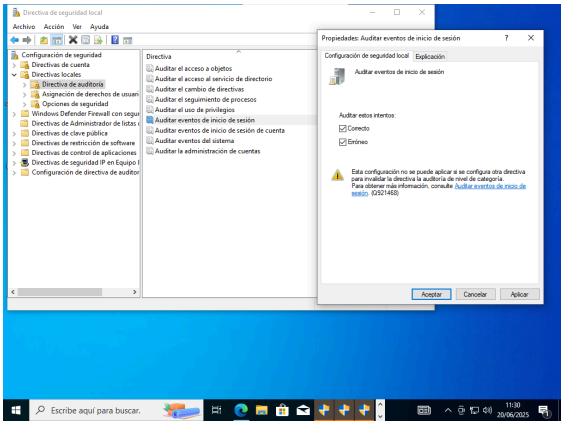
# Laboratorio 4: Seguridad del Sistema

## Introducción

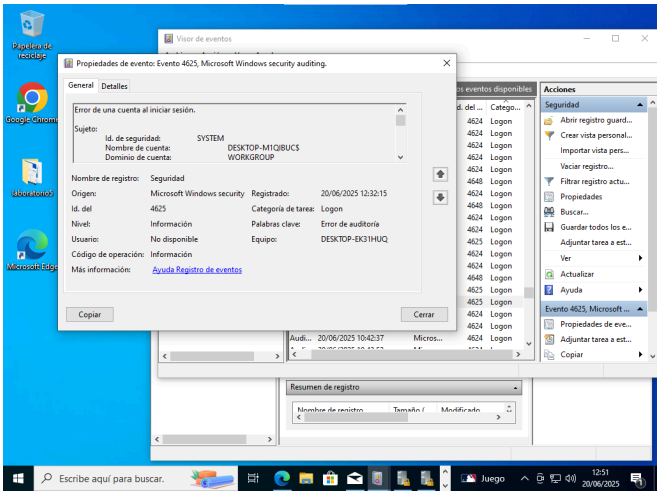
Este laboratorio tiene como objetivo aplicar prácticas fundamentales de seguridad en sistemas operativos, centrándose en auditoría, análisis de vulnerabilidades y mecanismos de respaldo y recuperación. Las actividades fueron realizadas en una máquina virtual con Windows, simulando eventos críticos y documentando el proceso.

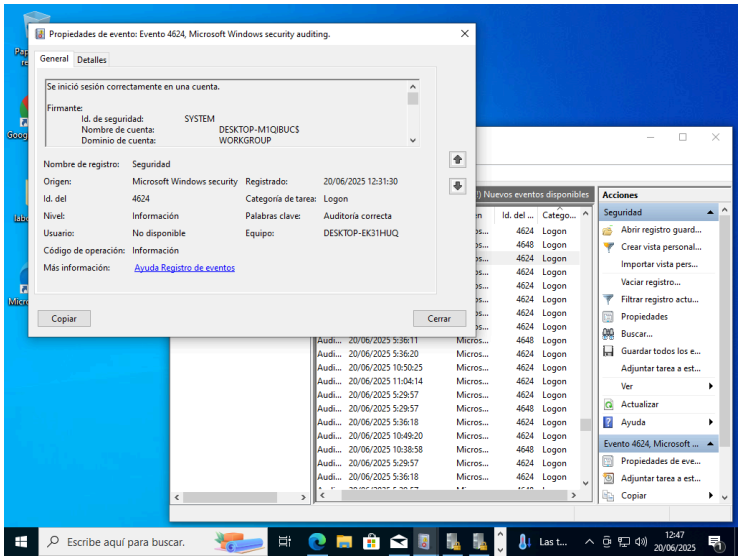
## 1. Auditoría de Seguridad

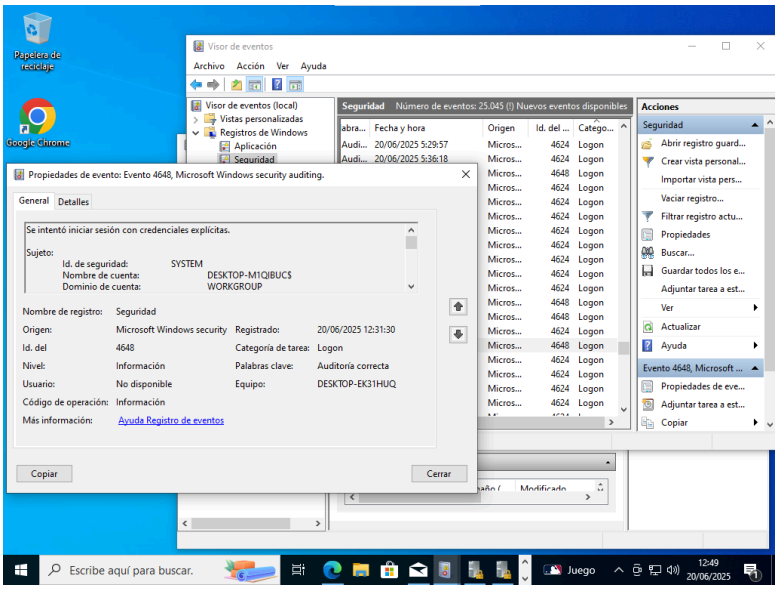
Se activaron los registros de seguridad en el Visor de eventos de Windows. Para validar su funcionamiento, se simularon intentos de inicio de sesión fallidos y accesos denegados a archivos protegidos.



Estos eventos generaron logs con identificadores como el 4625 (inicio de sesión fallido) y el 4648 (intento de acceso). El análisis de estos eventos confirmó que el sistema está registrando adecuadamente los intentos de acceso no autorizado.



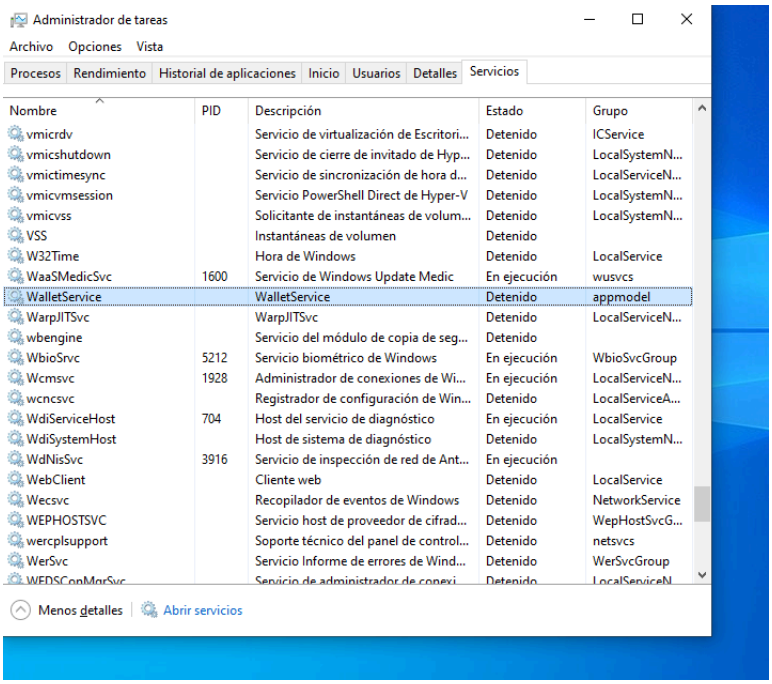



## 2. Análisis de Vulnerabilidades

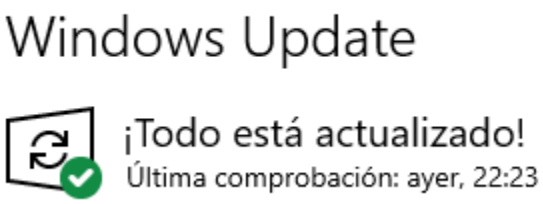
Se revisaron los servicios activos mediante la herramienta 'services.msc' en Windows. Se identificaron varios servicios innecesarios, entre ellos:

- Servicio de telefonía (Telephony)
- WalletService
- Otros servicios relacionados con funciones de red o móviles no utilizadas



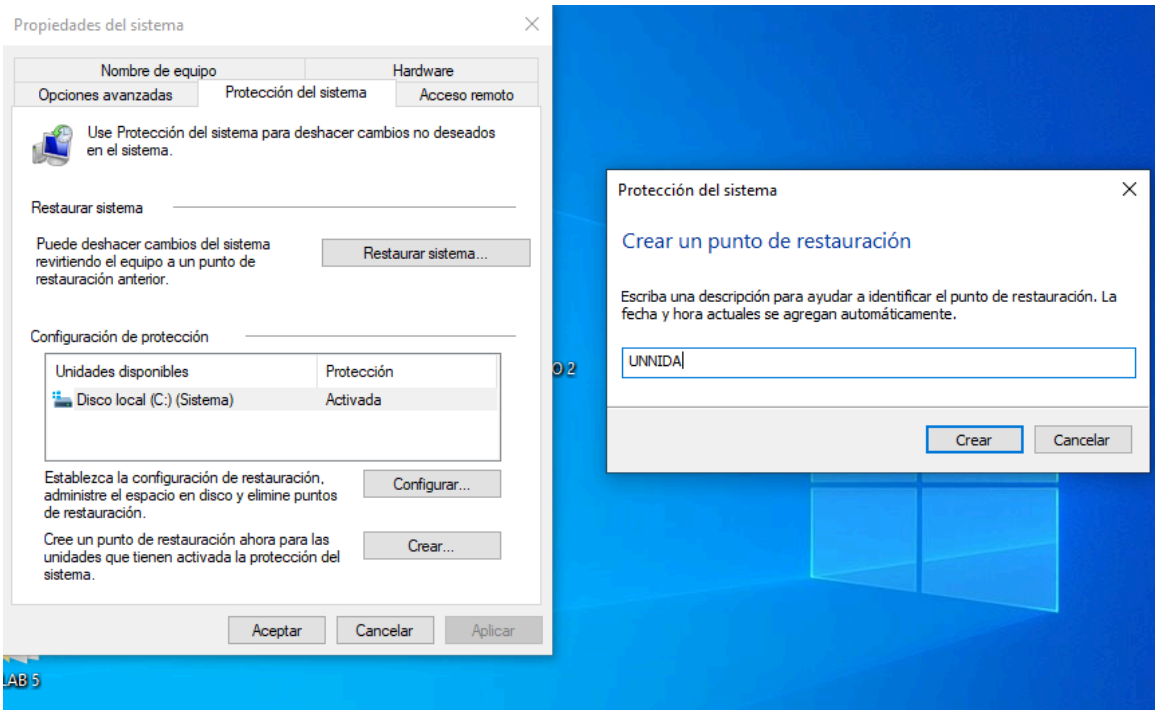
Estos servicios fueron desactivados para reducir la superficie de ataque y optimizar el rendimiento del sistema.

Se verificó también que el sistema estuviera actualizado utilizando Windows Update. No se encontraron actualizaciones pendientes.

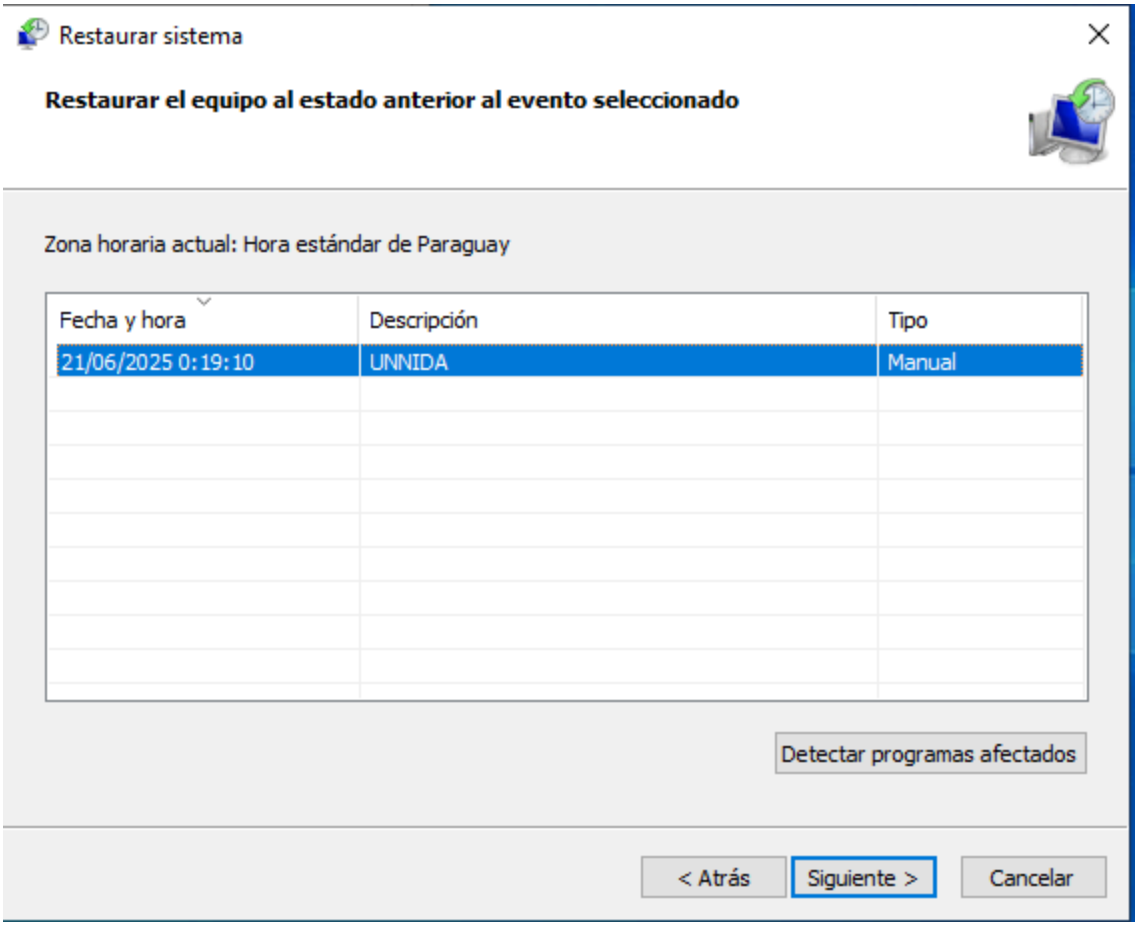



## 3. Respaldo y Recuperación

Antes de realizar los cambios en los servicios, se creó un punto de restauración utilizando la herramienta de Protección del Sistema. El proceso de creación tomó aproximadamente 3 minutos.




Posteriormente, se desactivaron los servicios identificados. Una vez finalizados los cambios, se restauró el sistema al punto previo para verificar la funcionalidad del mecanismo de recuperación.




La restauración se completó con éxito en aproximadamente 5 minutos. No se perdió información durante el proceso.

Tiempos registrados:

- Creación del punto de restauración: 3 minutos
- Desactivación de servicios: 7 minutos
- Restauración del sistema: 5 minutos

## 4. Checklist de Seguridad

✔ Logs de seguridad activados
✔ Eventos simulados registrados
✔ Servicios innecesarios identificados
✔ Sistema actualizado
✔ Punto de restauración creado
✔ Restauración verificada

## Conclusión

Durante este laboratorio se pusieron en práctica técnicas fundamentales de seguridad en sistemas operativos Windows. La auditoría permitió visualizar intentos de acceso no autorizados, mientras que el análisis de vulnerabilidades permitió desactivar servicios innecesarios que representan riesgos potenciales. Finalmente, se comprobó la efectividad de los puntos de restauración como mecanismo de recuperación. Estas prácticas refuerzan la importancia de mantener una configuración segura y controlada.