Informe
Laboratorio 4 Seguridad del Sistema

Auditoría de Seguridad

Activación de registros

Se procedió a habilitar la auditoría de eventos de seguridad del sistema operativo, permitiendo registrar tanto accesos exitosos como fallidos a través del Visor de eventos. En lugar de utilizar secpol.msc (inaccesible en Windows Home), se usó el comando auditpol desde la consola para activar el monitoreo de inicios de sesión y accesos a objetos restringidos. Esta configuración fue esencial para capturar eventos relacionados con intentos de ingreso no autorizados.

Directiva	Configuración de seguri...
Auditar el acceso a objetos	Correcto, Erróneo
Auditar el acceso al servicio de directorio	Sin auditoría
Auditar el cambio de directivas	Sin auditoría
Auditar el seguimiento de procesos	Sin auditoría
Auditar el uso de privilegios	Sin auditoría
Auditar eventos de inicio de sesión	Correcto, Erróneo
Auditar eventos de inicio de sesión de cuenta	Sin auditoría
Auditar eventos del sistema	Sin auditoría
Auditar la administración de cuentas	Sin auditoría

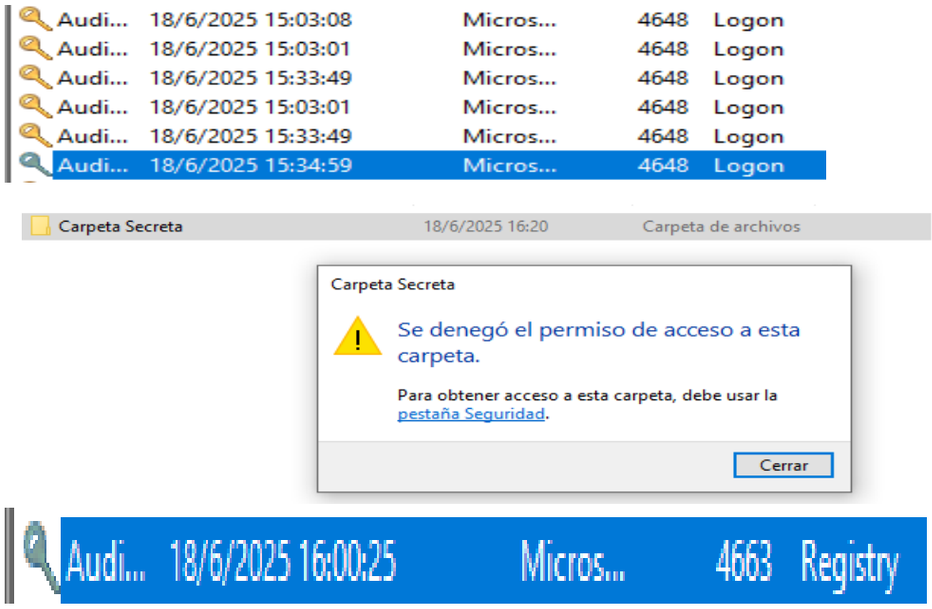
Simulación de eventos

Para generar registros auditables, se realizaron las siguientes acciones:
- Se introdujo una contraseña incorrecta en la pantalla de inicio de sesión.
- Se intentó ingresar a una carpeta protegida por permisos.

Ambos sucesos quedaron registrados en el sistema como eventos relevantes para la auditoría.

Ambos eventos fueron capturados por el sistema y registrados como:

Error...	18/6/2025 15:34:16	Micros...	4625	Logon
Error...	18/6/2025 15:34:19	Micros...	4625	Logon
Error...	18/6/2025 15:34:17	Micros...	4625	Logon
Error...	18/6/2025 15:34:21	Micros...	4625	Logon
Error...	18/6/2025 15:34:14	Micros...	4625	Logon
Error...	18/6/2025 15:33:55	Micros...	4625	Logon



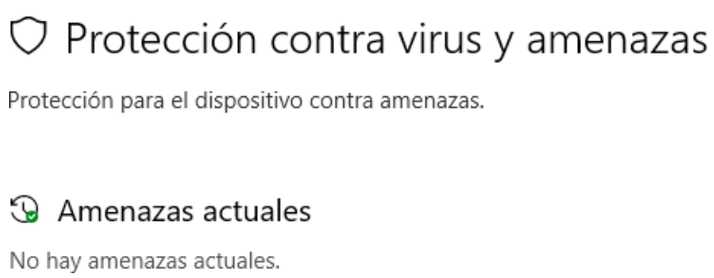
Análisis de los logs

Los eventos generados fueron localizados en el Visor de eventos, específicamente bajo “Registros de Windows > Seguridad”. Se observaron identificadores como el 4625, correspondiente a intentos de inicio de sesión fallidos. Cada log contenía detalles clave: usuario afectado, dirección de acceso, hora del evento y tipo de acción bloqueada.

Análisis de Vulnerabilidades

Escaneo de amenazas

Se hizo un análisis rápido usando **Windows Defender**. No se detectaron archivos maliciosos ni aplicaciones sospechosas en ese momento.

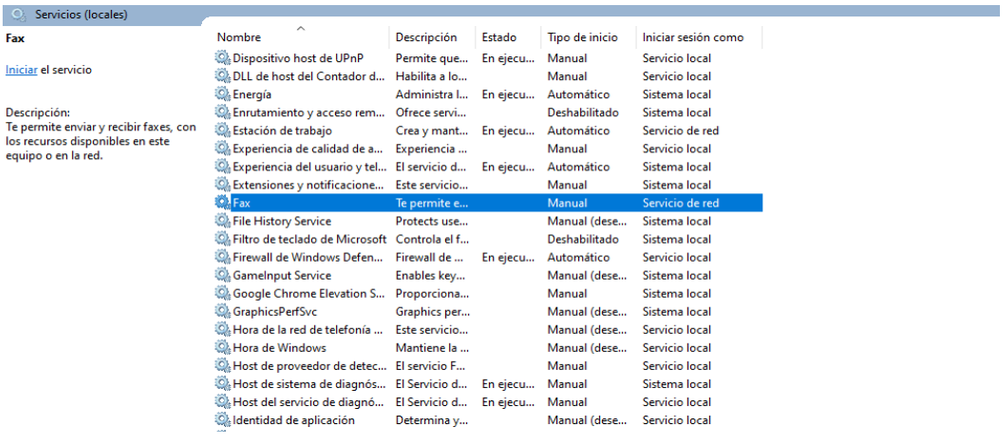


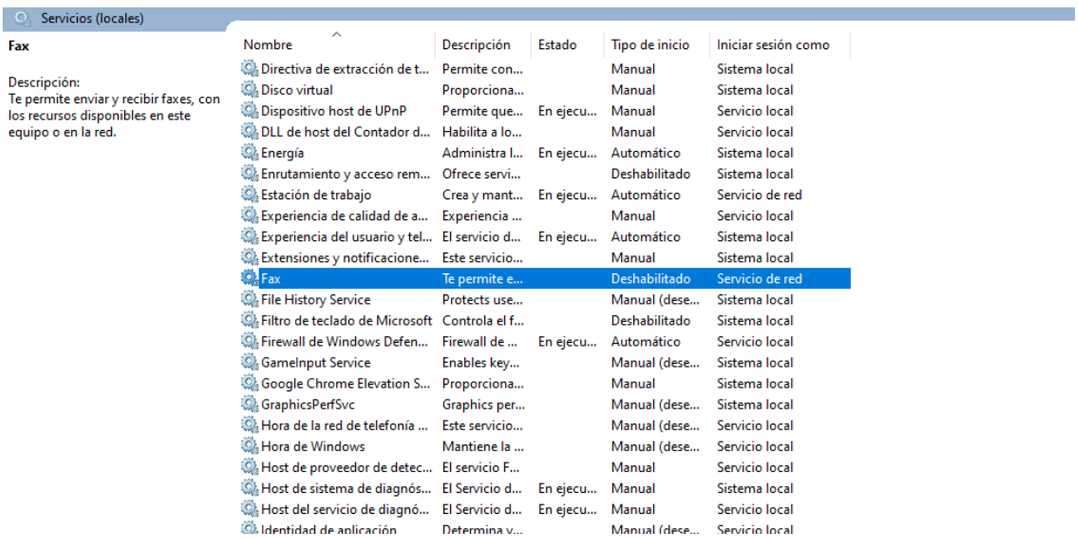
Servicios innecesarios

Se revisó la lista de servicios activos en el sistema y se encontraron varios que no eran necesarios para el uso actual del equipo. Por ejemplo:

- **Fax**
- **WalletService**
- **Bluetooth Support**
- **Remote Registry**

Todos fueron **deshabilitados** para reducir riesgos y consumo de recursos innecesarios. Por ejemplo:





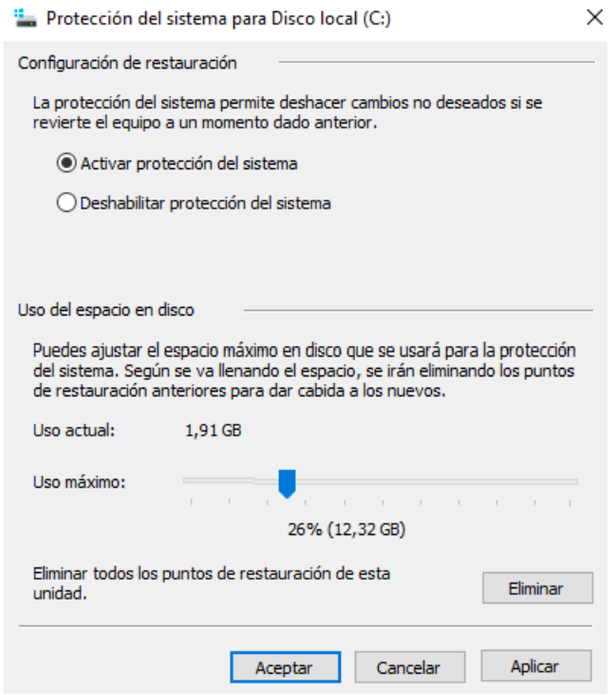
Actualizaciones

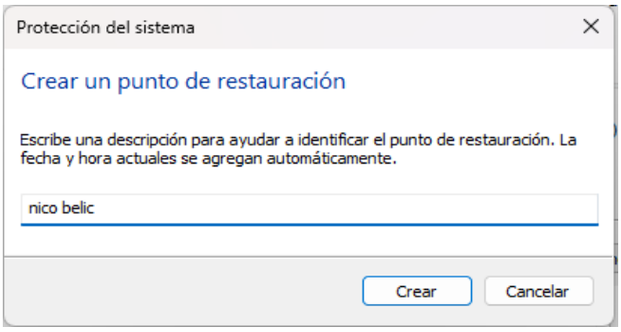
A través del panel de configuración de Windows Update, se comprobó que el sistema estaba completamente actualizado.

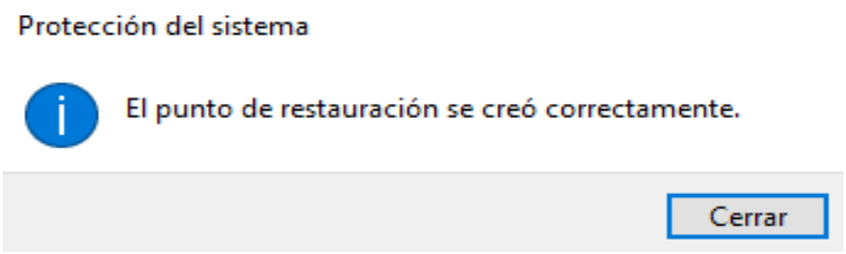
Respaldo y recuperación

Punto de restauración

Antes de realizar cambios en el sistema, se creó un **punto de restauración** para asegurar una reversión rápida en caso de errores o problemas.







Cambios apliados

Se realizaron modificaciones como:

- Instalación de Firefox (que falló por un problema en su instalador).
- Asociación de tipos de archivo modificados.
- Algunas apps dejaron de abrir correctamente.

Restauración y verificación

Se restauró el sistema usando el punto previamente creado. El proceso duró alrededor de 10 minutos y permitió recuperar el estado anterior. Los cambios fueron revertidos correctamente.

- Firefox fue eliminado (como estaba antes de instalarse).
- Las aplicaciones volvieron a abrir correctamente.
- Se comprobó que el sistema quedó estable nuevamente.

Conclusión

Este laboratorio demostró que la seguridad del sistema incluye el monitoreo de eventos, el control de servicios activos, el uso de usuarios limitados y la capacidad de restaurar el sistema. Estas herramientas aseguran un entorno informático más seguro, estable y recuperable.

Además, se reforzó la comprensión sobre cómo las amenazas pueden ser identificadas tempranamente mediante registros de auditoría, y cómo el respaldo adecuado permite recuperar el sistema ante eventos inesperados. En conjunto, estas prácticas fomentan una cultura de prevención y protección en la administración de equipos personales o empresariales.