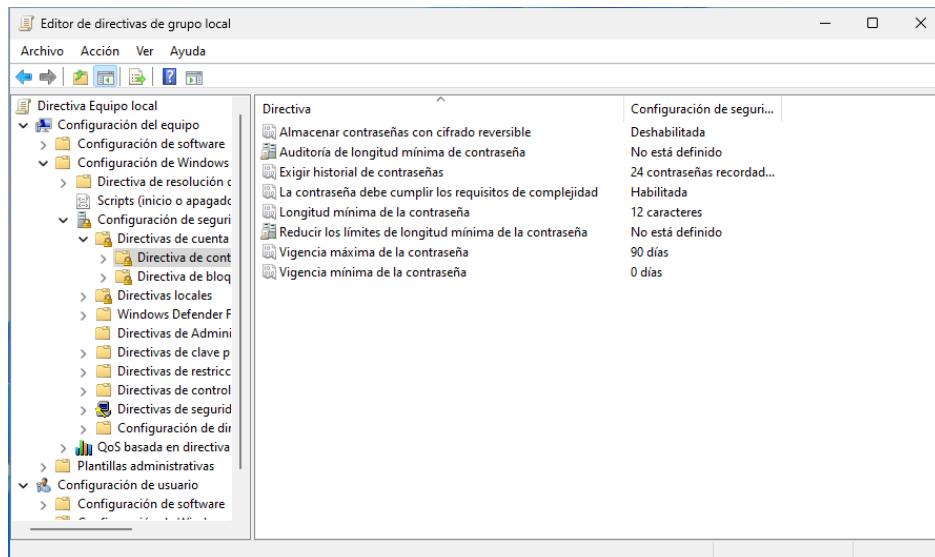
Ln 1, Col 1 | 1.839 caracteres. | 100% | Windows (CRLF) | UTF-16 LE
```

Ahora eliminamos la carpeta **Scripts** previamente creada.

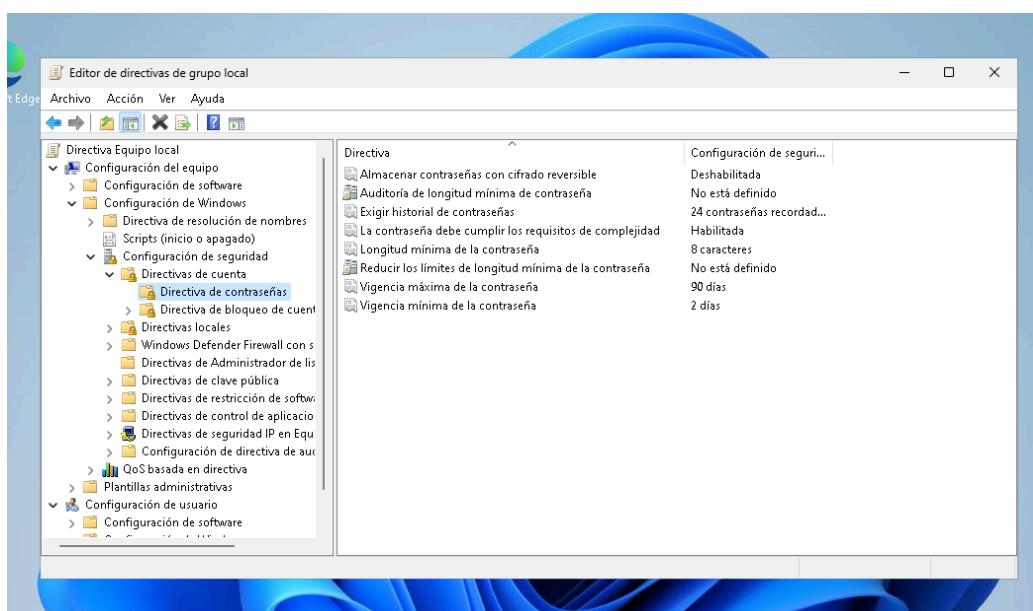
## 2 - ¿Qué diferencias existen comparándolo con el despliegue de seguridad que se realizó con las anteriores prácticas?

### 2.1 - Políticas Contraseñas

En clase hemos definido la siguiente política de contraseñas siguiendo los apuntes dados en clase:



Sin embargo, si vemos la política de contraseñas aplicada por el script, podemos ver que difiere en algunos puntos:

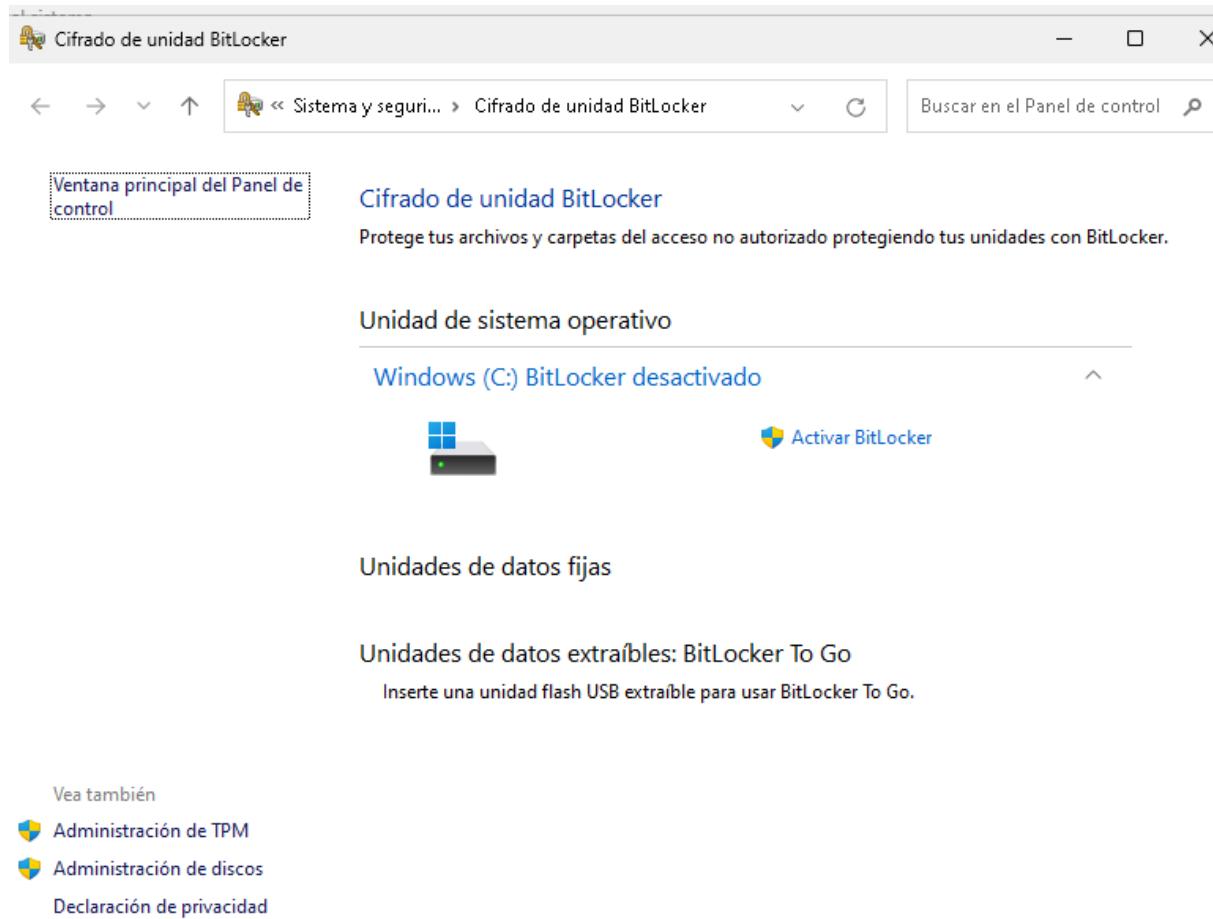


Diferencias:

- Nosotros hemos establecido 12 caracteres de contraseña y el script puso 8.
- Nosotros no hemos definido una vigencia mínima de contraseña y el script establece una de 2 días.

## 2.2 - Bitlocker

En el nivel de seguridad establecido con el script, Bitlocker no se encuentra activado.



The screenshot shows the Windows Control Panel interface. The title bar reads "Cifrado de unidad BitLocker". The left sidebar has a highlighted link "Ventana principal del Panel de control". The main content area is titled "Cifrado de unidad BitLocker" with the sub-instruction "Protege tus archivos y carpetas del acceso no autorizado protegiendo tus unidades con BitLocker". Below this, under "Unidad de sistema operativo", it shows "Windows (C:) BitLocker desactivado" with an "Activar BitLocker" button and a small icon of a hard drive. Further down, under "Unidades de datos fijas", there is a section for "Unidades de datos extraíbles: BitLocker To Go" with the instruction "Inserte una unidad flash USB extraíble para usar BitLocker To Go.". At the bottom, there is a "Vea también" section with links to "Administración de TPM", "Administración de discos", and "Declaración de privacidad".

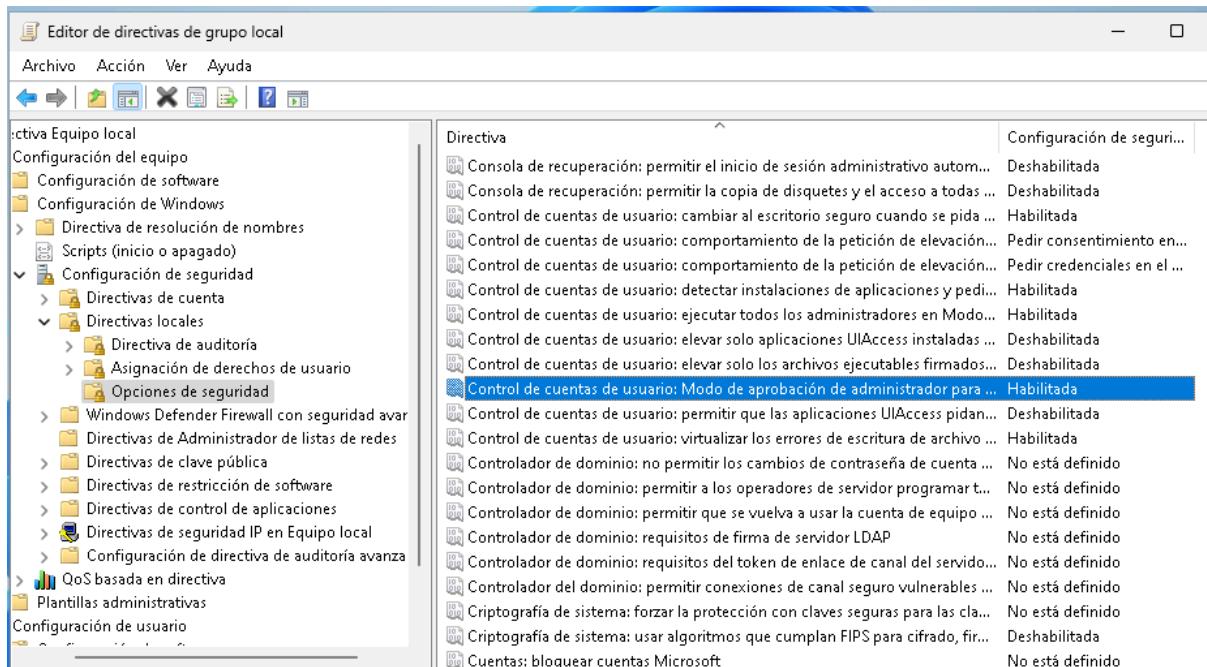
## 2.3 - IPv6

Podemos ver que IPv6 está activado, a pesar de que nosotros lo desactivamos en la práctica

## 2.4 - UAC y políticas de seguridad generales

Nosotros, en las prácticas previas, hemos establecido la configuración que considerábamos que era más oportuna. Sin embargo, el script ha cambiado algunos parámetros que nosotros dejamos tal y como estaban por defecto.

El script también activa la UAC.



The screenshot shows the Windows Local Group Policy Editor window. The left pane displays a tree structure of policy settings under 'Equipo local'. The 'Configuración de seguridad' node is expanded, showing various security-related policies. The 'Control de cuentas de usuario' policy is selected, and its details are shown in the right pane. The specific setting 'Control de cuentas de usuario: Modo de aprobación de administrador para...' is highlighted with a blue selection bar, indicating it is enabled. Other listed policies include 'Consola de recuperación: permitir el inicio de sesión administrativo autom...', 'Control de cuentas de usuario: cambiar al escritorio seguro cuando se pida...', and 'Control de cuentas de usuario: comportamiento de la petición de elevación...'. Most policies are set to 'Deshabilitada' (Disabled), except for the one being viewed which is 'Habilitada' (Enabled).

Directiva	Configuración de seguridad
Consola de recuperación: permitir el inicio de sesión administrativo autom...	Deshabilitada
Consola de recuperación: permitir la copia de discuetos y el acceso a todas ...	Deshabilitada
Control de cuentas de usuario: cambiar al escritorio seguro cuando se pida ...	Habilitada
Control de cuentas de usuario: comportamiento de la petición de elevación...	Pedir consentimiento en el ...
Control de cuentas de usuario: comportamiento de la petición de elevación...	Pedir credenciales en el ...
Control de cuentas de usuario: detectar instalaciones de aplicaciones y pedir...	Habilitada
Control de cuentas de usuario: ejecutar todos los administradores en Modo...	Habilitada
Control de cuentas de usuario: elevar solo aplicaciones UIAccess instaladas ...	Deshabilitada
Control de cuentas de usuario: elevar solo los archivos ejecutables firmados...	Deshabilitada
<b>Control de cuentas de usuario: Modo de aprobación de administrador para ...</b>	<b>Habilitada</b>
Control de cuentas de usuario: permitir que las aplicaciones UIAccess pidan...	Deshabilitada
Control de cuentas de usuario: virtualizar los errores de escritura de archivo ...	Habilitada
Controlador de dominio: no permitir los cambios de contraseña de cuenta ...	No está definido
Controlador de dominio: permitir a los operadores de servicio programar t...	No está definido
Controlador de dominio: permitir que se vuelva a usar la cuenta de equipo ...	No está definido
Controlador de dominio: requisitos de firma de servidor LDAP	No está definido
Controlador de dominio: requisitos del token de enlace de canal del servido...	No está definido
Controlador del dominio: permitir conexiones de canal seguro vulnerables ...	No está definido
Criptografía de sistema: forzar la protección con claves seguras para las cla...	No está definido
Criptografía de sistema: usar algoritmos que cumplan FIPS para cifrado, fir...	Deshabilitada
Cuentas: bloquear cuentas Microsoft	No está definido

## 2.5 - Applocker

A diferencia de nosotros en las prácticas anteriores, el script no configura el applocker.

