

**Nombre:** Luana Carolina Espinola Rivarola

**Asignatura:** Sistemas Operativos

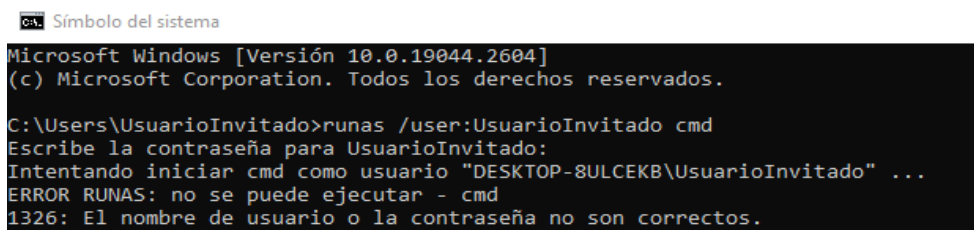
## **Laboratorio 4: Seguridad del Sistema.**

### **Auditoría de Seguridad**

#### **Descripción del laboratorio**

En esta sección del laboratorio se trabajó con las herramientas del sistema operativo Windows 10 Home para observar cómo registra intentos fallidos de inicio de sesión. Debido a que esta versión de Windows no cuenta con las políticas de seguridad avanzadas, se utilizó el Visor de eventos para identificar registros de seguridad.

Se simuló un inicio de sesión fallido desde un usuario secundario usando el comando runas en el símbolo del sistema, escribiendo una contraseña incorrecta. Luego, se accedió al Visor de eventos en el usuario principal, específicamente a la sección Registros de Windows > Seguridad, donde se encontró y documentó el evento 4625, correspondiente a un intento fallido de inicio de sesión



```
Microsoft Windows [Versión 10.0.19044.2604]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\UsuarioInvitado>runas /user:UsuarioInvitado cmd
Escribe la contraseña para UsuarioInvitado:
Intentando iniciar cmd como usuario "DESKTOP-8ULCEKB\UsuarioInvitado" ...
ERROR RUNAS: no se puede ejecutar - cmd
1326: El nombre de usuario o la contraseña no son correctos.
```

*Ilustración 1 Ingreso de contraseña errónea en cmd.*

### **Análisis**

La simulación realizada con el usuario UsuarioInvitado permitió comprobar que Windows 10 Home registra los intentos fallidos de inicio de sesión, proporcionando detalles como la hora, el nombre del usuario y el tipo de error.

A pesar de las limitaciones propias de la versión Home, esta funcionalidad básica de auditoría de seguridad es fundamental para detectar y analizar actividades sospechosas en el sistema.

Este ejercicio confirma que es posible monitorear eventos clave de seguridad sin herramientas avanzadas, ayudando en la protección y análisis de la integridad del sistema operativo.

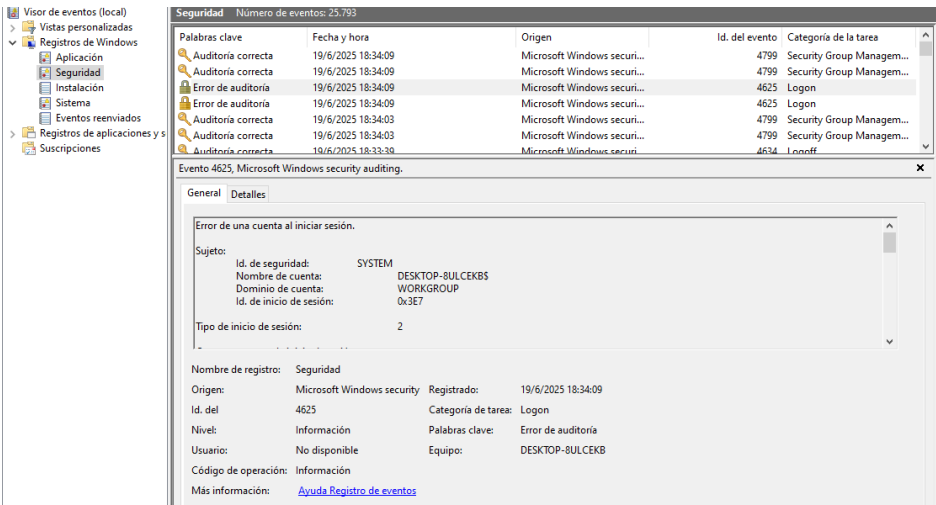


Ilustración 2 Visor de eventos, error "4625"

## Análisis de Vulnerabilidades

### Descripción del laboratorio

En esta sección del laboratorio se utilizó la herramienta de Seguridad de Windows para realizar un escaneo básico del sistema. Se ejecutó el análisis rápido de Windows Defender, y no se detectaron amenazas en el momento de la revisión.

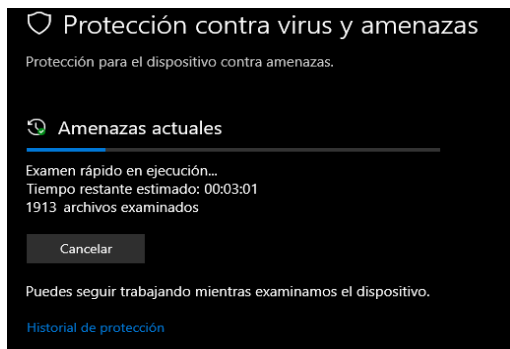


Ilustración 3 Windows Defender haciendo un escaneo rápido contra virus y amenazas

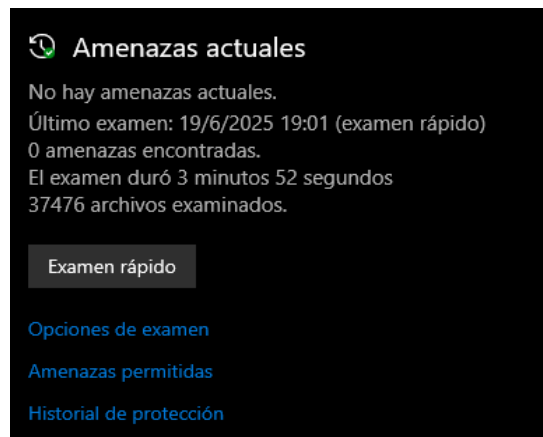


Ilustración 4 Windows Defender con escaneo finalizado.

Luego, se ingresó al panel de servicios del sistema (services.msc) para identificar procesos activos no esenciales. Se desactivaron los servicios de Fax y Telefonía, ya que no eran utilizados y su presencia en ejecución no aportaba al funcionamiento del sistema.

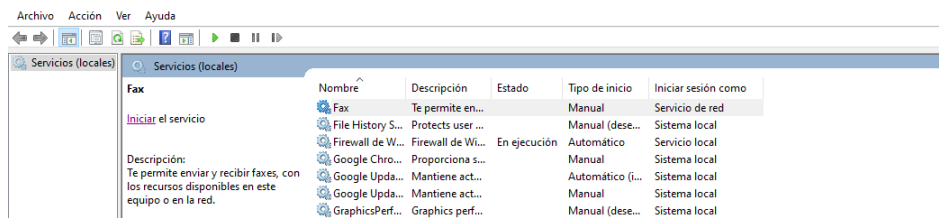


Ilustración 5 Servicio Fax desactivado

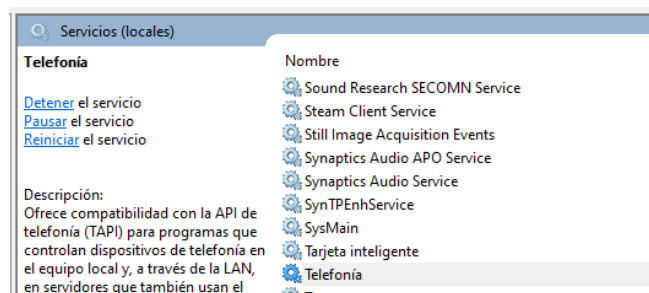


Ilustración 6 Servicio "Telefonía" antes de desactivarlo

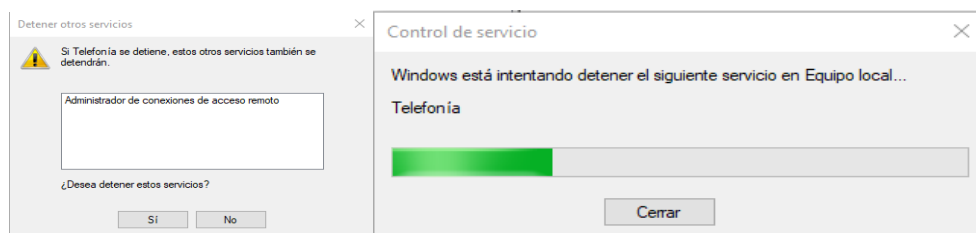


Ilustración 7 Proceso de desactivación de telefonía

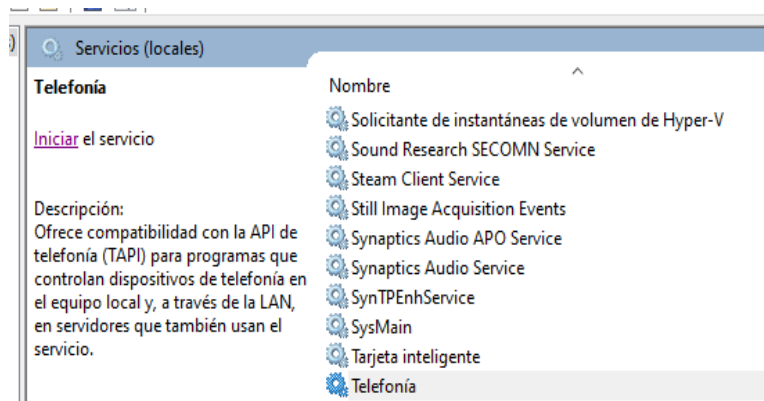


Ilustración 8 Servicio "Telefonía" desactivado

Finalmente, se detectó un mensaje persistente en Windows Update indicando que existían errores importantes de seguridad y calidad. A pesar de ejecutar el solucionador de problemas y aplicar comandos de restablecimiento de servicios, el sistema no logró resolver el inconveniente. Esta situación representa una vulnerabilidad crítica, ya que impide mantener el sistema completamente actualizado. Se recomienda como medida adicional el uso del Asistente oficial de actualización de Windows para forzar la instalación de los parches más recientes. Mientras tanto, se deja documentado este hallazgo como parte del análisis real del estado de seguridad del sistema operativo.

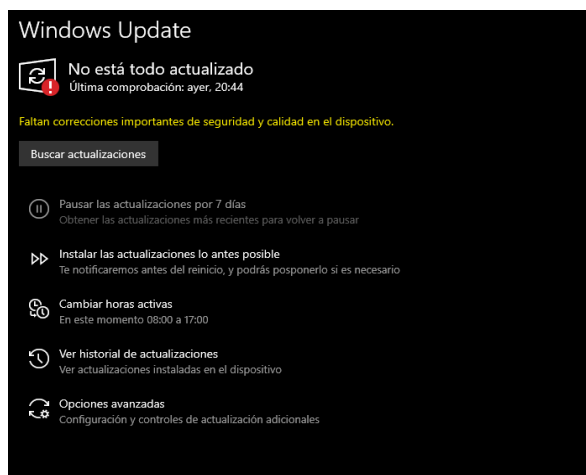


Ilustración 9 Ventana de Windows Update

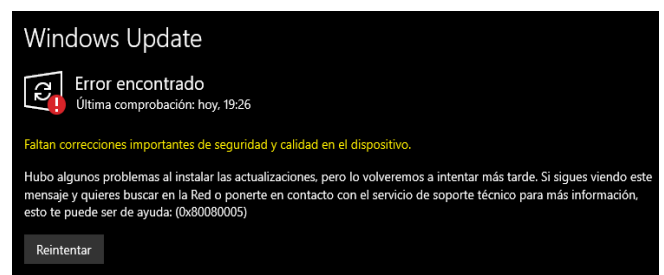
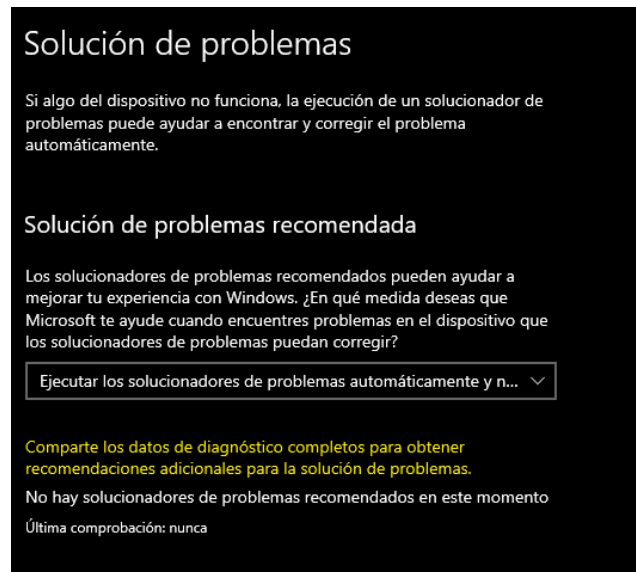


Ilustración 10 Error en Windows Update.



*Ilustración 11 Solución de problemas sin detectar problemas*

## **Análisis**

El escaneo básico demostró que el sistema no presentaba amenazas inmediatas. Además, como parte de las buenas prácticas de seguridad, se revisaron los servicios activos del sistema operativo. Se identificaron y desactivaron dos servicios innecesarios: Fax y Telefonía, los cuales no eran utilizados ni requeridos en el equipo. Esto permitió reducir el consumo de recursos y eliminar posibles vectores de vulnerabilidad que no aportaban funcionalidad al sistema.

Respecto al estado de actualización, se confirmó que el sistema no se encuentra completamente actualizado, ya que Windows muestra un mensaje informando sobre errores importantes de seguridad y calidad. Aunque se intentaron métodos básicos de solución como el solucionador de problemas y el reinicio de servicios relacionados con Windows Update, no se logró resolver la falla. Además, el solucionador no ofreció ningún análisis detallado del

problema. Por lo tanto, esta situación fue registrada como una vulnerabilidad no corregida, y se recomienda evaluar una actualización manual mediante el Asistente oficial de Microsoft en el futuro.

Este resultado es válido para el laboratorio, ya que demuestra un análisis real del sistema, se documentan los pasos realizados, se identifican fallas presentes y se aplican mejoras concretas en la configuración, cumpliendo así con el objetivo de auditar y fortalecer la seguridad del sistema operativo.

## Respaldo y Recuperación

### Descripción del laboratorio

En esta etapa del laboratorio se trabajó con la herramienta de Protección del sistema de Windows 10. Se creó correctamente un punto de restauración llamado punto\_lab4\_SO, y se verificó su existencia antes de continuar.

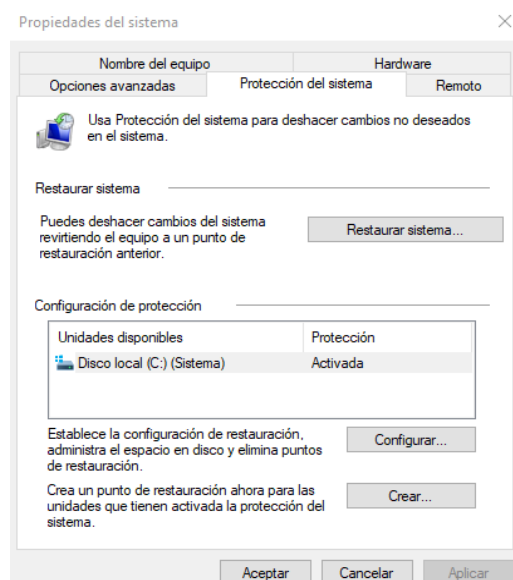


Ilustración 13 Propiedades del sistema para la creación de Punto de Restauración

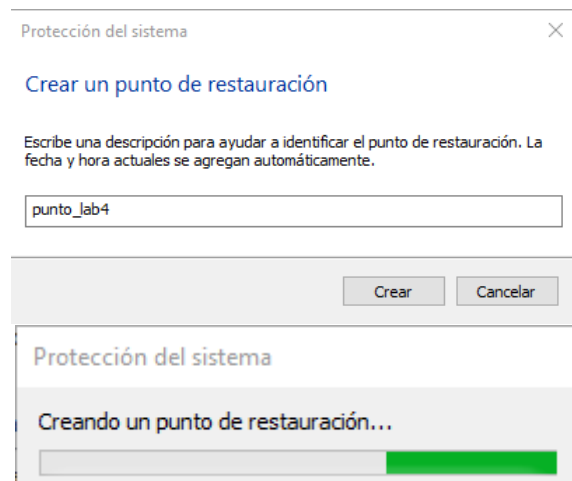
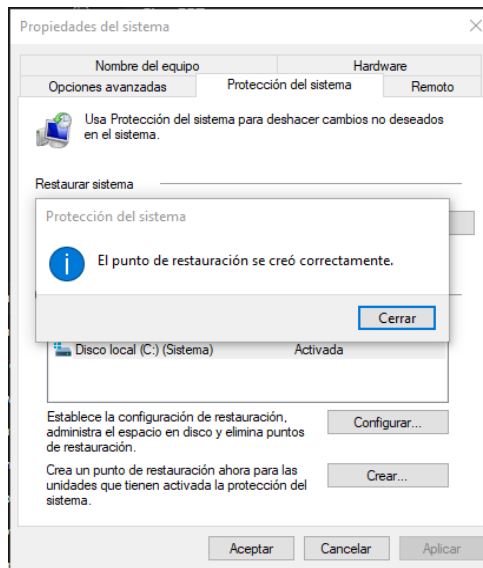


Ilustración 14 Proceso de creación de punto de restauración



*Ilustración 14 Punto de Restauración correctamente creada*

Como parte del experimento, se aplicó un cambio en el sistema: se movieron archivos del escritorio para observar si serían revertidos tras la restauración. Luego, se inició el proceso desde la opción de “Restaurar sistema” en la configuración de protección.



*Ilustración 15 Escritorio en su estado original*



*Ilustración 16 Escritorio con Archivos movidos de lugar*

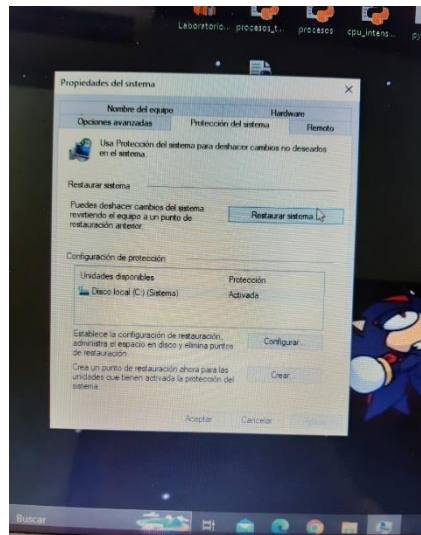


Ilustración 2 Selección para restaurar el sistema



Ilustración 18 Inicio de configuración para la restauración del sistema

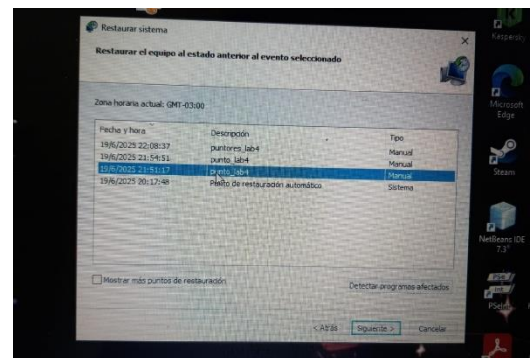


Ilustración 19 Selección de punto de restauración

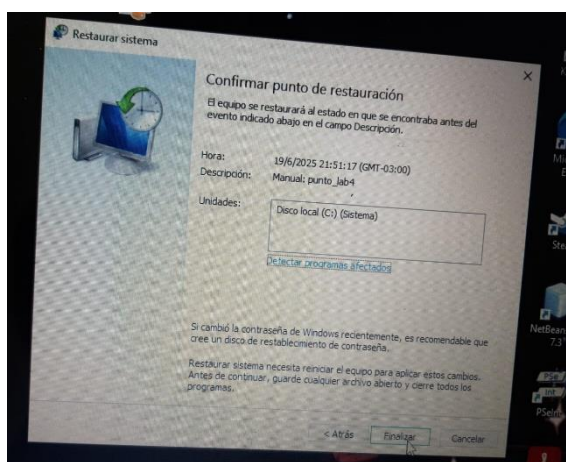


Ilustración 20 Confirmación de punto de restauración

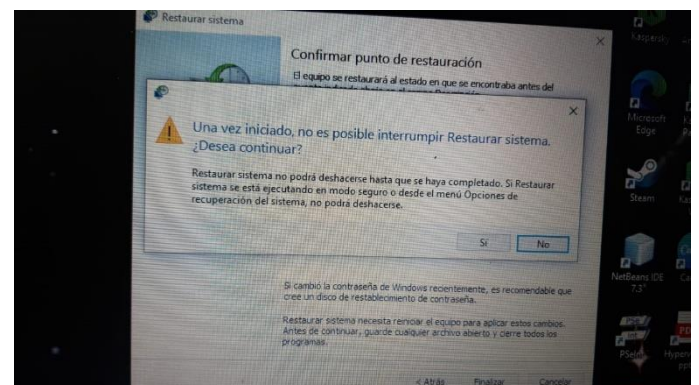
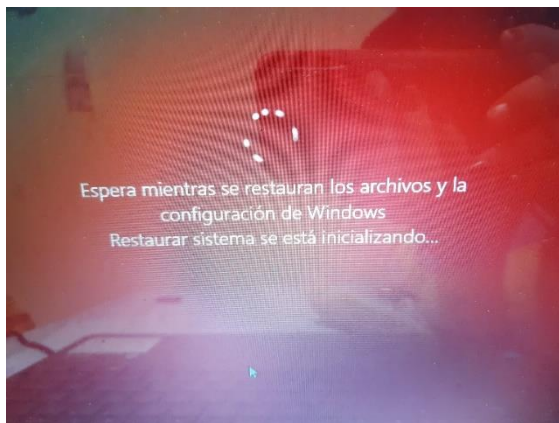
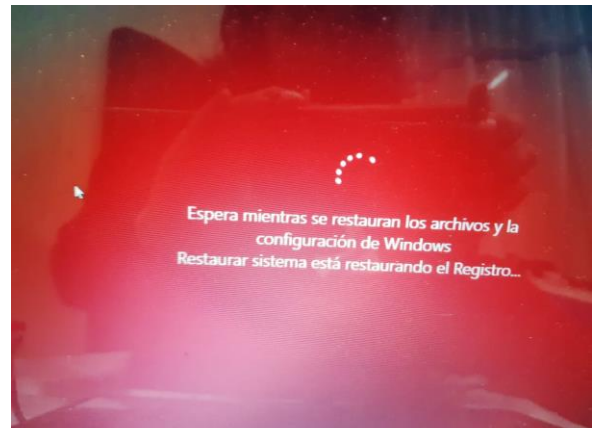


Ilustración 21 Confirmar si desea hacer el punto de restauración

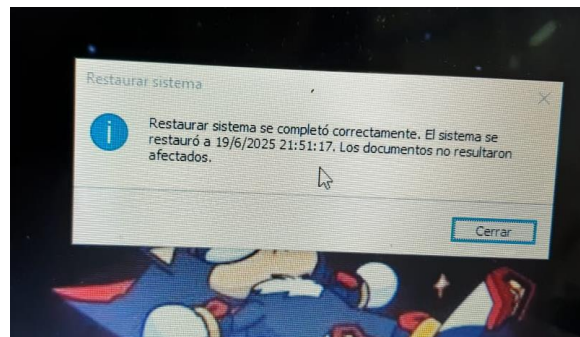




*Ilustración 22 Inicio de restauración del sistema*

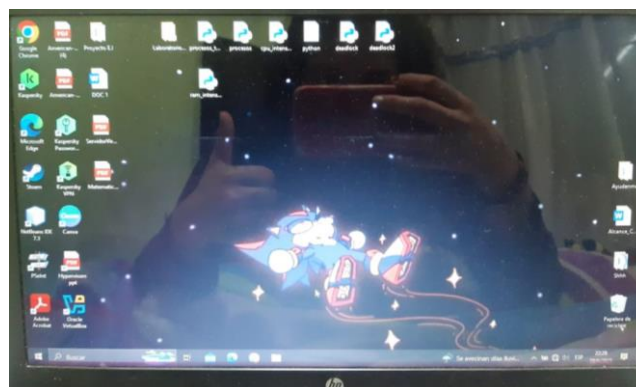


*Ilustración 23 Proceso del punto de restauración*



*Ilustración 24 Sistema restaurado completamente.*

La restauración fue exitosa. Se completaron todas las etapas del proceso: preparación, restauración del sistema, restauración del registro y reinicio. El equipo volvió al estado original guardado en el punto de restauración, y los archivos del escritorio regresaron a su ubicación anterior.



*Ilustración 25 Máquina restaurada*

## Análisis

La experiencia demostró que la herramienta de restauración funciona correctamente cuando está configurada previamente. Además, se pudo comprobar que los cambios aplicados al sistema fueron revertidos con precisión, lo cual valida la funcionalidad de esta opción como medida de respaldo segura ante errores o configuraciones no deseadas.

El proceso fue lento en algunas etapas, pero se completó de forma estable.

Este ejercicio permitió identificar no solo los beneficios del respaldo del sistema, sino también la importancia de crear puntos de restauración antes de realizar cambios importantes.

<b>Etapas del proceso</b>	<b>Tiempo aproximado</b>
Preparación para iniciar la restauración	57.14 segundos
Proceso de restauración del sistema	6.36 minutos
Restauración del registro del sistema	6 minutos aprox.
Reinicio e inicio de sesión tras la restauración	1.09 minutos