

Guía de Configuración y Prueba de Puntos de Restauración en Windows y Kali Linux

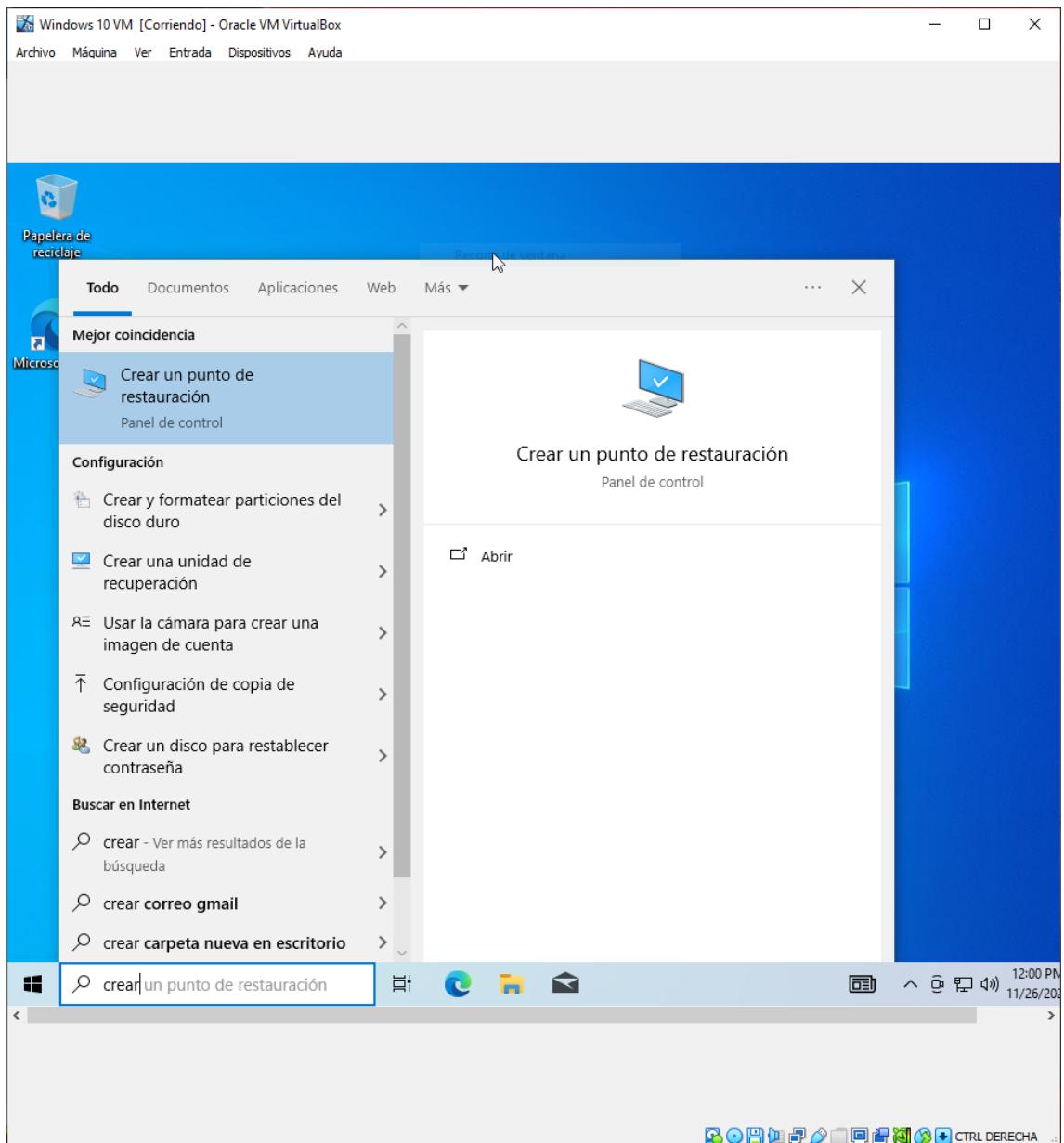
Introducción

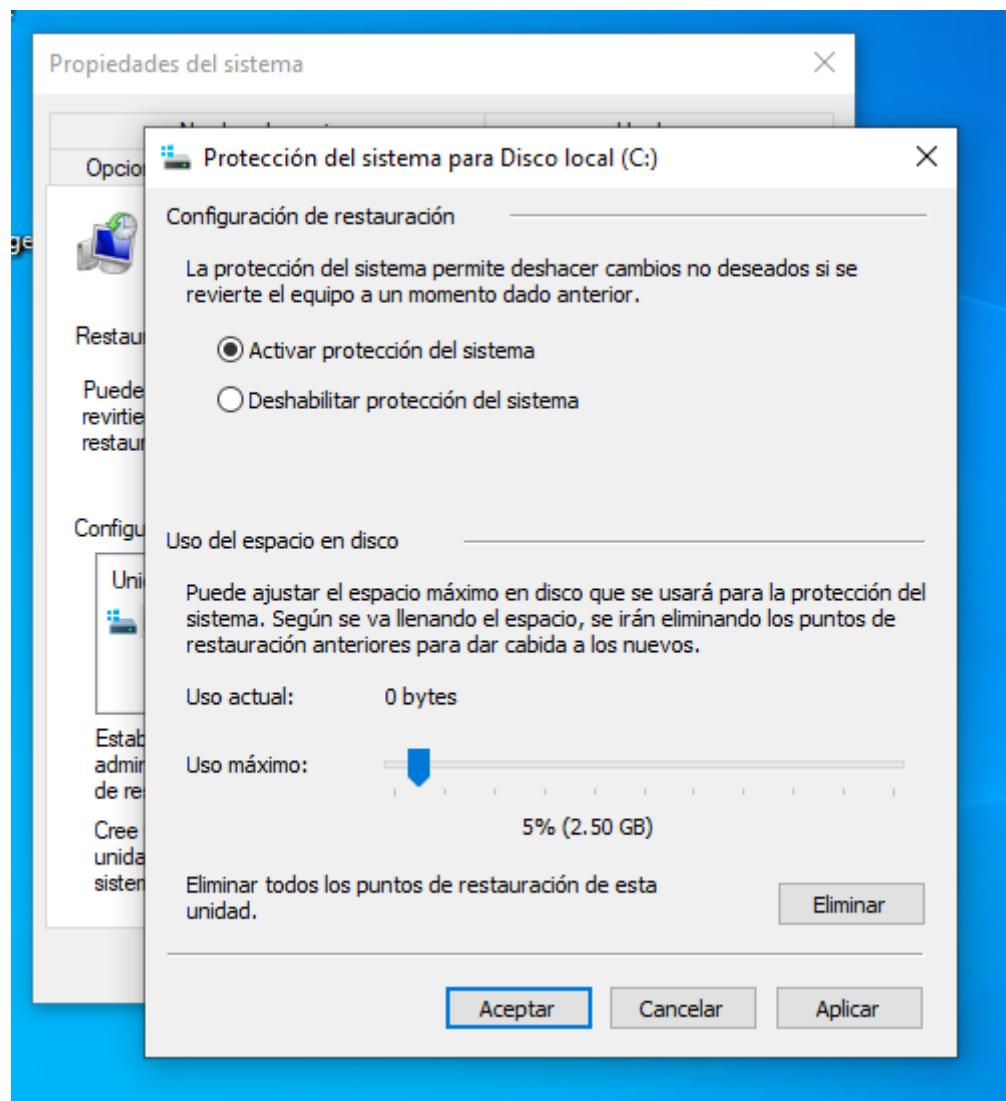
El propósito de este documento es demostrar la configuración, creación y recuperación de puntos de restauración en dos sistemas operativos distintos: Windows 10/11 y Kali Linux. Estas herramientas son esenciales para la continuidad del negocio y la seguridad personal, permitiendo revertir el sistema a un estado funcional anterior en caso de fallos críticos, infecciones de malware o errores humanos. A continuación, se detalla el procedimiento simulado en ambos entornos.

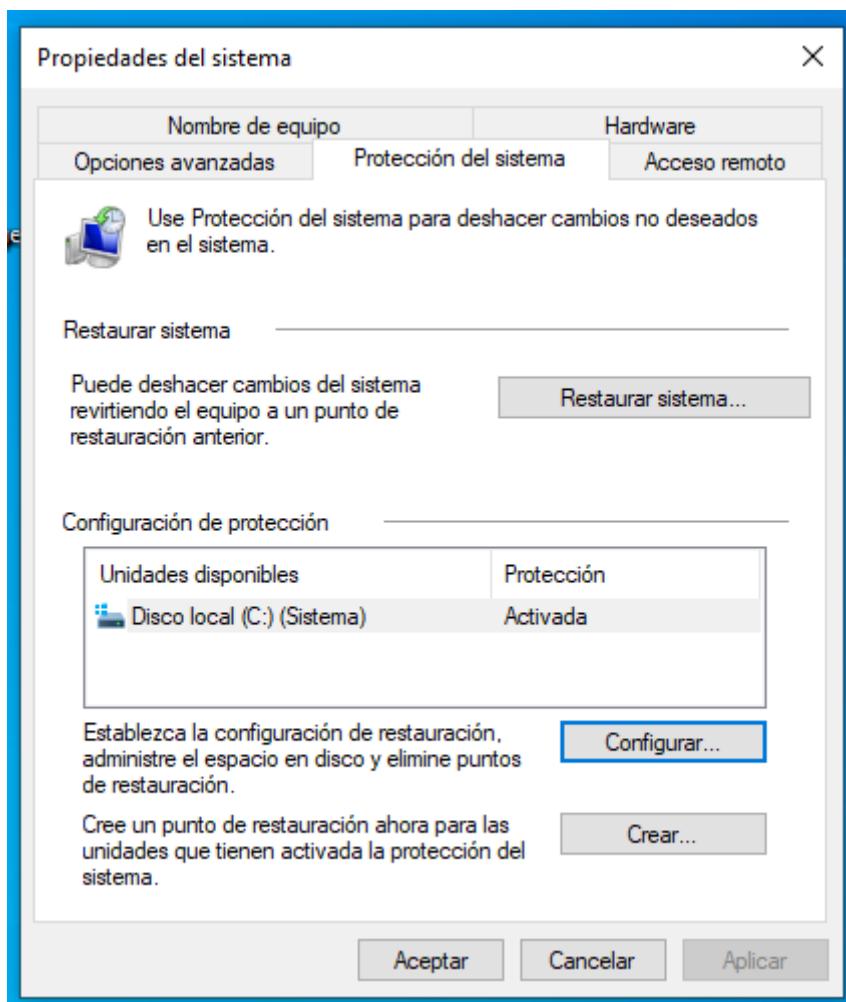
Parte 1: Sistema Operativo Windows (Restaurar Sistema)

Configuración y Creación del Punto de Restauración

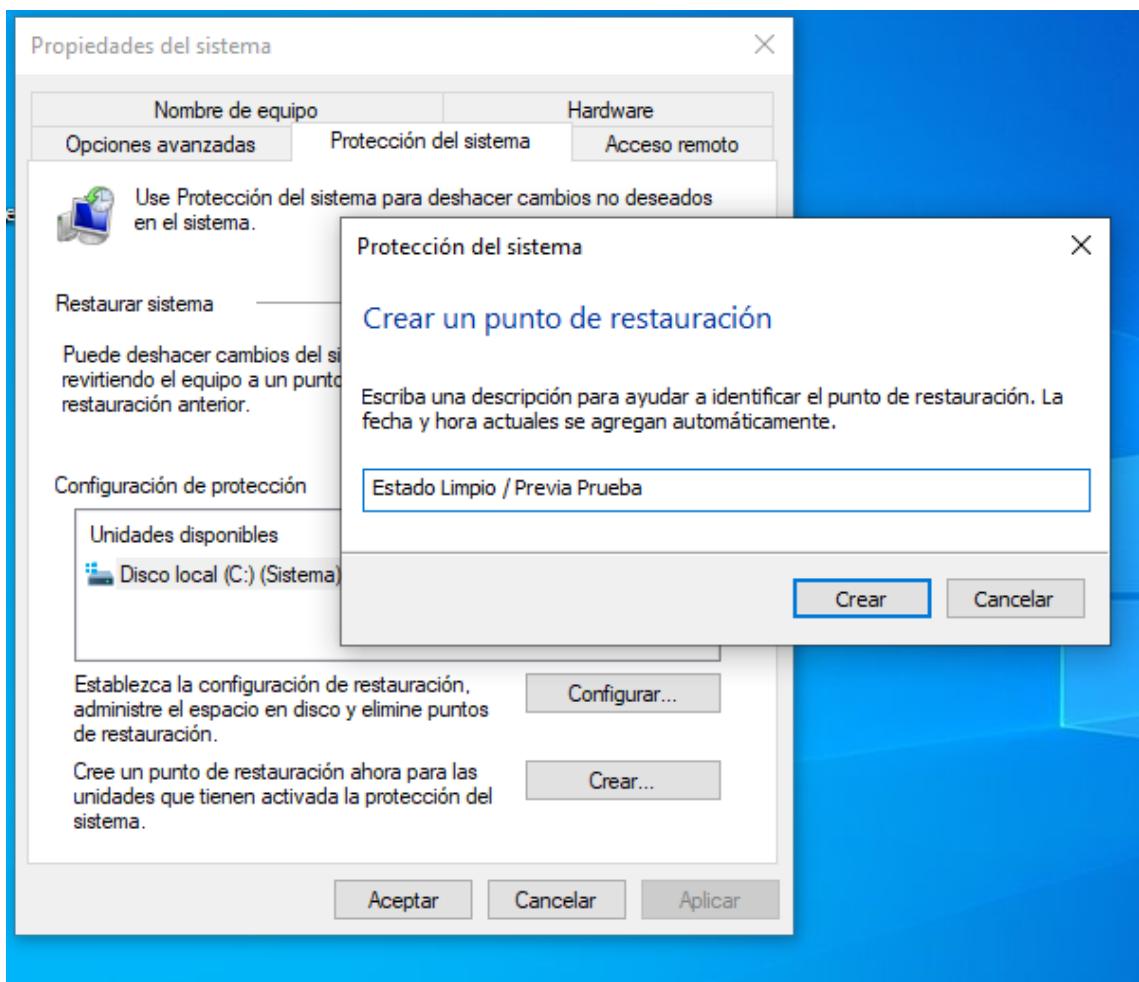
Para iniciar el proceso en Windows, es necesario acceder a las propiedades del sistema donde se gestiona la protección. Primero, se debe abrir el menú de inicio y escribir "Crear un punto de restauración", seleccionando la opción que aparece en el panel de control. Esto abrirá la ventana de "Propiedades del sistema" en la pestaña de "Protección del sistema". Es fundamental verificar que la protección esté activada para la unidad principal (generalmente C:). Si aparece como "Desactivada", se debe pulsar el botón "Configurar", seleccionar "Activar protección del sistema" y asignar un porcentaje de uso de disco (por ejemplo, entre 5% y 10%). Una vez configurado y aceptado, volvemos a la ventana anterior.

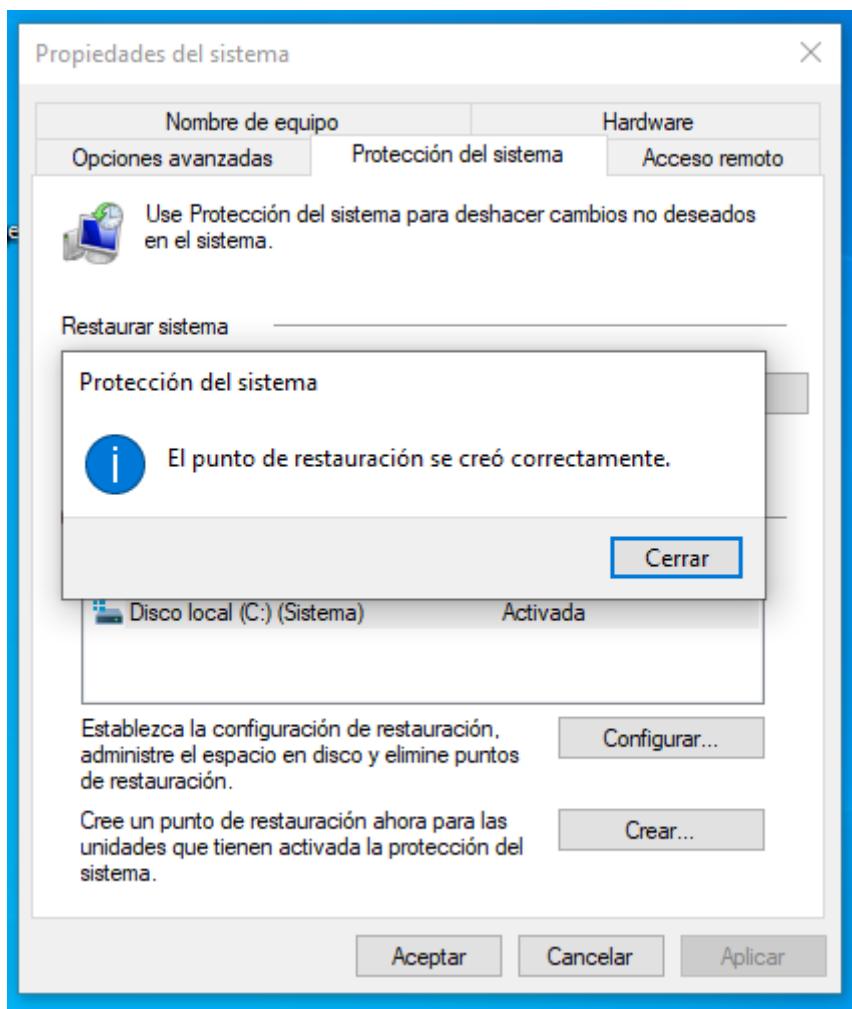






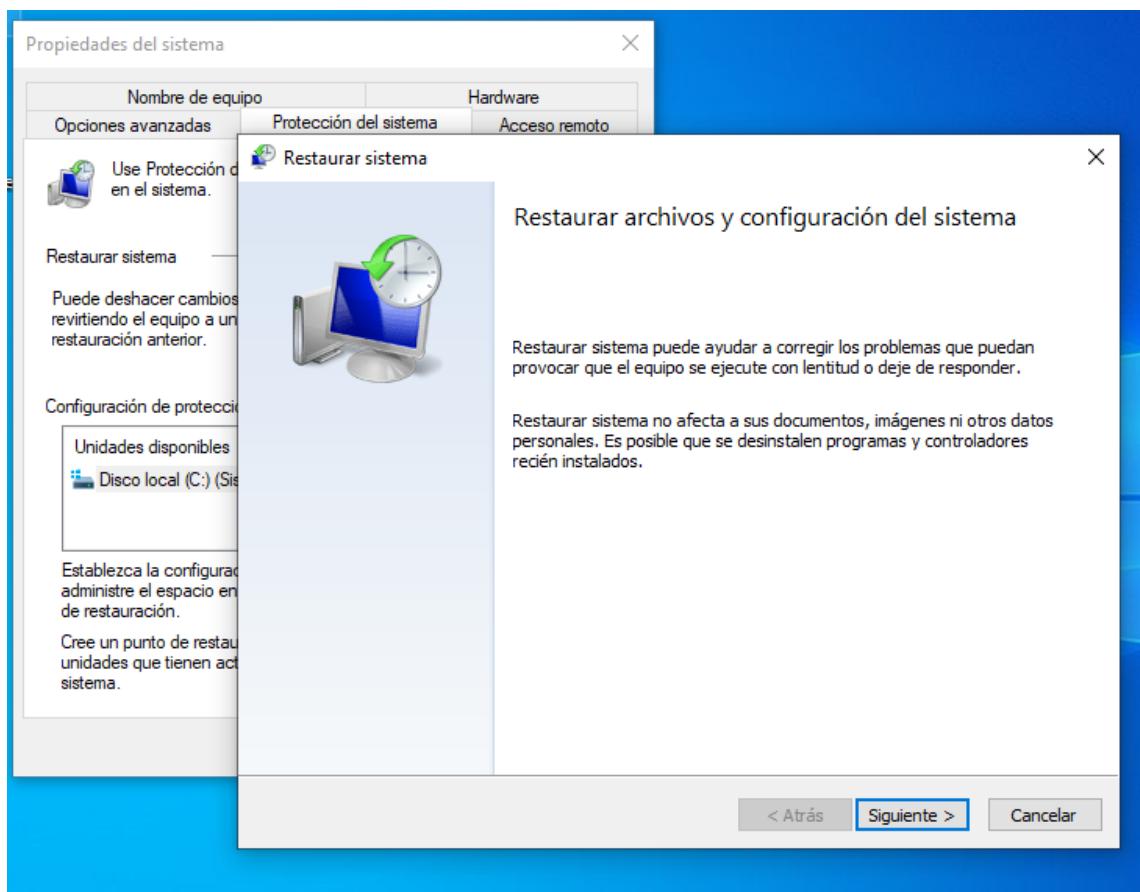
Con la protección activa, procedemos a crear el punto de restauración manual. En la misma pestaña de "Protección del sistema", se pulsa el botón "Crear". El sistema solicitará un nombre descriptivo para identificar este punto en el futuro; para esta prueba, se puede nombrar "Estado Limpio - Previa Prueba". Al hacer clic en "Crear", Windows guardará la configuración actual del registro y los archivos del sistema. Tras unos segundos, aparecerá un mensaje confirmando que el punto se ha creado correctamente.

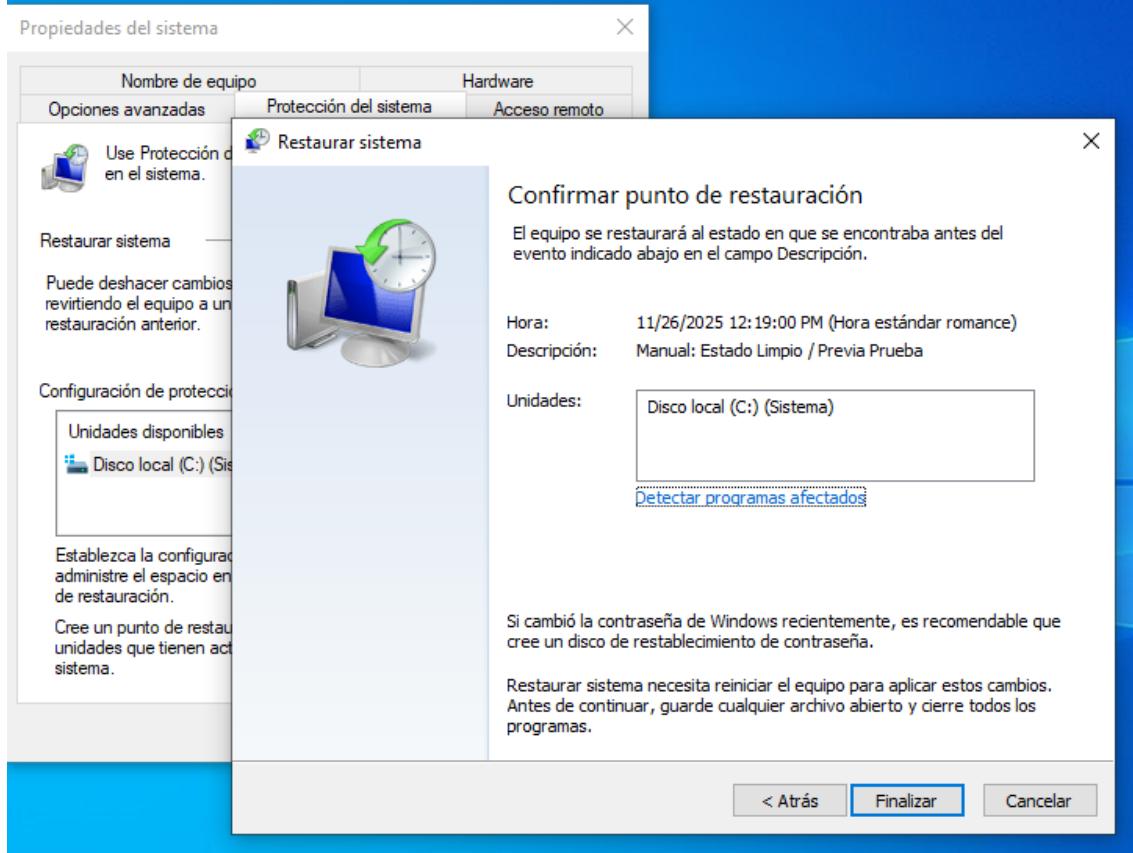
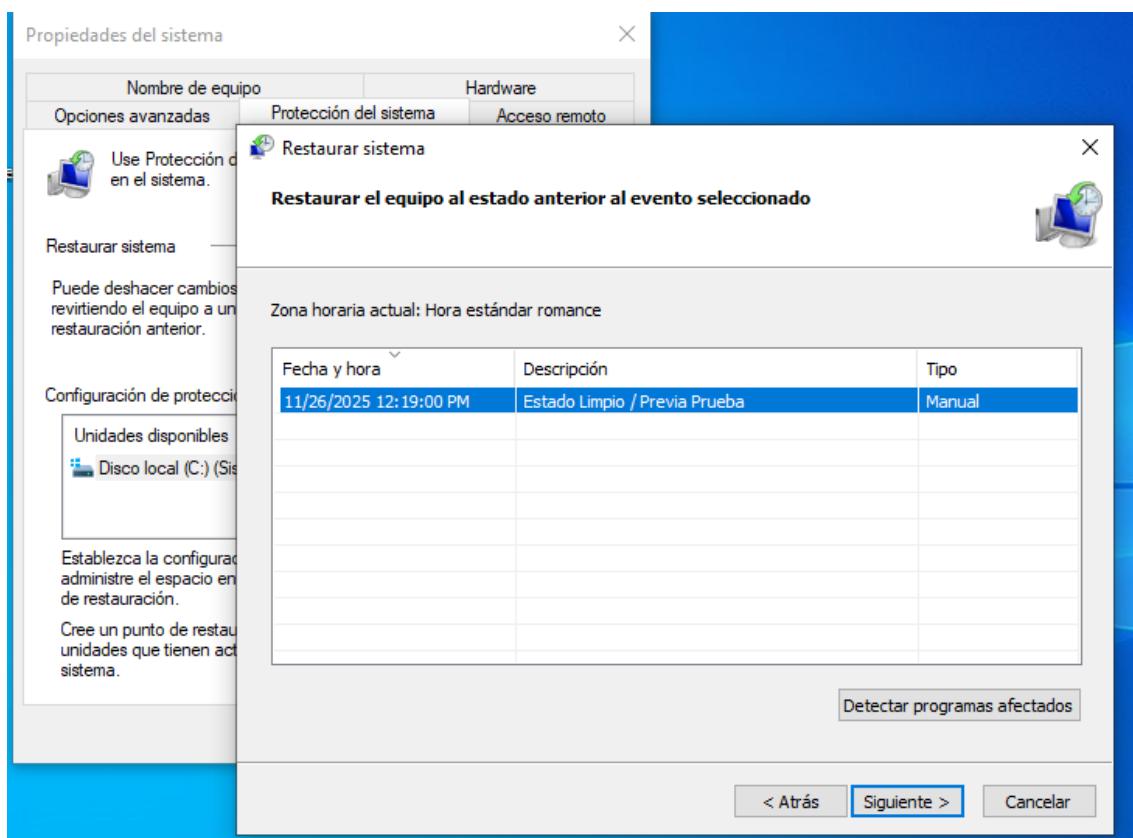


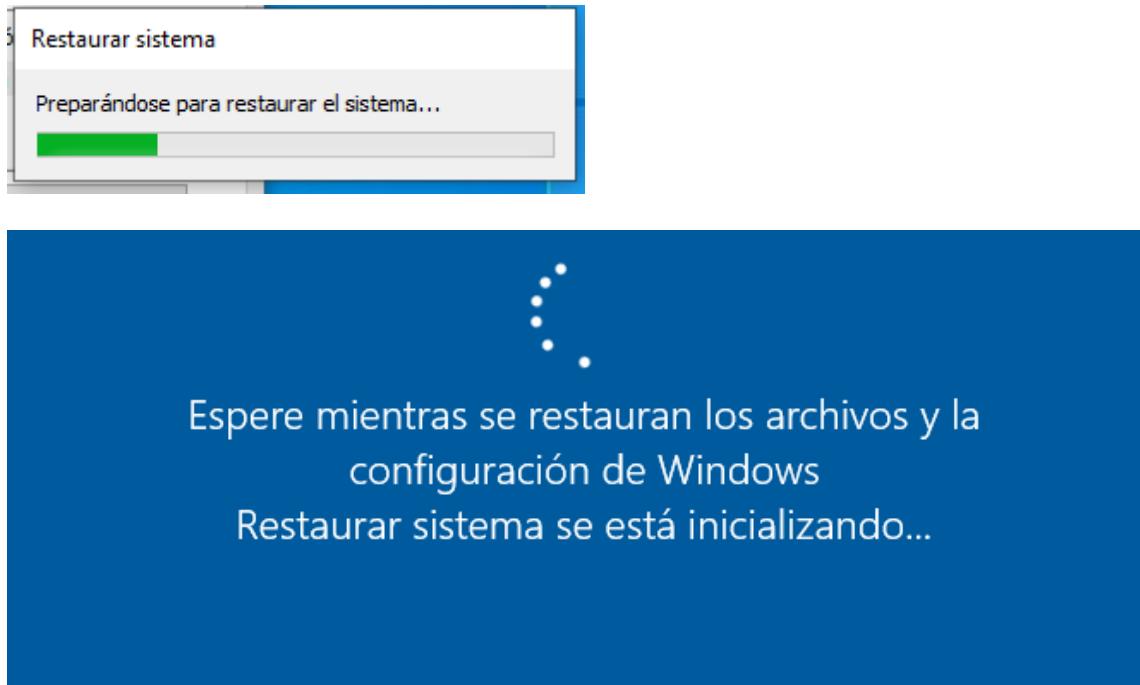


Simulación de Fallo y Recuperación

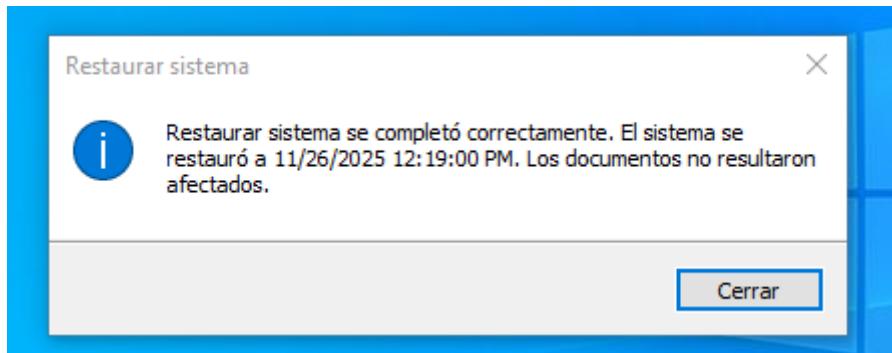
Para simular una situación que requiera recuperación, vamos a realizar un cambio "dañino" controlado. Procederemos a eliminar un controlador importante (simulado) o, más visualmente, desinstalar un programa crítico y borrar accesos directos del escritorio, creando un escenario de pérdida de configuración. Una vez realizado el daño, iniciaremos la recuperación. Volvemos a la herramienta de "Crear un punto de restauración", pero esta vez seleccionamos el botón "Restaurar sistema". Se abrirá un asistente donde elegiremos la opción "Elegir otro punto de restauración" y seleccionaremos el punto "Estado Limpio - Previa Prueba" que creamos anteriormente.







El sistema solicitará una confirmación final, advirtiendo que el proceso reiniciará el equipo y no podrá interrumpirse. Al aceptar, Windows se reiniciará y comenzará a cargar los archivos antiguos. Durante este proceso, la pantalla mostrará el progreso de la restauración del registro y los archivos. Al finalizar y volver a iniciar sesión en el escritorio, aparecerá una ventana emergente confirmando que el sistema se ha restaurado correctamente a la fecha y hora especificadas, y podremos verificar que los elementos borrados o los cambios realizados han sido revertidos.

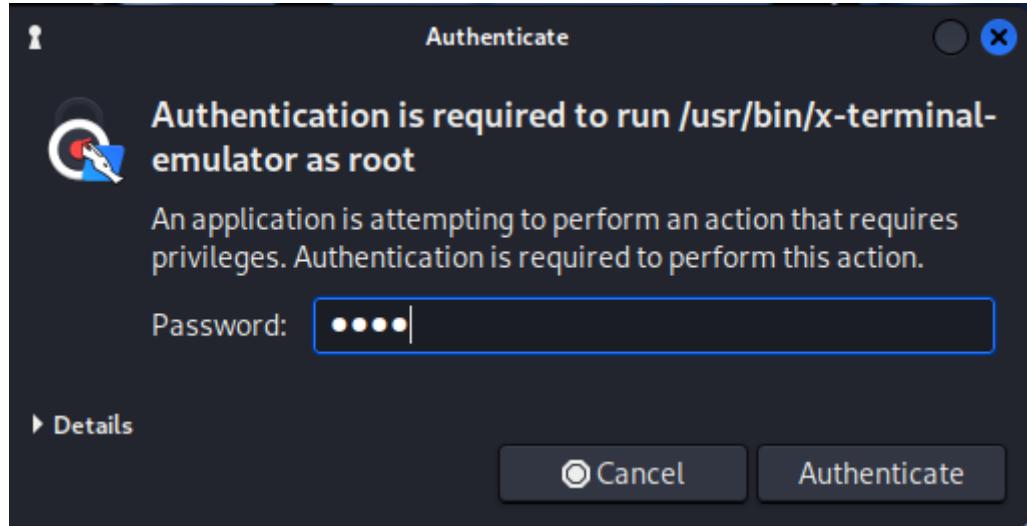


Parte 2: Sistema Operativo Kali Linux (Usando Timeshift)

Instalación y Configuración de Timeshift

A diferencia de Windows, Kali Linux no siempre trae una herramienta de "instantáneas" preconfigurada por defecto para el usuario final, por lo que utilizaremos **Timeshift**, el estándar en Linux para esta tarea. Lo primero es abrir una terminal con privilegios de root. Ejecutamos el comando `sudo apt update` seguido de `sudo apt install`

`timeshift` para instalar la herramienta. Una vez instalada, la abrimos desde el menú de aplicaciones. Al iniciarla por primera vez, se abrirá un asistente de configuración. Debemos seleccionar el tipo de instantánea; elegiremos "RSYNC" ya que es más flexible y no depende del sistema de archivos BTRFS, funcionando en casi cualquier instalación de Linux.

A screenshot of a terminal window titled 'root@kali: ~'. The window has a menu bar with 'Session', 'Actions', 'Edit', 'View', and 'Help'. The terminal shows a command-line session where the user is running 'apt update' as root. The output of the command is displayed, showing various package downloads from different repositories. The terminal window has a dark theme.

```
(root@kali)-[~]
└# sudo apt install timeshift
Installing:
  timeshift

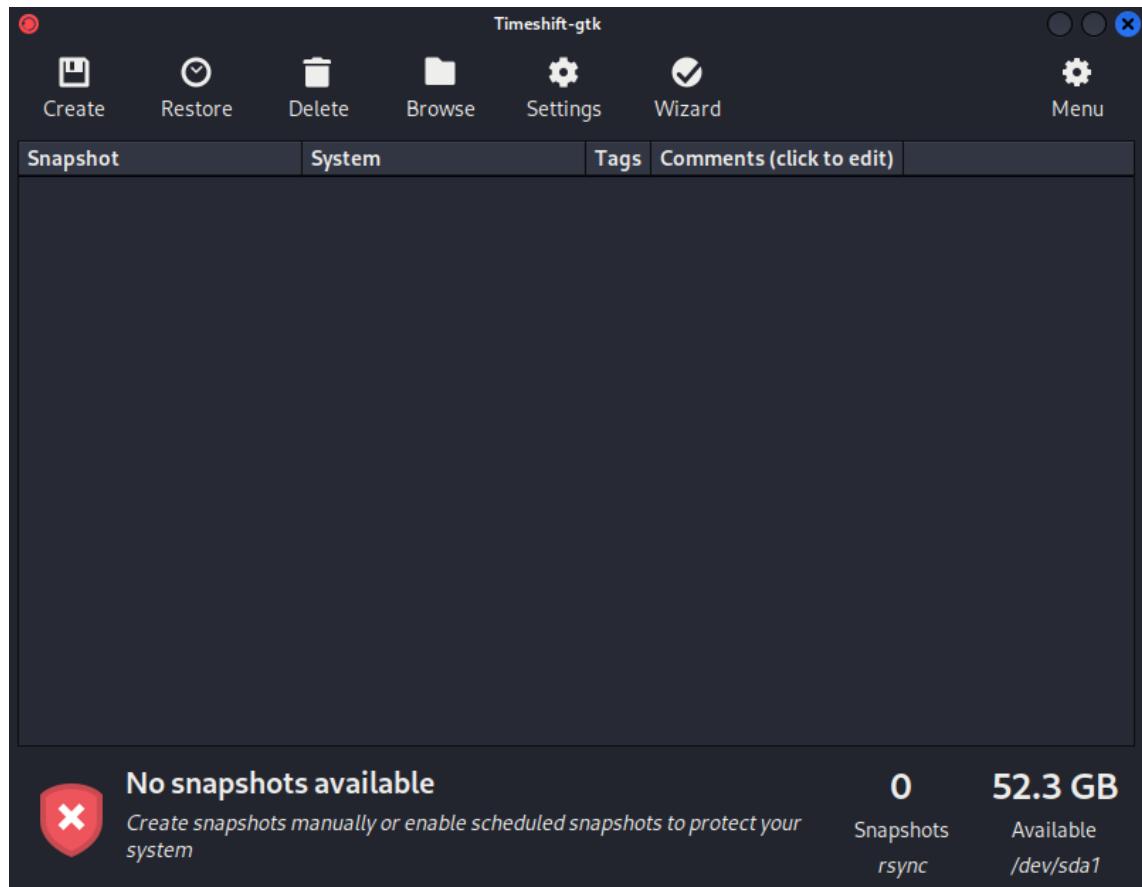
Installing dependencies:
  inxi          libgnomekbd8      mesa-utils      xapps-common
  libgee-0.8-2   libxapp-gtk3-module mesa-utils-bin
  libgnomekbd-common libxapp1       xapp-sn-watcher

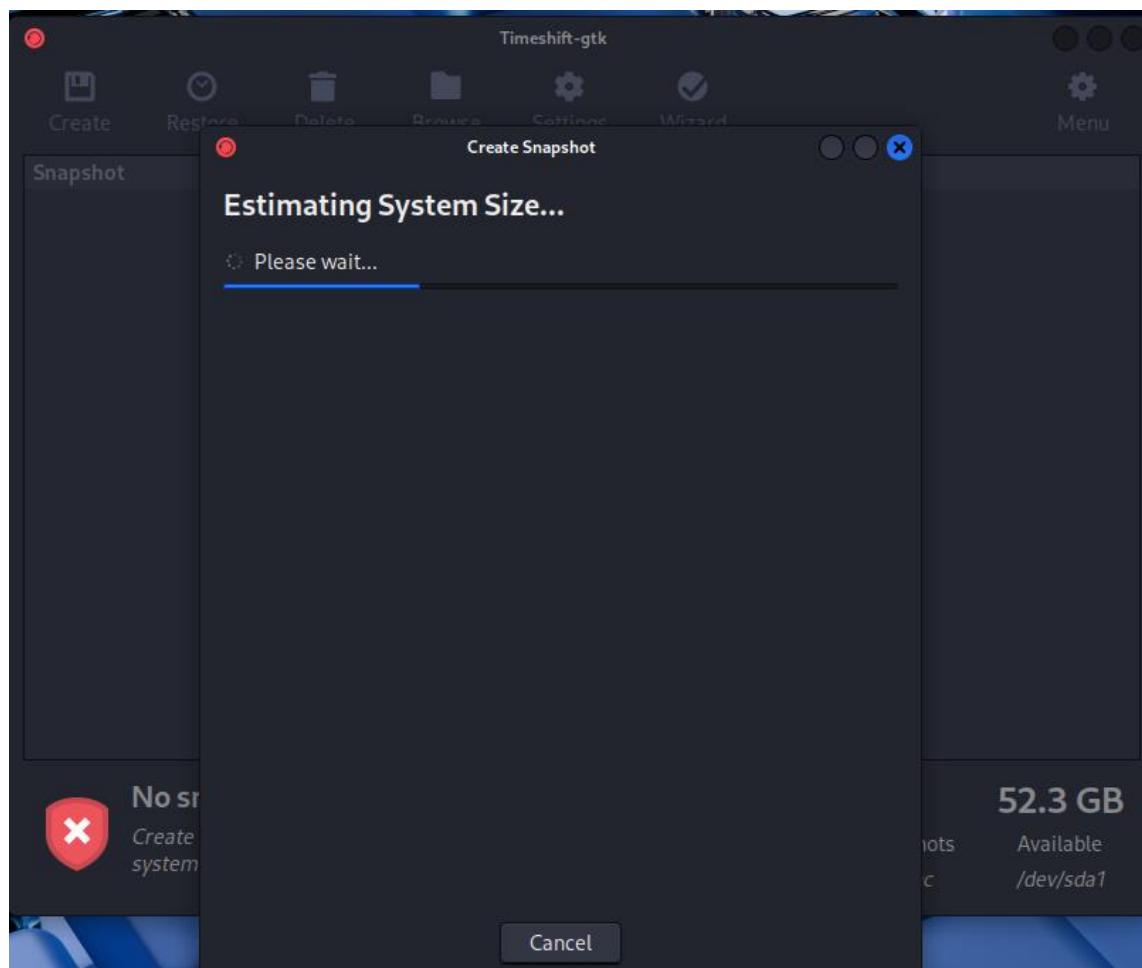
Suggested packages:
  libxml-dumper-perl  mate-xapp-status-applet

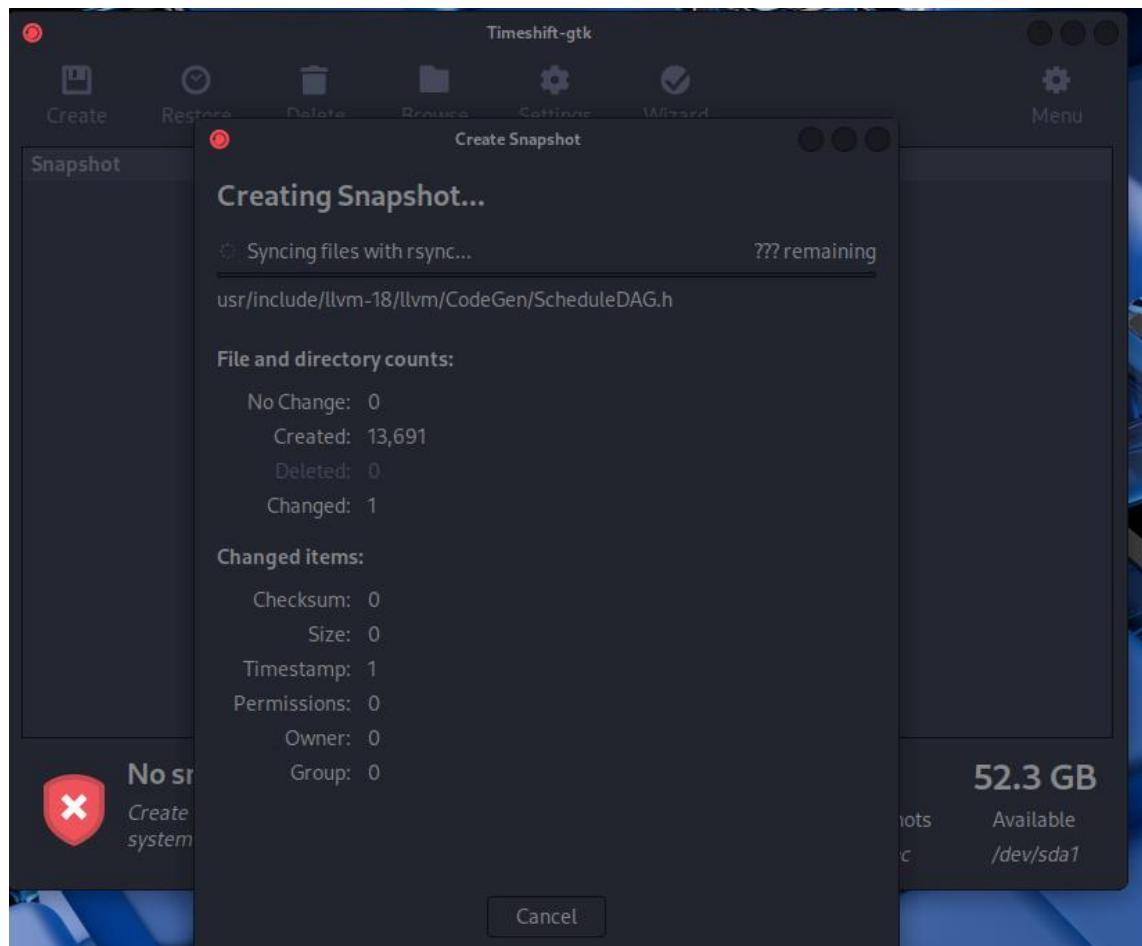
Summary:
  Upgrading: 0, Installing: 11, Removing: 0, Not Upgrading: 1215
  Download size: 3,022 kB
  Space needed: 12.0 MB / 62.0 GB available

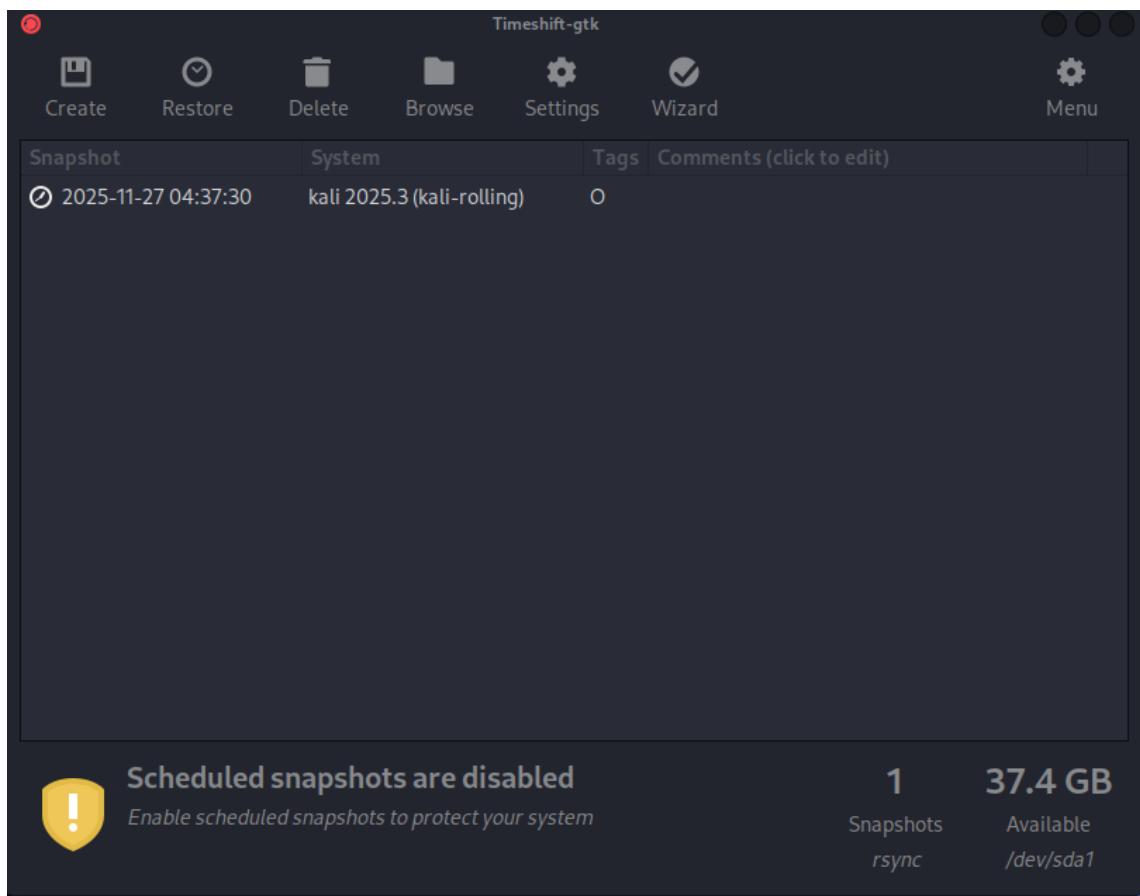
Continue? [Y/n] ■
```

El asistente luego pedirá seleccionar la ubicación donde se guardarán las instantáneas. Seleccionaremos la partición principal o un disco externo si estuviera conectado. Posteriormente, se nos permite configurar la frecuencia de las copias automáticas (diarias, semanales, etc.); para este laboratorio podemos dejarlas desactivadas o en modo manual, ya que haremos una al instante. Al finalizar el asistente, llegamos a la interfaz principal de Timeshift. Pulsamos el botón "Crear" en la barra de herramientas superior. El sistema comenzará a escanear los archivos y creará una instantánea completa del sistema operativo. Esto puede tardar unos minutos.





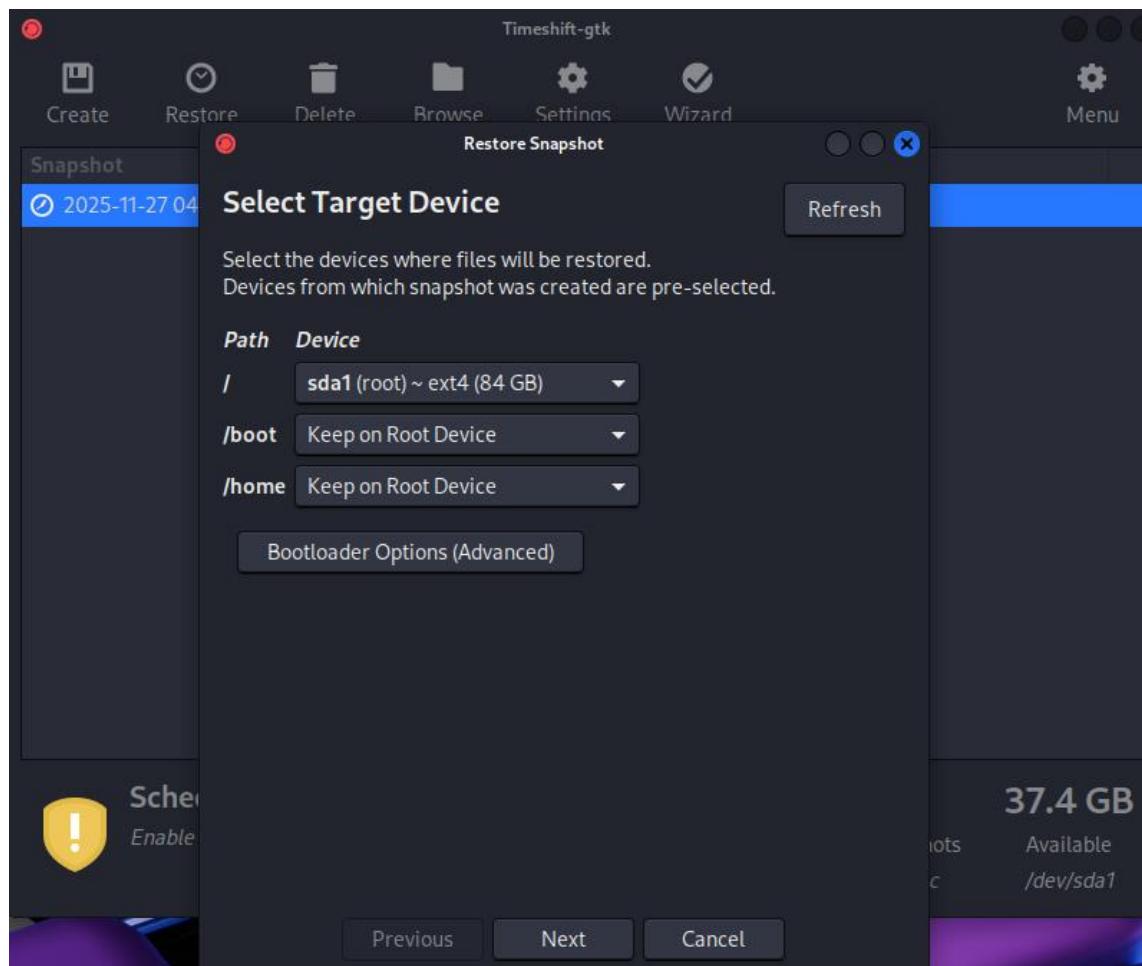


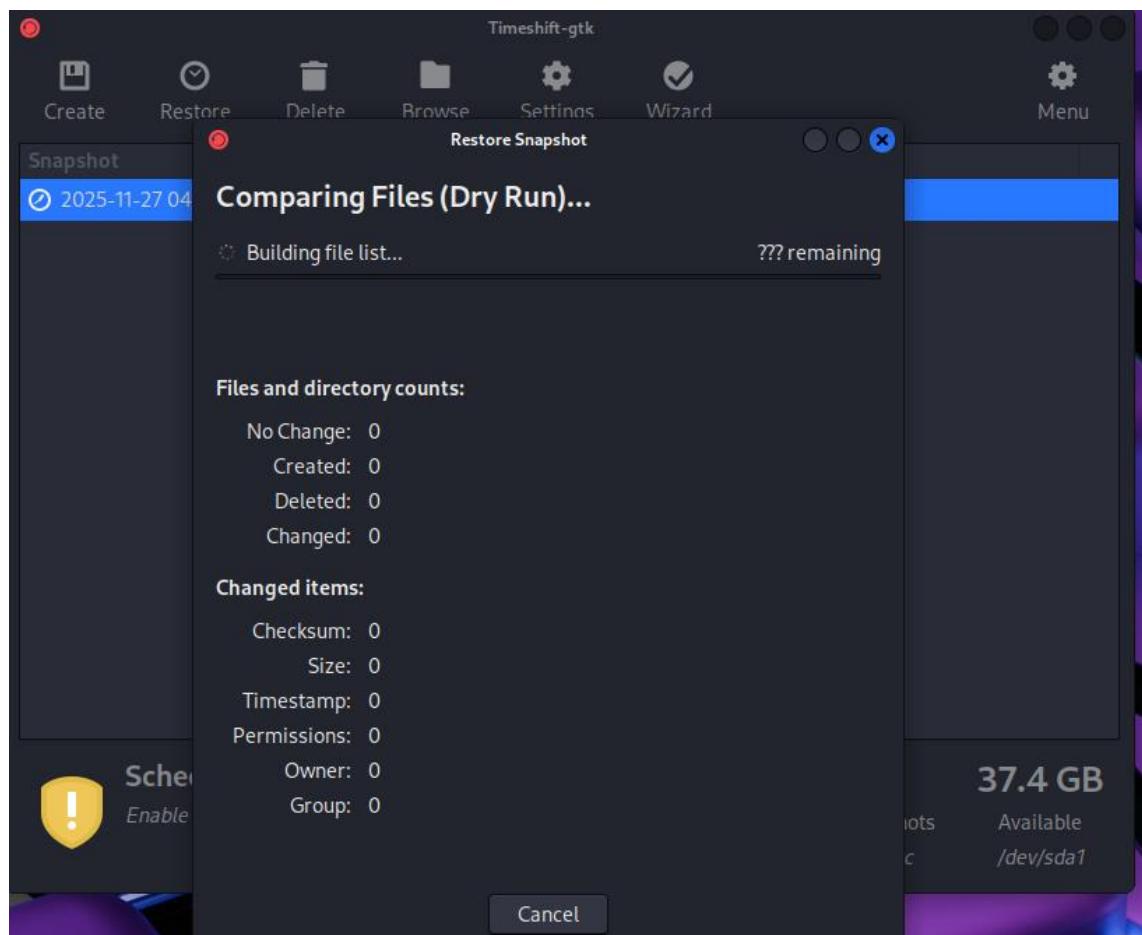


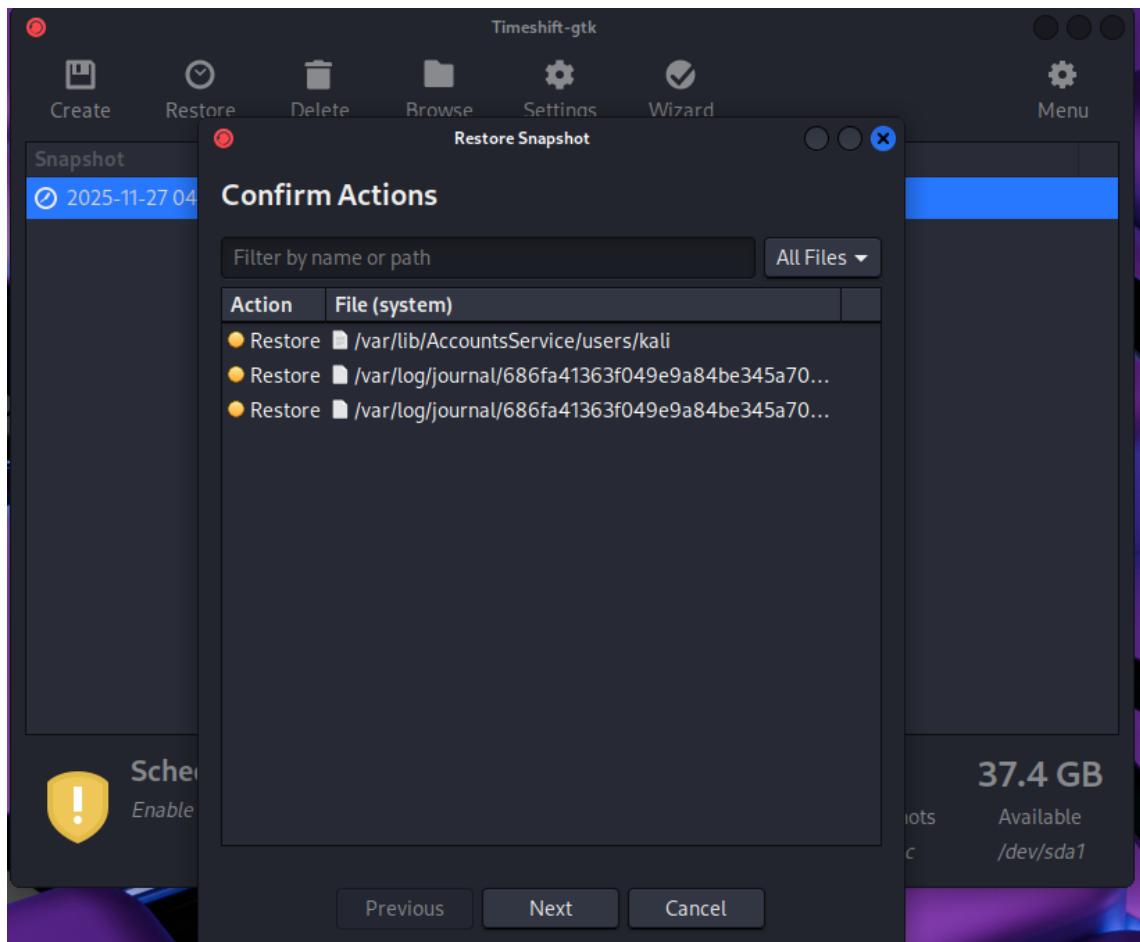
Simulación de Fallo y Recuperación

Para la simulación del desastre en Kali, realizaremos una acción destructiva en el sistema de archivos (con cuidado). Abriremos una terminal y borraremos un archivo de configuración no esencial pero visible, o instalaremos un paquete que "rompa" alguna configuración visual, por ejemplo, cambiando drásticamente el fondo de pantalla y borrando configuraciones del usuario en la carpeta `/etc/`. Una vez "dañado" el entorno, abrimos nuevamente Timeshift. En la lista principal, seleccionamos la instantánea que acabamos de crear y pulsamos el botón "Restaurar".

Antes de la restauración:







```
Please do not interrupt the restore process!
System will reboot after files are restored

building file list ...
```

Se abrirá una ventana mostrando los archivos que serán modificados (lo que se borrará y lo que se recuperará). Es importante revisar que el "Target Device" (Dispositivo de destino) sea correcto, generalmente la raíz /. Al confirmar, Timeshift advertirá que el proceso es delicado. Al proceder, el sistema comenzará a restaurar los archivos. Dependiendo de la configuración, puede pedir reiniciar. Tras el reinicio, verificaremos que el sistema Kali Linux ha vuelto exactamente al estado en que estaba al momento de la instantánea, con las configuraciones originales restauradas.

Después de la restauración:



Conclusión

Este laboratorio ha demostrado la eficacia de los puntos de restauración en entornos Windows y Linux. Mientras que Windows integra la solución de manera nativa y transparente para el usuario promedio, Linux ofrece a través de Timeshift un control más granular y potente sobre qué archivos exactos se están respaldando y restaurando. Ambos métodos son críticos para la administración de sistemas.