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

## 1. Reinicia el equipo y realiza las siguientes tareas

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

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

Iusrmgr - [Usuarios y grupos loo	ales (local)\Usuario	s]			-	×
Archivo Acción Ver Ayuda						
🗢 🄿 🞽 📰 🖸 🗟 🛛						
Usuarios y grupos locales (local) Usuarios Grupos	Nombre	Nombre completo	Descripción Cuenta integrada para la administ Cuenta de usuario administrada p Cuenta integrada para el acceso c Una cuenta de usuario que el siste	Acci	iones larios Acciones adicionales	

Archivo Acción Ver Ayuda

🚁 lusrmgr - [Usuarios y grupos locales (local)\Grupos]

– 🗆 🗙

Usuarios y grupos locales (local)	Nombre	Descripción	Acciones	
Usuarios	Administradores	Los administradores tienen acces	Grupos	
🦰 Grupos	Administradores de H	Los miembros de este grupo tiene	Accience adicionales	
	Duplicadores	Pueden replicar archivos en un do	Acciones adicionales	
	A IIS_IUSRS	Grupo integrado usado por Intern		
	A Invitados	De forma predeterminada, los invi		
	A Lectores del registro d	Los miembros de este grupo pue		
	🜆 Operadores criptográf	Los miembros tienen autorización		
	A Operadores de asisten	Los miembros de este grupo pue		
	A Operadores de config	Los miembros en este equipo pue		
	🜆 Operadores de copia	Los operadores de copia de seguri		
	nopietarios del dispo	Los miembros de este grupo pue		
	🜆 System Managed Acc	Los miembros de este grupo los a		
	A Usuarios	Los usuarios no pueden hacer ca		
	A Usuarios avanzados	Los usuarios avanzados se incluye		
	A Usuarios COM distrib	Los miembros pueden iniciar, acti		
	A Usuarios de administr	Los miembros de este grupo pue		
	🜆 Usuarios de escritorio	A los miembros de este grupo se l		
	🖓 Usuarios del monitor	Los miembros de este grupo tiene		
	🜆 Usuarios del registro d	Los miembros de este grupo pue		

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

#### Get-LocalUser

Seleccionar Windows Pow	verShell		-		×				
Windows PowerShell Copyright (C) Microso	oft Cor	poration. Todos los derechos reservados.							
Instale la versión má	nstale la versión más reciente de PowerShell para obtener nuevas características y mejoras. https://aka.ms/PSWindows								
PS C:\Users\MCBS> Get	S C:\Users\MCBS> Get-LocalUser								
Name En	nabled	Description							
Administrador Fa DefaultAccount Fa Invitado Fa MCBS Tr WDAGUtilityAccount Fa PS C:\Users\MCBS>	alse alse alse rue alse	Cuenta integrada para la administración del equipo o dominio Cuenta de usuario administrada por el sistema. Cuenta integrada para el acceso como invitado al equipo o dominio Una cuenta de usuario que el sistema administra y usa para escenarios de Proteco	ión d	le ap					

 $\times$ 

#### Get-LocalGroup

🔀 Windows PowerShell

ICBS True	
NDAGUtilityAccount False Una cuenta de usua	rio que el sistema administra y usa para escenarios de Protección de ap
PS C:\Users\MCBS> Get-LocalGroup	
vame	Description
Administradores Administradores de Hyper V	Los miembros do este grupo tioner acceso completo y sin restricciones al equi
Dunlicadores de Hyper-V	Dueden penlican anchivos en un dominio
	Grupo integrado usado por Internet Information Services.
Invitados	De forma predeterminada, los invitados tienen el mismo acceso que los
ectores del registro de eventos	Los miembros de este grupo pueden leer registros de eventos del equipo
Operadores criptográficos	Los miembros tienen autorización para realizar operaciones criptográfi
Operadores de asistencia de control de acceso	Los miembros de este grupo pueden consultar de forma remota los atribu
Operadores de configuración de red	Los miembros en este equipo pueden tener algunos privilegios administr
Operadores de copia de seguridad	Los operadores de copia de seguridad pueden invalidar restricciones de
Propietarios del dispositivo	Los miembros de este grupo pueden cambiar la configuración de todo el
System Managed Accounts Group	Los miembros de este grupo los administra el sistema.
Jsuarios	Los usuarios no pueden hacer cambios accidentales o intencionados en e
Jsuarios avanzados Jsuarios COM distribuidos	Los usuarios avanzados se incluyen para la compatibilidad con versione
Jsuarios com distribuidos	Los miembros pueden iniciar, activar y usar objetos de com distribuido
Isuarios de acemitaria nomata	A los miembros de este grupo pueden acceder a los recursos de writ median
Isuarios del monitor de sistema	Los miembros de este grupo se les concede el derecho de inicial sesi
Isuarios del registro de rendimiento	los miembros de este grupo pueden programar contadores de registro y r
starios del registro de l'endimiento	eos miemoros de este grupo paeden programar contadores de registro y riti
PS C:\Users\MCBS>	

#### Crea un usuario del grupo usuario de 2 formas distintas

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

$\leftarrow$	Configuración		— (	) ×
	MCBS Cuenta local	Cuentas > Otros usuarios		
		Otros usuarios		
Bus	car una configuración Q	Agregar otro usuario	Agregar cuen	ita
	Sistema			
8	Bluetooth y dispositivos	Configurar un quiosco multimedia		
-	Red e Internet	Quiosco multimedia           Convertir este dispositivo en un quiosco para utilizarlo como cartel digital, pantalla interactiva u otras cosas	Comenzar	
1	Personalización			
	Aplicaciones	Q Obtener ayuda		
12	Cuentas	Enviar comentarios		

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

← Configuración			- 0 ×
MCBS Cuenta local	Cuentas > Otros usuarios	5	
	Otros usuarios		
Buscar una configuración	Q	×	Agregar cuenta
Sistema			
8 Bluetooth y dispositivos	Microsoft		
💎 Red e Internet	·Cémo iniciaré co	sién asta	Comenzar
🥖 Personalización	persona?	esion esta	
Aplicaciones	Escribe la dirección de correc	o electrónico o el	
l 💄 Cuentas	número de teléfono de la pe agregar. Si usa Windows, Ofi OneDrive, Skyre o Xboy, esc	rrsona que quieres fice, Outlook.com, rribe la dirección de	
🕥 Hora e idioma	correo electrónico o el núme	ero de teléfono que usa	
😳 Juegos	para iniciar sesión.		
<b>4</b>	Correo electrónico o teléfon	o	
Accesibilidad			
Privacidad y seguridad	No tengo los datos de inicio de	e sesion de esta persona	
Ø Windows Update	Cano	celar Siguiente	
		Términos de uso Privacidad y cookies	

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

← Configuración		
MCBS Cuenta local	Cuentas > Otros usuarios	
Buscar una configuración Q	Otros usuarios Cuenta de Microsoft	x
Sistema		Agregar cuenta
8 Bluetooth y dispositivos		
Red e Internet		Comenzar
🥖 Personalización	Microsoft	
Aplicaciones	Crear cuenta	
Cuentas	alguien@example.com	_
Juegos	Obtener una nueva dirección de correo electró	ónico
🕇 Accesibilidad	Atrác S	initiante
Privacidad y seguridad	Autos	
Windows Update		

Tras eso nos permitirá crear un nuevo usuario:

	MCBS Cuenta local	Cuentas > Otros usuarios	
	Cacina local	Otros usuarios	
	r	Cuenta de Microsoft X	
Bus	car una configuración Q		Agregar cuenta
	Sistema	Crear un usuario para este equipo	
8	Bluetooth y dispositivos		
•	Red e Internet	Si esta cuenta es para niños o adolescente, considera la posibilidad de seleccionar <b>volver</b> y crear una cuenta Microsoft. Cuando los miembros de la familia más jóvenes inicien sesión con una cuenta de Microsoft, tendrán protección de privacidad centrada	Comenzar
/	Personalización	en su edad.	
*	Aplicaciones	Si quieres usar una contraseña, elige algo que te resulte fácil de recordar, pero que sea	
• •	Cuentas		
0	Hora e idioma	¿Quién va a usar este PC?	
•	Juegos	NuevoUsuarioGUI ×	
×	Accesibilidad	Dale seguridad.	
$\square$	Privacidad y seguridad	Introducir la contraseña	
8	Windows Update	Volver a introducir la contraseña	
		Siguiente Atrás	

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

$\leftarrow$	Configuración		– o ×
	MCBS Cuenta local	Cuentas > Otros usuarios	
		Otros usuarios	
Bus	car una configuración Q	Agregar otro usuario	Agregar cuenta
	Sistema		
8	Bluetooth y dispositivos	NuevoUsuarioGUI     Cuenta local	~
-	Red e Internet		
	Personalización	Configurar un quiosco multimedia	
	Aplicaciones	Quiosco multimedia           Convertir este dispositivo en un quiosco para utilizarlo como cartel digital, pantalla interactiva u otras cosas	Comenzar
12	Cuentas		
5	Hora e idioma	le Obtener ayuda	
•	Juegos	Enviar comentarios	
- 🕹	A 111111		

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

Last update: 2025/04/01 15:33



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

New-LocalUser -Name NuevoUsuarioPS



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

Add-LocalGroupMember -Group Usuarios -Member nuevoUsuarioPS

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

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

Propiedades: Usuarios	?	$\times$
General		
Usuarios		
Descripción: Los usuarios no pueden hacer cambios accidentales	so <u>, .</u>	
Miembros:		
MCBS NT AUTHORITY\INTERACTIVE (S-1-5-4) NuevoUsuarioGUI InuevoUsuarioPS		
Agregar Quitar Cualquier cambio en la pertenence de usuarios no surtirá efecto hasta usuario inicie sesión de nuevo.	ia a grupo a que el	)S
Aceptar Cancelar Aplicar	Ауц	ıda

## 2. Revisa y documenta los siguientes puntos

#### Como podemos saber el estado de la licencia del sistema operativo

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

← Configuración		- 0 ×
MCBS Cuenta local	Sistema	
Buscar una configuración Q	MCBSW11 VirtualBox Cambiar nombre	<ul> <li>Windows Update</li> <li>Requiere atención</li> </ul>
Sistema		
8 Bluetooth y dispositivos	Windows no está activado.	Activar ahora
Red e Internet		
🥖 Personalización	Pantalla     Monitores, brillo, luz nocturna, perfil de pantalla	>
Aplicaciones	- Sanida	
💄 Cuentas	Solito     Niveles de volumen, salida, entrada, dispositivos de sonido	>
🕥 Hora e idioma	○ Notificaciones	
😳 Juegos	Alertas de aplicaciones y sistema, no molestar	
X Accesibilidad	O Concentración Reducir las distracciones	>
<ul> <li>Windows Update</li> </ul>	U Energía y batería Suspensión, uso de la batería, ahorro de batería	>
	Almacenamiento     Espacio de almacenamiento, unidades, reglas de configuración	>
	Uso compartido en proximidad Detectabilidad, ubicación de archivos recibidos	>
	Acoplar ventanas, escritorios, cambio de tareas	>
	ዋስ Para programadores	>
	🖶 🔍 Búsqueda 🛛 😻 🧟 🖬 🖕 😭 📾 👫 🍇 🧕 💆 🖉 🗠 🗠 ESP	「計 di) <b>御</b> 15:33 🌲 01/04/2025

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

Q	activ			
$\leftarrow$	Todo Aplicaciones Docume	ntos V	Veb Configuración Carpetas 🕨 💀 🖓	
Mejo	or coincidencia			
0	Ver si Windows está activado Configuración del sistema		$\bigcirc$	
Con	figuración		Ver si Windows está activado	
	Activar o desactivar las características de Windows	>		
÷	Activar el Modo Juego	>	🖸 Abrir	
2	Activar o desactivar el protector de pantalla	>	Obtén ayuda rápida desde Internet Buscar la clave de producto	×
Buse	car en Internet			
Q	<b>activ</b> - Ver más resultados de la búsqueda	>		
All VEIDA	Activision	>		
Q	activar bluetooth	>		2
Q	activar windows	>		
Q	activision ban appeal	>		

← Configuración		- a ×
MCBS Cuenta local	Sistema > Activación	
Buscar una configuración Q	Windows 11 Enterprise	
Sistema		
8 Bluetooth y dispositivos	Estado de activación	No está activo  🐧 🔨
Red e Internet     Personalización	No es posible activar Windows en este dispositivo porque la clave de producto ya se ha usado en otro dispositivo. Si crees que no se ha usado en otro dispositivo, selecciona Solución de problemas, a continuación. Código de error: 0xC004C020	Solucionar problemas
Cuentas	Cambiar la clave de producto	Cambiar
🕥 Hora e idioma	Obtener ayuda	Abrir Obtener ayuda
🥶 Juegos 🏌 Accesibilidad	D Id. del producto	00329-10430-00098-AA232
<ul> <li>Privacidad y seguridad</li> <li>Windows Update</li> </ul>	Clave de producto	XXXX-XXXX-XXXX-TMT44
	Soporte técnico relacionado	
	Ayuda con Activación	^
	Vinculación de una cuenta de Microsoft a una licencia digital Comprobar si tu Windows está activado Activar Windows con clave de producto	
	Obtener ayuda	
	🖬 Q Búsqueda 😻 🤽 🦛 🖬 🔚 💼 🍇 💩 🙋 🔼 🗠 🗞	ESP 🖵 🕬 🖢 15:38 🌻

### ¿Está activo el DEP?¿Dónde podemos verlo?

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

Cuenta local		.1011	
scar una configuración Q	MCBSW11 VirtualBox		Cambiar el nombre de este equipo
Sistema	Especificaciones del dispositivo	3	Copiar
Bluetooth y dispositivos			
Red e Internet	Nombre del dispositivo Procesador	MCBSW11	
	RAM instalada	6.03 GB	
Personalización	Identificador de dispositivo	EC160C62-8EE9-42B5-87FB-7DFA892F6278	
Aplicaciones	ld. del producto	00329-10430-00098-AA232	
	Tipo de sistema	Sistema operativo de 64 bits, procesador basado en x64	
Cuentas	Lápiz y entrada táctil	La entrada táctil o manuscrita no está disponible para esta pantalla	3
Juegos Accesibilidad	Vinculos relacionados Dominio o g	grupo de trabajo Protección del sistema Configuración avanzad	a del sistema
Privacidad y seguridad			
Windows Update	Edición	Windows 11 Enterprise	
	version	23H2 30/03/2024	
	Versión del sistema operativo	22631 2861	
	Experiencia	Windows Feature Experience Pack 1000,22681,1000,0	
	Contrato de servicios de Micro Términos de licencia del softwa	soft are de Microsoft	
	Contrato de servicios de Micro Términos de licencia del softwa Relacionado	soft are de Microsoft	

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

Nombre de equ	ipo	Hardware
Opciones avanzadas	Protección del sistema	Acceso remot
Para realizar la mayoría de Rendimiento	e estos cambios, inicie sesión	como administrador
Para realizar la mayoría de Rendimiento Efectos visuales, prograr memoria virtual	e estos cambios, inicie sesión mación del procesador, uso de	como administrador e memoria y

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

noto dor. ón de datos e ayuda a e seguridad. ndows epto los que	pones avanzadas       Protección del sistema       Acceso remoto         realizar la mayoría de estos cambios, inicie sesión como administrador.       Iniciante         Opciones de rendimiento       Efectos visuales       Opciones avanzadas         Prevención de ejecución de ejecución de datos       Iniciante         Image: Como functional       Iniciante         Opciones avanzadas       Prevención de ejecución de datos         Image: Como functional       Iniciante         Opciones avanzadas       Prevención de ejecución de datos         Image: Como functional       Iniciante         Opciones avanzadas       Prevención de datos (DEP) le ayuda a protegerse contra virus y otras amenazas a la seguridad.         Cómo functional       Opciones y servicios de Windows erencialer	BSW11 ualBox Para Especificaciones del disposi Nombre del dispositivo Procesador Co
ón de datos e ayuda a seguridad. ndows pto los que	ealizar la mayoría de estos cambios, inicie sesión como administrador. diminate Opciones de rendimiento Efectos visuales Opciones avanzadas Prevención de ejecución de datos La Prevención de ejecución de datos (DEP) le ayuda a protegerse contra virus y otras amenazas a la seguridad. Cómo funcionas Activar DEP solo para los programas y servicios de Windows esenciales	Para Para Especificaciones del disposi Nombre del dispositivo Procesador Co
ón de datos e ayuda a seguridad. ndows epto los que	Opciones de rendimiento  Efectos visuales Opciones avanzadas Prevención de ejecución de datos  La Prevención de ejecución de datos (DEP) le ayuda a protegerse contra virus y otras amenazas a la seguridad. Cómo funciona3  Activar DEP solo para los programas y servicios de Windows erencialer.	Especificaciones del disposi Nombre del dispositivo Procesador Co
x con de datos e ayuda a i seguridad. indows ipto los que	Opciones de rendimiento         Efectos visuales       Opciones avanzadas       Prevención de ejecución de datos         Image: State of the state of t	Especificaciones del disposi Nombre del dispositivo Procesador Co
ón de datos copiar e ayuda a seguridad. ndows epto los que	Efectos visuales       Opciones avanzadas       Prevención de ejecución de datos         Image: Strain	Especificaciones del disposi Nombre del dispositivo Procesador Co
e ayuda a i seguridad. ndows ipto los que	<ul> <li>La Prevención de ejecución de datos (DEP) le ayuda a protegerse contra virus y otras amenazas a la seguridad.</li> <li>Cómo funcional</li> <li>Activar DEP solo para los programas y servicios de Windows esenciales</li> </ul>	Nombre del dispositivo Procesador DAM instalado
e ayuda a seguridad. ndows pto los que	<ul> <li>La Prevención de ejecución de datos (DEP) le ayuda a protegerse contra virus y otras amenazas a la seguridad.</li> <li>Activar DEP solo para los programas y servicios de Windows especiales</li> </ul>	Procesador Co
ndows pto los que	Activar DEP solo para los programas y servicios de Windows eservicias	PAM instalada
ndows pto los que	<ul> <li>Activar DEP solo para los programas y servicios de Windows esenciales</li> </ul>	E / 1 1 / 1 / 1 / 1 / 1 / 1 / 1 / 1 / 1
pto los que	esenciales	
pto los que	escriciales	
	<ul> <li>Activar DEP para todos los programas y servicios excepto los que seleccione:</li> </ul>	Id. del producto
		Tipo de sistema
		Lápiz y entrada táctil
lel sistema		culos relacionados Dominio
Copiar		Especificaciones de Window
		Edición V
		Versión 2
Quitar	Agregar Quitar	Instalado el 3
en	El procesador del equipo es compatible con DEP basado en	Versión del sistema operativo
	hardware.	Experiencia
		Contrata da sanúcios da Misrasoft
		Términos de licencia del software o
Aplicar	Aceptar Cancelar Aplicar	leminos de licencia del software d
Quitar en Aplicar	Agregar Quitar El procesador del equipo es compatible con DEP basado en hardware. Aceptar Cancelar Aplicar	Edición V Versión 2 Instalado el 3 Versión del sistema operativo 2 Experiencia V Contrato de servicios de Microsoft Términos de licencia del software d

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

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

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

← Configuración		– D ×
MCBS Cuenta local	Windows Update > Opciones avanzadas	
Buscar una configuración Q	O Recibir actualizaciones de otros productos de Microsoft Obtenga las actualizaciones de Microsoft Office y otras junto con las de Windows	Desactivado
<ul> <li>Sistema</li> <li>Bluetooth y dispositivos</li> </ul>	Ponme al día Reiniciar lo antes posible (incluso durante las horas de actividad) para terminar la actualización, y notificarme 15 minutos antes de reiniciar para que pueda asegurarme de que este dispositivo está encendido y enchufado	Desactivado 🔵
<ul> <li>Red e Internet</li> <li>Personalización</li> </ul>	Descargar actualizaciones en conexiones de uso medido     Pueden aplicarse cargos de datos	Desactivado 🕚
Aplicaciones	Q Notificarme cuando sea necesario reiniciar para finalizar la actualización Muestra una notificación cuando el dispositivo requiere un reinicio para terminar la actualización	Desactivado
<ul> <li>Guerras</li> <li>Hora e idioma</li> </ul>	S Horas activas Actualmen No reiniciaremos su dispositivo durante estas horas	te de 8:00 a 17:00 🗸
<ul> <li>Juegos</li> <li>Accesibilidad</li> </ul>	Opciones adicionales	
Privacidad y seguridad	Actualizaciones opcionales     Actualizaciones de características, calidad y controladores	Disponible: 1 >
Vindows Opdate	Dptimización de distribución Límites de ancho de banda para actualizaciones, descargas de otros dispositivos	>
	五 Recuperación Reiniciar, inicio avanzado, volver	>
	Co Reiniciar las aplicaciones Guardar automáticamente las aplicaciones reiniciables al cerrar sesión y reiniciarlas después de iniciar sesión	>
	Directivas de actualización configuradas	>

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

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

.\icacls.exe C:\ /T



Donde los permisos son:

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

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

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

Administrador de tareas: <ul> <li>Busque un nombre, publicador o PID</li> <li>Aplicaciones de arranque</li> <li>Ege Ejecutar nueva tarea</li> <li>Habilitar</li> <li>O cetababilitar</li> <li>Propiedades</li> <li>Outimo tiempo de BIOS: 1.6 segundos</li> </ul> <li>Nombre</li> <li>Anunciante</li> <li>Etado</li> <li>Impacto de ini</li> <li>O concebrixe (0)</li> <li>SecurityHealthSystray</li> <li>Spotify AB</li> <li>Deshabilitado</li> <li>Ninguno</li> <li>Bajo</li> <li>VBox Tray</li> <li>VBox Tray</li> <li>Sotify AB</li> <li>SecurityHealthSystray</li> <li>Spotify AB</li> <li>SecurityHealthSystray</li> <li>Spotify AB</li> <li>Deshabilitado</li> <li>Ninguno</li> <li>VBox Tray</li> <li>VBox Tray</li>	2025	/04/01 15:33	15/28		[Fo	rt] Práctica	7: Configuraci	ón general de Wir	ndows 11 y secu	urización
Apicaciones de arranque	<u>, 1 1</u>	Administrador de tareas		Q Busq	ue un nombre, p	oublicador o	PID		– u	^
Image: Property of the second of the sec	≡	Aplicaciones de arra	anque		Ejecutar	nueva tarea	🗸 Habilitar	🖉 Deshabilitar	E Propiedades	
Nombre       Anunciante       Estado       Impacto de ini         Impacto de ini       Habilitado       Alto         Impacto de ini       Impacto de ini       Habilitado       Bajo         Impacto de ini       Spotify HealthSystray       Spotify AB       Deshabilitado       Ninguno         Impacto de ini       Impacto de ini       Habilitado       Bajo         Impacto de ini       Impacto de ini       Habilitado       Bajo         Impacto de ini       Impacto de ini       Impacto de ini         Impacto de ini       Spotify HealthSystray       Spotify AB       Deshabilitado       Ninguno         Impacto de ini         Impacto de ini       Impacto de ini       Impacto de ini       Impacto de ini       Impacto de ini         Impacto de initiano       Spotify AB       Deshabilitado       Ninguno       Impacto de ini       Impacto de ini         Impacto de initiano       Microsoft Corporation       Deshabilitado       Bajo       Impacto de ini         Impacto de initiano         Impacto de initin	₽							Último tie	mpo de BIOS: 1.6 se	egundos
<ul> <li>OneDrive (6)</li> <li>Security HealthSystray</li> <li>Spotify</li> <li>Terminal</li> <li>Vox Tray</li> </ul>	4-	Nombre		Anunciante	Estado	Impacto de	ini			
<ul> <li>SecurityHealthSystray Spotify</li> <li>Spotify AB</li> <li>Deshabilitado</li> <li>Ninguno</li> <li>Deshabilitado</li> <li>Ninguno</li> <li>VBoxTray</li> </ul>	U	> 🦲 OneDrive (6)			Habilitado	Alto				
Spotify     Spotify AB     Deshabilitado     Ninguno       Image: Terminal     Microsoft Corporation     Deshabilitado     Ninguno       Image: VBox Tray     Habilitado     Bajo	r.y.	SecurityHealth	Systray		Habilitado	Bajo				
Image: Solution in Terminal     Microsoft Corporation     Deshabilitado     Ninguno       Image: Solution in Terminal     VBox Tay     Habilitado     Bajo	00	Spotify	5	Spotify AB	Deshabilitado	Ninguno				
VBoxTray Habilitado Bajo	ö	Terminal	I	Microsoft Corporation	Deshabilitado	Ninguno				
	i≡	🥳 VBoxTray			Habilitado	Bajo				
	ŝ									
	£\$3									

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

Archivo Edición Ver Favoritos Ayuda Equipo\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	
Equipo\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	
> Diagnostics     Nombre     Tipo     Datos       > Explorer     B()Predeterminado)     REG_SZ     (valor no establecido)       > Ext     B()Predeterminado)     REG_SZ     "C:\Users\MCBS\AppData\Local\Microsoft\OneDr"       > Feeds     FileHistory     B()Predeterminado)     REG_SZ     "C:\Users\MCBS\AppData\Local\Microsoft\OneDr"       > Group Policy     FileHistory     FileHistory     FileHistory     FileHistory       > Group Policy     FileHistory     FileHistory     FileHistory       > Group Policy     FileHistory     FileHistory       > Group Policy     FileHistory     FileHistory       > Group Policy     FileHistory     FileHistory       > InstraitService     FileHistory     FileHistory       > Internet Settings     FileHistory       > Internet Settings     FileHistory       > Nohtifications     FileHistory       > OOBE     FileHistory       > PrevisionTouchPad     FileHistory       > Privacy     FileHistory	

## 3. Realiza las siguientes tareas

### Deshabilitar la gestión de hibernación del equipo

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

powercfg /hibernate off

```
Administrador: Windows PowerShell
PS C:\Windows\system32> powercfg /hibernate off
PS C:\Windows\system32> _
```

#### Deshabilita las conexiones de asistencia remota al equipo

Vamos al menú windows y escribimos asistencia remota:

Q asistencia re		
Codo Aplicaciones Document	os W	Veb Configuración Carpetas 🕨 … 🌍
Mejor coincidencia		
Permitir que este equipo envíe invitaciones de Asistencia remota Panel de control		
Buscar en Internet		Permitir que este equipo envíe invitaciones de Asistencia remota
Q <b>asistencia re</b> - Ver más resultados de la búsqueda	>	Panel de control
Q asistencia remota windows 10	>	🖸 Abrir
Q asistencia remota windows 11	>	
Q asistencia remota de windows	>	
Q asistencia re <b>unión apoderados</b>	>	
Q asistencia remesas banco atlántida	>	
Q asistencia re <b>unión</b>	>	
Q asistencia remota chrome	>	
Q asistencia re <b>mota google</b>	>	

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

Propiedades del sistema			>		
Nombre de equi	ро		Hardware		
Opciones avanzadas	Protección de	l sistema	Acceso remoto		
Asistencia remota          Permitir conexiones de Asistencia remota a este equipo         ¿Qué sucede si se habilita Asistencia remota?					
		Opcione	es a <u>v</u> anzadas		
Escritorio remoto Haga clic en una opción y O permitir las conexio	y especifique quié ones remotas a est	n puede con te equipo	ectarse.		
<ul> <li>Permitir las conexiones</li> </ul>	s remotas a este e	quipo			
Permitir solo las con Escritorio remoto co (recomendado)	ne <u>x</u> iones desde eo on Autenticación a	quipos que ej a nivel de red	jecuten J		
<u>Ayudarme a eleqir</u>		Selecció	onar usuarios		
	Aceptar	Cance	elar Apli <u>c</u> ar		

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

MCBS Cuenta local	Sistema > Informa	ción	
uscar una configuración O	MCBSW11 VirtualBox		Cambiar el nombre de este equi
Sistema	i Especificaciones del dispositivo	0	Copiar
Bluetooth y dispositivos	Nombre del dispositivo	MCRSW11	
Red e Internet	Procesador	Intel(R) Core(TM) i5-8250U CPU @ 1.60GHz 1.80 GHz	
Personalización	RAM instalada Identificador de dispositivo	6,03 GB EC160C62-8EE9-42B5-87FB-7DFA892F6278	
Aplicaciones	Id. del producto	00329-10430-00098-AA232	
Cuentas	Tipo de sistema Lápiz y entrada táctil	Sistema operativo de 64 bits, procesador basado en x64 La entrada táctil o manuscrita no está disponible para esta pantalla	a
Hora e idioma			
Juegos	Vinculos relacionados Dominio o	grupo de trabajo Protección del sistema Configuración avanzad	a del sistema
Accesibilidad			

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

En la ventana que sale presionamos en configurar:

Ę

Propiedades del sistema				×
Nombre de equipo		H	Hardware	
Opciones avanzadas	Protección del	sistema	Acceso remoto	)
Use Protección del sistema para deshacer cambios no deseados en el sistema.				
Restaurar sistema				-
Puede deshacer cambios del s revirtiendo el equipo a un punt restauración anterior.	sistema o de	Resta	aurar sistema	
Configuración de protección				-
Unidades disponibles		Protección		
📥 Windows (C:) (Sistema)		Desactivad	a	
Establezca la configuración d administre el espacio en disco de restauración. Para crear un punto de restau primero la protección; para el unidad y haga clic en Configu	le restauración o y elimine pun uración, habilite lo, seleccione e urar.	tos (	Configurar Crear	
	Aceptar	Cance	lar Aplica	r

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

Protección del sistema para Windows (C:)	×
Configuración de restauración	_
La protección del sistema permite deshacer cambios no deseados si se revierte el equipo a un momento dado anterior.	
<ul> <li>Activar protección del sistema</li> </ul>	
O Deshabilitar protección del sistema	
Uso del espacio en disco	_
Puede ajustar el espacio máximo en disco que se usará para la protección d sistema. Según se va llenando el espacio, se irán eliminando los puntos de restauración anteriores para dar cabida a los nuevos.	el
Uso actual: 0 bytes	
Uso máximo:	
15% (11,92 GB)	
Eliminar todos los puntos de restauración de esta unidad.	)
Aceptar Cancelar Aplicar	)

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

Q rendimiento	
← Todo Aplicaciones Documento	s Web Configuración Carpetas 🕨 … 🌍
Mejor coincidencia	
Monitor de <b>rendimiento</b> Sistema	
Configuración	Monitor de rendimiento
Ajustar la apariencia y <b>rendimiento</b> de Windows	>
Rendimiento y estado del dispositivo	<ul> <li>Abrir</li> <li>Ejecutar como administrador</li> </ul>
🌮 Configuración del Modo Juego	> Abrir ubicación de archivo
Optimizar el dispositivo en función del uso y el <b>rendimiento</b> de la	<ul> <li>Anclar a Inicio</li> <li>Anclar a la barra de tareas</li> </ul>
Buscar en Internet	
Q <b>rendimiento</b> - Ver más resultados de la búsqueda	>
Q rendimiento afore 2025	>
Q rendimiento afore 2024	
Q rendimiento <b>afore</b>	>

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

Opciones de ren	dimiento		2
Efectos visuales	Opciones avanzadas	Prevención de ejecución de datos	
Elija la configu de Windows e	iración que desea usa n este equipo.	ar para la apariencia y rendimiento	
O Dejar que V equipo	Vindows elija la confi	guración más adecuada para el	
🔿 Ajustar par	a obtener la mejor ap	ariencia	
🔿 Ajustar par	a obtener el mejor re	ndimiento	
O Personaliza	r:		
Animacio	nes en <mark>la barra de ta</mark> r	eas	1
🗹 Animar la	s ventanas al minimiz	zar y maximizar	
🗹 Animar lo	s controles y elemen	tos dentro de las ventanas	
Atenuar lo	os elementos despuér	s de hacer clic	

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

Opciones de ren	dimiento		×
Efectos visuales	Opciones avanzadas	Prevención de eje	cución de <mark>d</mark> atos
Programació Elija cómo o	ón del procesador desea asignar los recu	irsos del procesad	or.
Ajustar para	n mejorar el rendimie	nto de:	
O Program	as O Se	rvicios en segund	o plano
Memoria vir	tual		
Un archivo Windows us	de paginación es un sa como si fuese RAN	área en el disco dι 1.	iro que
Tamaño tot para todas l	al del archivo de pagi as unidades:	inación 1728 N	ИВ
			Cambiar

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

Nemoria virtual X				
Administrar automáticamente el tamaño del archivo de paginación para todas las unidades				
<b>Tamaño del archivo de paginación para cada unidad</b> Unidad [etiq, de volumen] Tamaño del arch, de paginación (MB)				
[C: [///indows] Administrado por el sistem				
Unidad seleccionada: C: [Windows] Espacio disponible: 59344 MB				
─ Tamaño personalizado: Tamaño inicial (MB):				
Tamaño máximo (MB):				
<ul> <li>Tamaño administrado por el sistema</li> <li>Sin archivo de paginación</li> <li>Establecer</li> </ul>				
Tamaño total del archivo de paginación para todas las unidades Mínimo permitido: 16 MB Recomendado: 1667 MB Asignado actualmente: 1728 MB				
Aceptar Cancelar				

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

Opciones de rendimiento					
Efectos visuales (	Opciones avanzadas	Prevención de ejecución	de datos		
Elija la configuración que desea usar para la apariencia y rendimiento de Windows en este equipo.					
O Dejar que Wi equipo	indows elija la config	guración más adecuada	para el		
Ajustar para	obtener al mejor ap	dimiente			
	obtener er mejor rer	laimiento			
O Personalizar:					
<ul> <li>Animaciones en la barra de tareas</li> <li>Animar las ventanas al minimizar y maximizar</li> <li>Animar los controles y elementos dentro de las ventanas</li> <li>Atenuar los elementos después de hacer clic</li> <li>Atenuar o deslizar la información sobre herramientas en la vista</li> <li>Atenuar o deslizar los menús en la vista</li> <li>Deslizar los cuadros combinados al abrirlos</li> <li>Desplazamiento suave de los cuadros de lista</li> <li>Guardar vistas previas de miniaturas de la barra de tareas</li> <li>Habilitar Peek</li> <li>Mostrar el contenido de la ventana mientras se arrastra</li> <li>Mostrar sombra bajo el puntero del mouse</li> <li>Mostrar sombras bajo las ventanas</li> <li>Mostrar vistas en miniatura en lugar de iconos</li> <li>Suavizar bordes para las fuentes de pantalla</li> <li>Usar sombras en las etiquetas de iconos en el Escritorio</li> </ul>					
	Ace	ptar Cancelar	Aplicar		

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

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

	Fecha y hora	× > Fecha y hora	
-	Fecha y hora Relojes adicionales Hora de Internet		
usc	Este equipo está configurado para sincronizarse automáticamente con "time.windows.com".	e verano automáticamente	Activado
	Este equipo está configurado para sincronizarse automáticamente de form	utomáticamente	Activado 💽
•	programada.	Configuración de hora de Internet  Configure la hora de Internet:	Activado 💽
•	Cambiar la configuración	Sincronizar con un servidor horario de Internet Servidor: roa.hora.es	
		Este equipo está configurado para sincronizarse automáticamente de forma programada.	Sincronizar ahora
0 7	Aceptar Cancelar Aplicar	Aceptar Cancelar	No mostrar calendarios adicionales 🛛 🗸
	Privacidad y seguridad Vínculos relacionados		
Ð	Windows Update Market Mindows y algun	n as aplicaciones formatean las fechas y la hora en función de su región	>
	Relojes adicionales Relojes para zonas horari	ias diferentes	ß

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

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

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

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

Pulsamos Windows+R y Escribimos gpedit.msc:

🧾 Editor de directivas de g	rupo local		-	×
Archivo Acción Ver Ayuda				
<ul> <li>Directiva Equipo local</li> <li>Configuración del ec</li> <li>Configuración de</li> <li>Configuración de</li> <li>Plantillas adminis</li> <li>Configuración de usi</li> <li>Configuración de</li> <li>Configuración de</li> <li>Plantillas adminis</li> </ul>	Directiva Equipo local Seleccione un elemento para ver su descripción.	Nombre R Configuración del equipo Configuración de usuario		
	Extendido Estándar			
	(/			

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

#### Configuración directivas de grupo local I

Configuración del equipo  $\rightarrow$  Configuración de Windows  $\rightarrow$  Configuración de seguridad  $\rightarrow$  Directivas de cuenta  $\rightarrow$  Directiva de contraseñas



En esta sección podemos encontrar las siguientes directivas:

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

#### Configuración de directivas de grupo local II

Configuración del equipo  $\rightarrow$  Configuración de Windows  $\rightarrow$  Configuración de seguridad  $\rightarrow$  Directivas locales  $\rightarrow$  Opciones deSeguridad

Editor de directivas de grupo local			_	×
Archivo Acción Ver Ayuda				
💠 🔿 🚾 🗙 🗟   🛛 🖬				
<ul> <li>Directiva Equipo local</li> <li>Configuración del equipo</li> <li>Configuración de software</li> <li>Configuración de Windows</li> <li>Directiva de resolución de nombres</li> <li>Scripts (inicio o apagado)</li> <li>Configuración de seguridad</li> <li>Directivas de cuenta</li> <li>Directivas de auditoría</li> <li>Directivas de auditoría</li> <li>Asignación de derechos de ust</li> <li>Opciones de seguridad</li> <li>Directivas de clave pública</li> <li>Directivas de control de aplicacior</li> <li>Directivas de seguridad IP en Equip</li> <li>Configuración de directiva de aud</li> </ul>	Directiva Acceso a redes: canalizaciones con nombre accesibles anóni Acceso a redes: modelo de seguridad y uso compartido par Acceso a redes: no permitir el almacenamiento de contrase Acceso a redes: no permitir enumeraciones anónimas de cu Acceso a redes: no permitir enumeraciones anónimas de cu Acceso a redes: permitir la aplicación de los permisos Todos Acceso a redes: recursos compartidos accesibles anónimam Acceso a redes: retursos compartidos accesibles anónimam Acceso a redes: retursos compartidos accesibles anónimam Acceso a redes: rutas del Registro accesibles remotamente Acceso a redes: rutas y subrutas del Registro accesibles rem Acceso a redes: rutas y subrutas del Registro accesibles rem Acceso a redes: rutas y subrutas del Registro accesibles rem Acceso de red: evitar que clientes con permiso realicen llam Acceso de red: permitir traducción SID/nombre anónima Apagado: borrar el archivo de paginación de la memoria virt Auditoría: apagar el sistema sin tener que iniciar ses Auditoría: auditar el acceso de objetos globales del sistema Auditoría: auditar el acceso de objetos globales del sistema Auditoría: auditar el acceso de subcategorías de la dire Auditoría: forzar la configuración de subcategorías de la dire Cliente de redes de Microsoft: enviar contraseña sin cifrar a Cliente de redes de Microsoft: firmar digitalmente las comu Cliente de redes de Microsoft: firmar digitalmente las comu Cliente de redes de Microsoft: firmar digitalmente las comu	Configuración de seguri Clásico: usuarios locales Deshabilitada Habilitada Deshabilitada Deshabilitada No está definido Habilitada System\CurrentControlS System\CurrentControlS No está definido Deshabilitada Deshabilitada Deshabilitada Deshabilitada Deshabilitada Deshabilitada Deshabilitada Deshabilitada Deshabilitada		

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

#### From: https://knoppia.net/ - **Knoppia**

Permanent link: https://knoppia.net/doku.php?id=master\_cs:fortificacion:p7



Last update: 2025/04/01 15:33