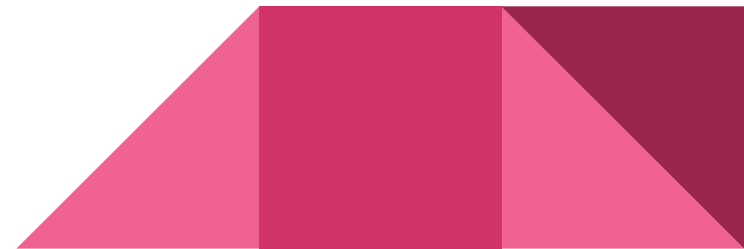


UD4 – WINDOWS – ADMINISTRACIÓ I CONFIGURACIÓ-III

1º DAW - CFGS

Prof. Manuel Enguidanos
menguidanos@fpmislata.com

4.6. COPIES DE SEGURETAT



4.6. Copias de seguridad

En Windows 11, las copias de seguridad se pueden realizar desde **Configuración → Cuentas → Copias de seguridad**. Hay que sincronizar el equipo con una cuenta de Microsoft One Drive y guardar allí las copias de seguridad de los archivos.

En Windows 10, las copias de seguridad están en **Configuración → Actualización y seguridad → Copia de seguridad**. Allí debe agregarse la unidad donde se van a guardar las copias y en **Más opciones** ir a **Historial de archivos** para terminar de configurar las copias.

En ambos sistemas se pueden realizar las copias utilizando directamente la utilidad **Historial de archivos** del Panel de Control. Hay que seleccionar una ubicación externa o una ubicación de red, y después activar el historial de archivos (Figura 4.49). Por defecto vienen seleccionados los archivos de Bibliotecas, Escritorio, Contactos y Favoritos. En **Configuración avanzada** puede seleccionarse la frecuencia con la que realizar las copias y el tiempo que se deseen tener las versiones almacenadas.

4.6. Copias de seguridad

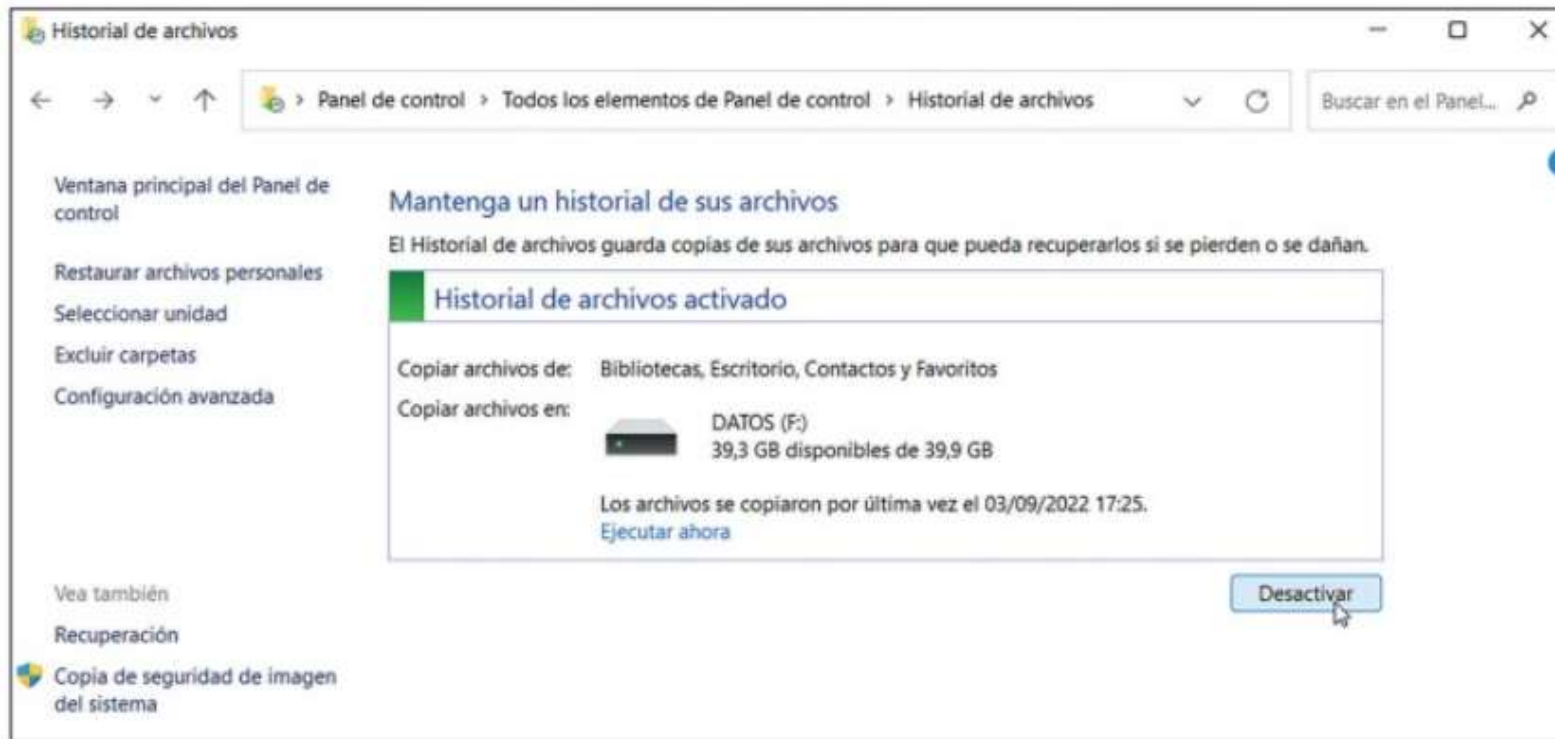


Figura 4.49. Activación de las copias de seguridad de Bibliotecas, Escritorio, Contactos y Favoritos en una unidad externa para datos.

4.6. Copias de seguridad

Historial de archivos

← → ↕ ↶ ↷ > Panel de control > Sistema y seguridad > Historial de archivos

Ventana principal del Panel de control

Restaurar archivos personales

Seleccionar unidad

Excluir carpetas


Configuración avanzada

Mantenga un historial de sus archivos

El Historial de archivos guarda copias de sus archivos para que pueda recuperarlos si se pierden o se dañan.

Historial de archivos desactivado

Copiar archivos de: Bibliotecas, Escritorio, Contactos y Favoritos

Copiar archivos en:  Manu (E:)
15,7 GB disponibles de 115 GB

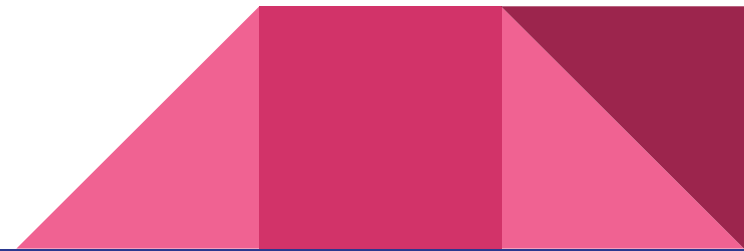
Activar

Vea también

Recuperación

 Copia de seguridad de imagen del sistema

4.7. PROGRAMACIÓ DE TASQUES

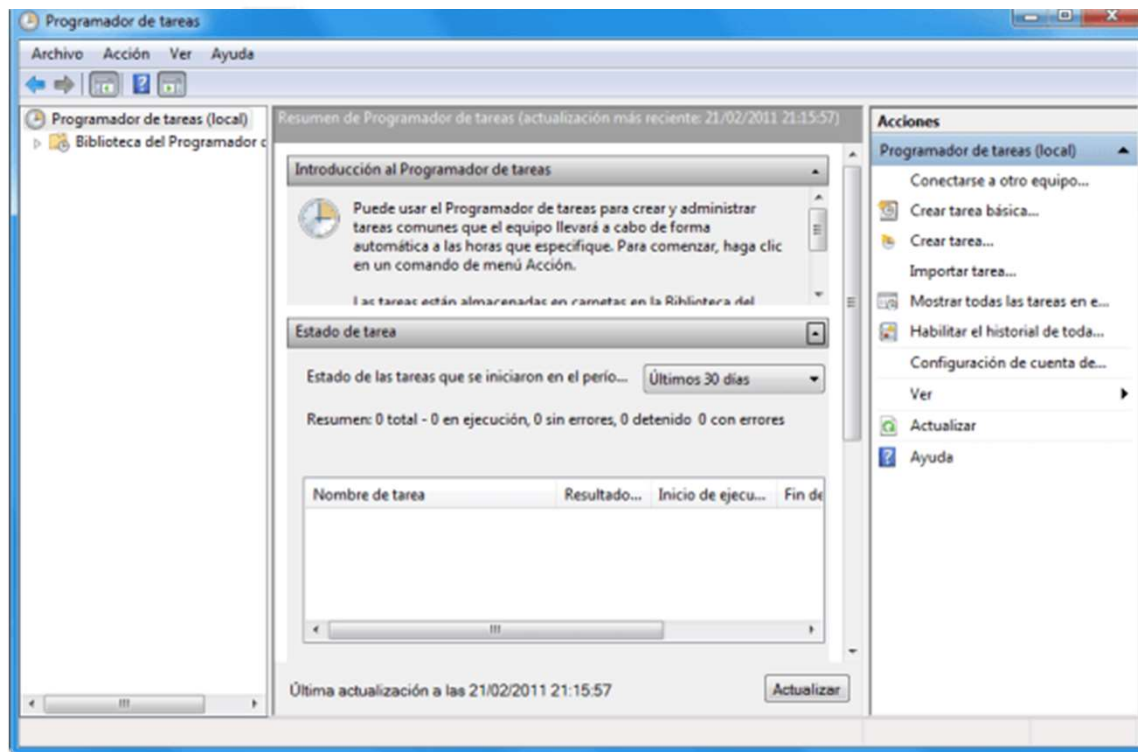


4.7. Programación de tareas

Herramientas administrativas (Windows 10)

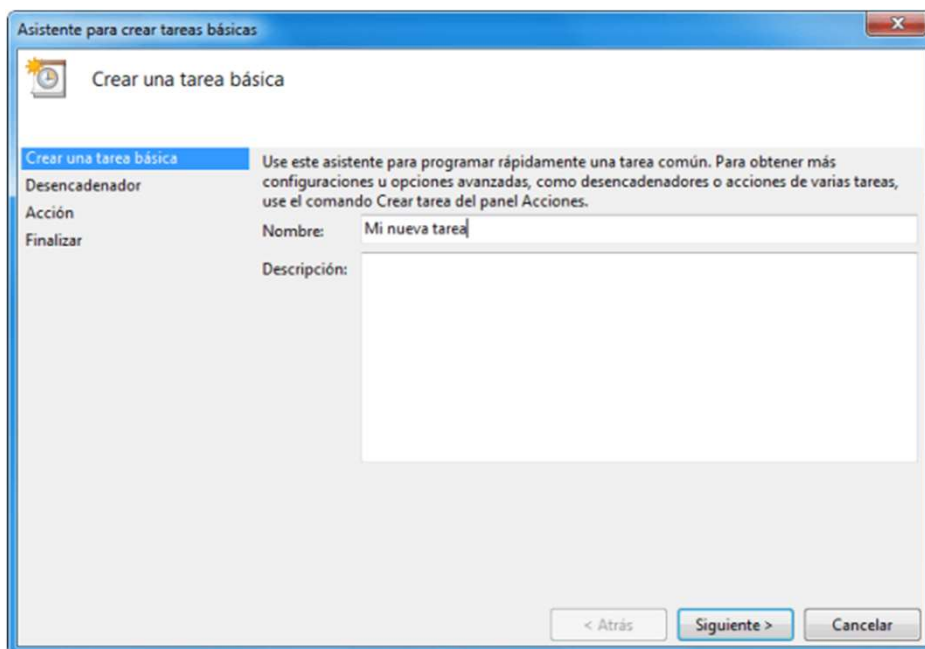
Herramientas de Windows (Windows 11)

Panel de control > Sistema y seguridad > Herramientas administrativas



4.7. Programación de tareas

Crear tareas



Asistente para crear tareas básicas

Crear una tarea básica

Use este asistente para programar rápidamente una tarea común. Para obtener más configuraciones u opciones avanzadas, como desencadenadores o acciones de varias tareas, use el comando Crear tarea del panel Acciones.

Desencadenador

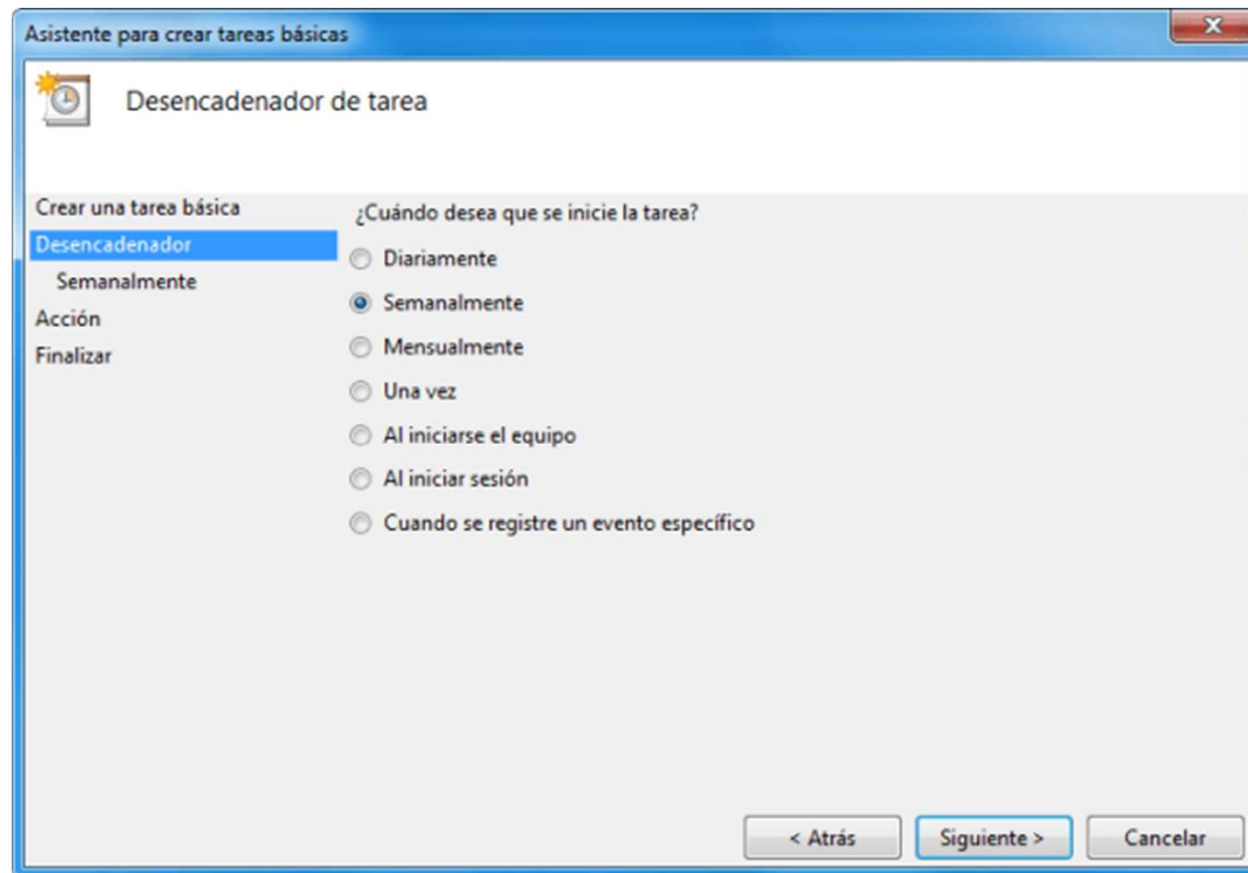
Acción

Finalizar

Nombre: Mi nueva tarea

Descripción:

< Atrás Siguiente > Cancelar



Asistente para crear tareas básicas

Desencadenador de tarea

Crear una tarea básica

Desencadenador

Semanalmente

Acción

Finalizar

¿Cuándo desea que se inicie la tarea?

☐ Diariamente

☒ Semanalmente

☐ Mensualmente

☐ Una vez

☐ Al iniciarse el equipo

☐ Al iniciar sesión


☐ Cuando se registre un evento específico

< Atrás Siguiente > Cancelar

■ 4.7. Programación de tareas

Crear tareas

Asistente para crear tareas básicas

 Iniciar un programa

Crear una tarea básica

Desencadenador
Semanalmente

Acción
Iniciar un programa

Finalizar

Programa o script:
"E:\Program Files\CCleaner\CCleaner64.exe" Examinar...

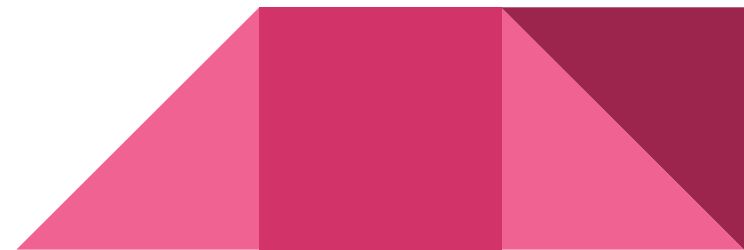
Agregar argumentos (opcional):
/AUTO

Iniciar en (opcional):

< Atrás **Siguiente >** Cancelar



Realitzar Activitats Resoltes





Actividad resuelta 4.12

Programa una tarea para que realice un apagado del equipo cada noche a las 23:30.

Solución

Ve al Programador de tareas. En la ventana **Acciones** pincha sobre **Crear tarea básica**. En el asistente que te muestra, en **Nombre**, escribe **Apagar**. Si quieres, puedes añadir alguna descripción de lo que realiza la tarea.

Pulsa sobre **Siguiente** y, en **Desencadenar**, selecciona **Diariamente** y pulsa **Siguiente**. En **Inicio**, elige el día que quieres que empiece a funcionar la tarea, por ejemplo el mismo día en el que estás. En la hora escribe **23:30:00**, especifica **Repetir cada 1 días** y pulsa **Siguiente**.

En programa o script escribe **shutdown** y si no lo encuentra pulsa en **Examinar** y busca **shutdown.exe**. En argumentos opcionales escribe **/s**. Pulsa sobre **Finalizar** y ya está la tarea programada (Figura 4.50).

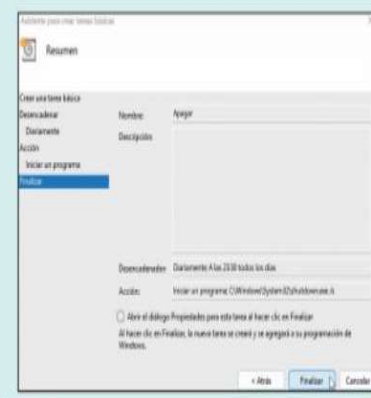


Figura 4.50. Apagado del equipo programado diariamente a las 23:30 horas.

Una vez programada puedes modificarla, haciendo doble clic sobre ella. Allí, en **General** puedes elegir que se ejecute tanto si el usuario ha iniciado sesión como si no lo ha hecho. También puedes marcar **Ejecutar** con los privilegios más altos. En la pestaña **Desencadenadores** puedes modificar la hora a la que se va a ejecutar. En la pestaña **Condiciones** puedes hacer que la tarea se inicie solo si el equipo ha estado inactivo durante un tiempo determinado, o bien si está conectado a la corriente alterna, si es un portátil.

Si quieres hacer un seguimiento del historial de las veces que la tarea se ha ejecutado, en la ventana **Acciones** de la derecha pincha sobre **Habilitar el historial de todas las tareas**.

Si quieres ver si la tarea se ejecuta correctamente, selecciónala y pulsa sobre **Ejecutar**.

En programa o script escribe **shutdown** y si no lo encuentra pulsa en **Examinar** y busca **shutdown.exe**. En argumentos opcionales escribe **/s**. Pulsa sobre **Finalizar** y ya está la tarea programada (Figura 4.50).

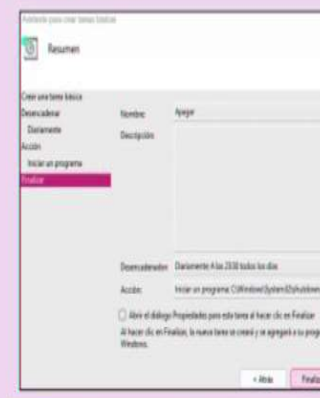


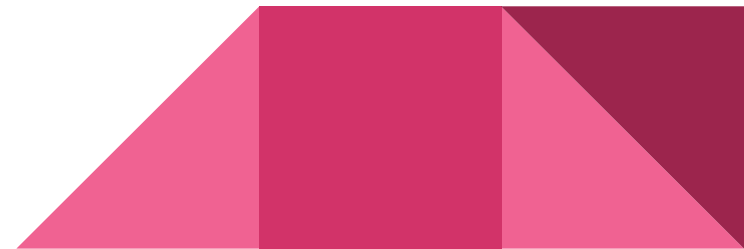
Figura 4.50. Apagado del equipo programado diariamente a las 23:30 horas.

Una vez programada puedes modificarla, haciendo doble clic sobre ella. Allí, en **General** puedes elegir que se ejecute tanto si el usuario ha iniciado sesión como si no lo ha hecho. También puedes marcar **Ejecutar** con los privilegios más altos. En la pestaña **Desencadenadores** puedes modificar la hora a la que se va a ejecutar. En la pestaña **Condiciones** puedes hacer que la tarea se inicie solo si el equipo ha estado inactivo durante un tiempo determinado, o bien si está conectado a la corriente alterna, si es un portátil.

Si quieres hacer un seguimiento del historial de las veces que la tarea se ha ejecutado, en la ventana **Acciones** de la derecha pincha sobre **Habilitar el historial de todas las tareas**.

Si quieres ver si la tarea se ejecuta correctamente, selecciónala y pulsa sobre **Ejecutar**.

4.8. MONITORITZACIÓ DEL SISTEMA

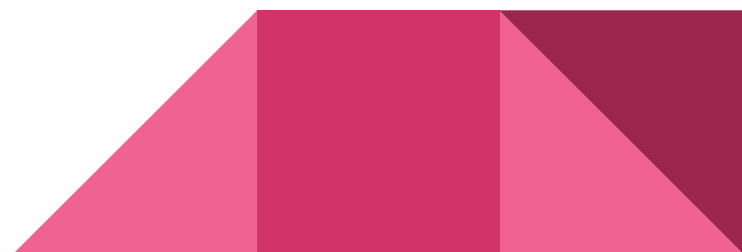


■ 4.8. Monitorización del sistema

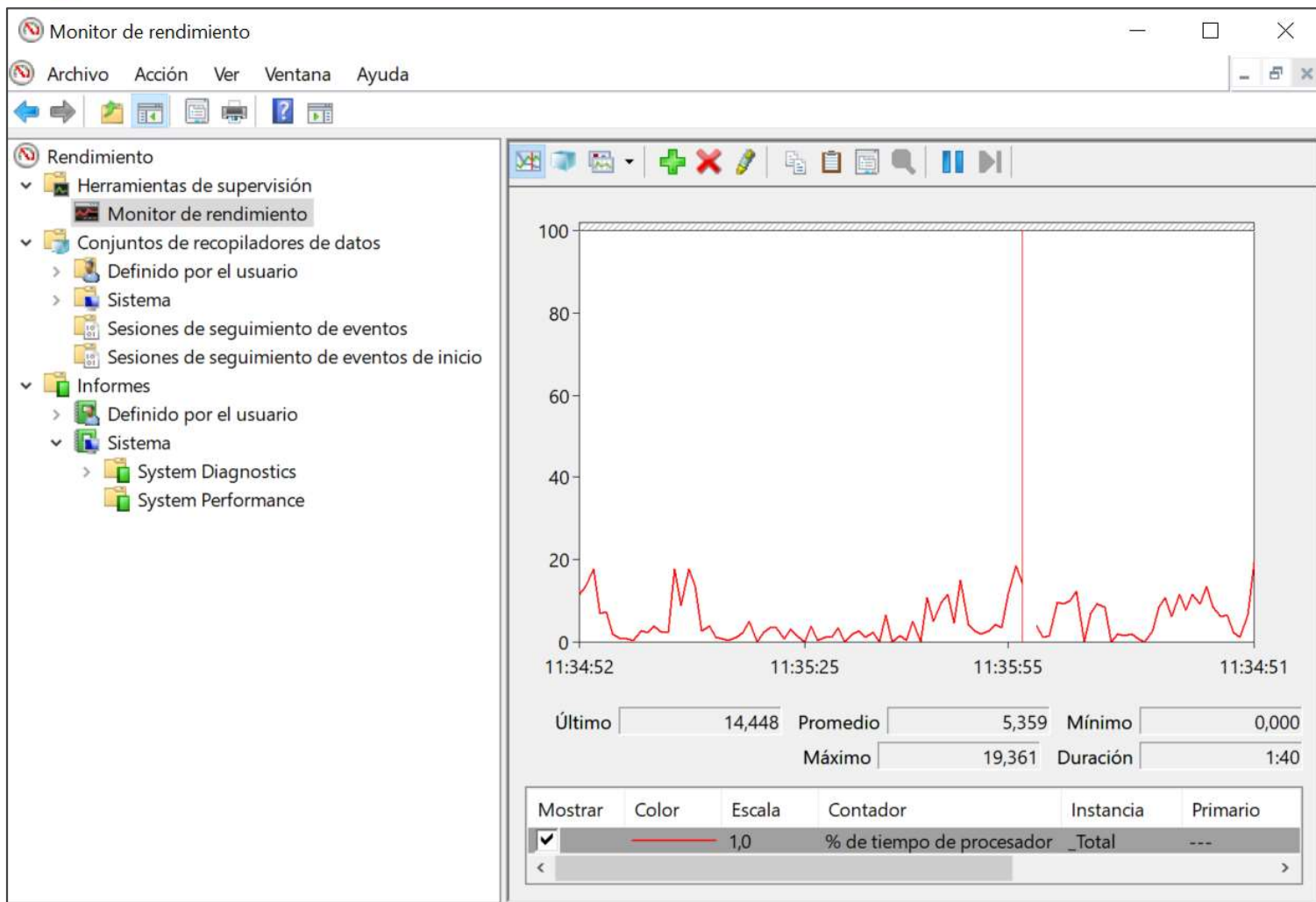


Se puede monitorizar el funcionamiento del sistema a través del Administrador de tareas, en la pestaña **Rendimiento**, en el **Monitor de recursos** y en el **Monitor de rendimiento**.

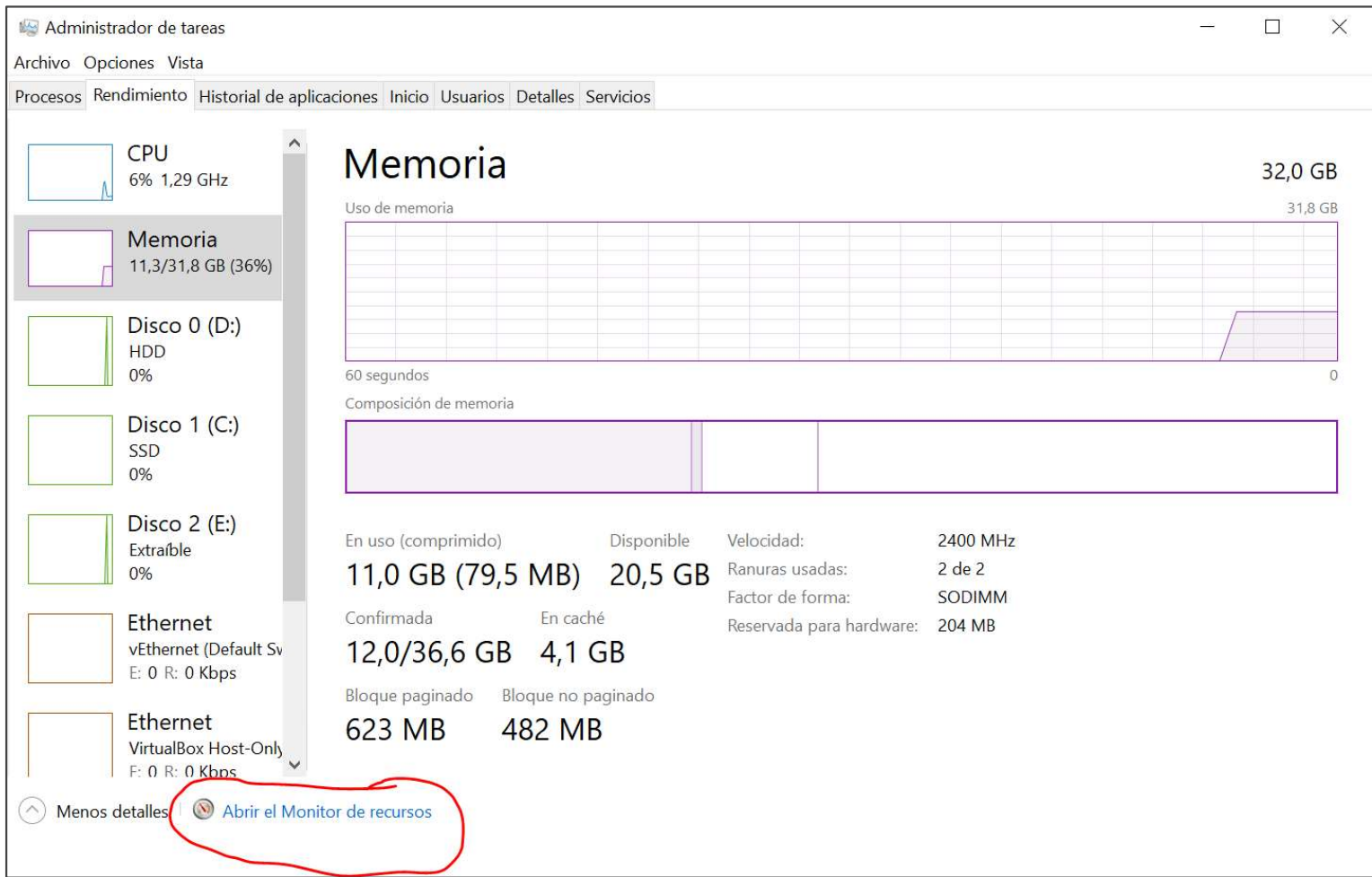
Para ver el rendimiento del sistema se puede ir a Administrador de tareas de Windows y después seleccionar la pestaña **Rendimiento** (Figura 4.51). Allí se puede obtener información sobre los dispositivos siguientes: CPU, memoria, disco, Ethernet, wifi, GPU y su funcionamiento en tiempo real.



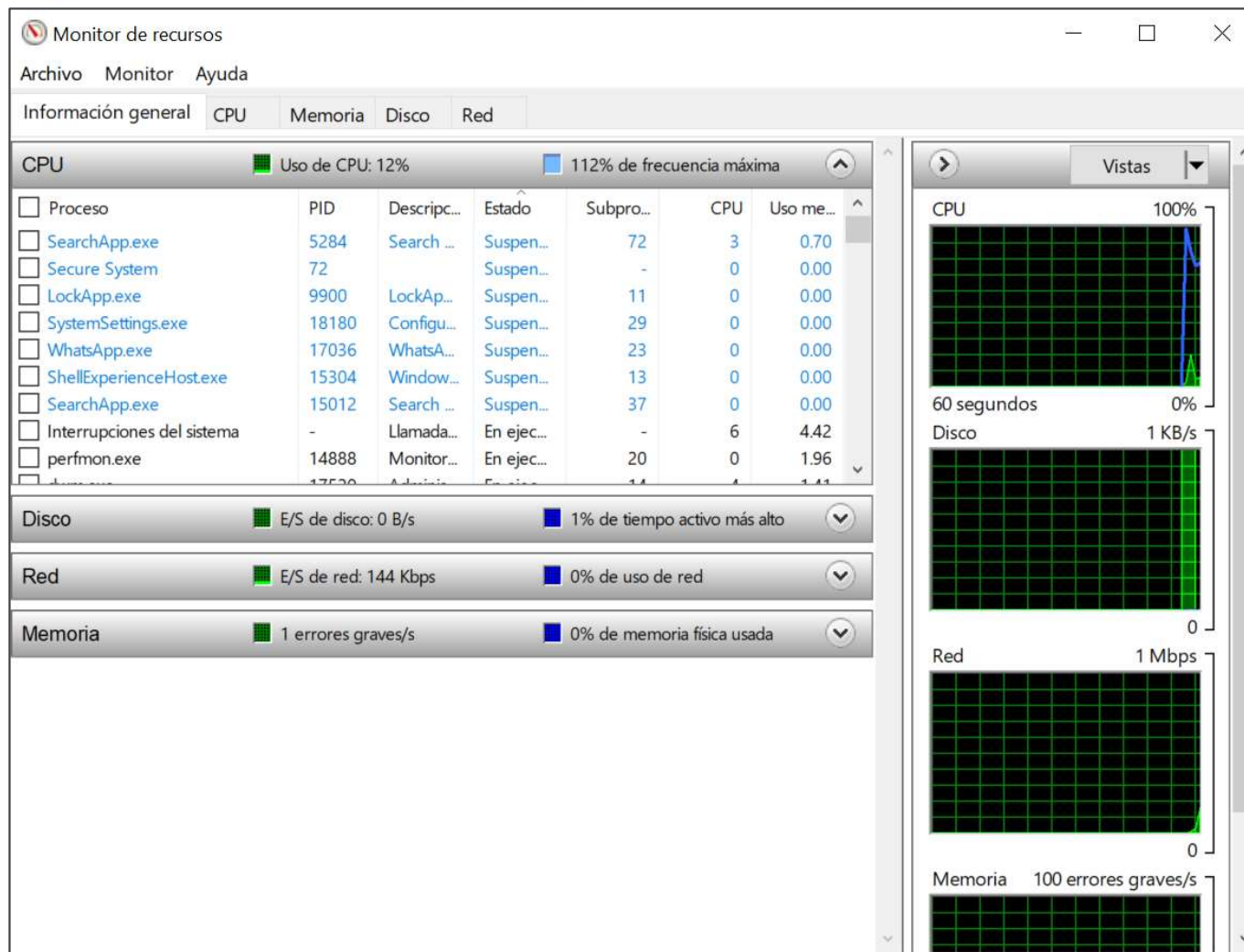
4.8. Monitorización del sistema



4.8. Monitorización del sistema



4.8. Monitorización del sistema



■ 4.8. Monitorización del sistema

■ ■ Visor de eventos



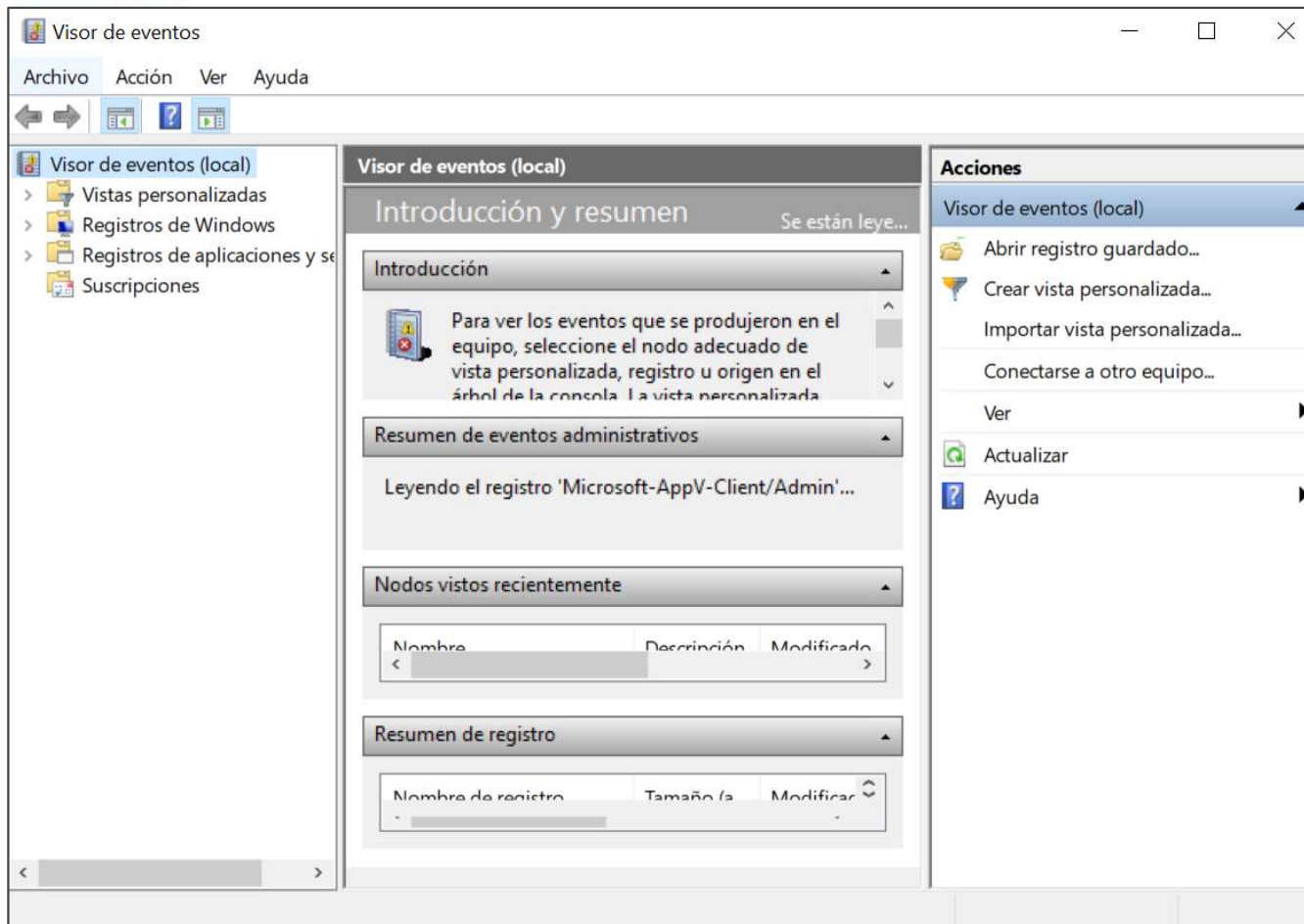
El Visor de eventos proporciona información sobre los eventos que han ocurrido en el sistema. Para abrirlo se acude a **Visor de eventos**, que se encuentra en Herramientas administrativas. También se puede abrir ejecutando el programa `eventvwr.exe` o abriendo la consola `eventvwr.msc`.

Una vez abierto se puede buscar información de los eventos que han ocurrido en el sistema relacionados con los registros de Windows: aplicación, seguridad, instalación, sistema y eventos reenviados (equipos remotos). También registra los eventos relacionados con aplicaciones y servicios.

De cada tipo de registro se pueden ver todos los eventos o filtrarlos por niveles de eventos, usuarios, equipos, etc. Los niveles de eventos que se pueden buscar son: crítico, advertencia, detallado, error e información.

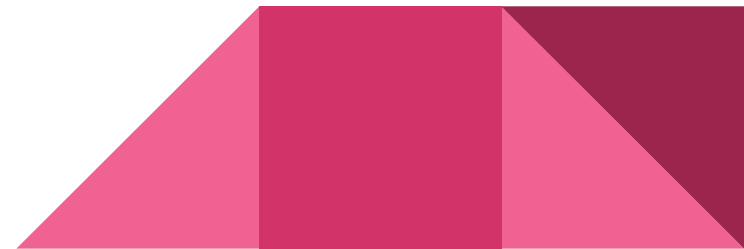
4.8. Monitorización del sistema

Visor de eventos





Realitzar Activitats Resoltes





Actividad resuelta 4.13

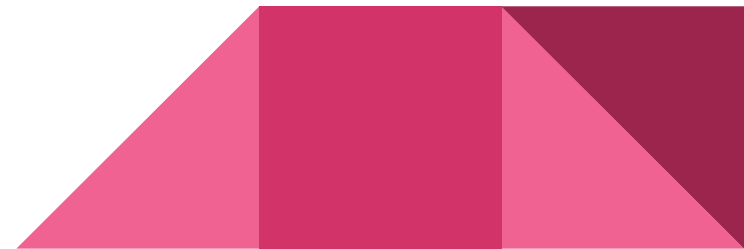
Entra en el sistema, equivócate con la contraseña al iniciar sesión y comprueba el registro del evento.

Solución

Intenta iniciar la sesión en tu sistema tres veces con el nombre de usuario, pero utilizando otra contraseña. Entra finalmente con la contraseña correcta.

Abre el Visor de eventos. Despliega **Registros de Windows** y selecciona **Seguridad**. Busca el identificador de evento 4625 (que es el identificador de que un usuario ha intentado iniciar sesión con un nombre de usuario desconocido o con un nombre de usuario conocido y contraseña errónea) y la palabra clave **Error de auditoría**. Podrás ver los tres intentos de inicio de sesión no válidos. En la categoría de la tarea aparecerá **Logon** y en la columna **Fecha y hora** el momento en el que se produjo el intento de inicio de sesión.

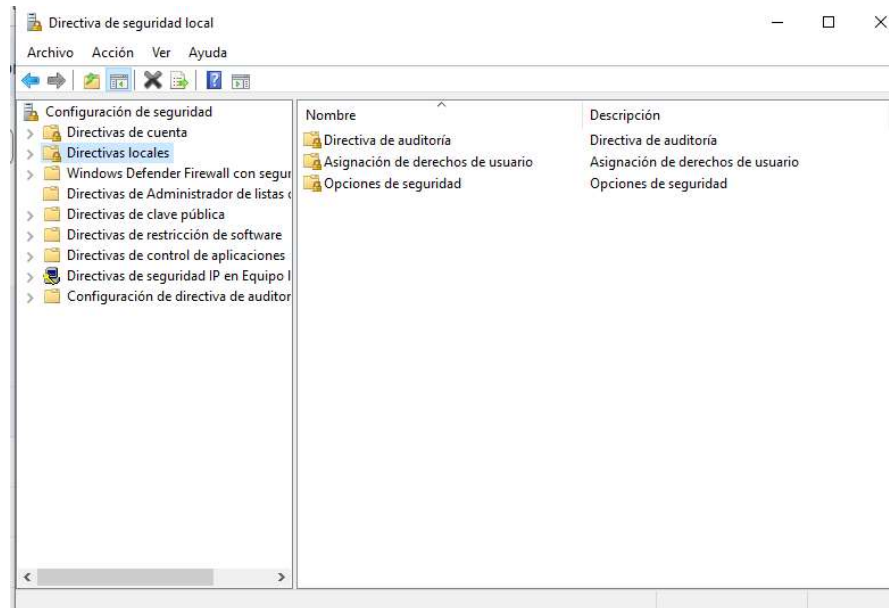
4.9. DIRECTIVES DE SEGURETAT



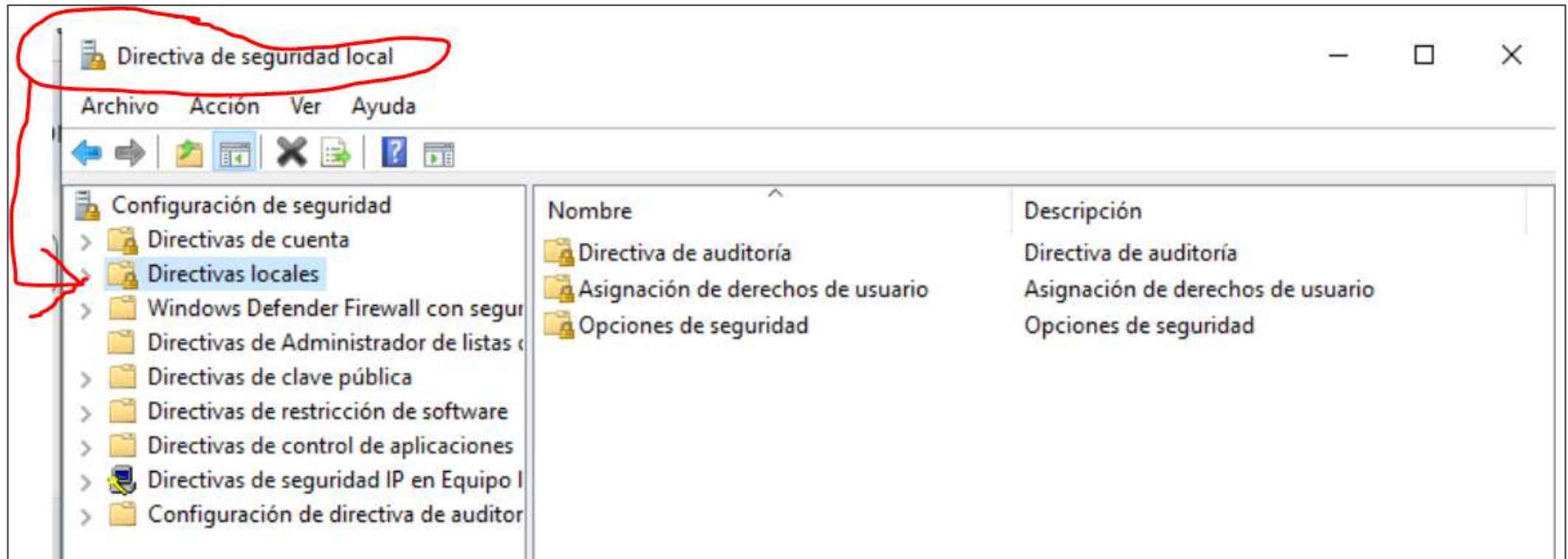
4.9. Directivas de seguridad



Las directivas definen el comportamiento del sistema informático y sus elementos en cuestiones de seguridad. Con las herramientas que se utilizan para modificar las directivas, pueden realizarse cambios en la configuración de seguridad del sistema. Las directivas de seguridad pueden ser a nivel local, de dominio o de controlador de dominio, y se aplican mediante los objetos de directivas de grupo (GPO).




4.9. Directivas de seguridad

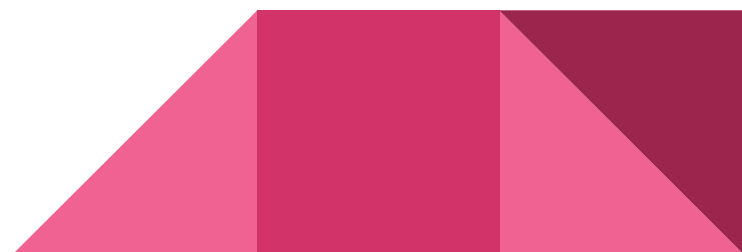


■ 4.9. Directivas de seguridad

■ ■ 4.9.1. Directiva de equipo local

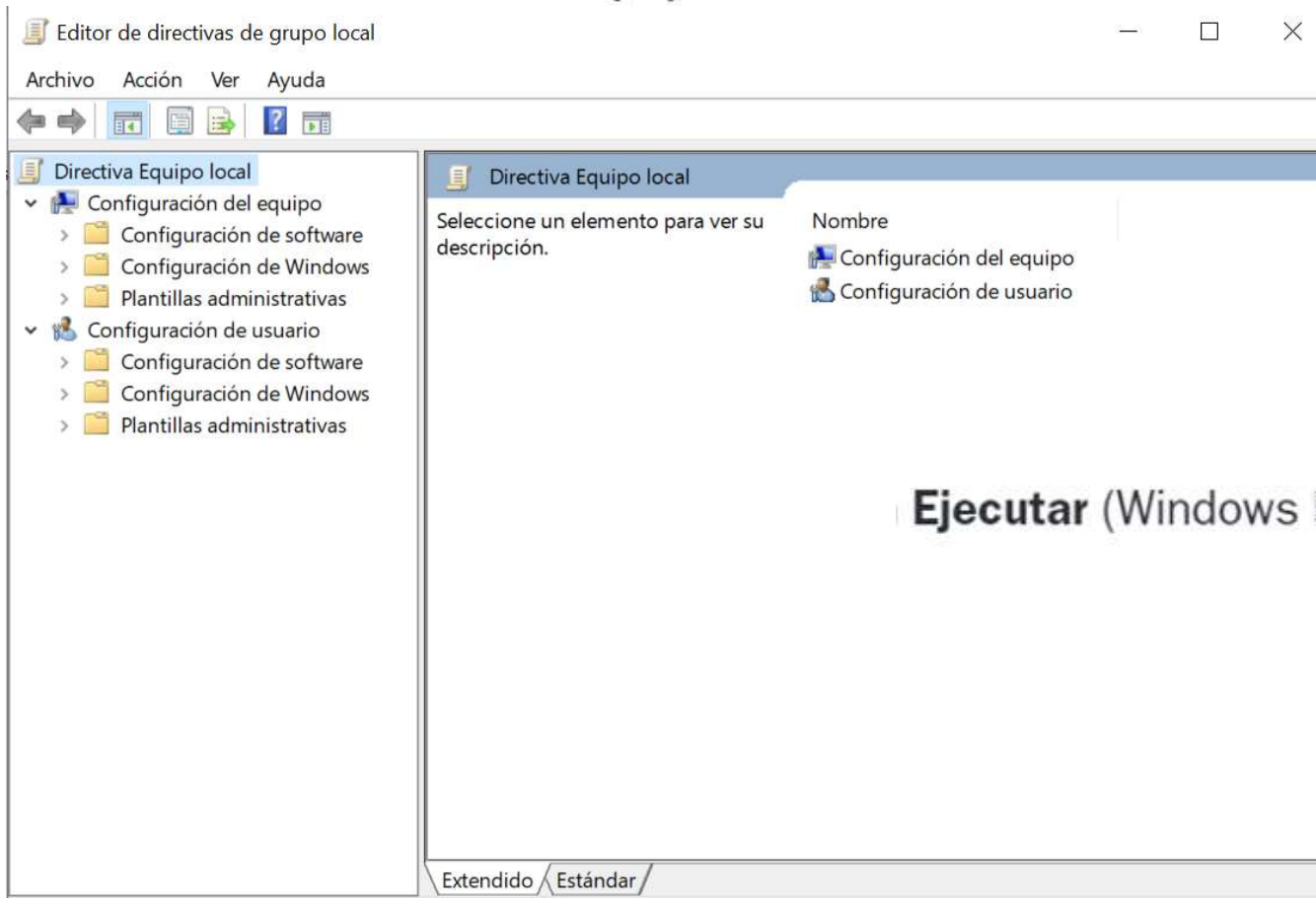
Para abrir estas directivas hay que ir al **Editor de directivas de grupo local**. Desde **Inicio** o en **Ejecutar** (Windows  + R) se escribe `gpedit.msc`. El editor de objetos de directivas de grupo permite editar los objetos de directivas de grupo local almacenados en un equipo. Desde aquí se puede configurar el equipo o el usuario. Dentro de cada configuración se encuentra lo siguiente:


- Configuración de *software*: sobre instalación y gestión de *software*.
- Configuración de Windows: con los *scripts* de inicio y fin y la configuración de seguridad.
- Plantillas administrativas: modifican el comportamiento de componentes de Windows y del sistema.



4.9. Directivas de seguridad

4.9.1. Directiva de equipo local



Ejecutar (Windows  + R) se escribe `gpedit.msc`.

■ 4.9. Directivas de seguridad

■ ■ 4.9.2. Directiva de seguridad local

Se puede acceder desde Herramientas administrativas (Windows 10) o Herramientas de Windows (Windows 11). También desde **Inicio** o desde **Ejecutar** (Windows+R) escribiendo `secpol.msc`. Permite definir directivas de seguridad para los equipos de un dominio. Es posible cambiar aspectos como los siguientes (Figura 4.53):

- Directivas de cuenta.
- Directivas locales.
- *Firewall* de Windows con seguridad avanzada.
- Directivas de administrador de listas de redes.
- Directivas de clave pública.
- Directivas de restricción de *software*.
- Directivas de control de aplicaciones.
- Directivas de seguridad IP en el equipo local.
- Configuración de directivas de auditoría avanzada.

Existe también una utilidad en la línea de comandos para este fin, `secedit.exe`. Este complemento extiende el comportamiento de las directivas de grupo y puede utilizarse para definir directivas de seguridad a los equipos de un dominio.



4.9. Directivas de seguridad

4.9.2. Directiva de seguridad local

Directiva de seguridad local

ArchivoAcciónVerAyuda

←→

✕

?

Configuración de seguridad

> Directivas de cuenta

> Directivas locales

> Windows Defender Firewall con seguridad avanzada

> Directivas de Administrador de listas de redes

> Directivas de clave pública

> Directivas de restricción de software

> Directivas de control de aplicaciones

> Directivas de seguridad IP en Equipo local

> Configuración de directiva de auditoría avanzada

Nombre	Descripción
Directivas de cuenta	Directivas de bloqueo de contraseña y cuenta
Directivas locales	Directivas de opciones de seguridad, derechos d...
Windows Defender Firewall con seguridad...	Windows Defender Firewall con seguridad avan...
Directivas de Administrador de listas de re...	Directivas de grupo de ubicación, icono y nomb...
Directivas de clave pública	
Directivas de restricción de software	
Directivas de control de aplicaciones	Directivas de control de aplicaciones
Directivas de seguridad IP en Equipo local	Administración del protocolo de seguridad de l...
Configuración de directiva de auditoría av...	Configuración de directiva de auditoría avanzada



4.9. Directivas de seguridad

4.9.2. Directiva de seguridad local

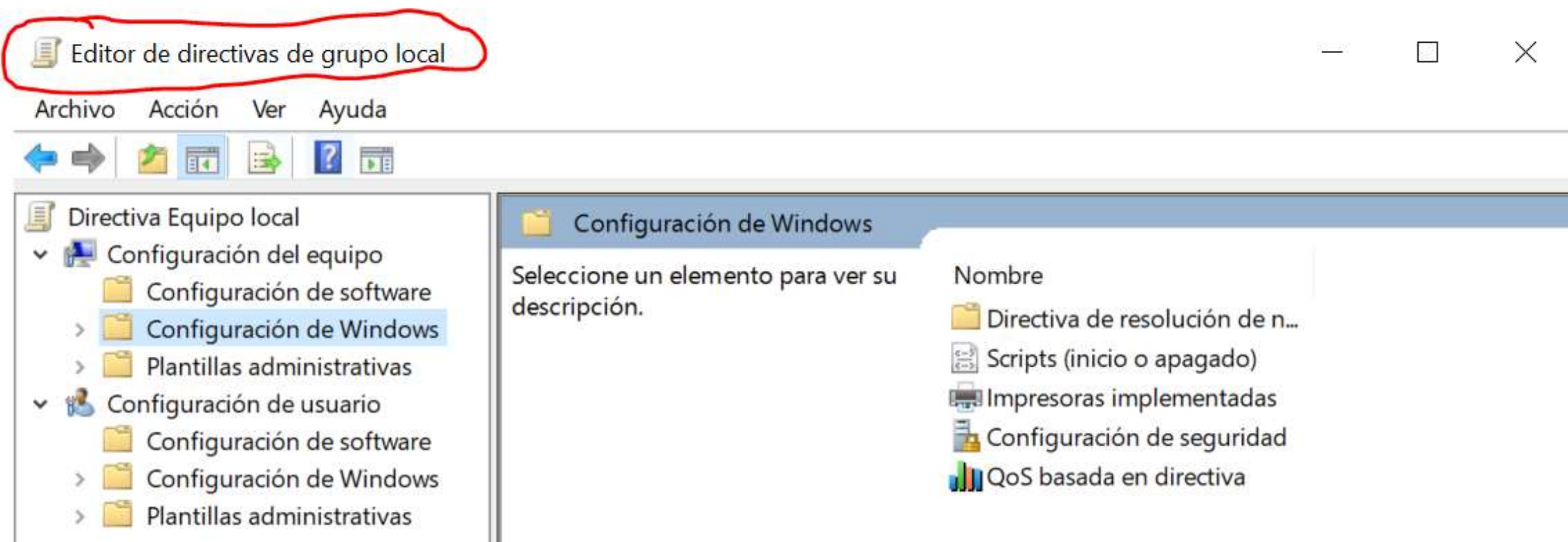
The screenshot shows the Windows Security Policy console. The title bar is "Directiva de seguridad local". The menu bar includes "Archivo", "Acción", "Ver", and "Ayuda". The toolbar contains icons for navigation and actions. The left pane shows a tree view of security policies, with "Directiva de contraseñas" selected and highlighted in blue. Red arrows point to the title bar, the selected policy, and the policy list. The right pane displays a list of password-related policies, with several items circled in red. The status of each policy is shown on the far right.

Directiva	Configuración de seguridad
Almacenar contraseñas con cifrado reversible	Deshabilitada
Auditoría de longitud mínima de contraseña	No está definido
Exigir historial de contraseñas	0 contraseñas recordadas
La contraseña debe cumplir los requisitos de complejidad	Deshabilitada
Longitud mínima de la contraseña	0 caracteres
Reducir los límites de longitud mínima de la contraseña	No está definido
Vigencia máxima de la contraseña	42 días
Vigencia mínima de la contraseña	0 días

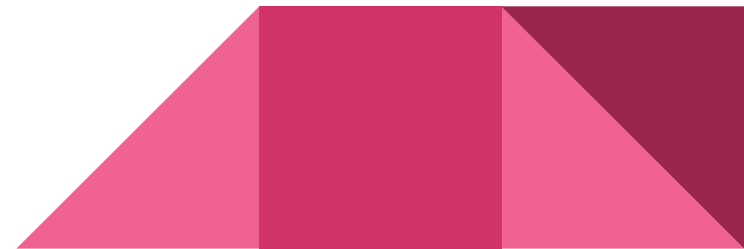
4.9. Directivas de seguridad

4.9.3. Directivas de grupo

Dentro de las directivas de grupo están las directivas de grupo local (LGPO) y las directivas de grupo de dominio (GPO). Como se ha visto en el Apartado 4.9.1, para entrar en el editor de directivas de grupo local hay que escribir `gpedit.msc`.



4.10. REGISTROS DE WINDOWS



4.10. Registro de Windows

Es una base de datos formada por una serie de archivos donde se almacena información sobre el sistema, el sistema operativo, los programas instalados, qué programa es el predeterminado para abrir un tipo de archivo, los usuarios y, en general, cualquier dato necesario para la configuración del equipo. Cada vez que se modifica cualquier elemento del sistema, se modifica el Registro.

Los archivos del Registro de Windows se encuentran en la carpeta **%SystemRoot%\System32\config** y para cada usuario en **%UserProfile%**, dentro del fichero oculto **NTUSER.DAT**.

Para acceder al Registro hay que entrar en el Editor del Registro, desde **Inicio** escribiendo **Editor de Registro**, desde las Herramientas administrativas (Windows 10) o Herramientas de Windows (Windows 11) o bien, desde **Ejecutar** (Win+R) escribiendo **regedit** o desde **Inicio** escribiendo **editor del registro**.

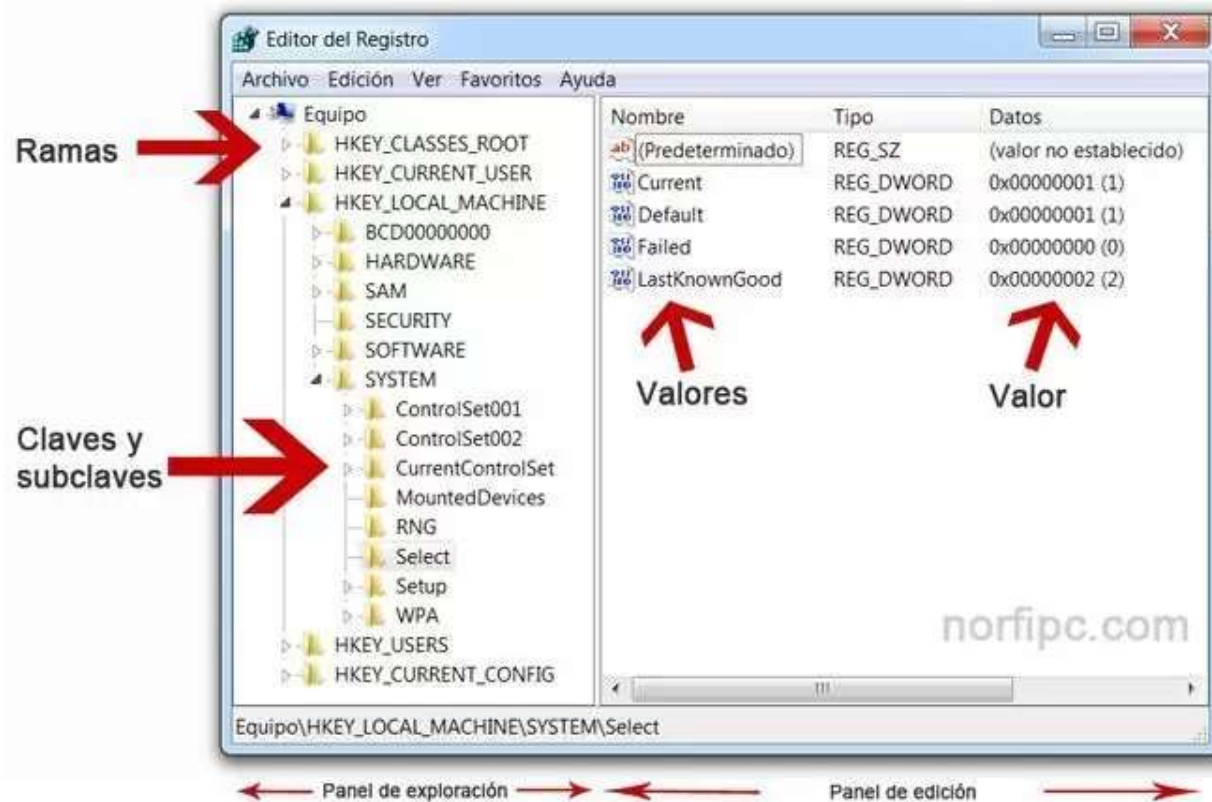
Otra forma de acceder al Editor del Registro es desde la herramienta Configuración del sistema (**msconfig.exe**) y, en la pestaña **Herramientas**, seleccionando la herramienta **Editor del Registro** y pulsando sobre **Iniciar**.

■ 4.10. Registro de Windows

En el Registro hay una serie de claves, que a su vez contienen una serie de subclaves. Las claves son las siguientes:

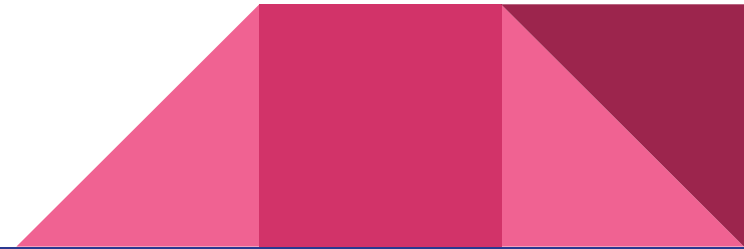
- **HKEY_CLASSES_ROOT:** contiene información sobre los tipos de archivos, cómo utilizarlos y con qué programas se asocian.
- **HKEY_CURRENT_USER:** contiene información sobre la configuración del usuario actual.
- **HKEY_LOCAL_MACHINE:** contiene información necesaria para el inicio del equipo y el sistema operativo.
- **HKEY_USERS:** contiene información sobre todos los usuarios del sistema.
- **HKEY_CURRENT_CONFIG:** contiene información sobre la configuración del *hardware* instalado en el equipo.

4.10. Registro de Windows





Realitzar Activitats Resoltes





Actividad resuelta 4.14

Realiza una copia de seguridad del Registro de Windows en un fichero llamado **registro.reg**.

Solución

Abre el Editor de Registro: **Inicio** → **regedit**. Cuando te pregunte si quieres permitir que la aplicación haga cambios en el dispositivo, responde que sí. Una vez abierto, ve a **Archivo** → **Exportar....** Puedes dejar la carpeta para que lo guarde en Documentos; en **Nombre** escribe **registro.reg**, en **Tipo** deja **Archivos de Registro (*.reg)** y en **Intervalo de exportación** selecciona **Todo**. Pulsa sobre **Guardar**.



Actividad resuelta 4.15

Busca en el Registro del sistema de Windows la clave correspondiente al tipo de archivo **.html**.

Solución

Abre el Editor de Registro: **Inicio** → **regedit**. Cuando te pregunte si quieres permitir que la aplicación haga cambios en el dispositivo, responde que sí. Una vez abierto, selecciona **Edición** → **Buscar...** y, en la ventana emergente que se abre, escribe en **Buscar:** **.html** y deja seleccionado **Claves** y **Solo cadenas completas** (Figura 4.56). Al pulsar sobre **Buscar siguiente**, encontrará la clave dentro de **Equipo\HKEY_CLASSES_ROOT\.html**.

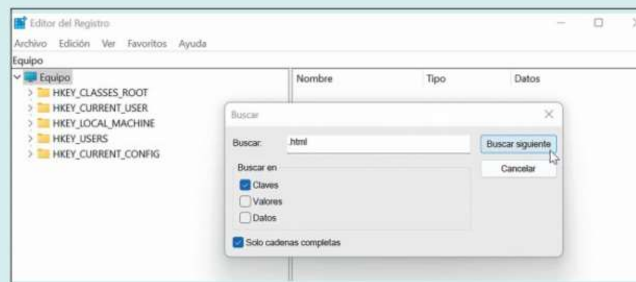


Figura 4.56. Búsqueda de las claves que contengan la cadena completa **.html**.

Una vez que lo haya encontrado, haz doble clic sobre el nombre, y en la subclave **OpenWithProgids** podrás ver las aplicaciones con las que se puede abrir ese tipo de archivo.

Si una de ellas es **MSEdgeHTM**, busca esa cadena marcando **Claves** y **Solo cadenas completas**. Al encontrarla te mostrará información sobre esa aplicación (Figura 4.57). Las claves **Application** y **DefaultIcon** proporcionan información sobre la aplicación, su ubicación, su icono predeterminado.... La clave **shell** define las acciones que se pueden realizar, como **open**, comando para abrir la aplicación, o **runas**, comando para ejecutar como otro usuario.



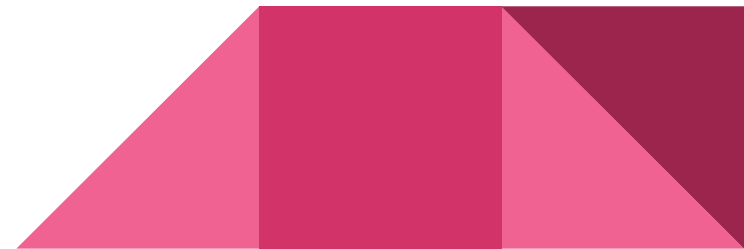
Figura 4.57. Información que tiene el Registro sobre la aplicación **MSEdgeHTM**.

Si no tienes instalado Edge, puedes realizar el ejercicio con otra aplicación, como Chrome o cualquier otro navegador que tengas instalado. Selecciona la opción **Edición** → **Buscar**. Escribe **chrome** como cadena a buscar y selecciona **Claves**. Te mostrará información sobre la aplicación y en la subclave **shell\open\command** mostrará la ruta y el comando para ejecutar la aplicación (Figura 4.58).



Figura 4.58. Información sobre el comando que abre la aplicación **Chrome**.

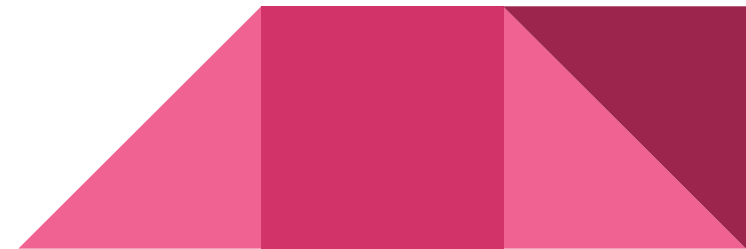
4.10. REGISTROS DE WINDOWS



■ 4.11. Introducción a los *scripts* en Windows

Los *scripts* son unos ficheros de texto que contienen comandos y permiten automatizar tareas en un sistema operativo para no tener que repetirlas, tal y como se vio en el Apartado 3.10.

En Windows están los *scripts* asociados a Símbolo del sistema, que se pueden ejecutar desde cualquier lugar y tienen la extensión `.bat`, y los *scripts* de PowerShell, cuya extensión es `.ps1`.



■ 4.11. Introducción a los *scripts* en Windows

PowerShell dispone de un entorno de desarrollo para ejecutar los *scripts*, llamado PowerShell ISE (**PowerShell Integrated Scripting Environment**). Para utilizarlo y poder ejecutar cualquier *script* de PowerShell en un sistema operativo es necesario activar las políticas de ejecución de *scripts*. Los posibles valores son los siguientes:

- **Restricted:** no permite ningún *script*.
- **Allsigned:** permite ejecutar los *scripts* firmados por un editor de confianza.
- **Remotesigned:** permite ejecutar los *scripts* firmados locales y remotos.
- **Unrestricted:** permite ejecutar cualquier *script*. No es muy recomendable por motivos de seguridad.
- **Bypass:** permite la ejecución de cualquier *script*. Se utiliza para cambiar la política de ejecución para la ejecución de un *script*.
- **Undefined:** ninguna restricción establecida.

■ 4.11. Introducción a los *scripts* en Windows

Para ver el valor que hay en el sistema se debe escribir lo siguiente en PowerShell:

```
Get-ExecutionPolicy
```

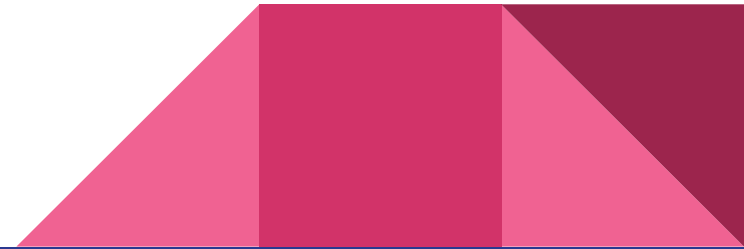
Para modificarla, se puede escribir ejecutando PowerShell con permisos de administrador:

```
Set-ExecutionPolicy -ExecutionPolicy Unrestricted -scope LocalMachine
```

```
Set-ExecutionPolicy -ExecutionPolicy Unrestricted -scope CurrentUser
```




Realitzar Activitats Resoltes





Actividad resuelta 4.16

Crear un *script* llamado **apagar.bat** que te muestre un aviso con tu nombre de usuario, el nombre del equipo y te indique que se va a apagar en 60 segundos. Crea otro *script* llamado **anular.bat** que anule el apagado.

Solución

Inicio → cmd

notepad apagar.bat

Te pregunta que si no existe, si quieres crear uno nuevo. Responde que sí y escribe dentro lo siguiente:

```
@echo off
shutdown /s /t 60 /c "%username%: El equipo %computername% se va a apagar
en 60 segundos. Ejecuta anular.bat para anularlo."
```

Archivo → Guardar

Archivo → Salir

```
notepad anular.bat
@echo off
shutdown /a
```

Archivo → Guardar

Archivo → Salir

Para probarlo, escribe **apagar**; te saldrá un mensaje indicando que el equipo se cerrará. Cierra el cuadro de diálogo y ejecuta **anular**. El sistema te avisará que se ha anulado el apagado (Figura 4.59).

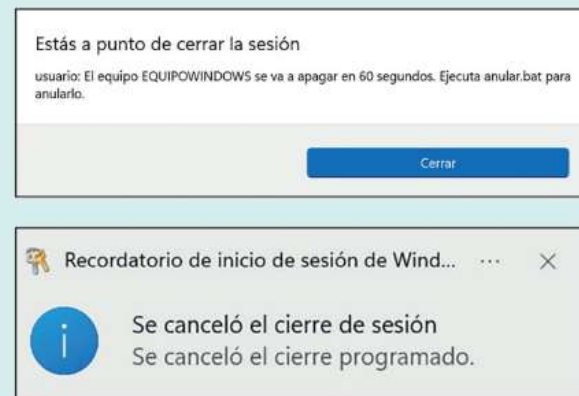


Figura 4.59. Aviso sobre que se va a apagar el ordenador en 60 segundos y aviso de que se canceló el cierre.



Actividad resuelta 4.17

Crea un *script* en PowerShell llamado **datos.ps1** y pruébalo.

Te debe borrar la pantalla, mostrar el nombre del equipo, el nombre del usuario y la fecha y hora.

Solución

Abre PowerShell, y allí escribe:

```
notepad datos.ps1
```

Te pregunta que si no existe, si quieres crear uno nuevo. Responde que sí y escribe dentro lo siguiente:

```
clear-host  
$env:computername  
$env:username  
Get-Date
```

Archivo → Guardar

Archivo → Salir

Para ejecutarlo escribe lo siguiente:

```
./datos.ps1
```

Recuerda que debes tener permitida la ejecución de *scripts*; si no, debes escribir abriendo PowerShell como administrador:

```
Set-ExecutionPolicy -ExecutionPolicy Unrestricted -scope CurrentUser
```

UD4 – WINDOWS – ADMINISTRACIÓ I CONFIGURACIÓ-II

1º DAW - CFGS

Prof. Manuel Enguidanos
menguidanos@fpmislata.com