

Universidad Autónoma de Baja California
Facultad de Ciencias Químicas e Ingeniería



Administración de Sistemas Operativos

Práctica No. 1:
Microsoft Active Directory

Ingeniería en Software y Tecnologías Emergentes
2023-2

Autores:

Arriaga Alonso, René Sebastián | **1280346**
Reyes Udasco, Richelle Nadine | **1288433**

Docente
M.I. Alma Leticia Palacios Guerrero

Fecha de entrega: 19 de octubre de 2023.



Microsoft Active Directory

Introducción

La administración de sistemas y redes implica comprender y aplicar herramientas y servicios que facilitan la gestión eficiente de recursos y usuarios, además de garantizar la seguridad y la continuidad operativa de la infraestructura. Esto incluye asignar y supervisar recursos, gestionar cuentas de usuario y autenticación, implementar medidas de seguridad, realizar copias de seguridad y recuperación de datos, así como mantener sistemas y software actualizados. Una gestión efectiva aborda estos aspectos clave para mantener un entorno tecnológico estable y seguro.

Uno de los componentes fundamentales en entornos Windows es Active Directory, un servicio de directorio de Microsoft que permite la administración centralizada de objetos de red y la autenticación de usuarios. Este reporte proporciona una visión detallada de Active Directory, sus funciones, disponibilidad en diferentes versiones de Windows, y su relación con políticas de configuración de computadora y usuario.

Además, se explorarán herramientas y conceptos relacionados, como el Editor de Políticas de Grupo, el antivirus de Microsoft (Windows Defender), el uso del lenguaje de scripting Power Shell para la automatización, y la importancia de los puntos de restauración como mecanismo de recuperación del sistema.



Desarrollo

I. Responda las siguientes preguntas

1. ¿Qué es Active Directory?

Active Directory es un servicio de directorio de Microsoft que almacena información sobre objetos de red como usuarios, permisos, recursos, grupos, etc. Esto permite la fácil administración centralizada de recursos y la autenticación de usuarios en una red.

2. ¿Para qué sirve?

Active Directory tiene la función de administrar de manera eficiente los recursos de red, así como administrar las políticas de grupo para dispositivo y usuario. De igual manera, Active Directory gestiona los objetos de red como usuarios, grupos, ordenadores y aplicaciones.

3. ¿Cuánto cuesta?

Active Directory es un servicio gratuito que está disponible en todas las versiones de Windows Server, sin embargo, hay algunas características adicionales que requieren una licencia de Windows Server, la cual se vende por usuario o núcleo. Esta implementación puede variar según el tamaño y las necesidades de la organización.

4. ¿En qué versiones de Windows está disponible?

Active Directory está disponible en todas las versiones de Windows Server desde Windows Server 2000.

5. ¿Cuál es la diferencia entre las políticas para configuración de computadora y Configuración de Usuario?

Por una parte, cuando se trata del ámbito o enfoque de cada política, las políticas para configuración de computadora se aplican a todos los dispositivos que están unidos a un dominio; mientras que las políticas para Configuración de Usuario se aplican a los usuarios individuales, independientemente del dispositivo que utilicen.



Otro punto a destacar es la diferencia que existe entre sus propósitos. Las políticas para configuración de computadora se utilizan para configurar el comportamiento de los dispositivos, como los permisos de acceso a los recursos, la configuración de la pantalla y las aplicaciones que se pueden instalar. Las políticas para Configuración de Usuario se utilizan para configurar las preferencias de los usuarios, como el fondo de escritorio, el color de la fuente y las opciones de visualización.

6. ¿Cómo se llama el antivirus de Microsoft?

El antivirus de Microsoft se llama Windows Defender y está incluido en todas las versiones de Windows desde Windows 10.

7. ¿Cómo se accede al editor de políticas de grupo?

Para acceder al Editor de Políticas de Grupo (gpedit.msc) en Windows, se puede realizar de distintas formas. Las formas más comunes son:

Utilizando el cuadro Ejecutar

01. Presionar "Win + R" para abrir el cuadro Ejecutar.
02. Escribir "gpedit.msc" en el cuadro de diálogo Ejecutar y presionar Enter.

Usando la búsqueda de Windows:

01. Presionar las teclas "Win + S" para abrir la búsqueda de Windows.
02. Escribir "gpedit.msc" y presionar Enter cuando aparezca en los resultados de la búsqueda.

Utilizando el menú Inicio:

01. Abrir el menú Inicio.
02. Escribe "gpedit.msc" en la barra de búsqueda del menú Inicio y selecciona el resultado cuando aparezca.

A través del Administrador de tareas:

01. Abrir el Administrador de tareas presionando "Ctrl + Shift + Esc" o "Ctrl + Alt + Supr" y seleccionar "Administrador de tareas".



02. En el menú "Archivo" del Administrador de tareas, seleccionar "Ejecutar nueva tarea".
03. Escribir "gpedit.msc" en el cuadro de diálogo "Ejecutar nueva tarea" y presionar Enter.

8. ¿Qué es el Power Shell?

Power Shell es un lenguaje de scripting, al igual que una plataforma de automatización desarrollada por Microsoft para administrar y automatizar tareas como la administración del Active Directory y otras funciones del sistema.

9. ¿Qué es un punto de restauración?

Un punto de restauración es una instantánea del estado del sistema y la configuración de un sistema operativo en un momento específico. Se crean para permitir que los usuarios seleccionen un estado del sistema anterior y para restaurar el sistema a ese estado en caso de problemas, como fallos de software o actualizaciones problemáticas.

II. Instale una máquina virtual o real con Windows y utilizando el Editor de Políticas de Grupo realice las siguientes actividades.

Para llevar a cabo estas actividades, se instaló Windows 10 Pro en una máquina física HP Pro. Para ello, se utilizó un dispositivo USB de arranque con un archivo ISO de Windows 10 Pro descargado de la fuente oficial de Microsoft.

Se configuró la máquina HP Pro para que arrancara desde el USB y se procedió con la instalación del sistema operativo, personalizando la configuración según las necesidades de las actividades a realizar. Estos pasos permitieron establecer un entorno de trabajo de Windows 10 Pro adecuado para aplicar políticas de grupo y realizar las tareas requeridas.

Una vez realizado esto, se realizaron las siguientes actividades.



1. Crear dos usuarios uno que se llame soporte y el otro que se llame alumno

Primeramente, mediante el Editor de Políticas de Grupo, configuraremos para que el nombre de la cuenta del Administrador fuera ‘soporte’. En las Figuras 1, 2, 3, 4, 5, 6 y 7.

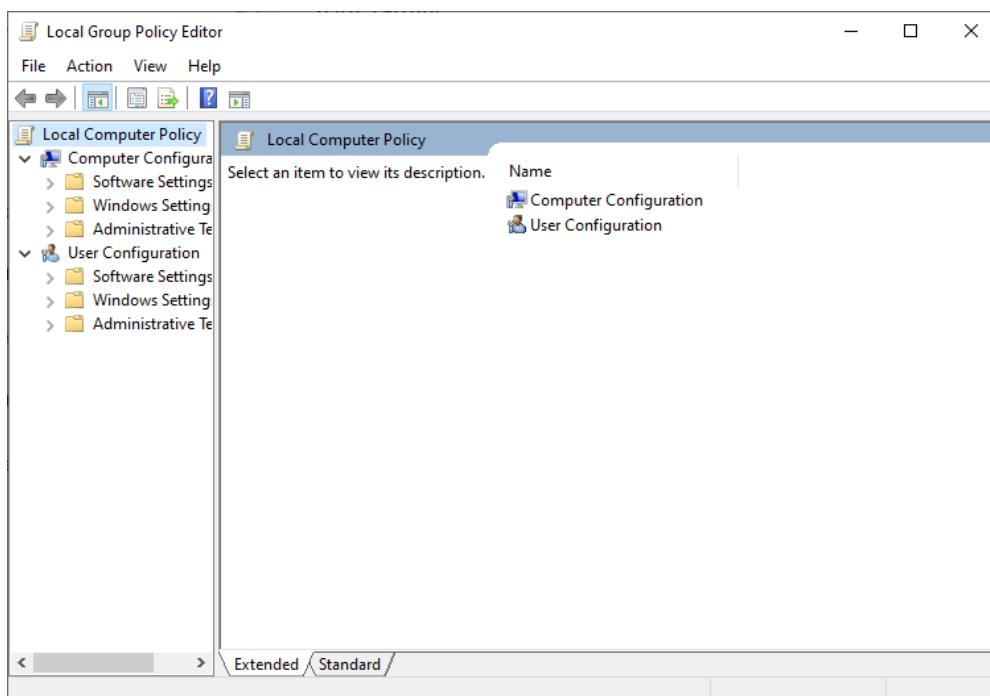


Figura 1. Se ingresa al Editor de Políticas de Grupo.

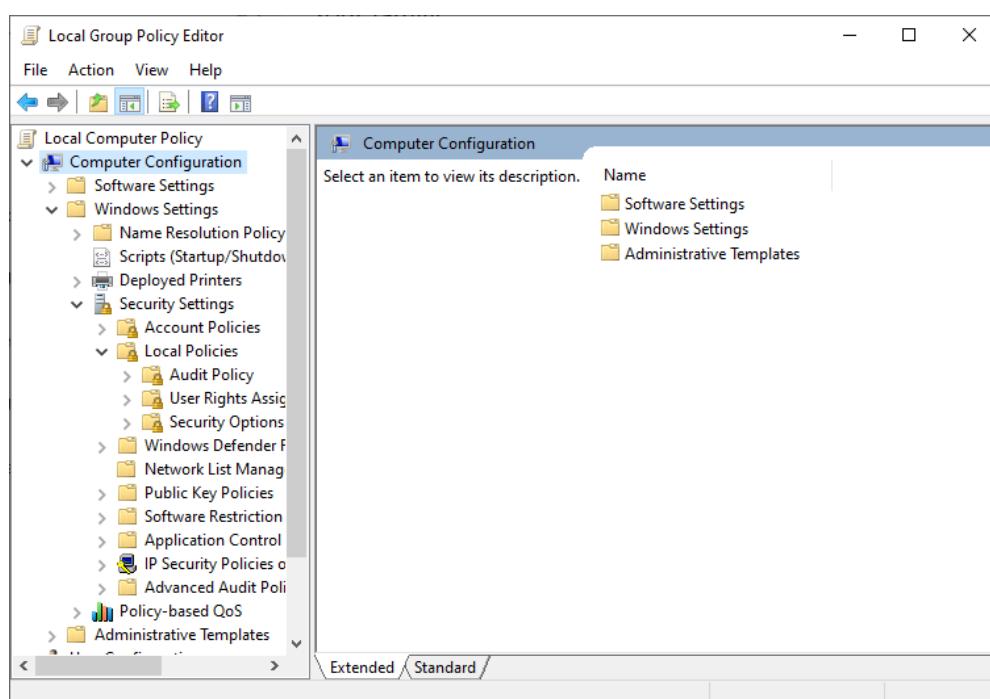


Figura 2. Se navega a la opción “Computer Configuration”.

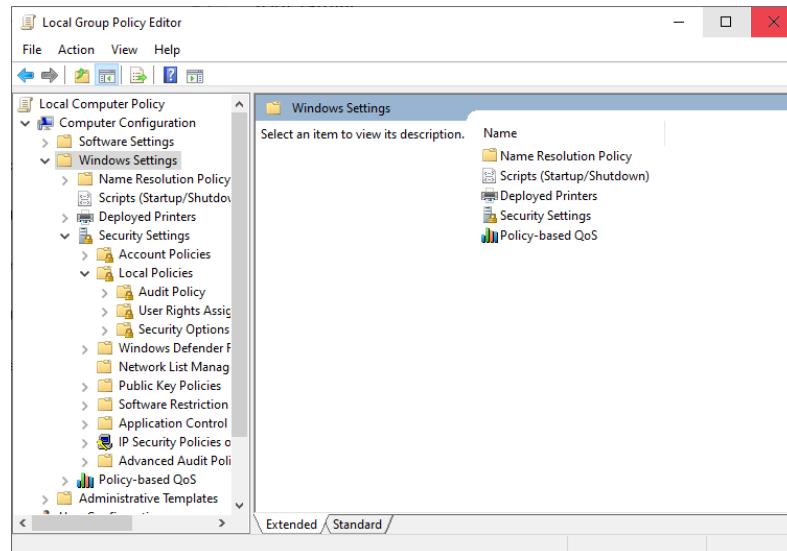


Figura 3. Se navega a la opción “Windows Settings”.

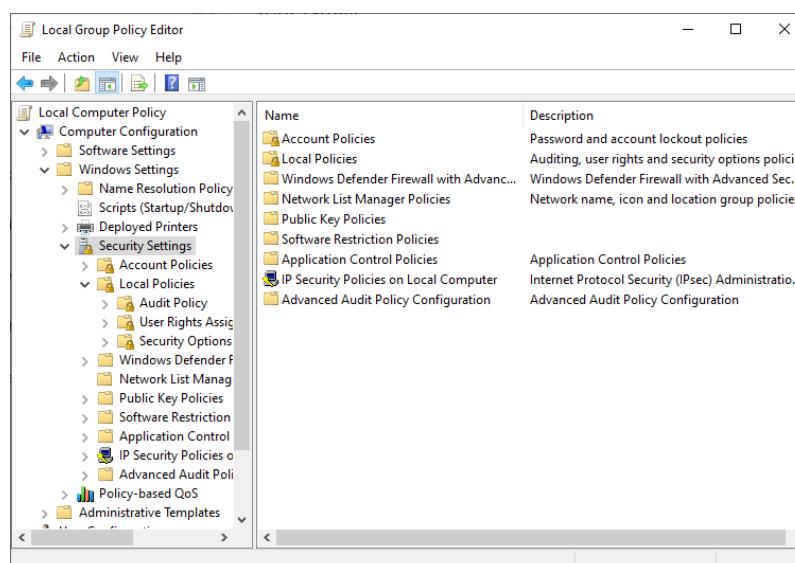


Figura 4. Se navega a la opción “Security Settings”.

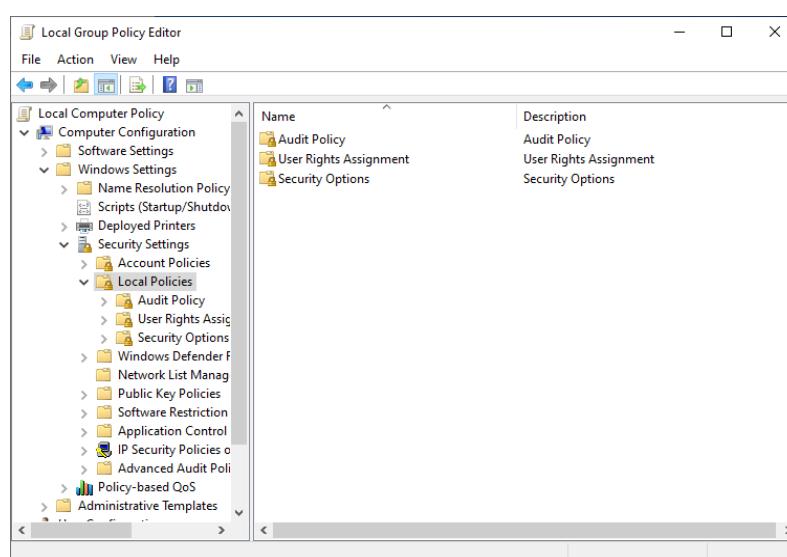


Figura 5. Se navega a la opción “Local Policies”.



The screenshot shows the Local Group Policy Editor window. The left pane displays a navigation tree under 'Local Computer Policy' for 'Computer Configuration'. Under 'Security Settings', the 'Local Policies' node is expanded, showing 'Audit Policy', 'User Rights Assignment', and 'Security Options'. The right pane lists various security policies with their current settings:

Policy	Security Setting
Accounts: Administrator account status	Disabled
Accounts: Block Microsoft accounts	Not Defined
Accounts: Guest account status	Disabled
Accounts: Limit local account use of blank passwords to co...	Enabled
Accounts: Rename administrator account	Administrator
Accounts: Rename guest account	Guest
Audit: Audit the access of global system objects	Disabled
Audit: Audit the use of Backup and Restore privilege	Disabled
Audit: Force audit policy subcategory settings (Windows Vis...	Not Defined
Audit: Shut down system immediately if unable to log secur...	Disabled
DCOM: Machine Access Restrictions in Security Descriptor D...	Not Defined
DCOM: Machine Launch Restrictions in Security Descriptor ...	Not Defined
Devices: Allow undock without having to log on	Enabled
Devices: Allowed to format and eject removable media	Not Defined
Devices: Prevent users from installing printer drivers	Disabled
Devices: Restrict CD-ROM access to locally logged-on user ...	Not Defined
Devices: Restrict floppy access to locally logged-on user only	Not Defined
Domain controller: Allow computer account re-use during d...	Not Defined
Domain controller: Allow server operators to schedule tasks	Not Defined
Domain controller: Allow vulnerable Netlogon secure chann...	Not Defined
Domain controller: LDAP server channel binding token requi...	Not Defined

Figura 6. Se navega a la opción “Security Options”.

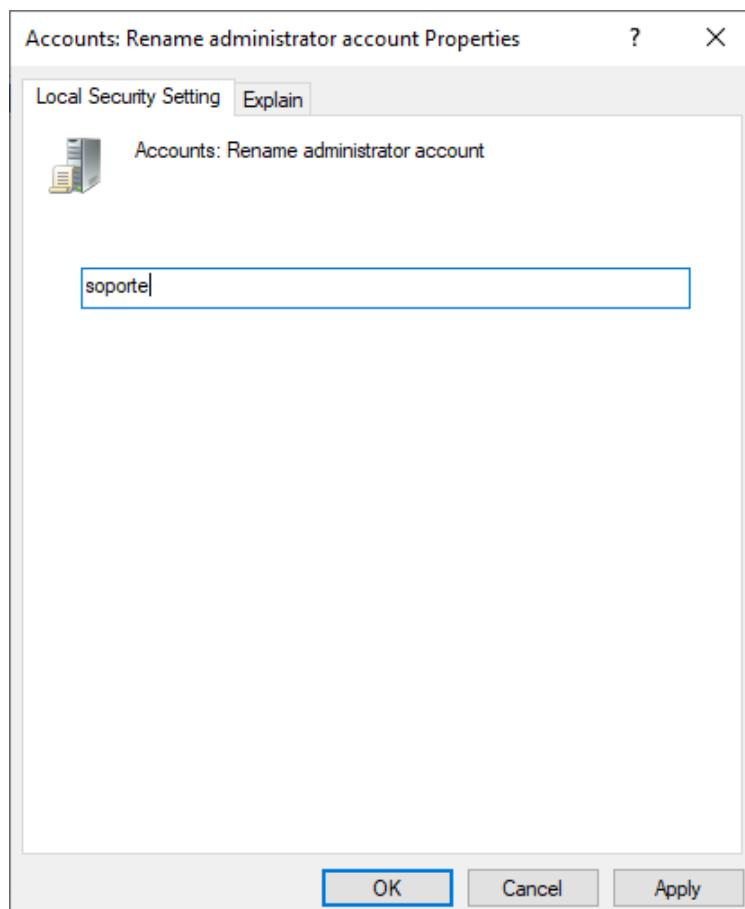


Figura 7. Se renombra a la cuenta del Administrador.

Después, con el Panel de Control se crea al usuario “alumno”.



Microsoft account

Create a user for this PC

If you want to use a password, choose something that will be easy for you to remember but hard for others to guess.

Who's going to use this PC?

alumno

Make it secure.

Enter password

Re-enter password

Next

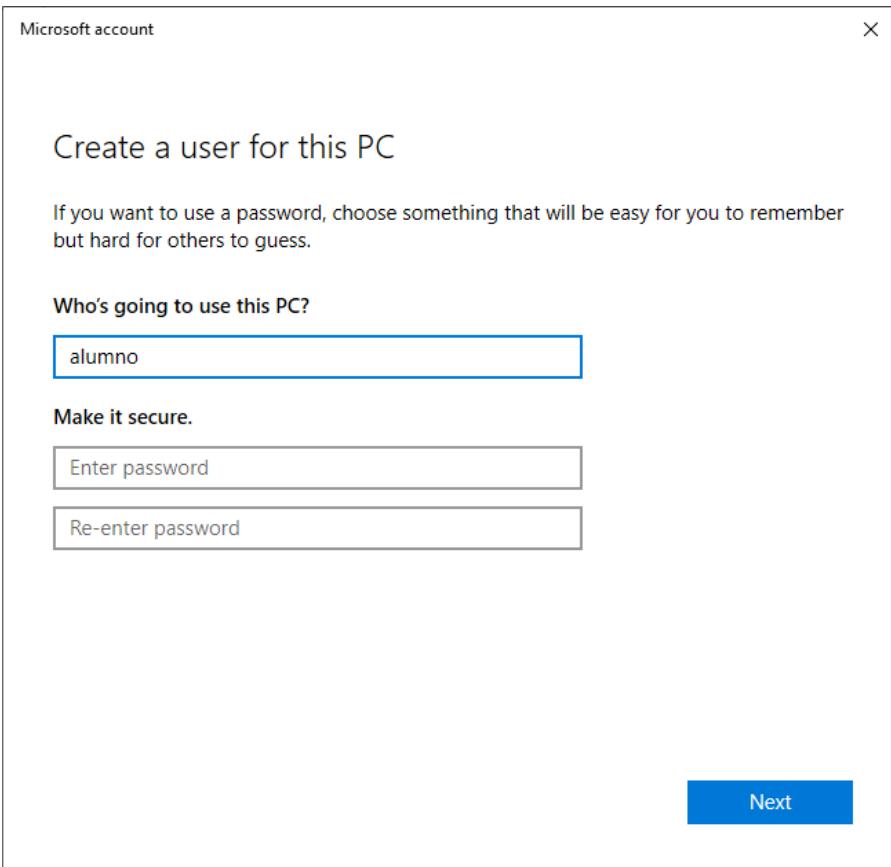


Figura 8. Se crea al usuario “alumno”.

Settings

Home

Find a setting

Accounts

Your info

Email & accounts

Sign-in options

Access work or school

Family & other users

Sync your settings

Family & other users

Your family

Sign in with a Microsoft account

Get help

Give feedback

Other users

Add someone else to this PC

+ alumno
Local account

soporte
Local account

Set up a kiosk

Assigned access

Set up this device as a kiosk—this could be a digital sign, interactive display, or public browser among other things.

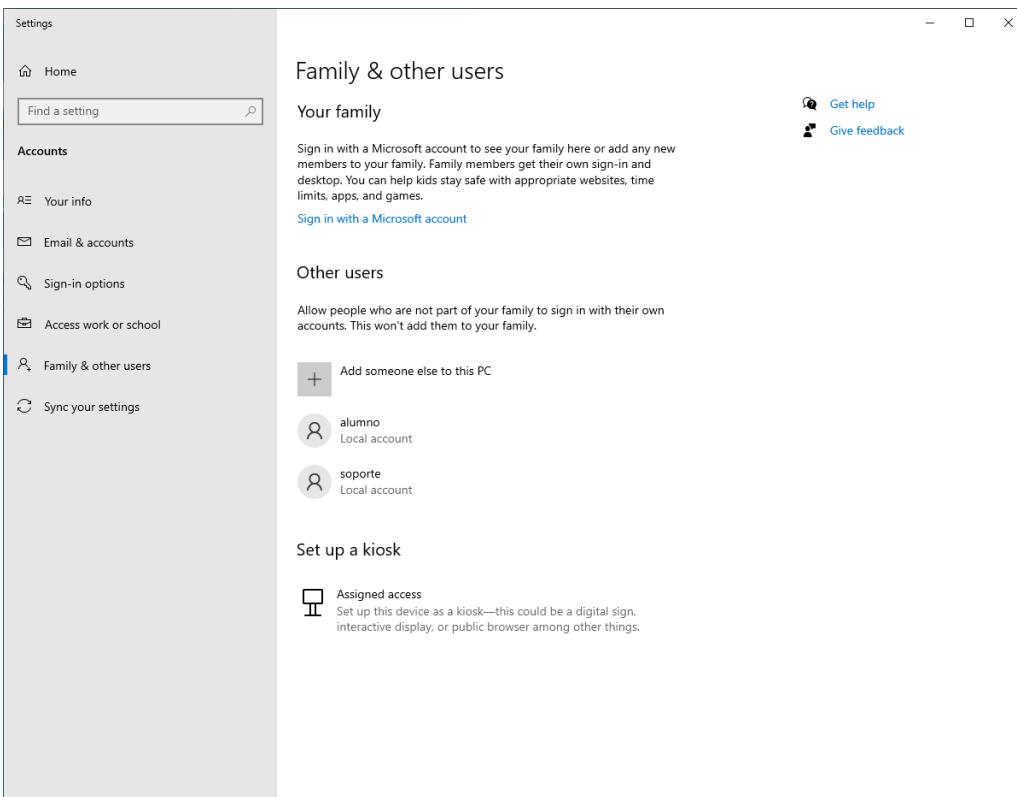


Figura 9. Se muestra que el usuario ya existe.



2. Programar para que la computadora se apague todos los días a las 10pm.

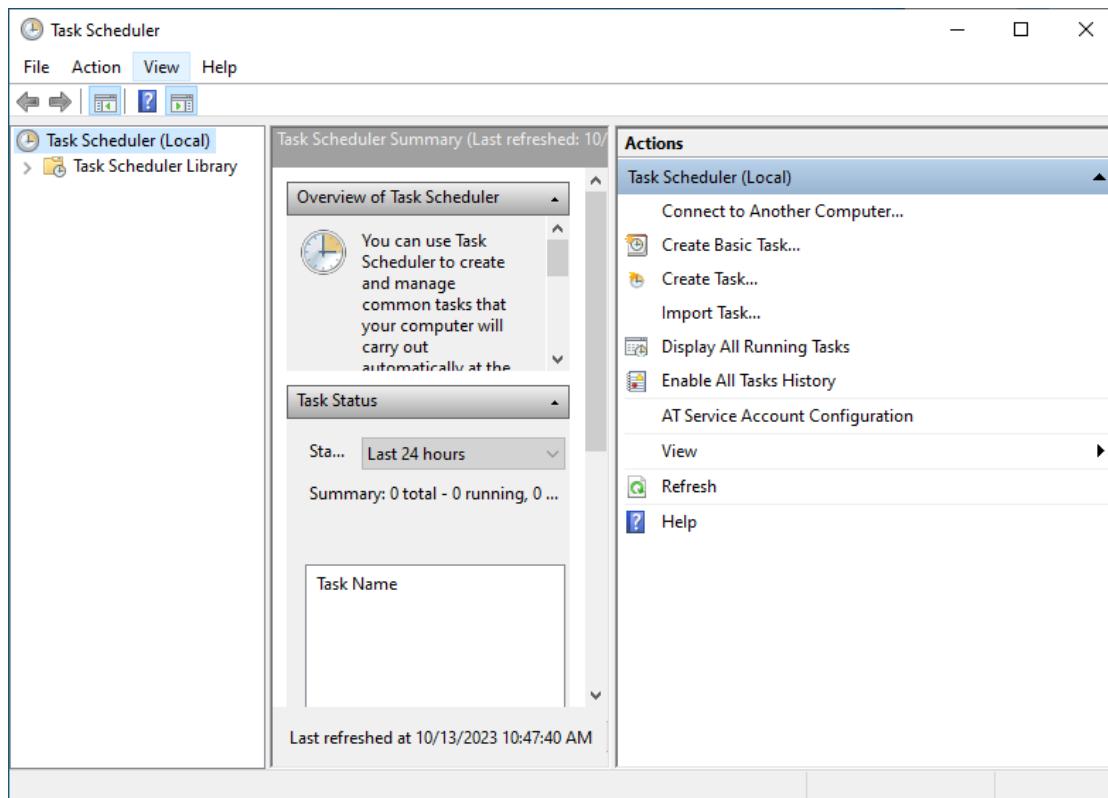


Figura 10. Se ingresa al programa “Task Scheduler”.

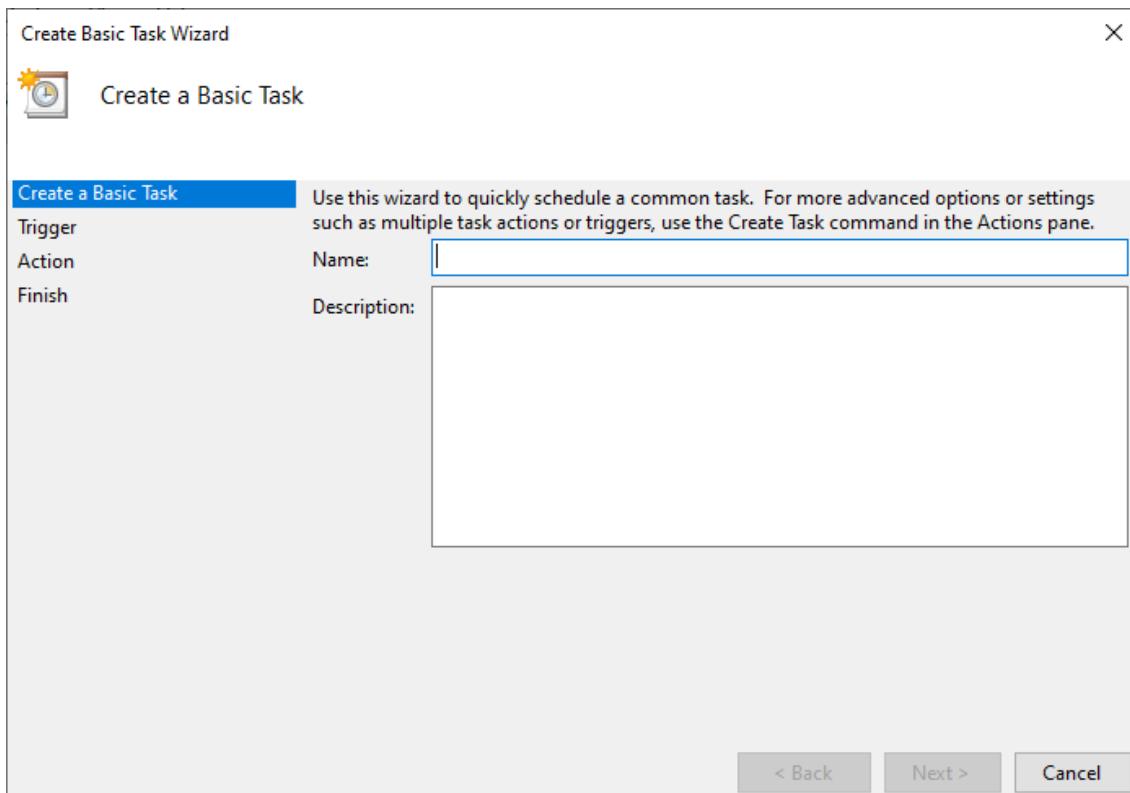


Figura 11. Se crea una nueva tarea básica.

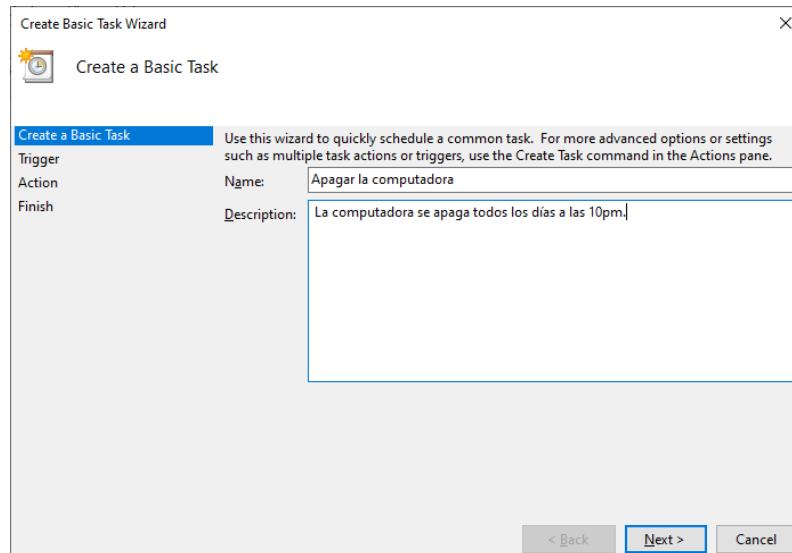


Figura 12. Se ingresan el Nombre y la Descripción de la tarea.

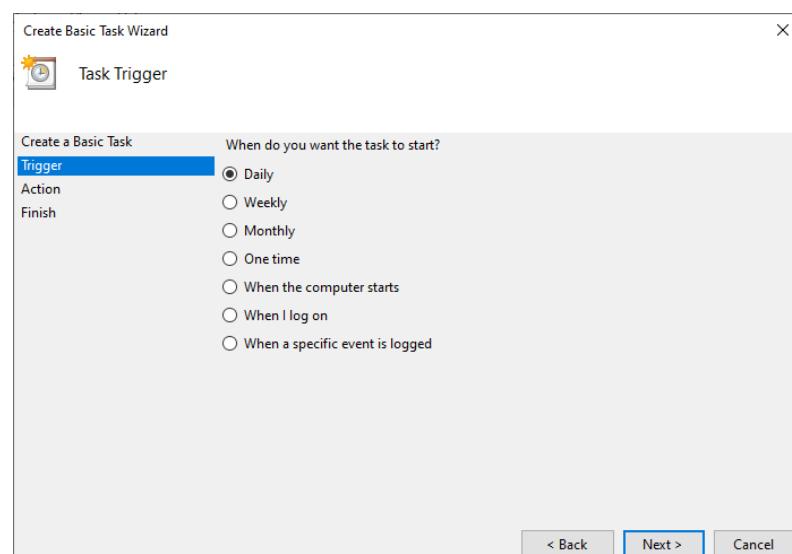


Figura 13. Se ingresa la frecuencia de la tarea.

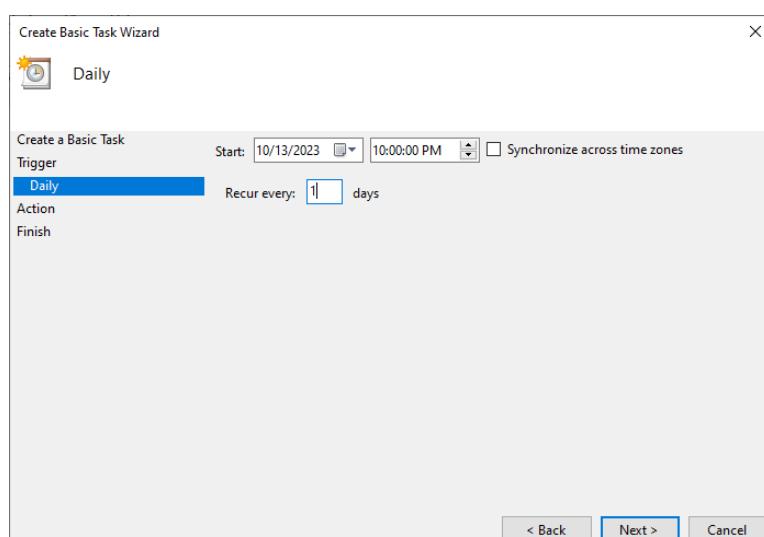


Figura 14. Se ingresan detalles de la frecuencia.

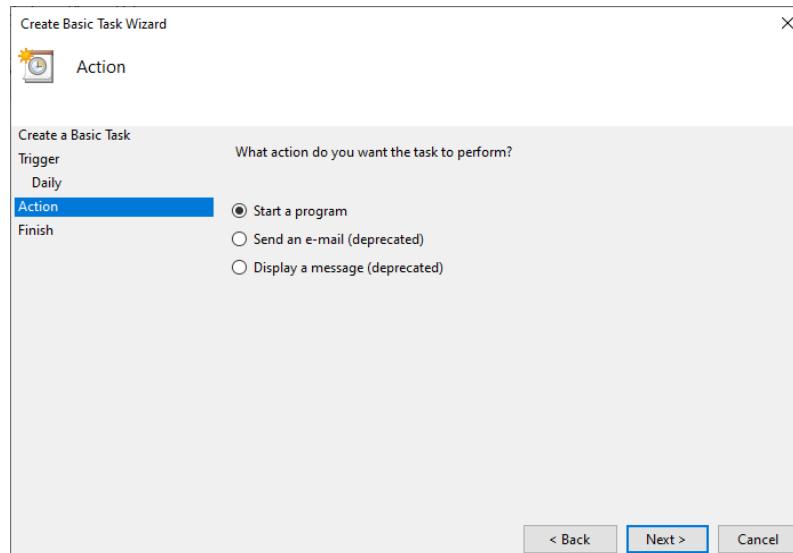


Figura 15. Se ingresa la acción que se quiere realizar.

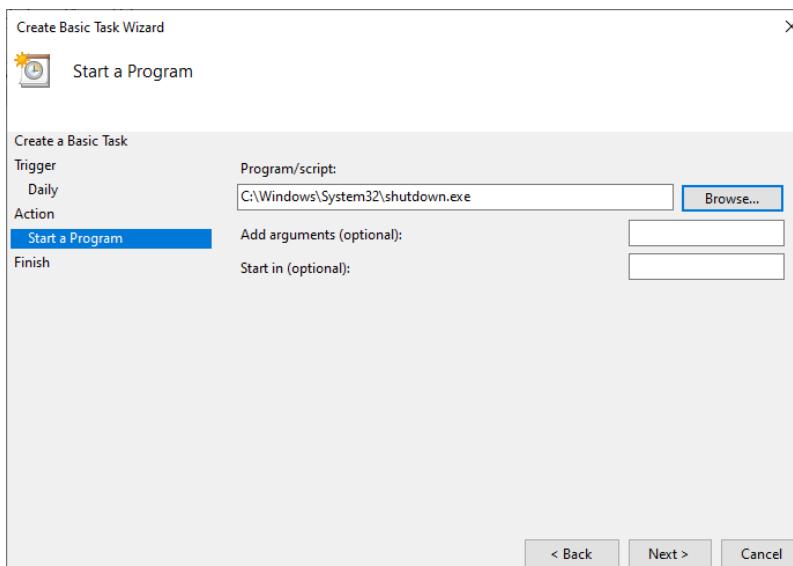


Figura 16. Se indica el programa que se quiere ejecutar.

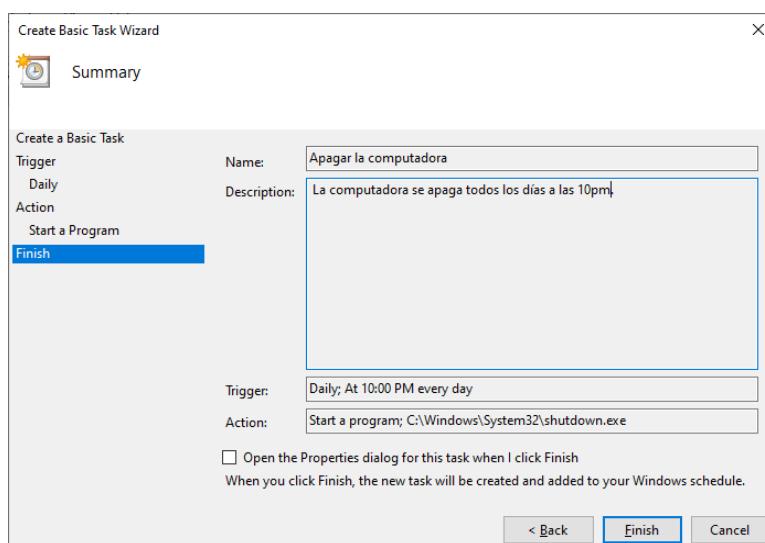


Figura 17. Se verifican los detalles.

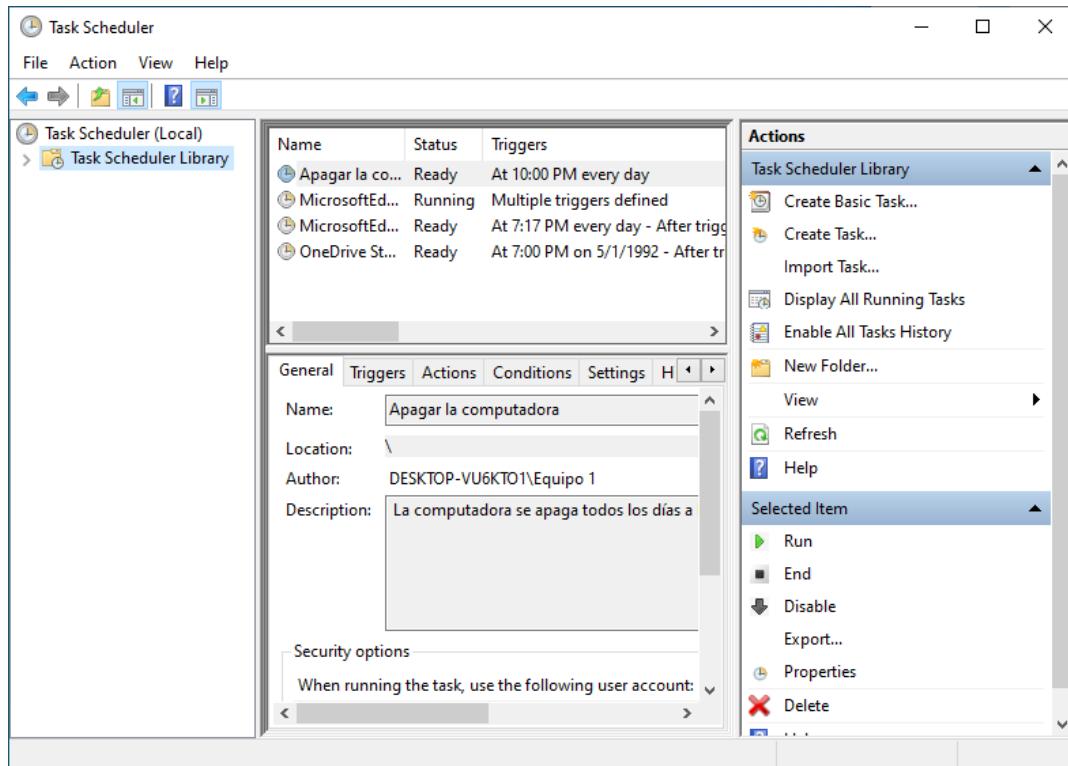


Figura 18. Se muestra que ya existe la tarea.

3. Evitar que cualquier usuario cambie el fondo

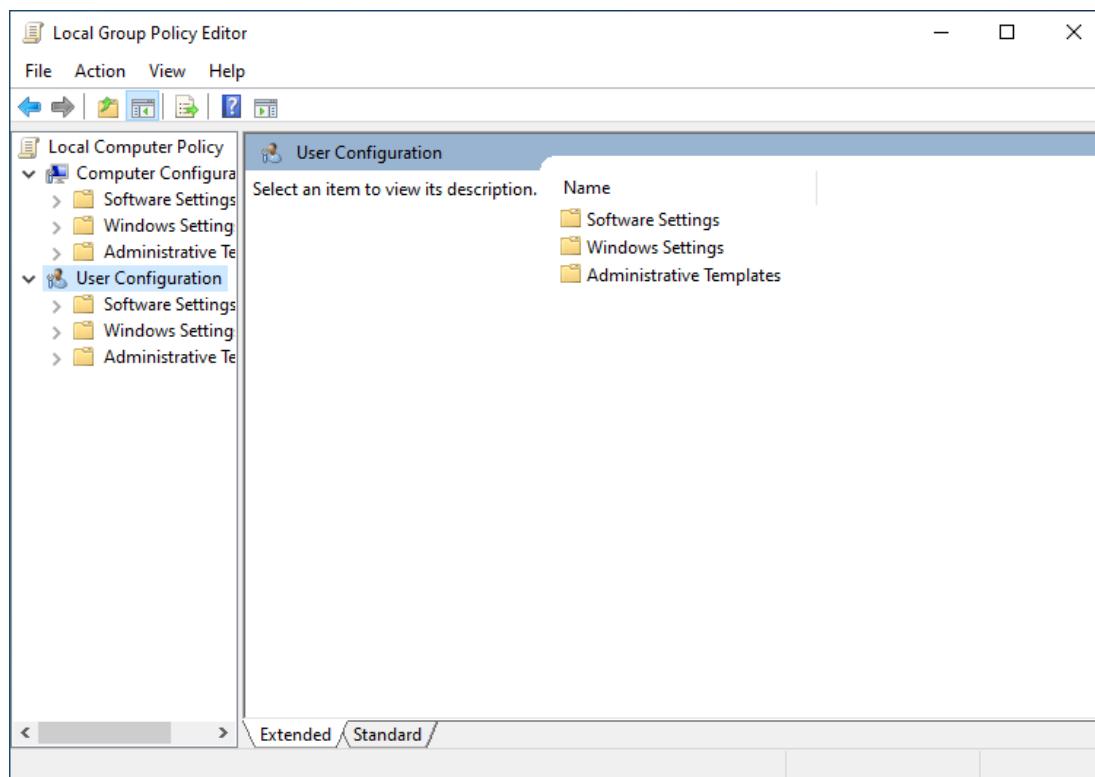


Figura 19. En el Editor de Políticas de Grupo, se navega a la opción “User Configuration”.

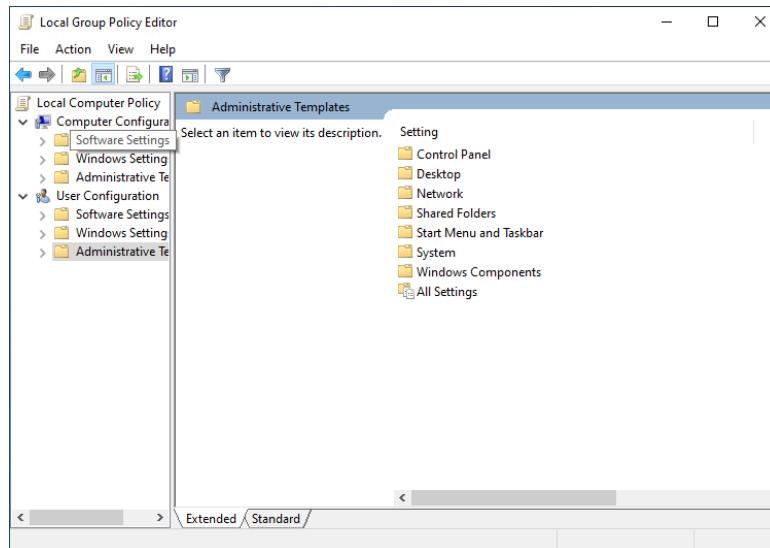


Figura 20. Se navega a la opción “Administrative Templates”.

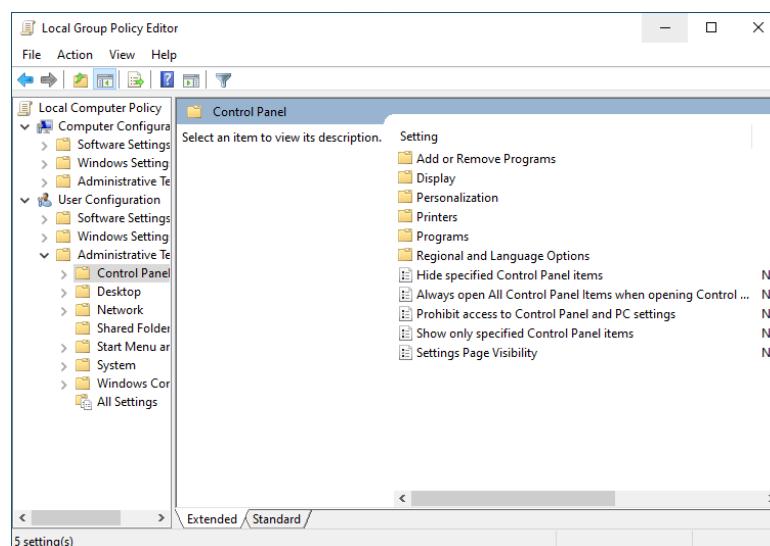


Figura 21. Se navega a la opción “Control Panel”.

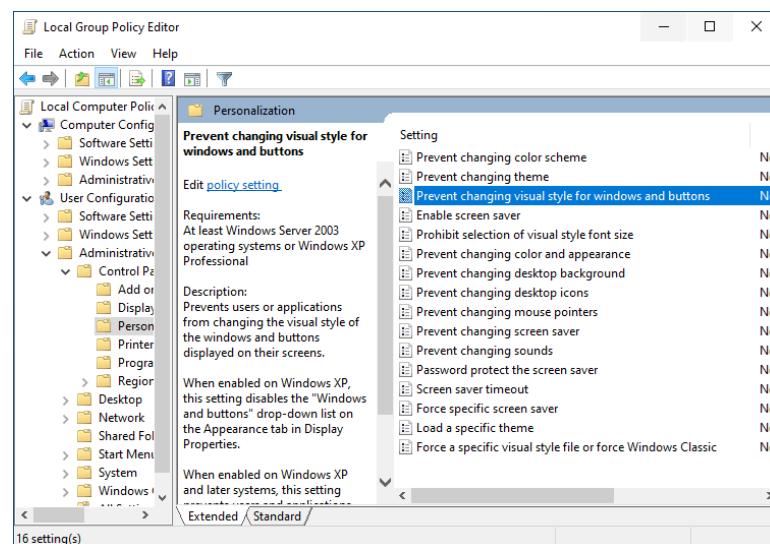


Figura 22. Se navega a la opción “Personalization”.

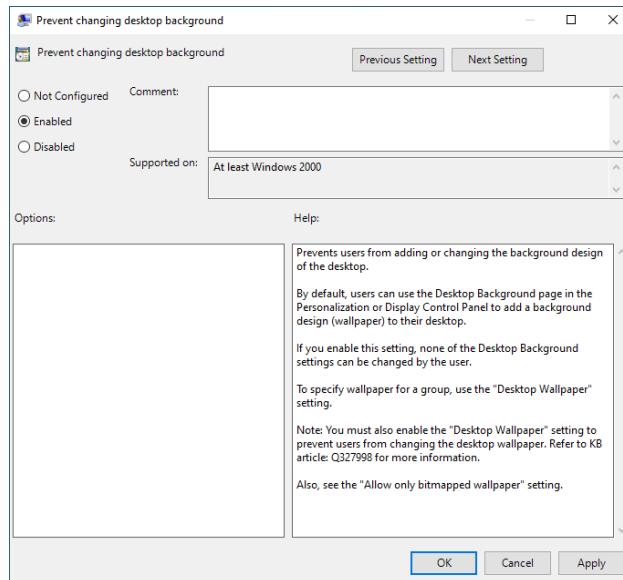


Figura 23. Se habilita la política "No permitir cambiar el fondo de escritorio".

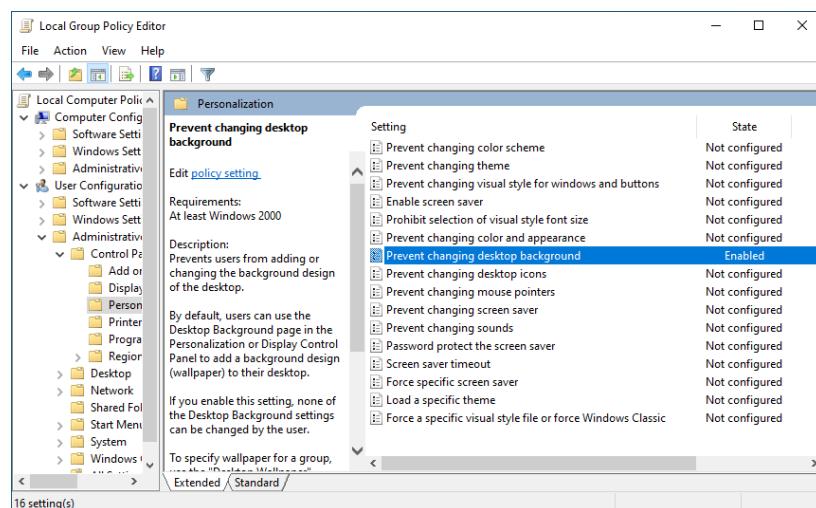


Figura 24. Se observa que ya se encuentra habilitada.

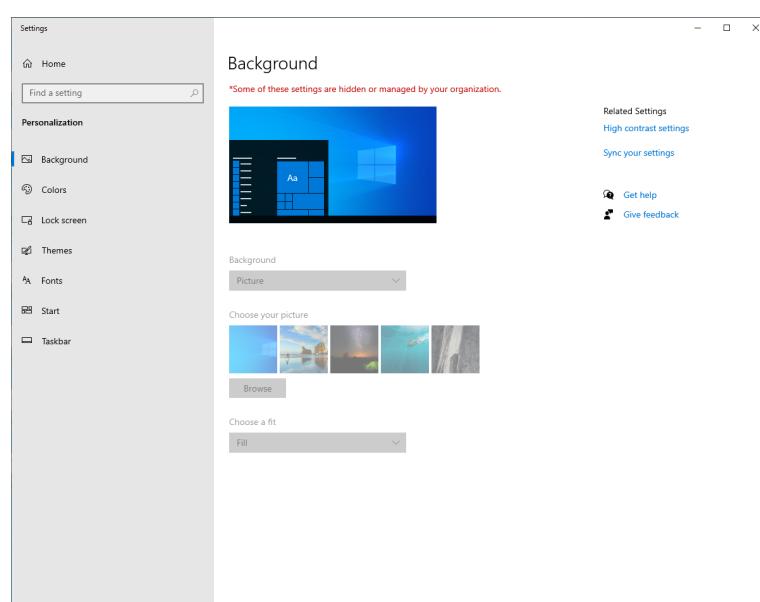


Figura 25. Al intentar cambiar el fondo de escritorio, se observa que ya no será posible.



4. Evitar que el usuario alumno pueda entrar al Panel de Control

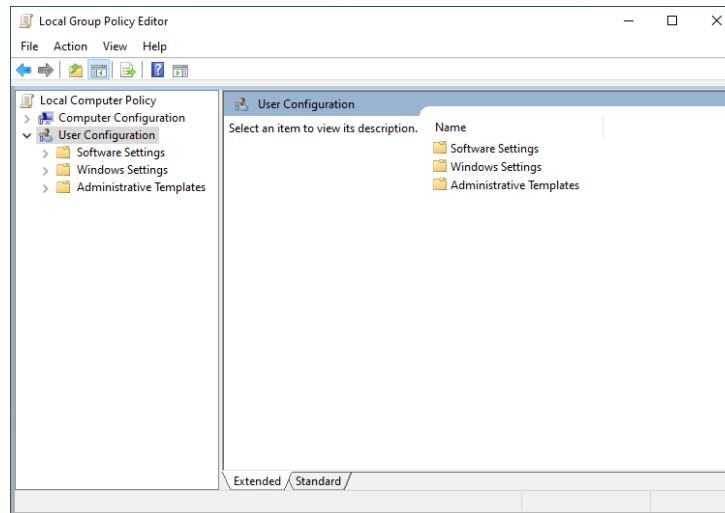


Figura 26. En el Editor de Políticas de Grupo, se navega a la opción “User Configuration”.

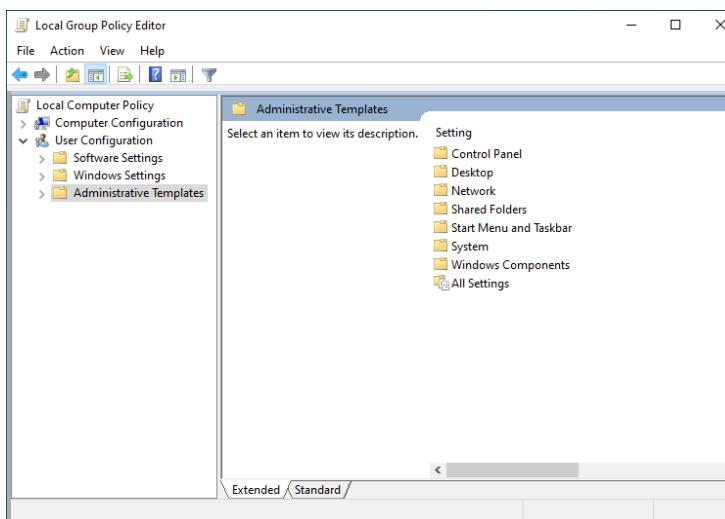


Figura 27. Se navega a la opción “Administrative Templates”.

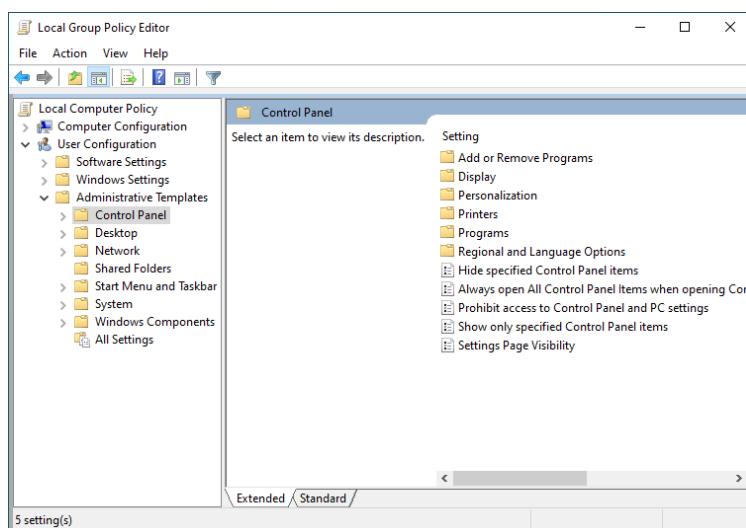


Figura 28. Se navega a la opción “Control Panel”.

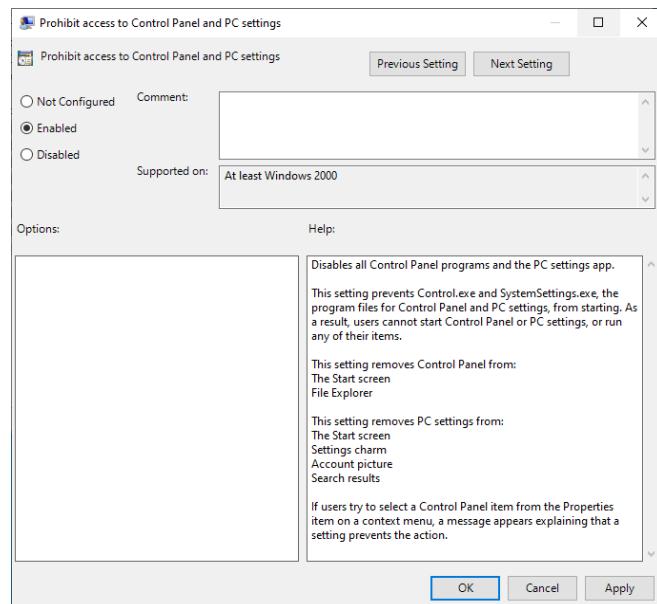


Figura 29. Se habilita la política "No permitir el acceso al Control Panel y Configuraciones de PC".

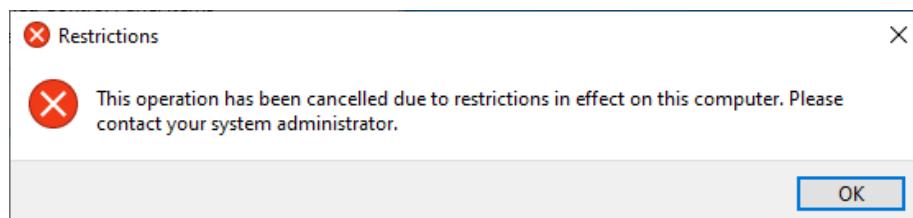


Figura 30. Se puede observar que ya no permite ingresar al Control Panel.

5. Evitar la búsqueda de impresoras en la red para todos los usuarios.

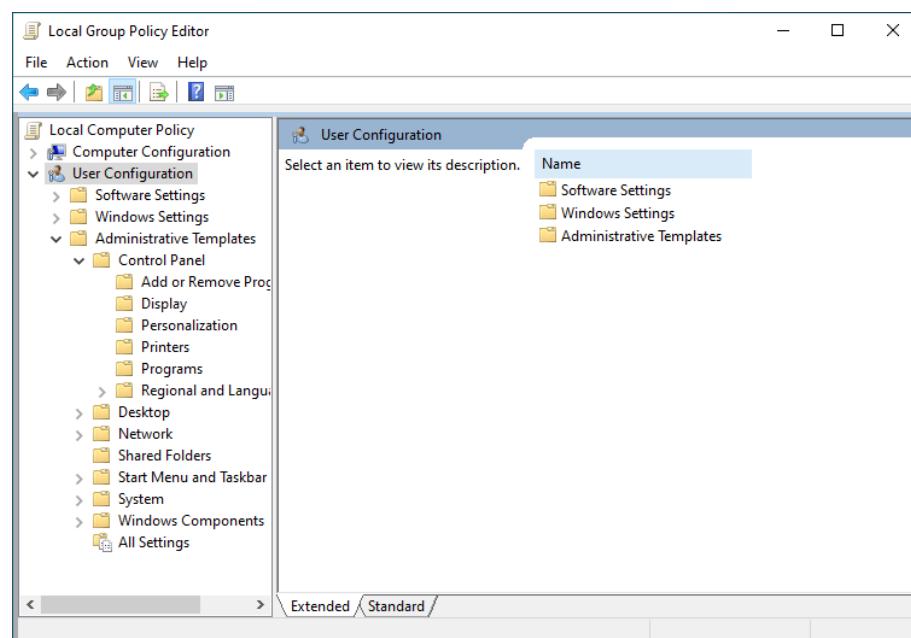


Figura 31. En el Editor de Políticas de Grupo, se navega a la opción “User Configuration”.

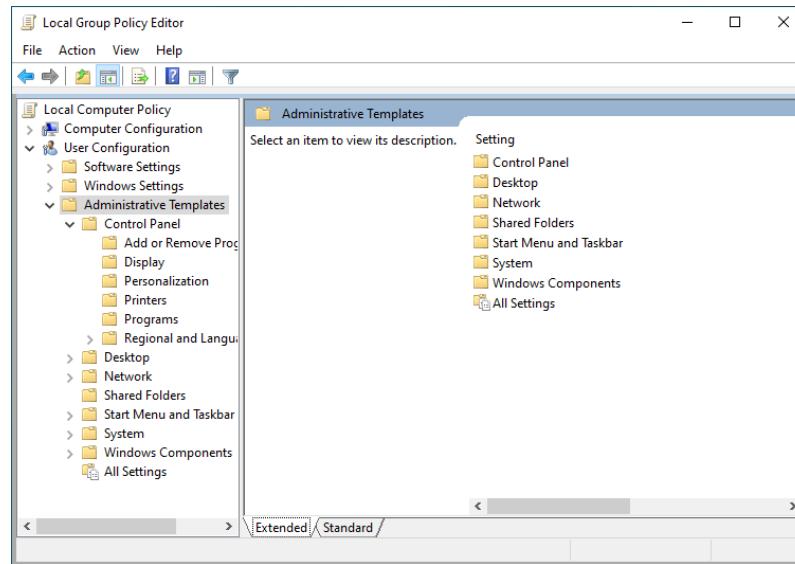


Figura 32. Se navega a la opción “Administrative Templates”.

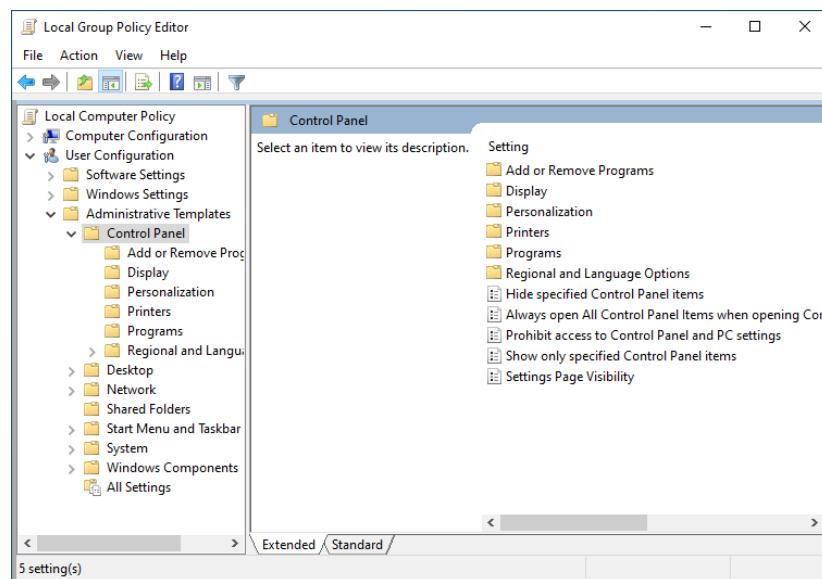


Figura 33. Se navega a la opción “Control Panel”.

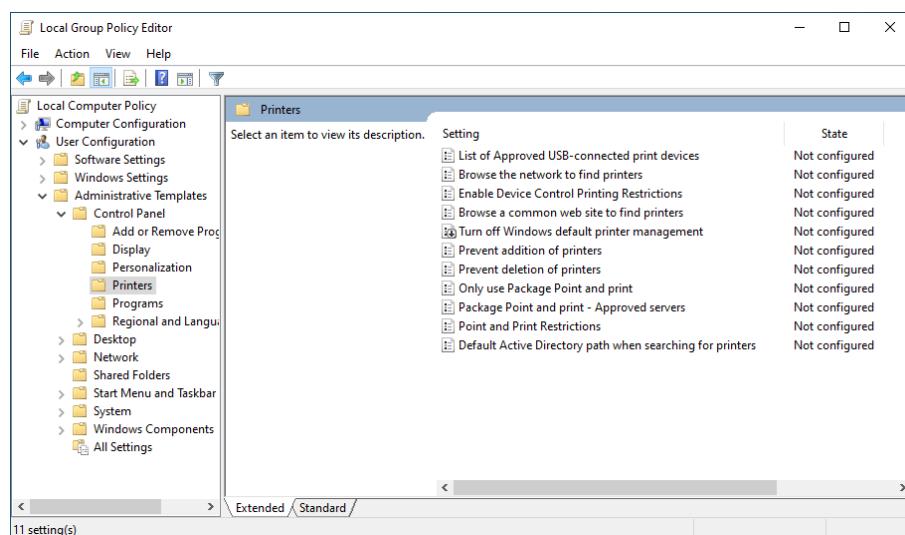


Figura 34. Se navega a la opción “Printers”.

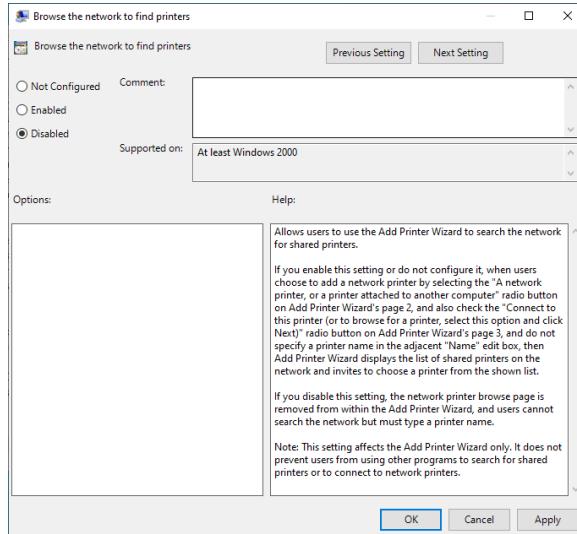


Figura 35. Se deshabilita la política "Permitir buscar impresoras en la red".

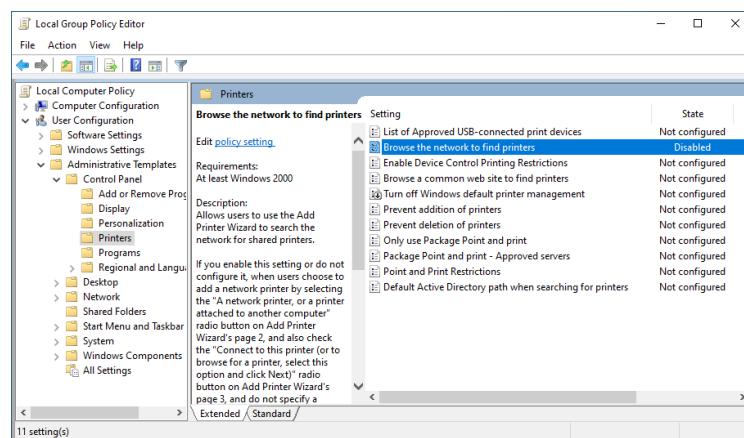


Figura 36. Se observa que ya se encuentra deshabilitada.

6. Deshabilitar los respaldos del sistema.

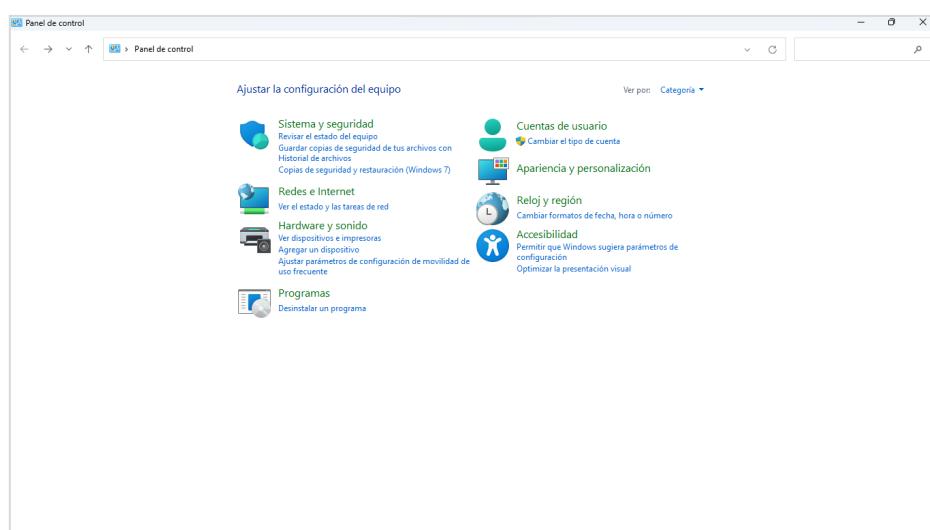


Figura 37. Se ingresa al Panel de Control del sistema.

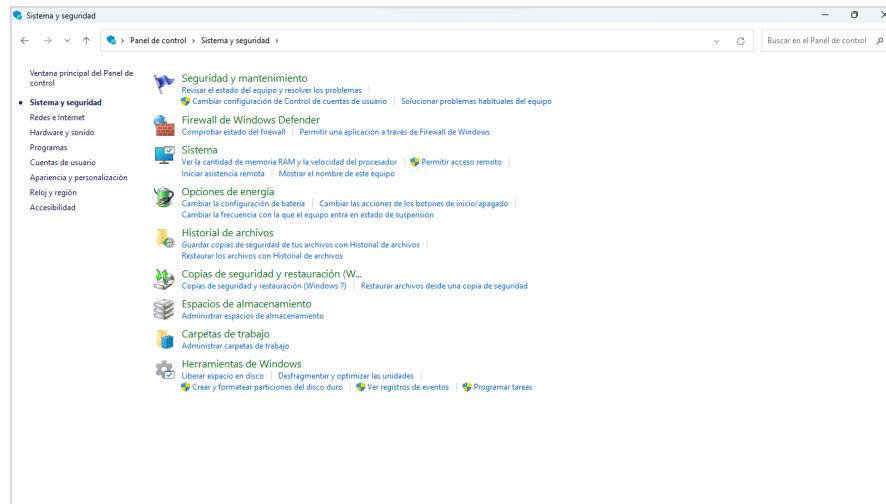


Figura 38. Se navega a la opción “Sistema y seguridad”.

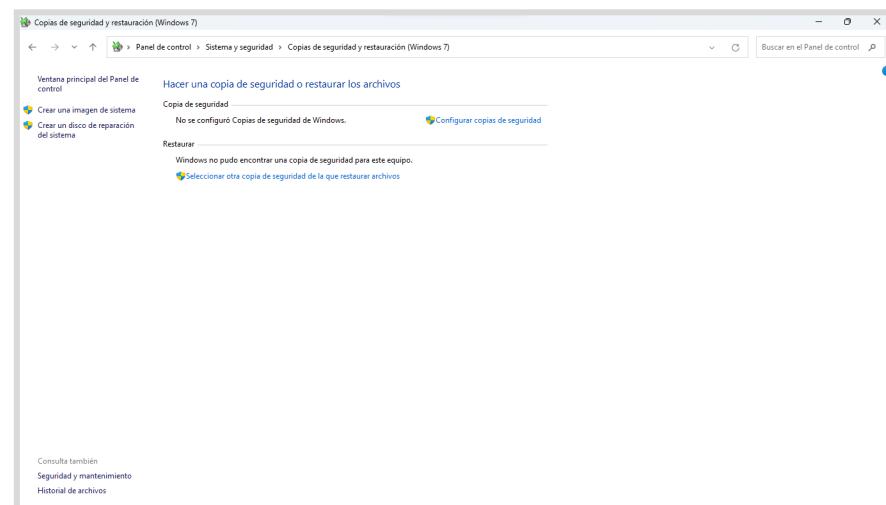


Figura 39. Se ingresa a “Copias de seguridad y restauración” y se observa que no se encuentra habilitada.

7. Evitar el historial de documentos recientemente abiertos, para alumno.

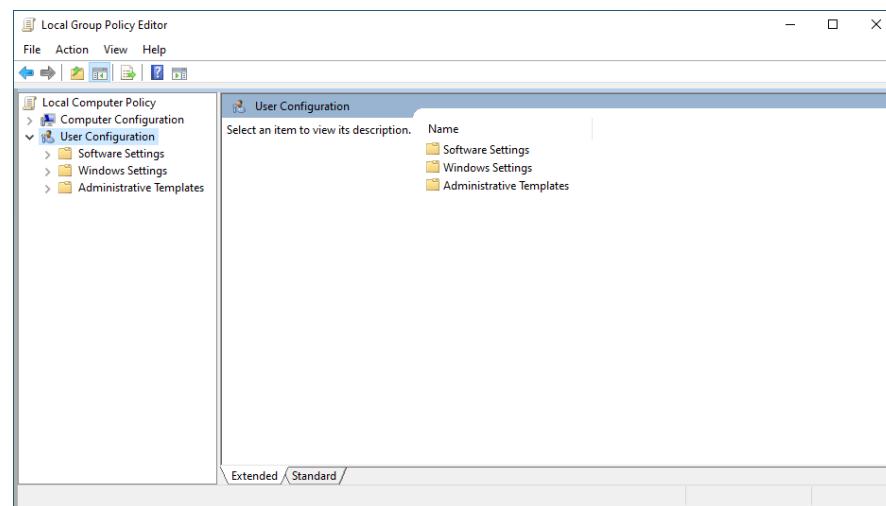


Figura 40. En el Editor de Políticas de Grupo, se navega a la opción “User Configuration”.

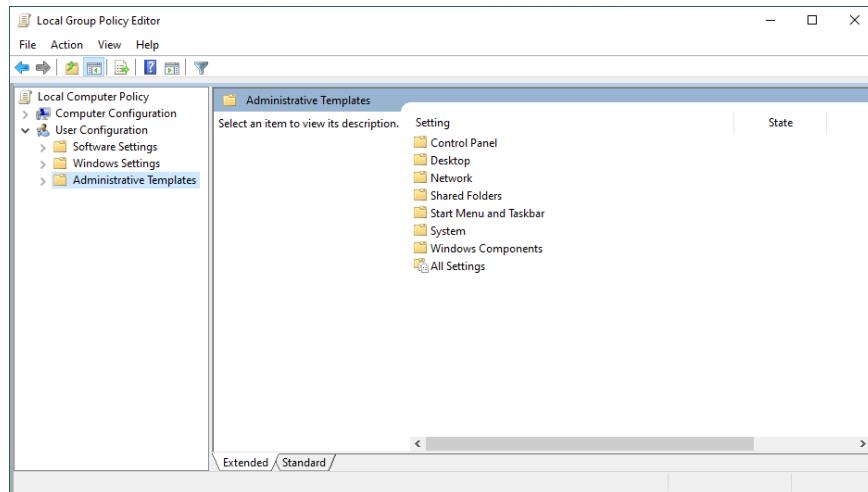


Figura 41. Se navega a la opción “Administrative Templates”.

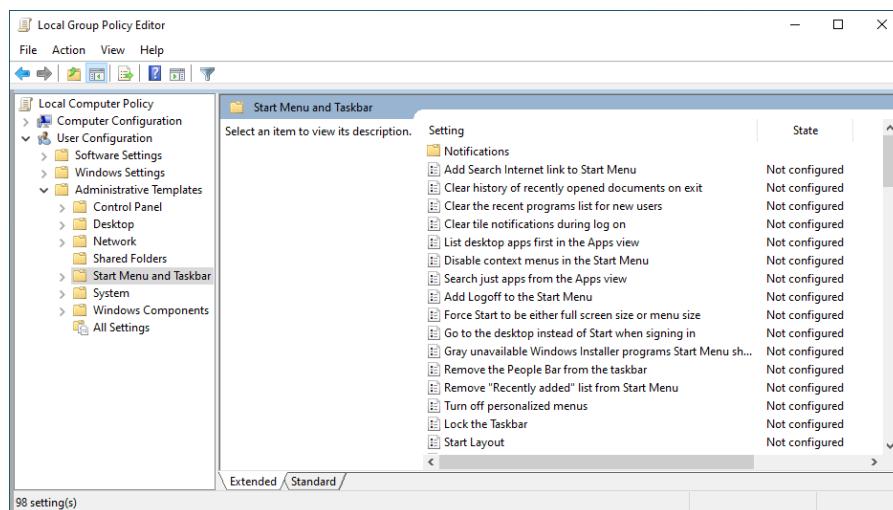


Figura 42. Se navega a la opción “Start Menu and Taskbar”.

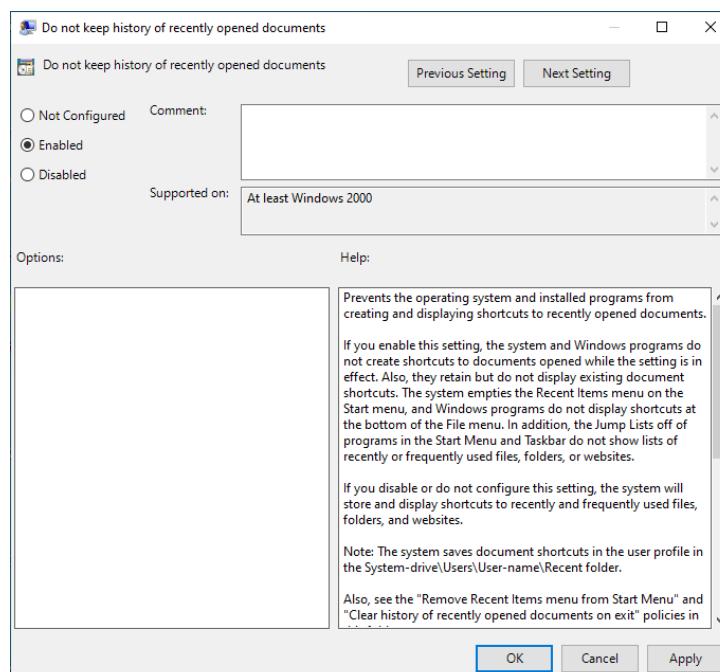


Figura 43. Se habilita la política "No mantener un listado de documentos recientes".

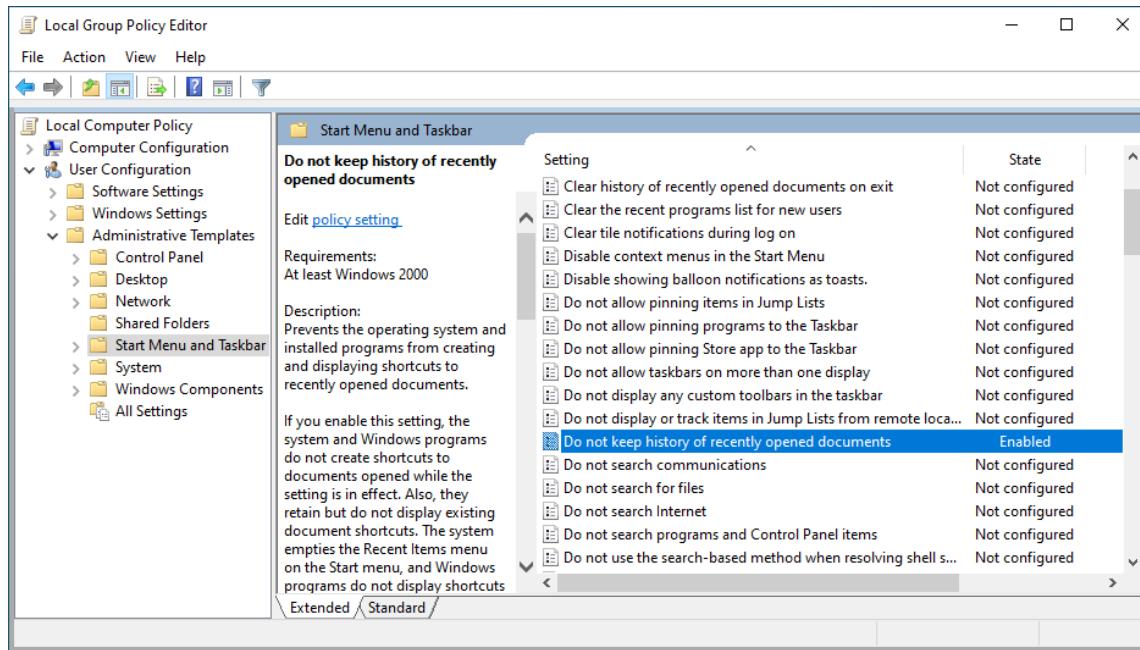


Figura 44. Se observa que ya se encuentra habilitada.

8. Habilitar la solicitud de Asistencia remota.

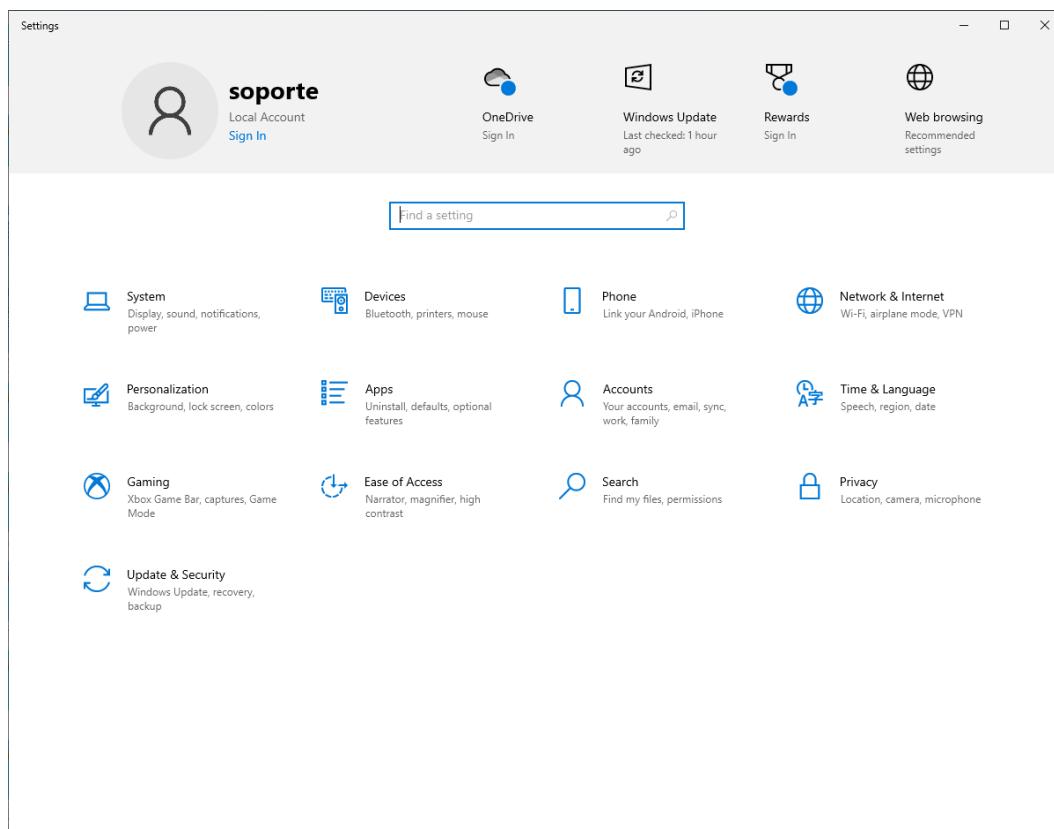


Figura 45. Se ingresa a las Configuraciones del equipo.

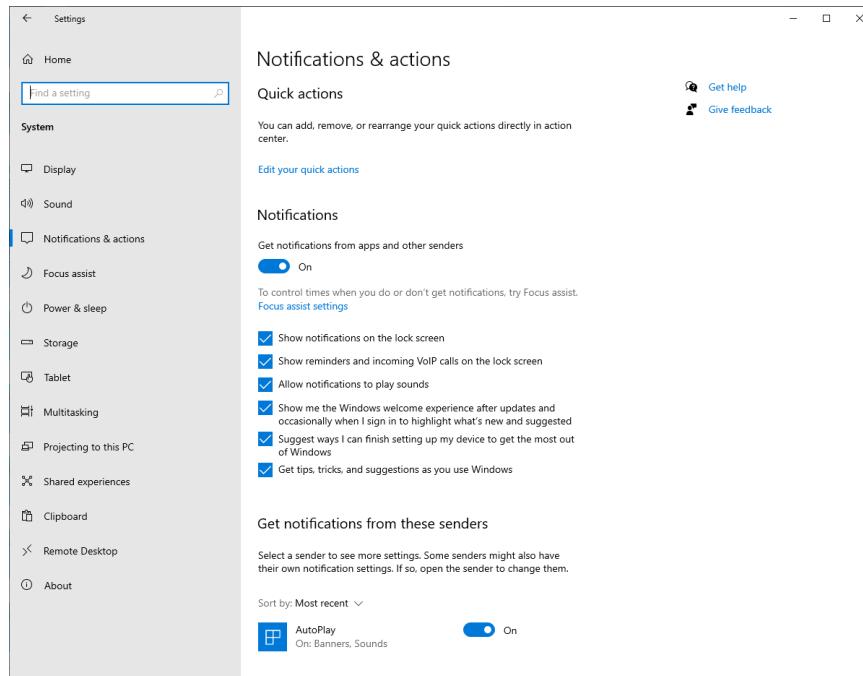


Figura 46. Se ingresa a la opción “System”.

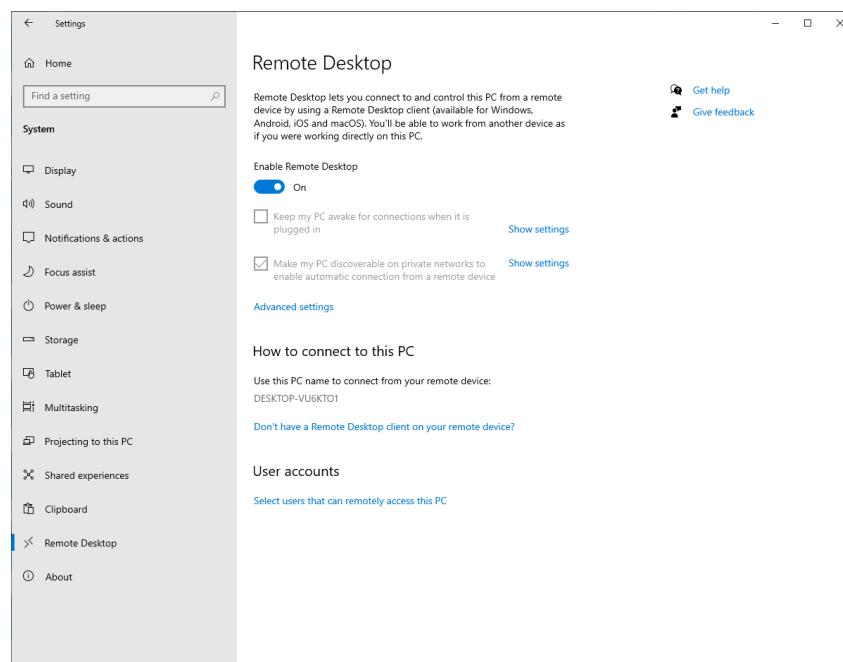


Figura 47. Se ingresa a la opción “Remote Desktop”.

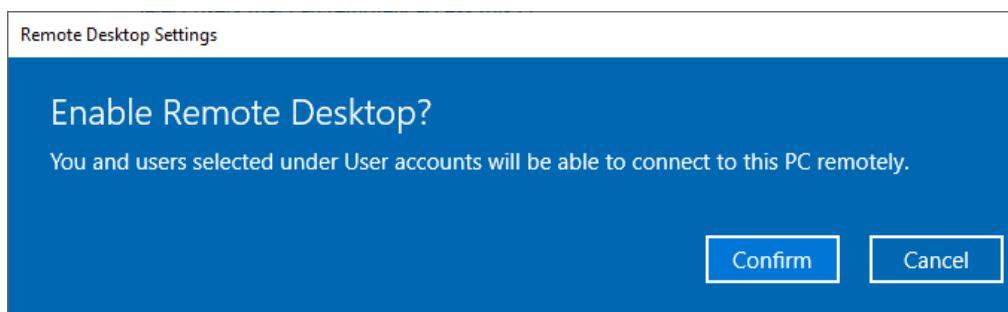


Figura 48. Se confirma que se quiere habilitar “Remote Desktop”.



9. Apagar el sonido cuando entra a Windows Solo para alumno.

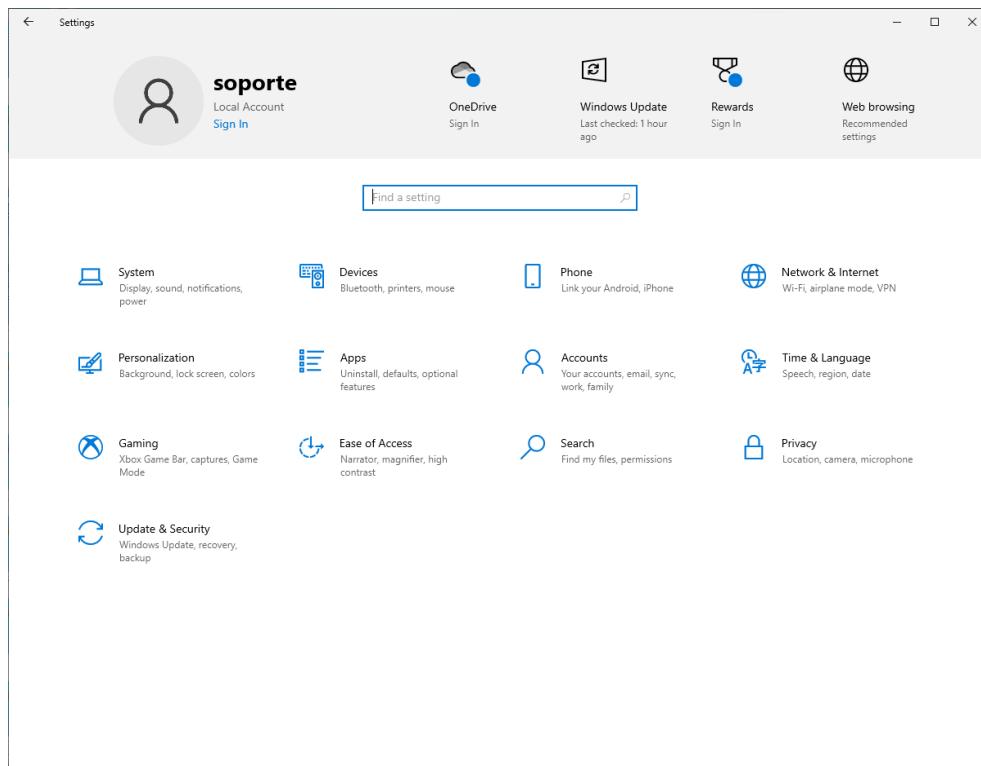


Figura 49. Se ingresa a las Configuraciones del equipo.

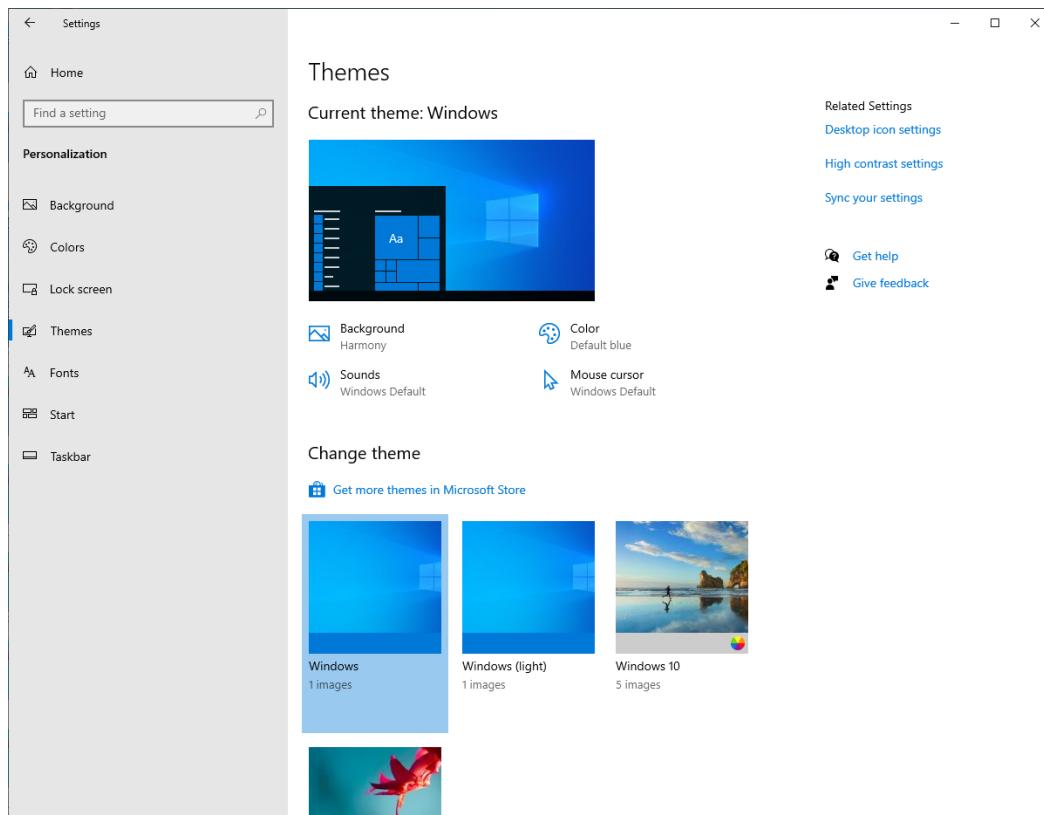


Figura 50. Se ingresa a la opción “Personalization”.

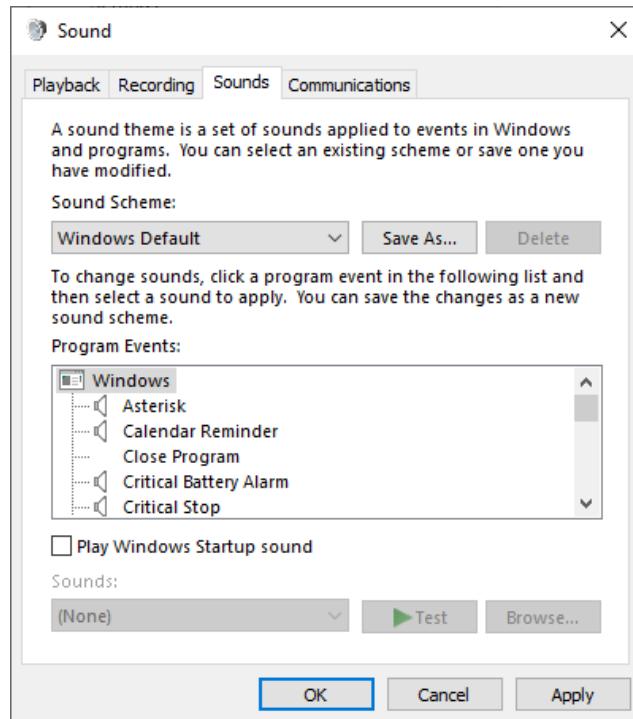


Figura 51. Se ingresa a la opción “Sounds” y se desactiva la opción de “Reproducir sonido Inicio de Windows”.

10. Apagar el Microsoft Defender para todos los usuarios

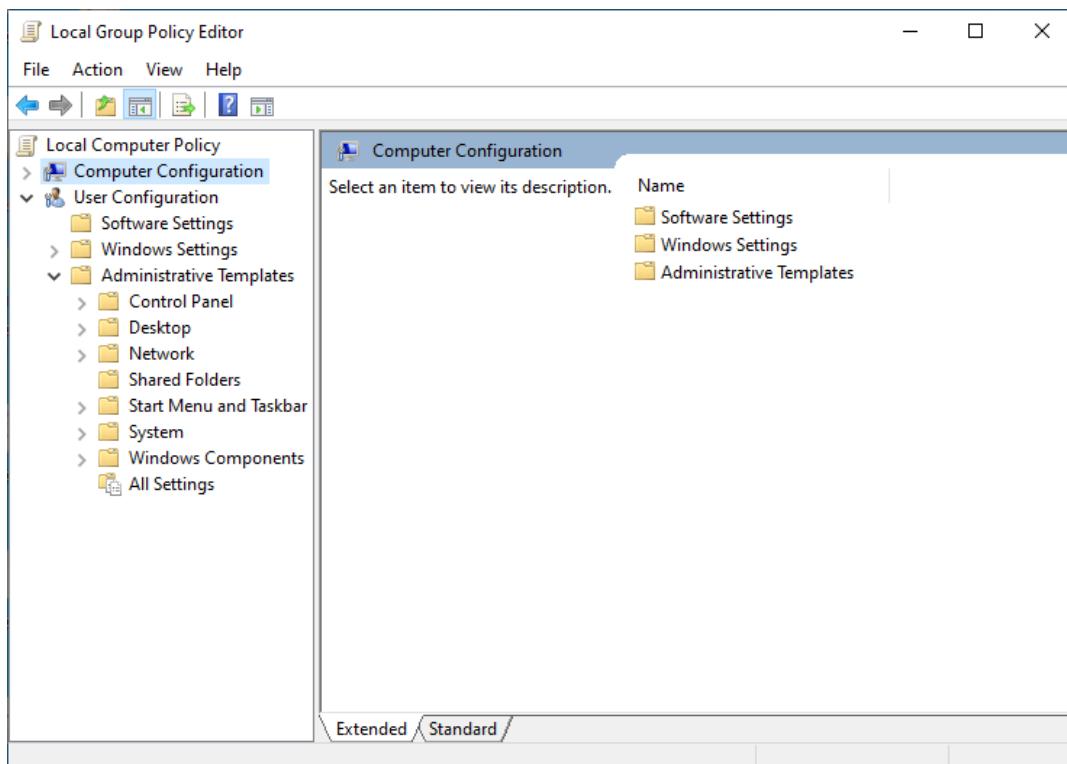


Figura 52. En el Editor de Políticas de Grupo, se navega a la opción “Computer Configuration”.

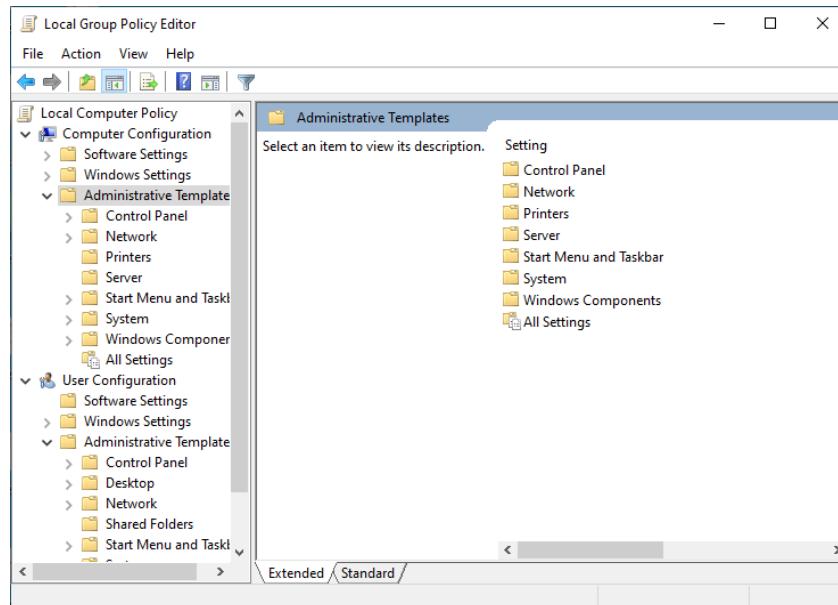


Figura 53. Se navega a la opción “Administrative Templates”.

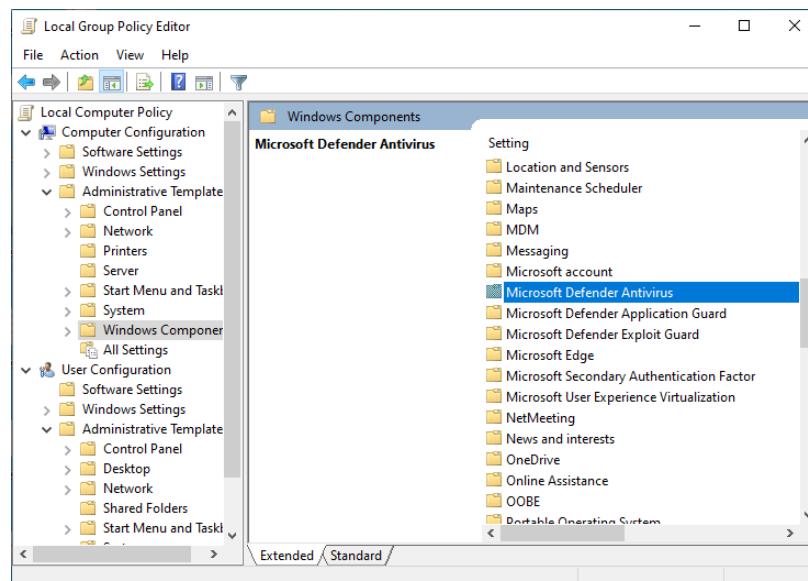


Figura 54. Se navega a la opción “Windows Components”.

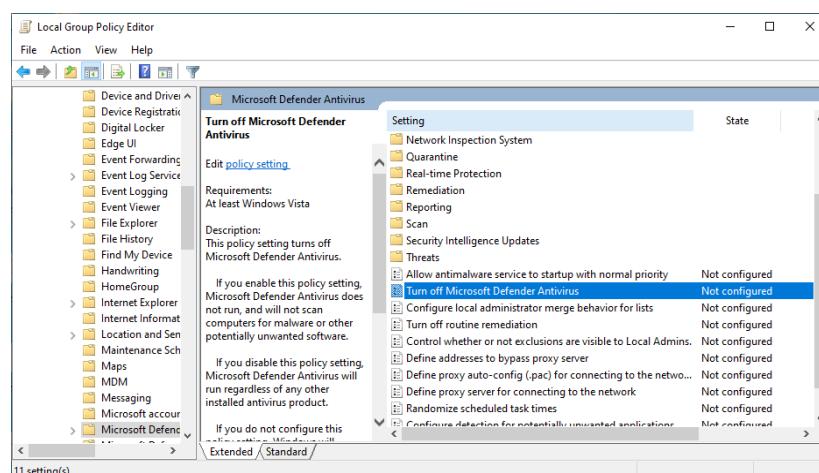


Figura 55. Se navega a la opción “Microsoft Defender Antivirus”.

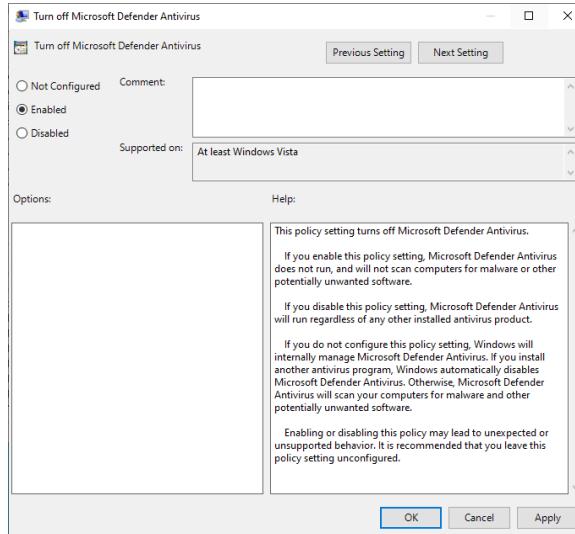


Figura 56. Se habilita la política "Desactivar Microsoft Defender Antivirus".

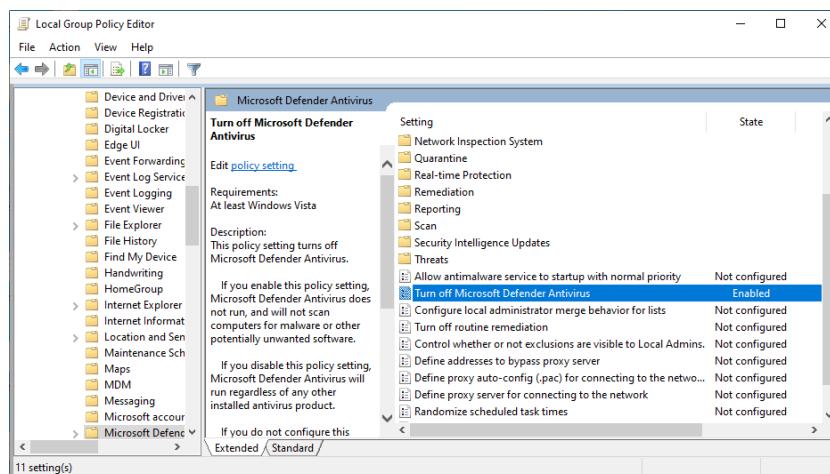


Figura 57. Se observa que ya se encuentra habilitada.

11. Configure los días que un programa o archivo está en cuarentena

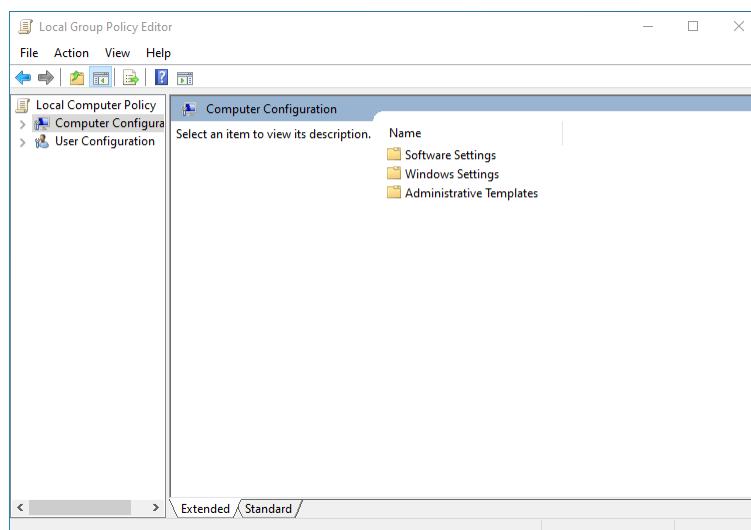


Figura 58. En el Editor de Políticas de Grupo, se navega a la opción “Computer Configuration”.

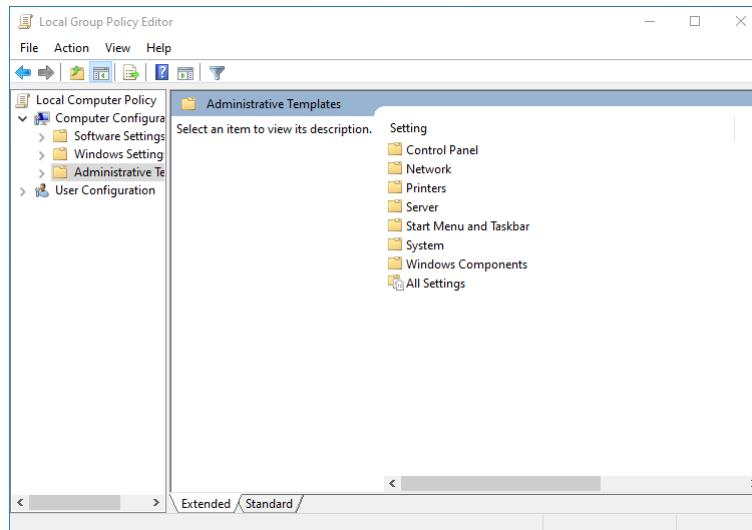


Figura 59. Se navega a la opción “Administrative Templates”.

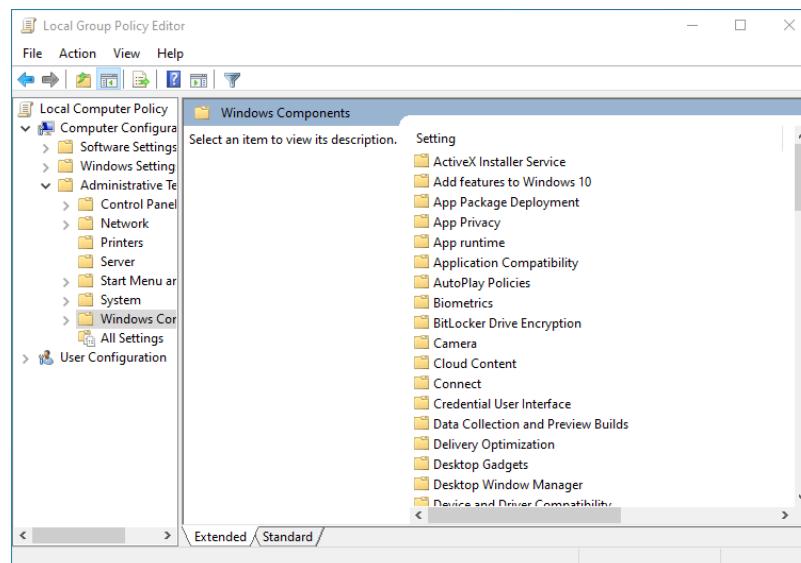


Figura 60. Se navega a la opción “Windows Components”.

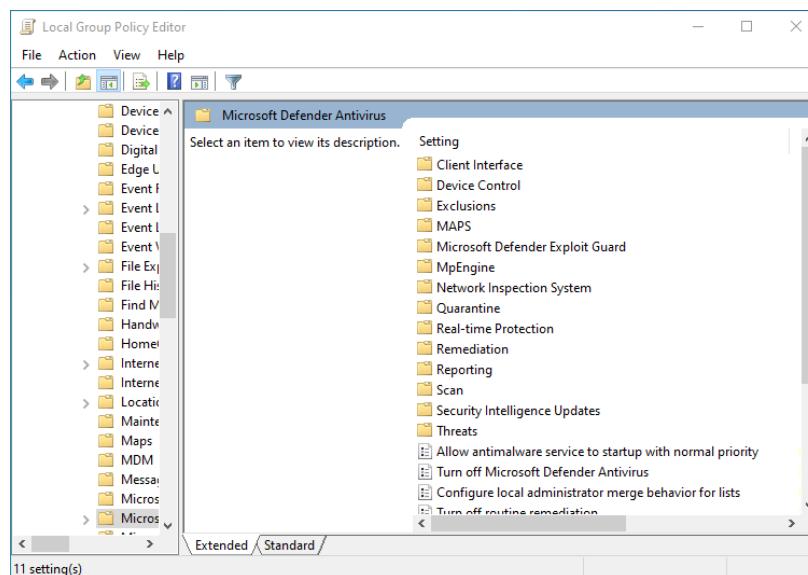


Figura 61. Se navega a la opción “Microsoft Defender Antivirus”.

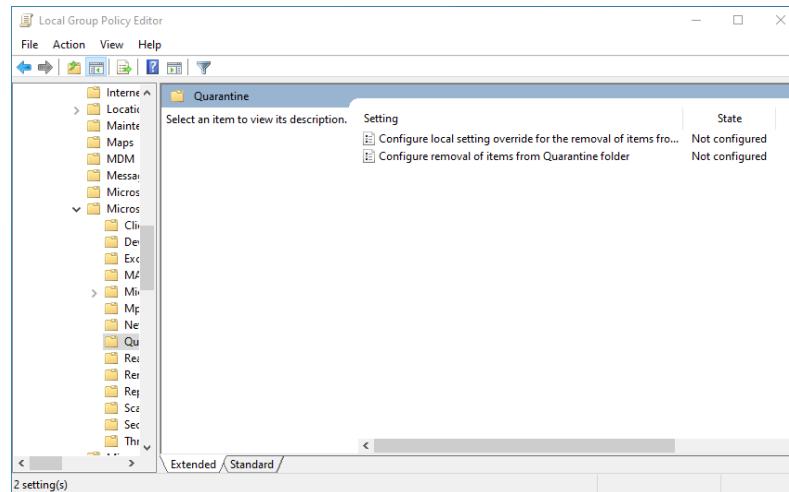


Figura 62. Se navega a la opción “Quarantine”.

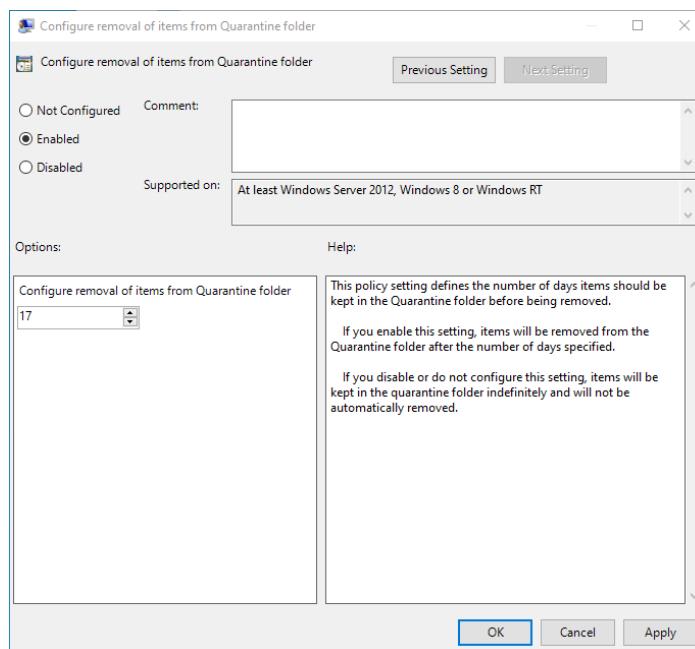


Figura 63. Se habilita la política “Configurar la eliminación de elementos de la carpeta de Cuarentena” y se configuran los días.

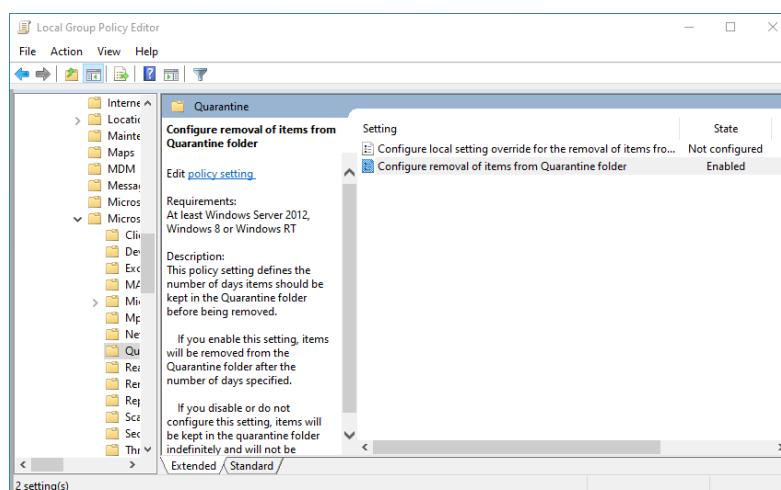


Figura 64. Se observa que ya se encuentra habilitada.



12. Apagar la protección en tiempo real

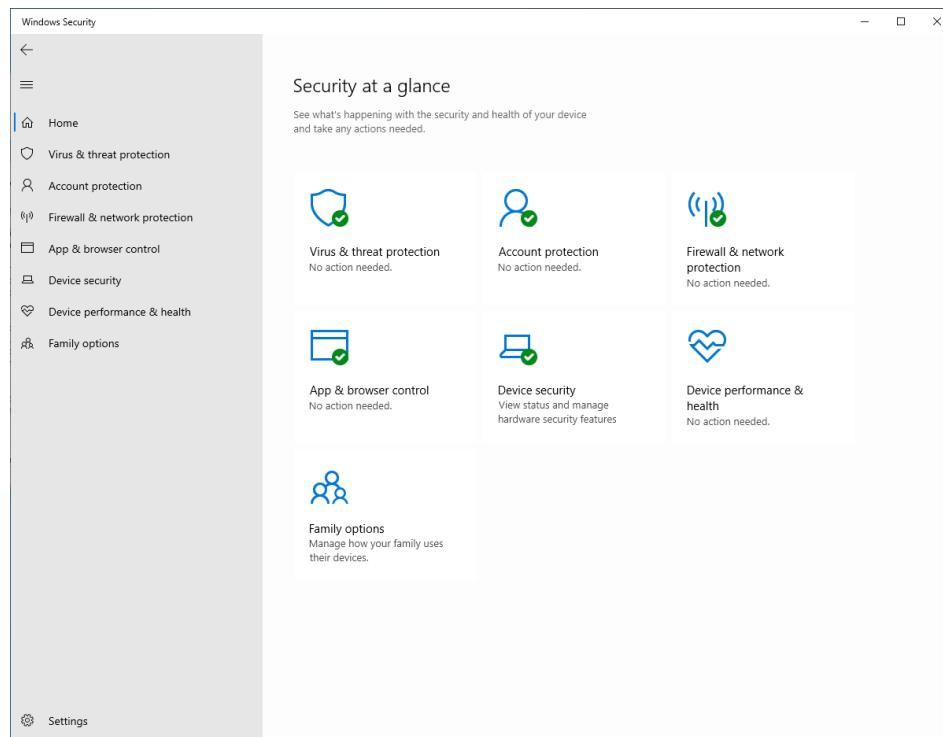


Figura 65. Se ingresa a la opción “Windows Security”.

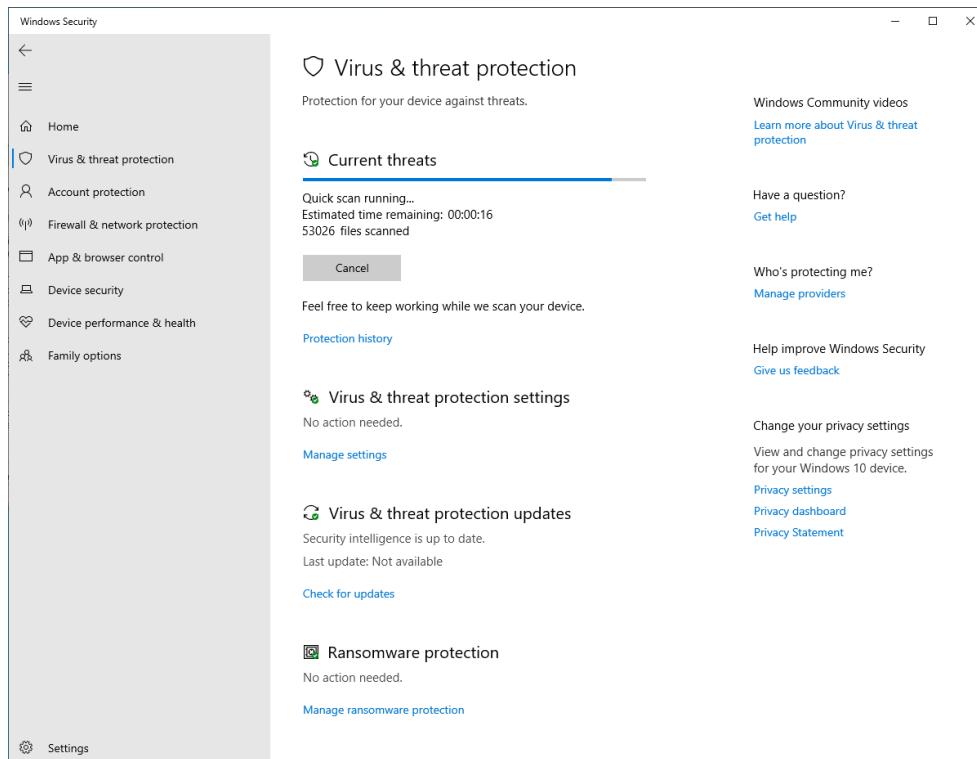


Figura 66. Se navega a la opción "Virus & threat protection".

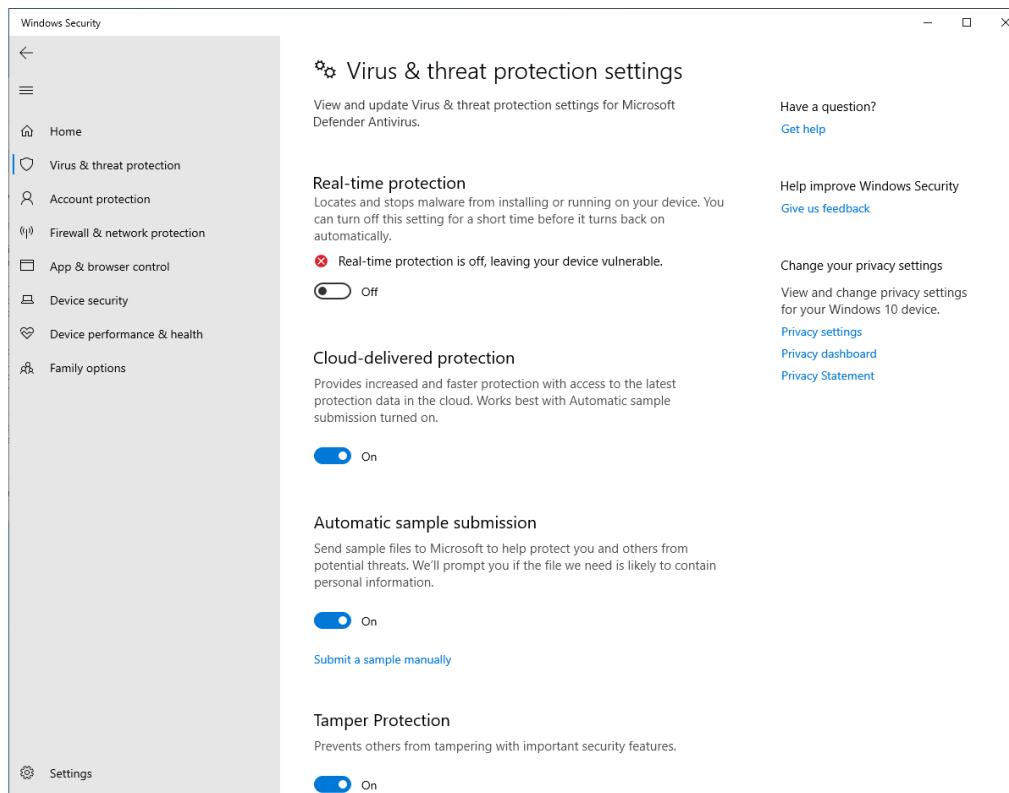


Figura 67. Se apaga la protección en tiempo real.

13. Configurar el escaneo de dispositivos móviles en busca de virus o software malicioso.

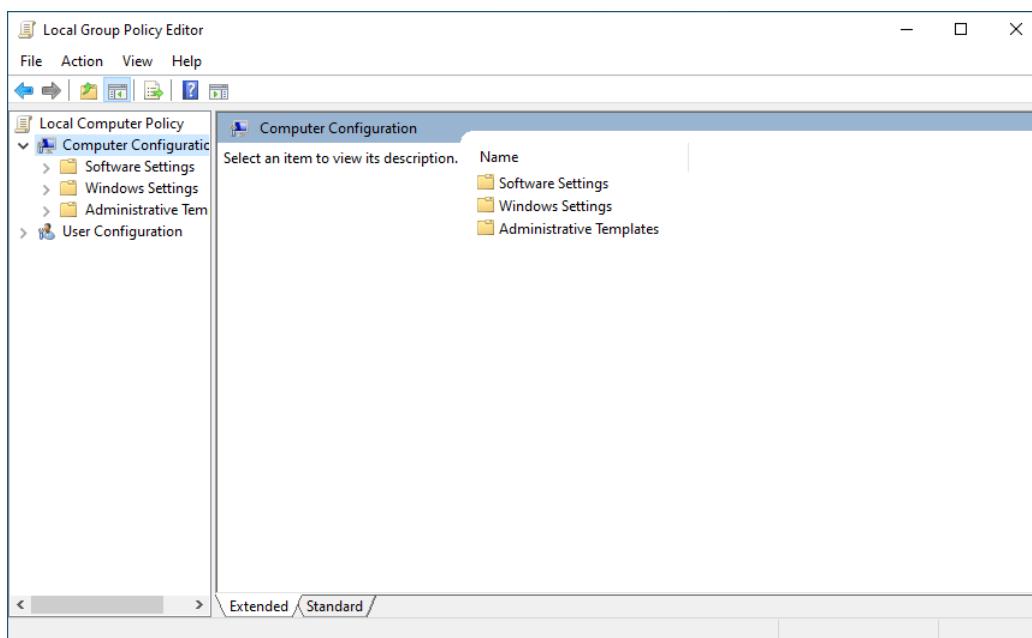


Figura 68. En el Editor de Políticas de Grupo, se navega a la opción “Computer Configuration”.

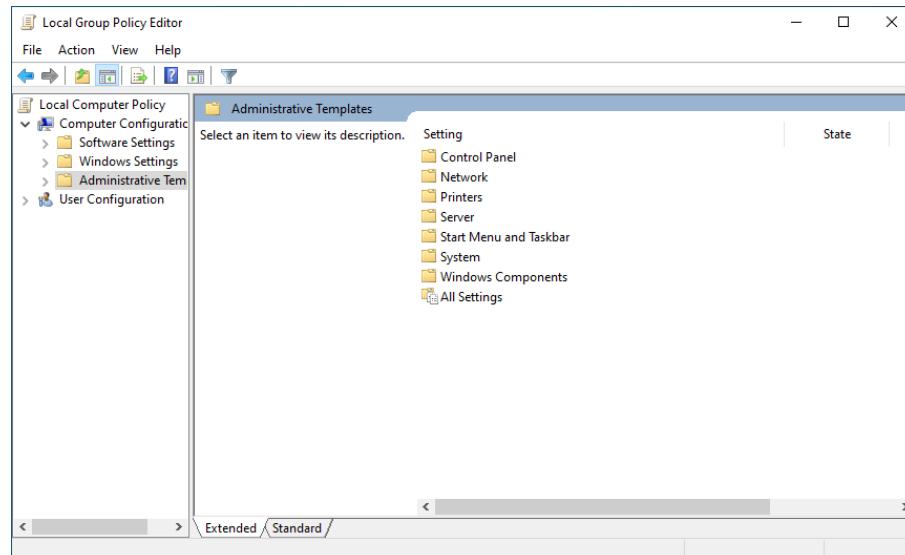


Figura 69. Se navega a la opción “Administrative Templates”.

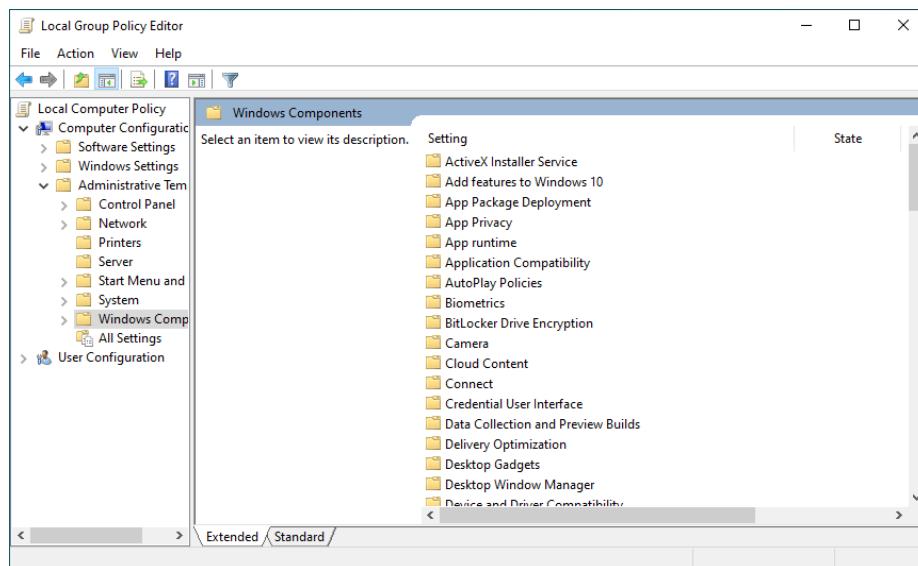


Figura 70. Se navega a la opción “Windows Components”.

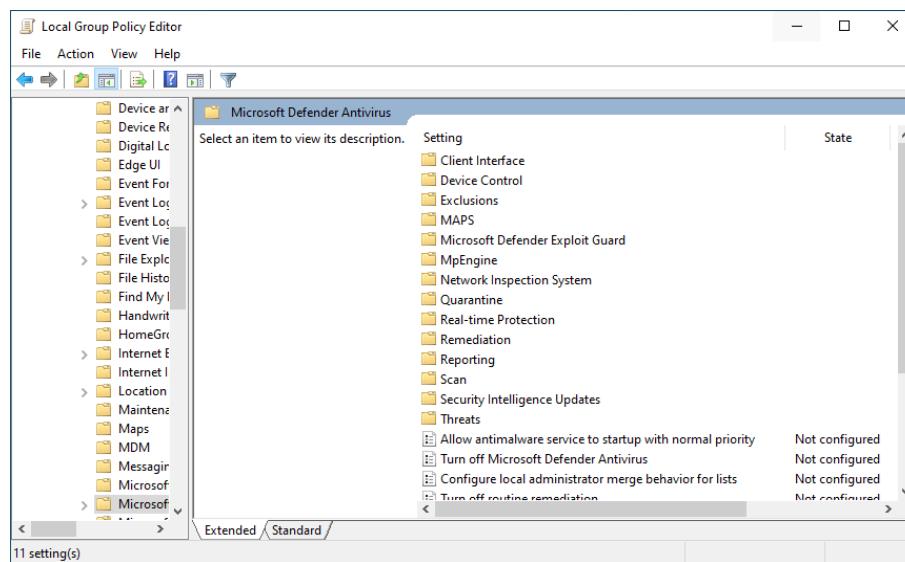


Figura 71. Se navega a la opción “Microsoft Defender Antivirus”.

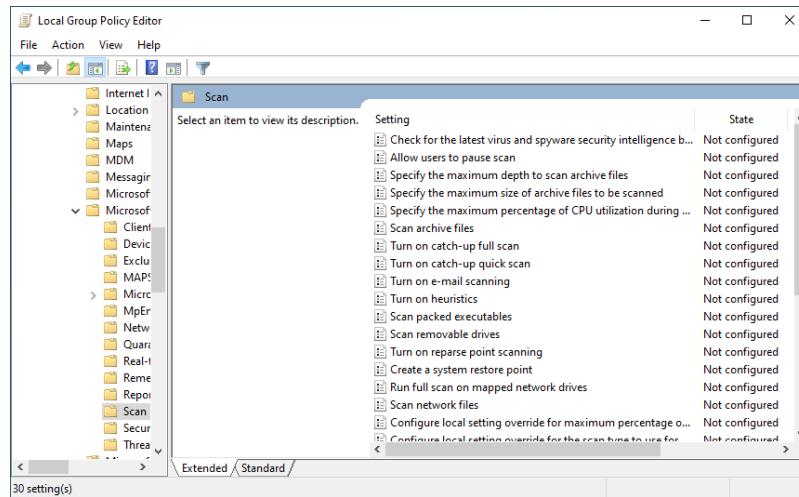


Figura 72. Se navega a la opción “Scan”.

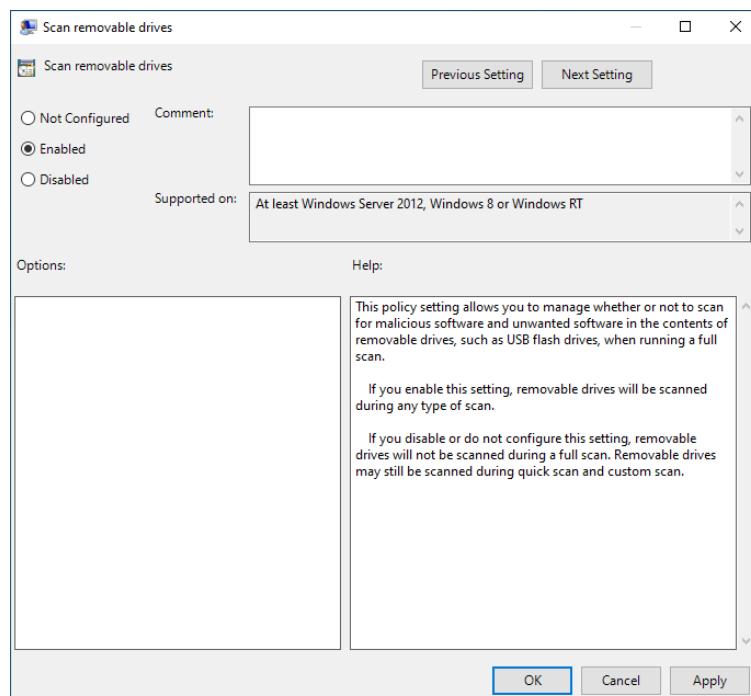


Figura 73. Se habilita la política “Escanear unidades extraíbles”.

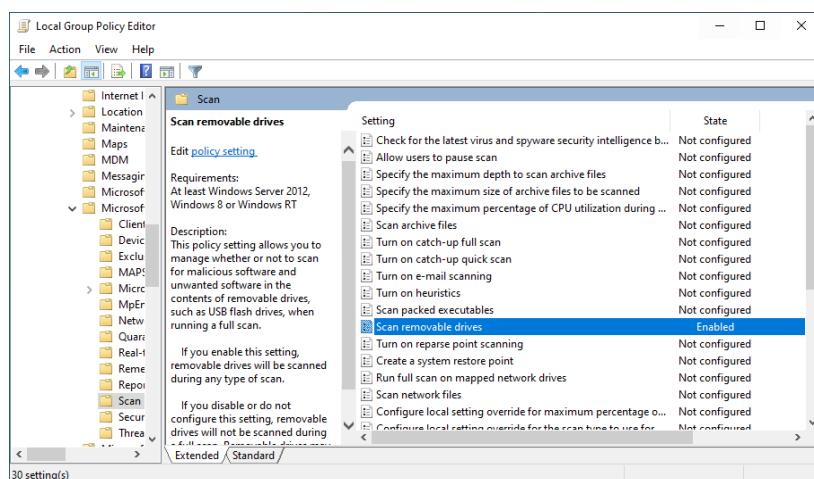


Figura 74. Se observa que ya se encuentra habilitada.



14. Deshabilitar las noticias e intereses en la barra de tareas.

En este caso, no es necesario ingresar al Editor de Políticas de Grupo.

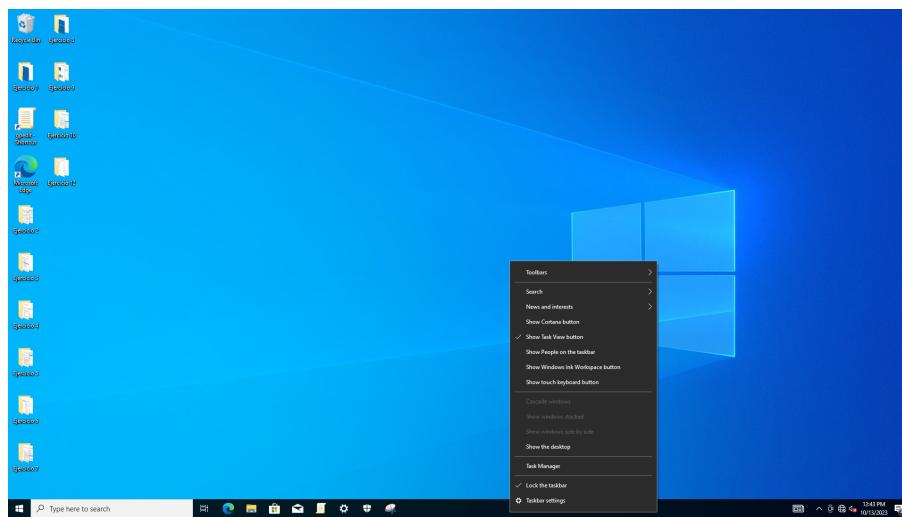


Figura 75. Se presiona en la barra de tareas con el botón derecho.

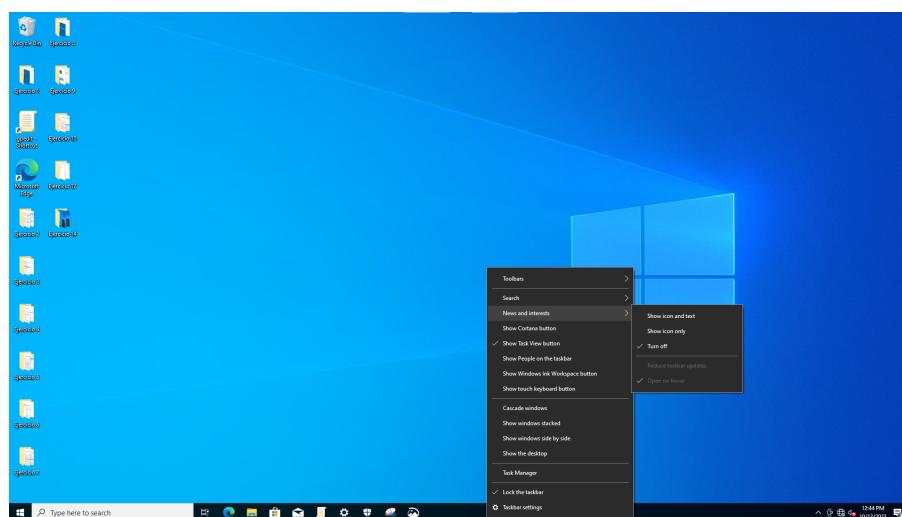


Figura 76. Se selecciona en la opción “News and interests”.

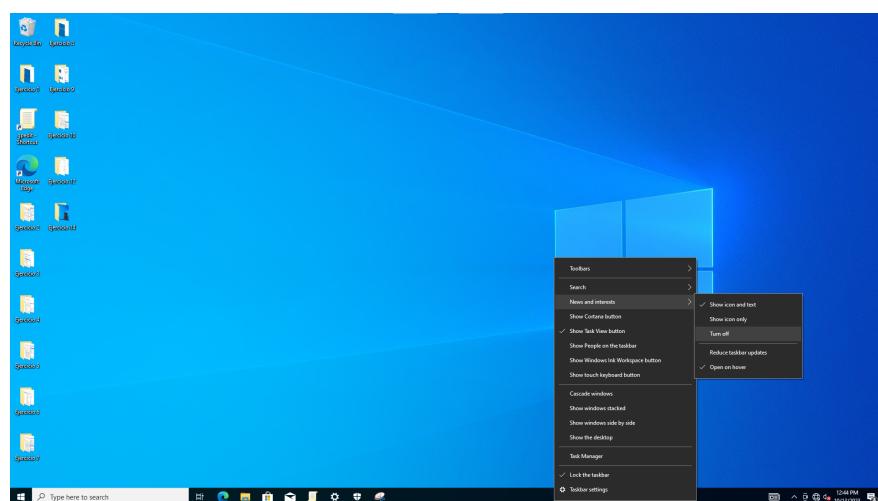


Figura 77. Se selecciona en la opción “Turn off” para apagarlo.



15. Apagar el auto reinicio para actualizaciones en horas de trabajo.

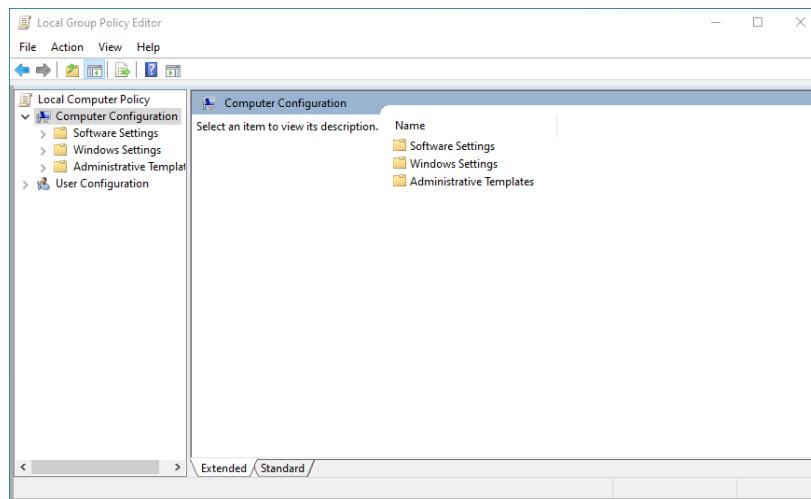


Figura 78. En el Editor de Políticas de Grupo, se navega a la opción “Computer Configuration”.

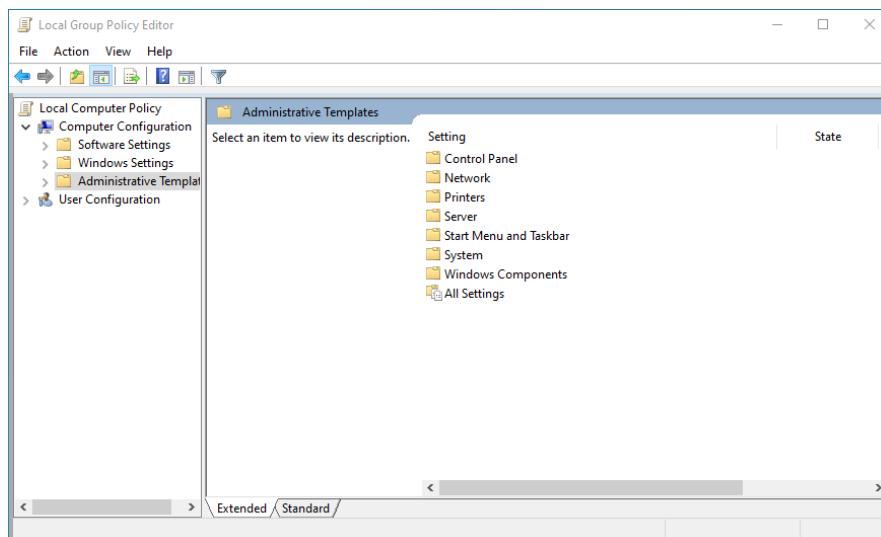


Figura 79. Se navega a la opción “Administrative Templates”.

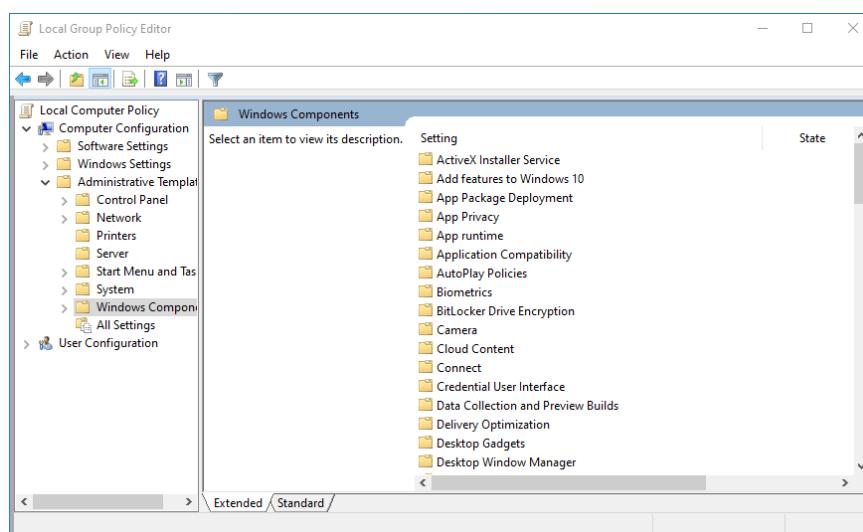


Figura 80. Se navega a la opción “Windows Components”.

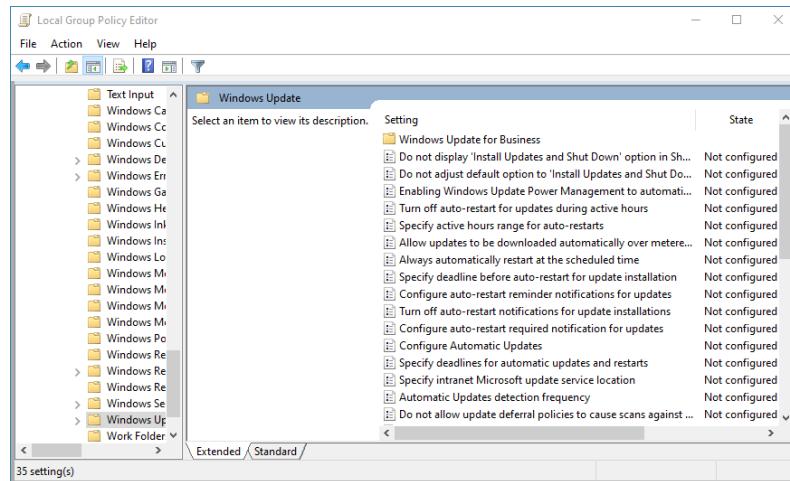


Figura 81. Se navega a la opción “Windows Update”.

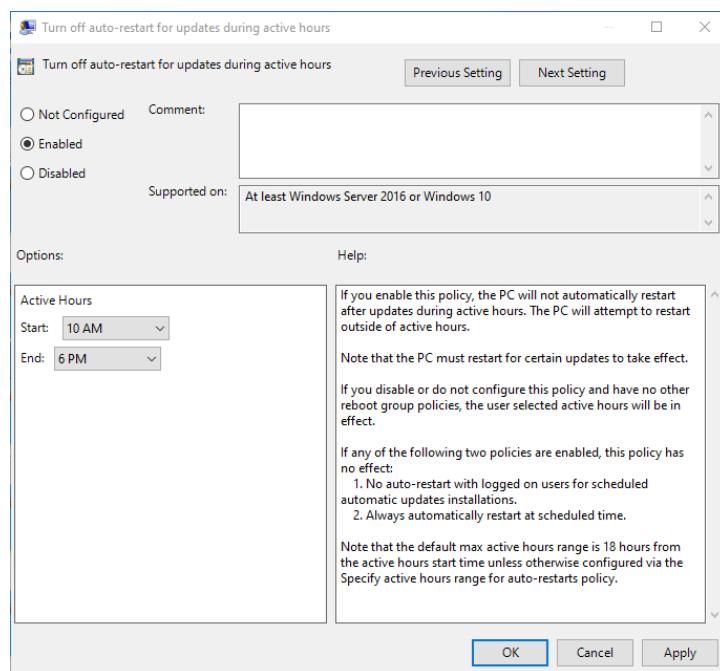


Figura 82. Se habilita la política "Apagar el auto-reinicio para actualizaciones durante horas de trabajo" y se configura este horario.

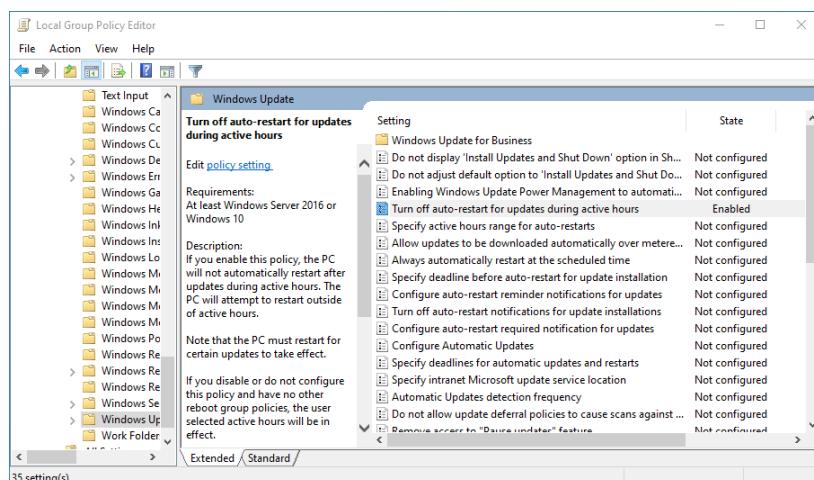


Figura 83. Se observa que ya se encuentra deshabilitada.



16. Habilitar la ejecución de scripts

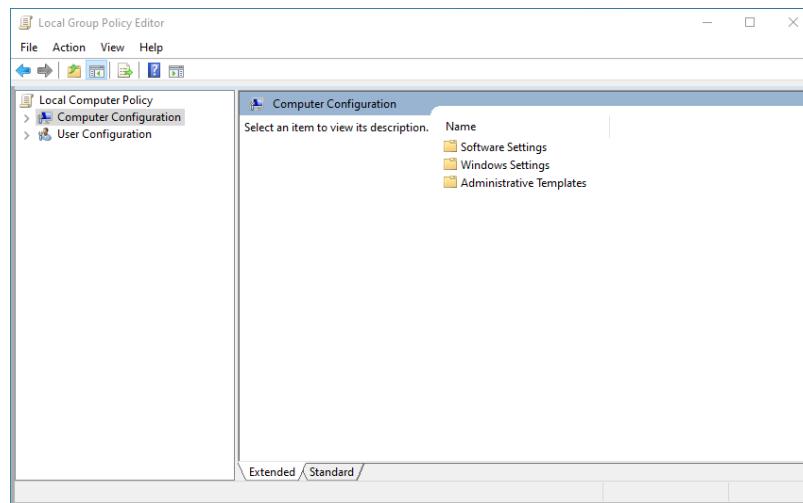


Figura 84. En el Editor de Políticas de Grupo, se navega a la opción “Computer Configuration”.

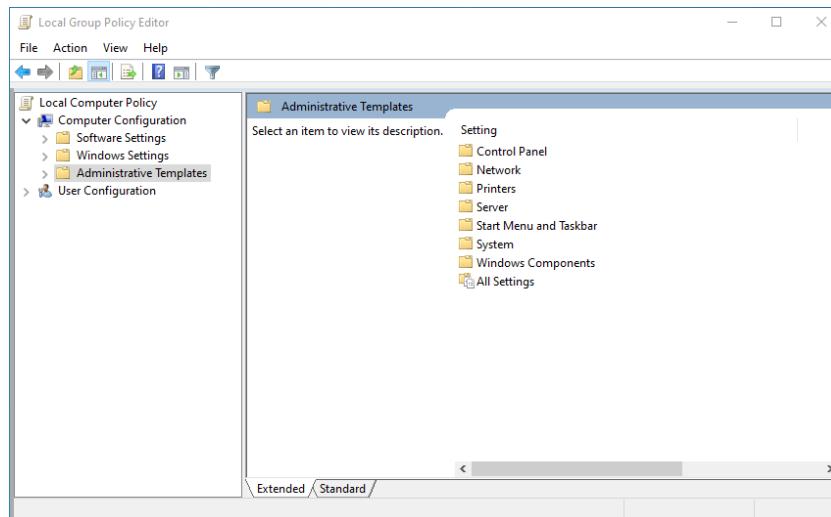


Figura 85. Se navega a la opción “Administrative Templates”.

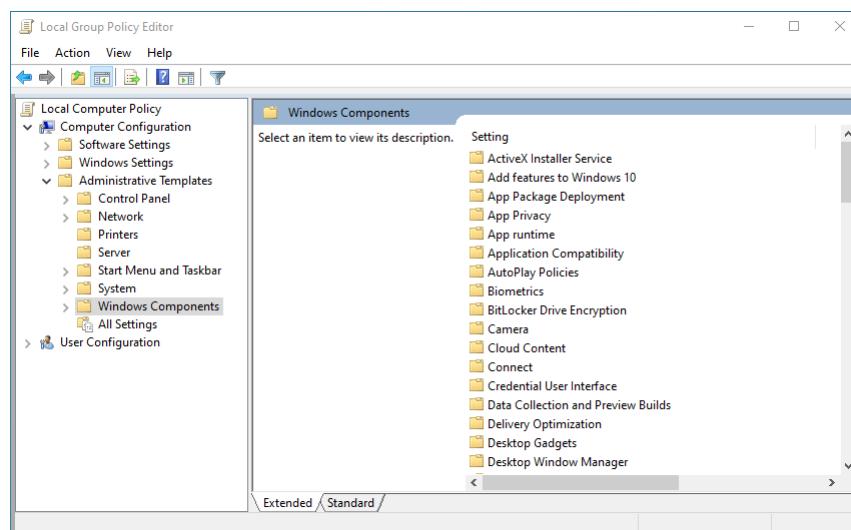


Figura 86. Se navega a la opción “Windows Components”.

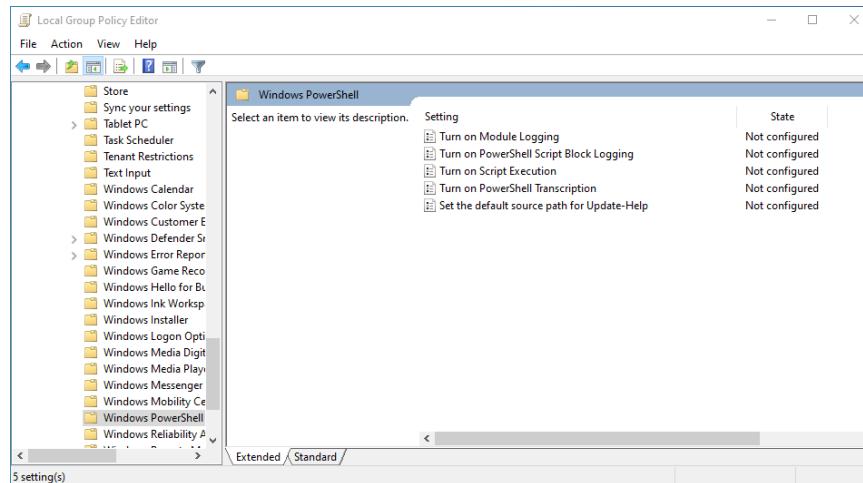


Figura 87. Se navega a la opción “Windows PowerShell”.

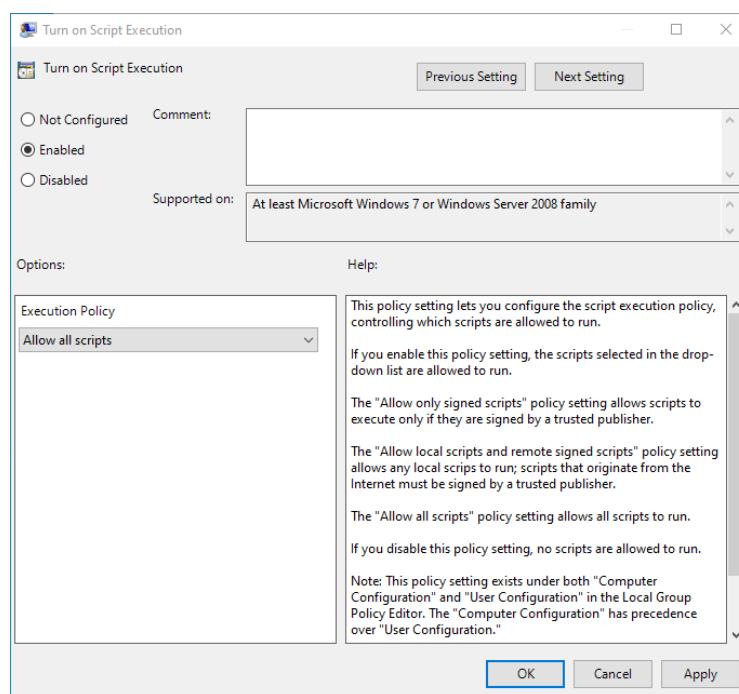


Figura 88. Se habilita la política “Prender la Ejecución de Scripts”.

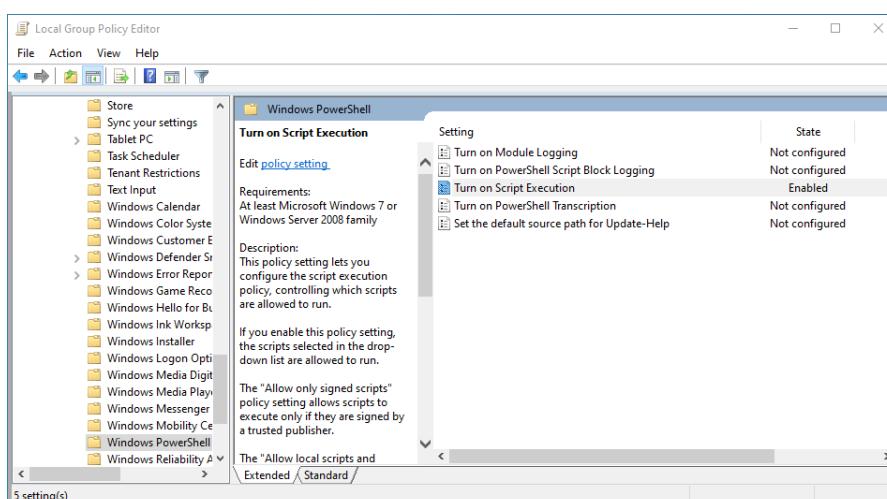


Figura 89. Se observa que ya se encuentra deshabilitada.



17. Habilitar la creación de puntos de restauración

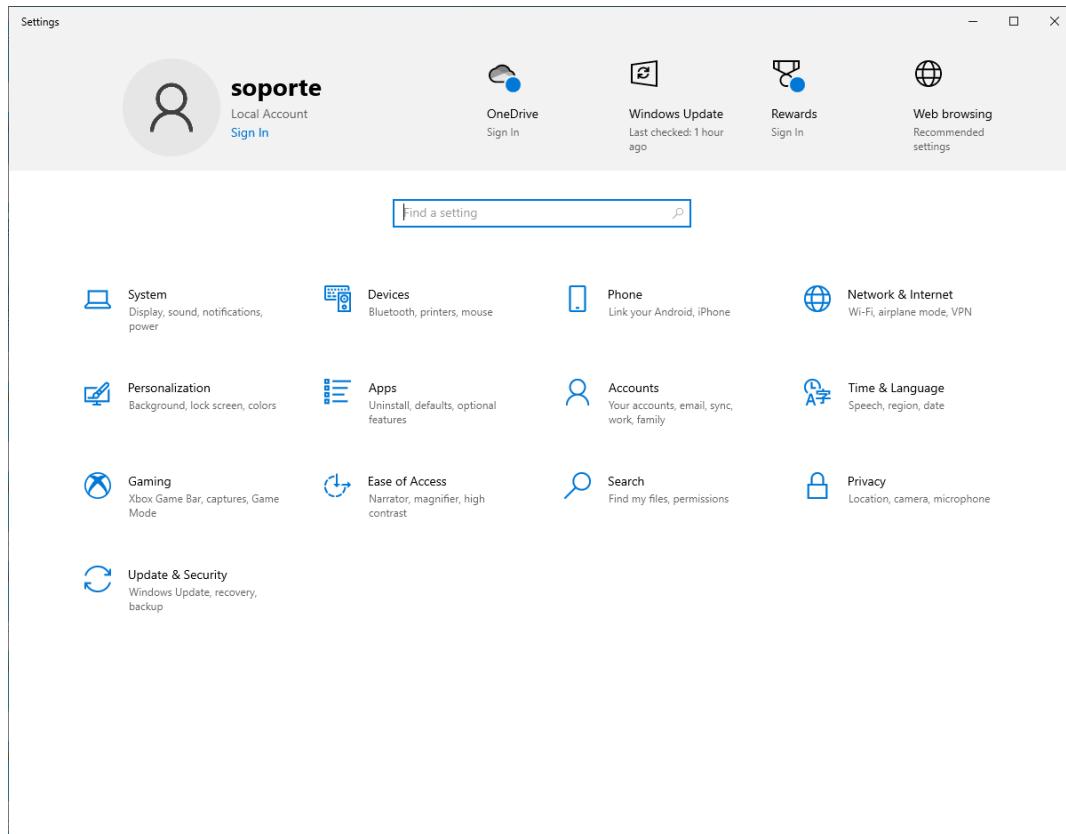


Figura 90. Se ingresa a las Configuraciones del equipo.

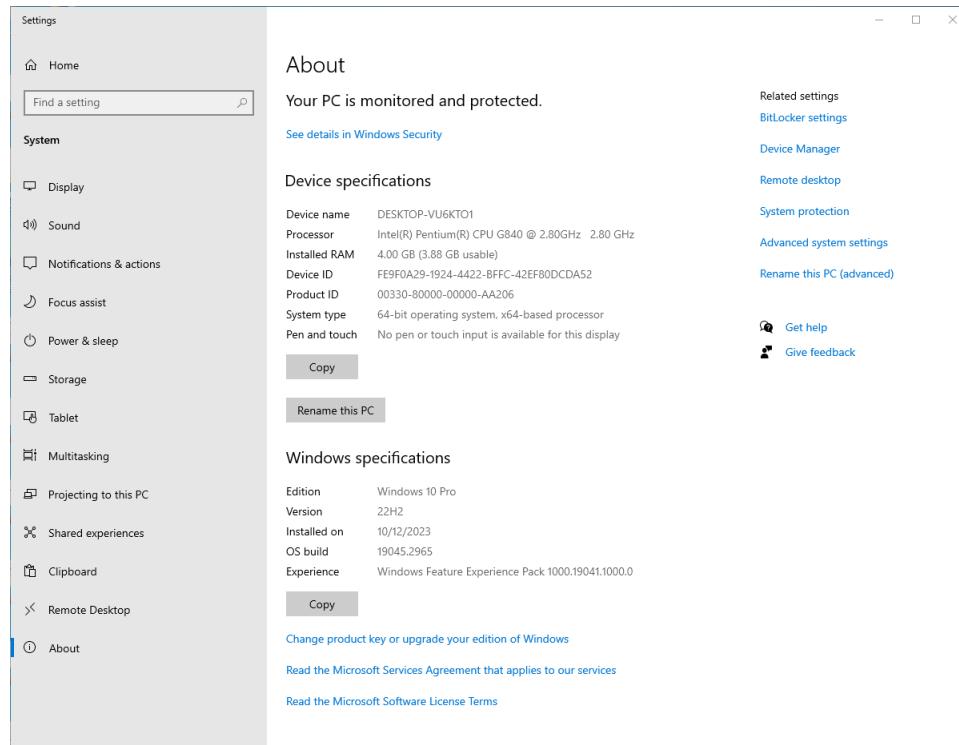


Figura 91. Se ingresa a la opción "System".

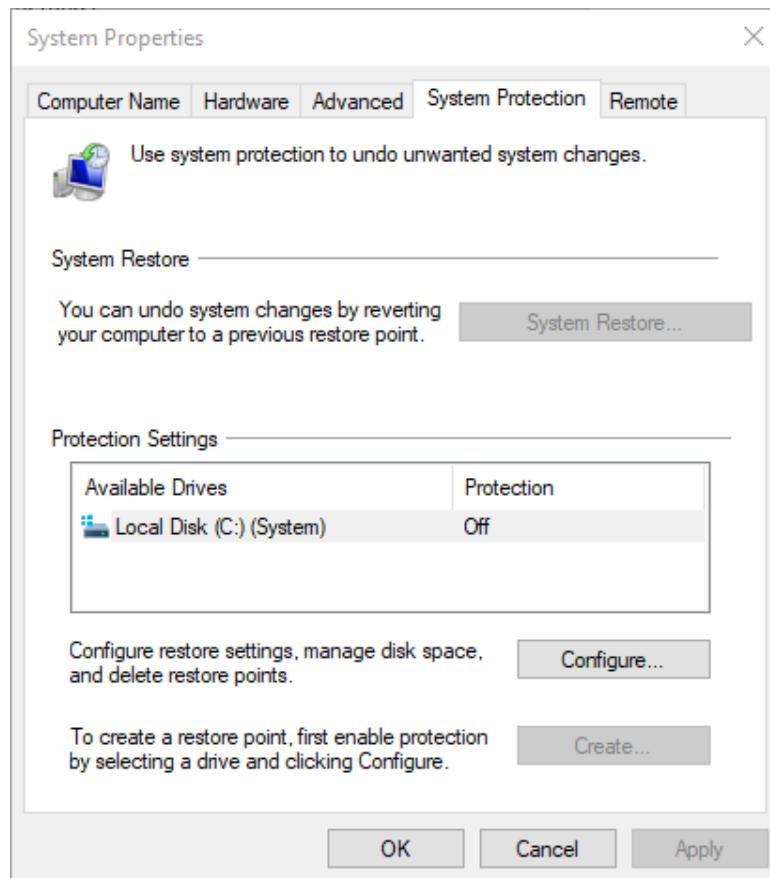


Figura 92. Se ingresa a la opción “System Properties”.

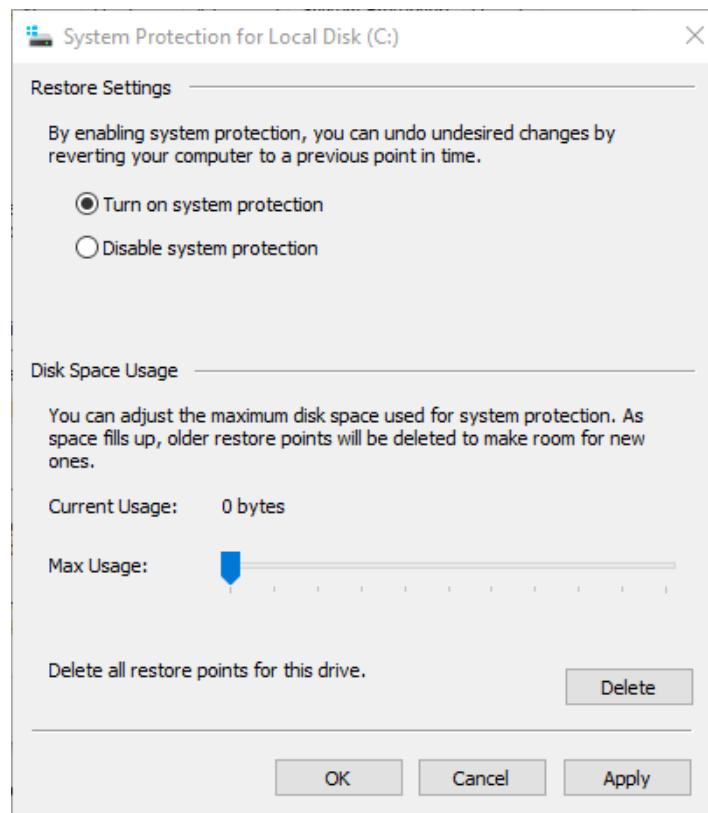


Figura 93. Se ingresa a la opción “Configure”, seleccionando al disco actual y se habilita la creación de puntos de restauración.

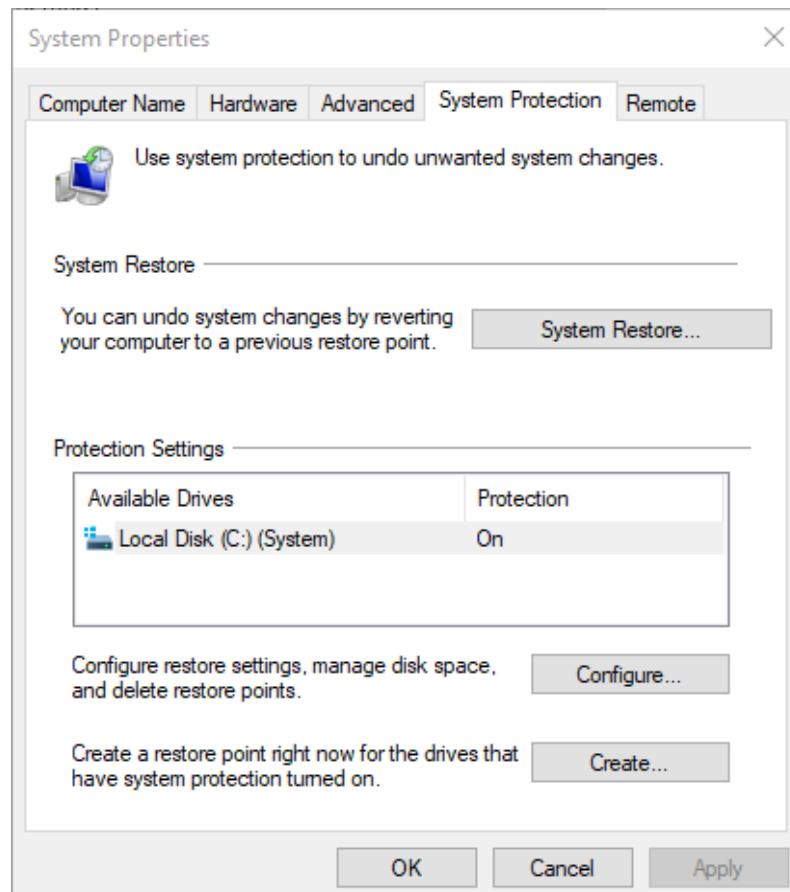


Figura 94. Se observa que ya se encuentra habilitada.

18. Ocultar la opción “agregar/remover programas?”

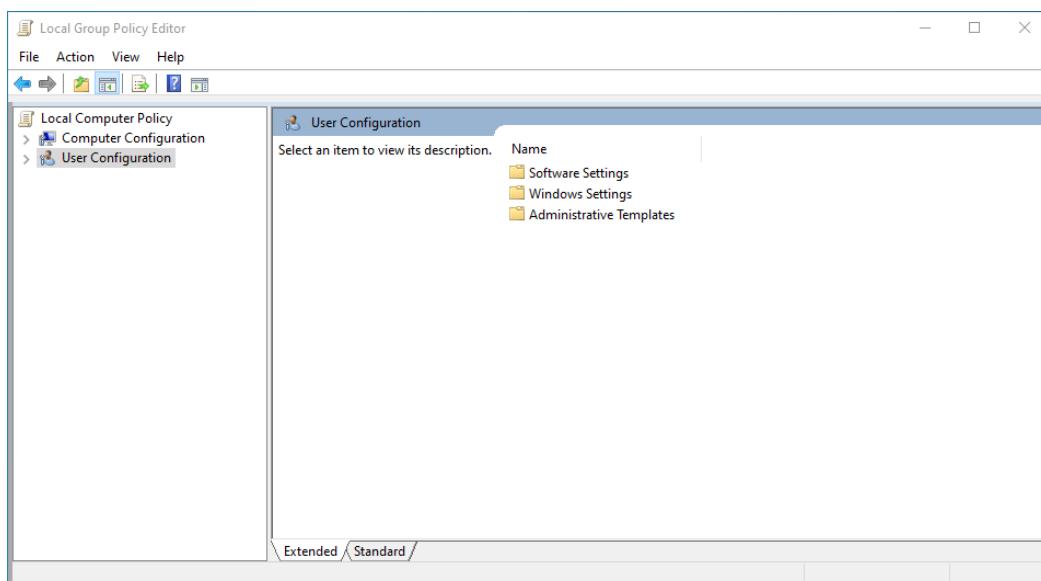


Figura 95. En el Editor de Políticas de Grupo, se navega a la opción “User Configuration”.

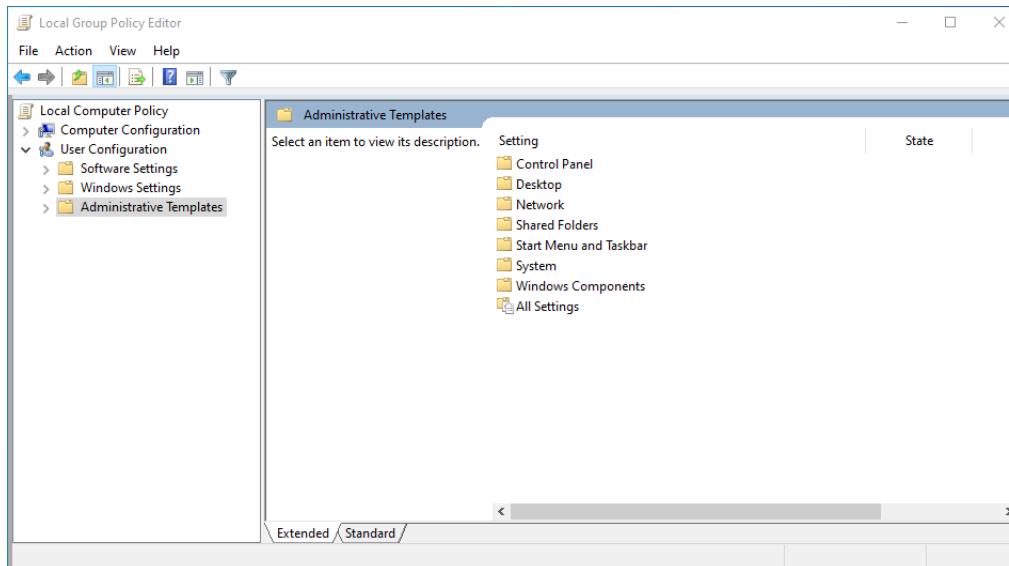


Figura 96. Se navega a la opción “Administrative Templates”.

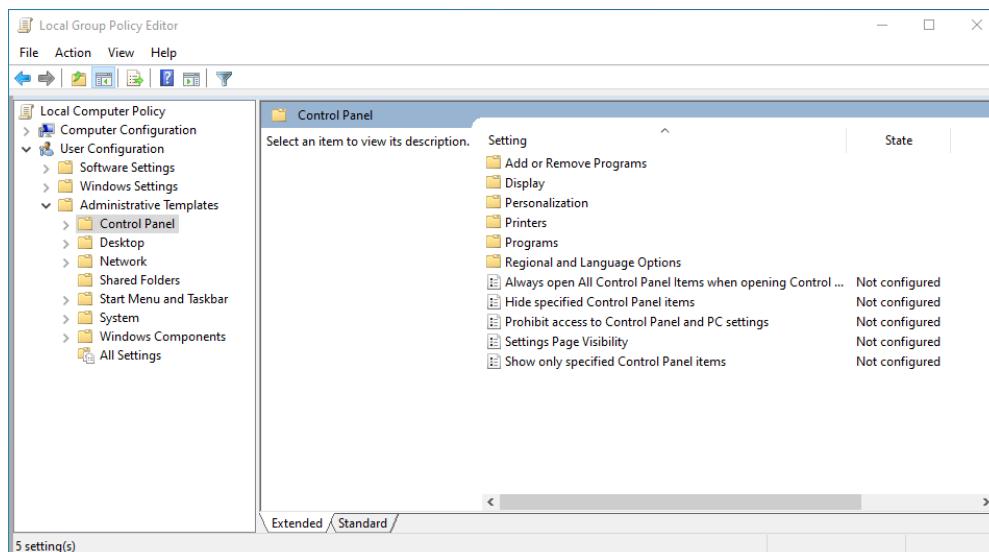


Figura 97. Se navega a la opción “Control Panel”.

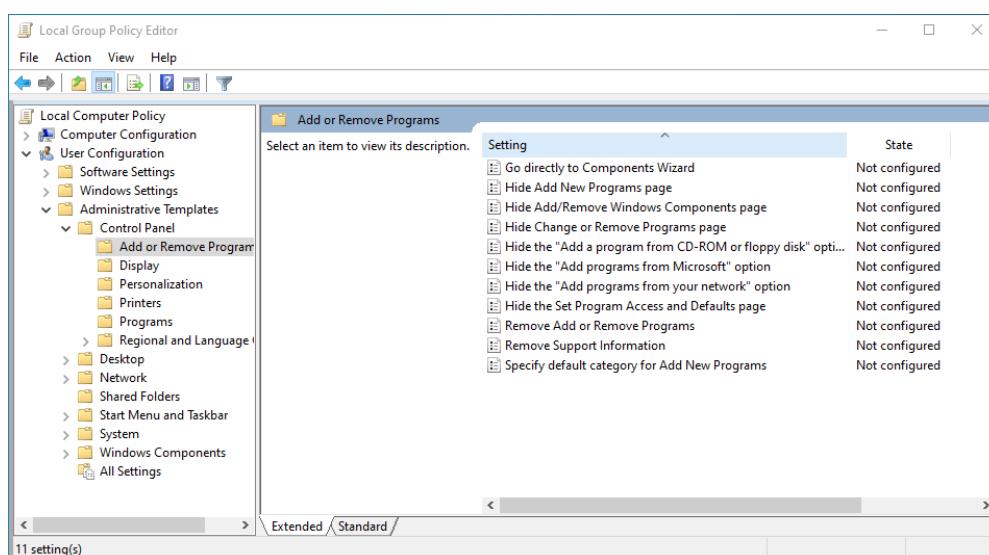


Figura 98. Se navega a la opción “Add or Remove Programs”.

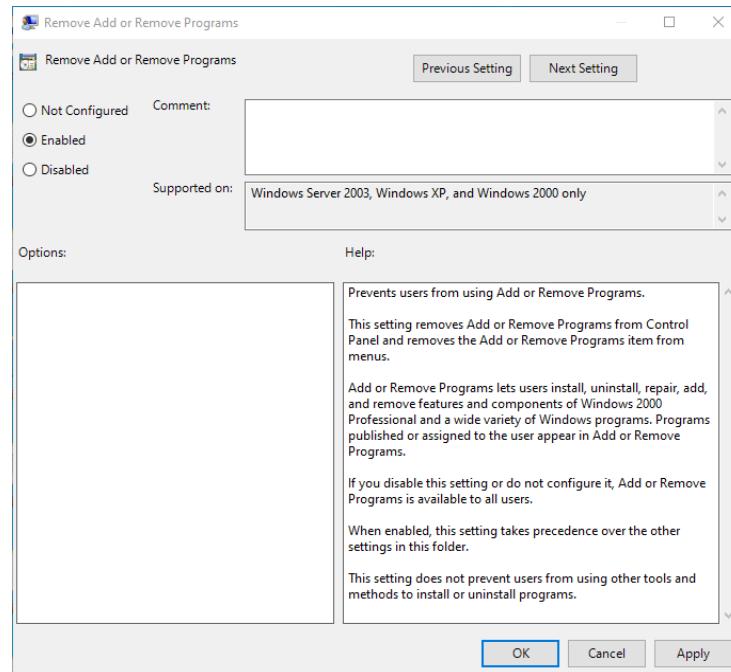


Figura 99. Se habilita la política de “Eliminar la opción de Agregar o Remover Programas”.

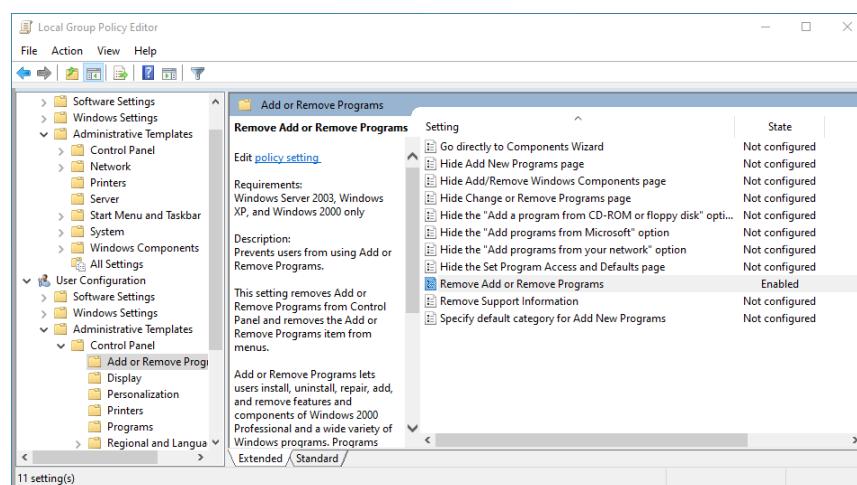


Figura 100. Se observa que ya se encuentra habilitada.

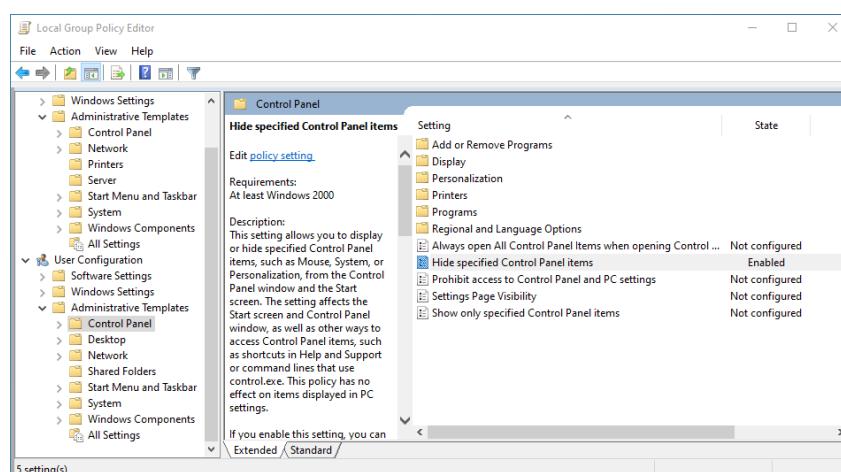


Figura 101. De igual manera, se habilita la política de “Esconder elementos específicos del Control Panel”.

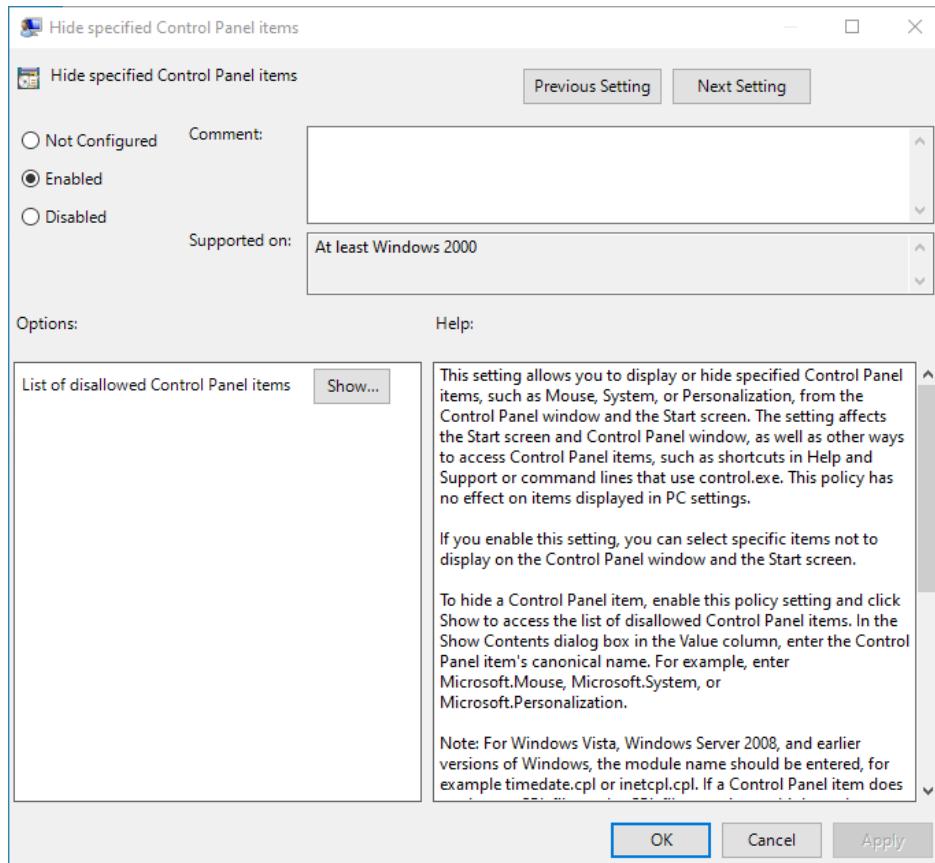


Figura 102. Se habilita la política.

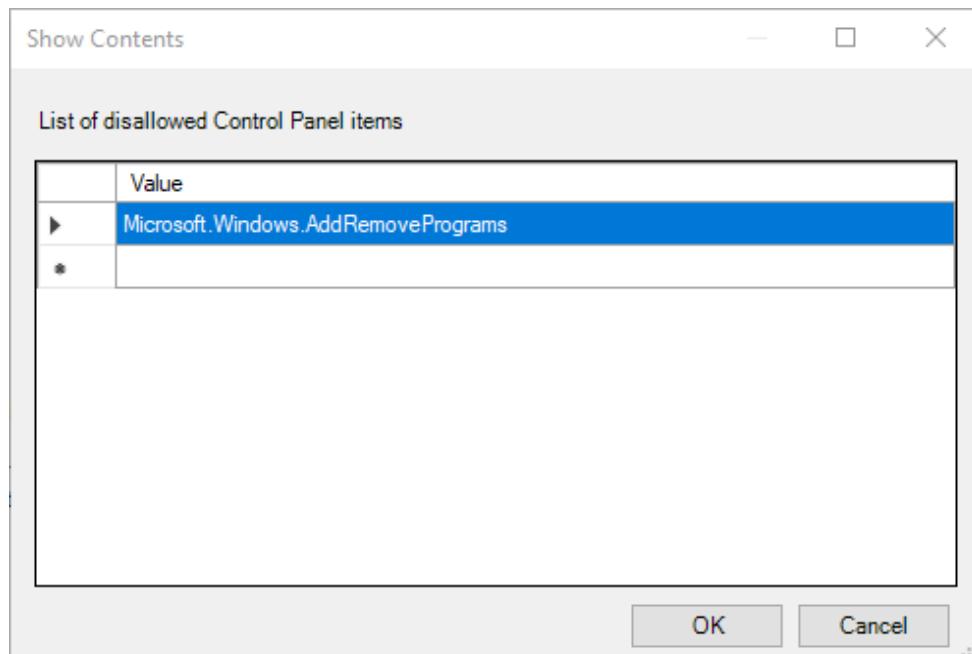


Figura 103. Se selecciona el elemento Agregar/Remover Programas.



19. Habilitar el Screen Saver

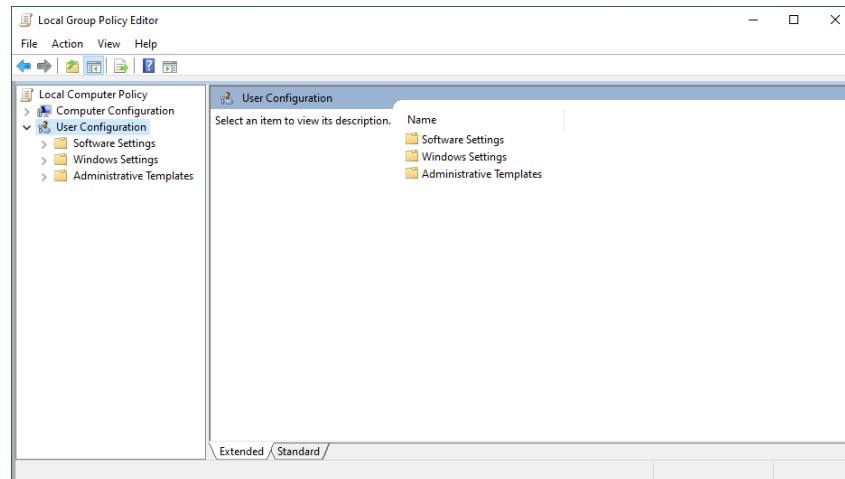


Figura 104. En el Editor de Políticas de Grupo, se navega a la opción “User Configuration”.

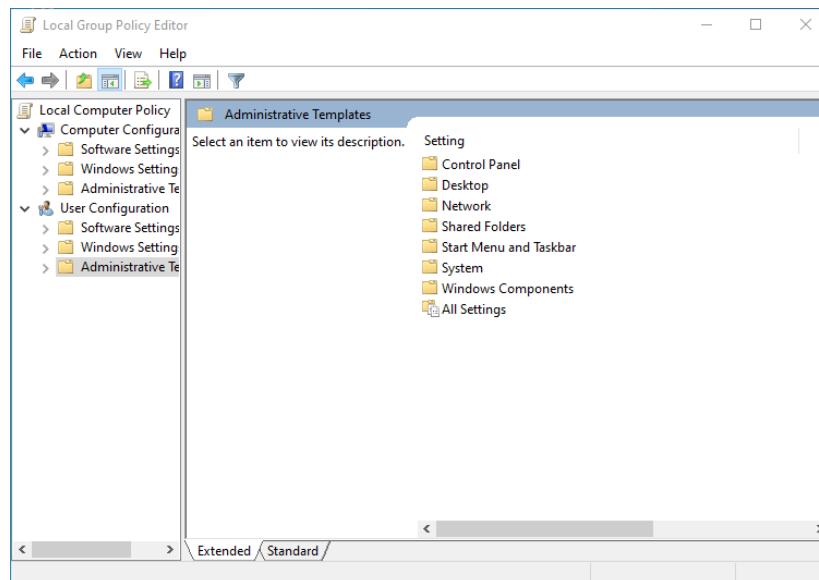


Figura 105. Se navega a la opción “Administrative Templates”.

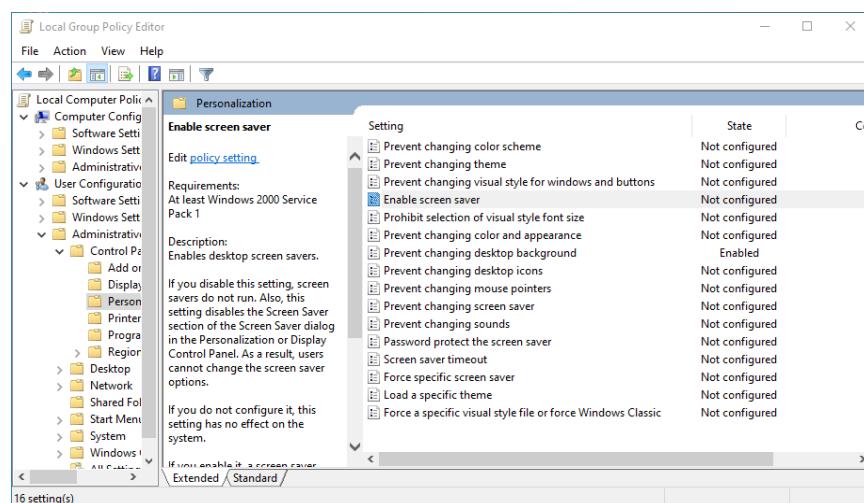


Figura 106. Se navega a la opción “Personalization”.

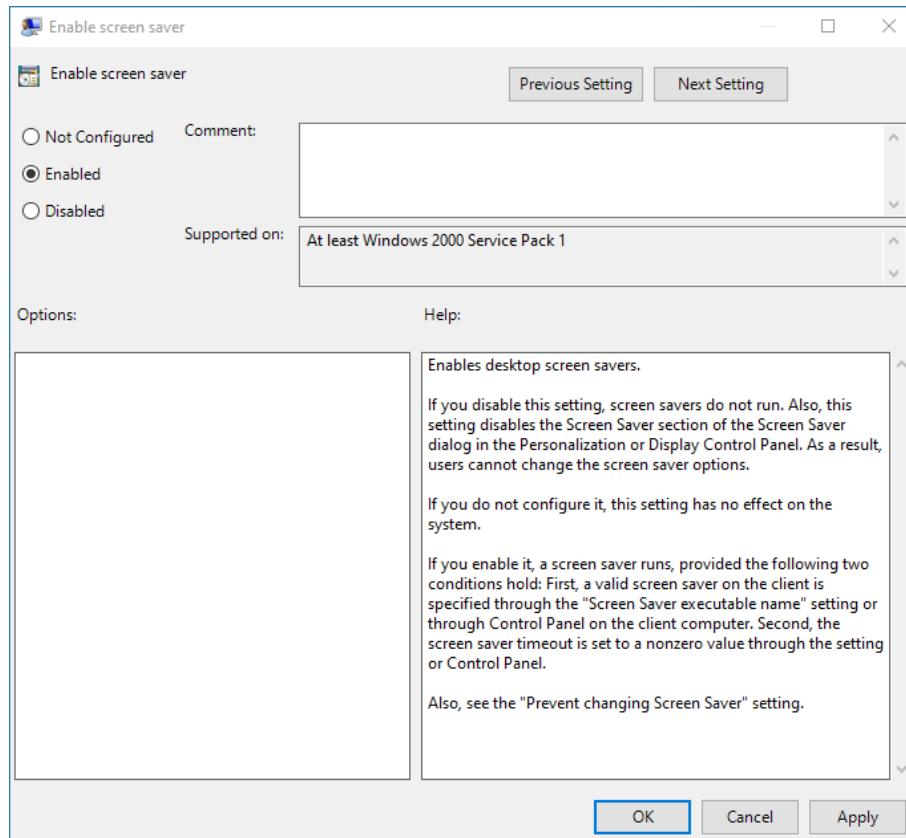


Figura 107. Se habilita la política "Habilitar Screen Saver".

Setting	State
Enable screen saver	Enabled
Prevent changing color scheme	Not configured
Prevent changing theme	Not configured
Prevent changing visual style for windows and buttons	Not configured
Prohibit selection of visual style font size	Not configured
Prevent changing color and appearance	Not configured
Prevent changing desktop background	Enabled
Prevent changing desktop icons	Not configured
Prevent changing mouse pointers	Not configured
Prevent changing screen saver	Not configured
Prevent changing sounds	Not configured
Password protect the screen saver	Not configured
Screen saver timeout	Not configured
Force specific screen saver	Not configured
Load a specific theme	Not configured
Force a specific visual style file or force Windows Classic	Not configured

Figura 108. Se observa que ya se encuentra habilitada.



Conclusión

René Sebastián Arriaga Alonso:

En conclusión, Active Directory se considera un pilar fundamental en la gestión de recursos y usuarios en entornos Windows, ofreciendo una solución centralizada para la administración de objetos de red. La capacidad de establecer políticas de configuración tanto para computadoras como para usuarios permite una personalización y control precisos en toda la red. Además, herramientas como el Editor de Políticas de Grupo y el lenguaje de scripting Power Shell proporcionan a los administradores las herramientas necesarias para automatizar tareas y mantener un sistema eficiente.

En el mundo de la gestión de sistemas y redes, Windows ofrece una gran variedad de herramientas que desempeñan un papel crucial en la administración eficiente de recursos y objetos de red. Estas herramientas no solo simplifican las tareas cotidianas de administración, sino que también contribuyen significativamente a la optimización de los procesos y a la seguridad de la red.

Richelle Nadine Reyes Udasco:

Las actividades relacionadas con la configuración de Windows y las políticas de grupo son fundamentales para administrar y personalizar el entorno de un sistema operativo Windows, y es justamente con lo que se trabajó en esta primera práctica.

Primeramente, considero que la práctica realizada es de suma importancia, ya que el Active Directory de Windows desempeña un papel fundamental en la gestión y organización de sistemas operativos de esta plataforma. Además de esto, el uso del Editor de Políticas de Grupo, que se ha explorado en detalle durante esta experiencia, se ha revelado como una herramienta de gran utilidad, particularmente en lo que respecta a la personalización y configuración de entornos de trabajo. De esta manera, con ambas herramientas se logró abarcar desde la seguridad hasta la personalización de la experiencia del usuario.



En conclusión, esta práctica no solo ha subrayado la importancia del Active Directory y el Editor de Políticas de Grupo, sino que también ha subrayado la necesidad de adquirir habilidades en su uso, dada la presencia de Windows en el mundo actual. En conjunto, estas herramientas y conceptos son fundamentales para administrar entornos Windows de una manera eficaz, garantizando así, la seguridad y estabilidad de los equipos.



Referencias Bibliográficas

1. ADMX. (s. f.). *No guardar historial de documentos abiertos recientemente.*
https://admx.help/?Category=Windows_7_2008R2&Policy=Microsoft.Policies.StartMenu::NoRecentDocsHistory&Language=es-es
2. Buckbee, M. (2022). Group Policy Editor Guide: Access Options and How to Use. *Varonis.* <https://www.varonis.com/blog/group-policy-editor>
3. Colaboradores de Microsoft. (2023). Introducción a Active Directory Domain Services. *Microsoft.*
<https://learn.microsoft.com/es-es/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview>
4. Colaboradores de Microsoft. (2023). Mantente protegido con Seguridad de Windows. *Microsoft.*
<https://support.microsoft.com/es-es/windows/mantente-protegido-con-seguridad-de-windows-2ae0363d-0ada-c064-8b56-6a39afb6a96>
5. Dan, T. (2022). What is the Local Group Policy Editor, and how do I use it?. *Digital Citizen.*
<https://www.digitalcitizen.life/simple-questions-what-local-group-policy-editor-how-use-it/>