



UNIVERSIDAD DE LA INTEGRACIÓN DE LAS AMÉRICAS
FACULTAD DE INGENIERÍA.

MATERIA
Sistemas Operativos.

TÍTULO
Laboratorio de Análisis de Sistemas Operativos.

INFORME DE LABORATORIO N°4:
Seguridad del Sistema.

Mg. Alan Vladimir Dioses Echegaray.
Lucio Vera.

ESTUDIANTE:
Jannely Magalí Guillén Capdevila.

Asunción- Paraguay.
2025.

Introducción.

Este laboratorio se centró en tres pilares de la seguridad de un sistema operativo: la auditoría de eventos para el análisis forense, el análisis de vulnerabilidades para la prevención de ataques, y los mecanismos de respaldo y recuperación para la resiliencia del sistema. Se realizaron pruebas prácticas en un entorno Windows para observar y verificar el comportamiento de estas funciones.

Materiales y Métodos.

Se utilizó un entorno de máquina virtual (Oracle VM VirtualBox) con Windows 10 Pro para garantizar un ambiente de pruebas controlado. Las herramientas empleadas incluyeron:

Visor de Eventos (eventvwr.msc): Para la inspección de los registros de seguridad generados.

Directiva de seguridad local (secpol.msc): Para la activación de las políticas de auditoría a nivel de sistema.

Propiedades de Seguridad de Carpetas: Para la configuración de Listas de Control de Acceso de Auditoría (SACL) a nivel de objeto.

Consola de Servicios (services.msc): Para el análisis de servicios en ejecución.

Utilidad de Restaurar Sistema: Para la creación y ejecución de puntos de restauración.

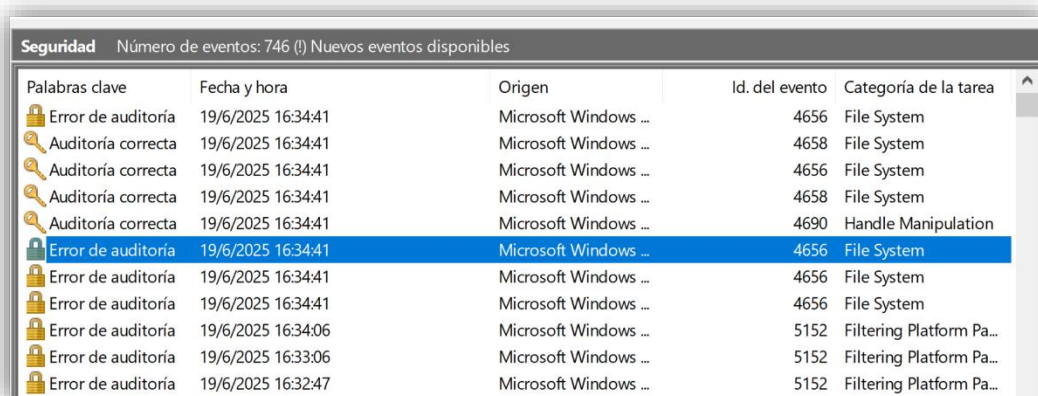
Desarrollo y Resultados.

Auditoría de Seguridad.

Procedimiento: Se configuraron las políticas de auditoría para registrar los intentos de acceso fallidos, tanto a nivel de inicio de sesión como de acceso a objetos del sistema de archivos. Se creó una regla de auditoría específica en la carpeta Acceso_Denegado para monitorear los fallos del usuario "janne".

Resultado: Las pruebas de un inicio de sesión fallido y un acceso a la carpeta denegada generaron los eventos esperados en el registro de seguridad de Windows.

Análisis: El análisis de los eventos (ID 4625 y 4656) demostró que el sistema operativo registró correctamente la información crítica, incluyendo la cuenta de origen de la acción (janne), el objeto del acceso (Acceso_Denegado) y la razón del fallo, confirmando el correcto funcionamiento del subsistema de auditoría.



Palabras clave	Fecha y hora	Origen	Id. del evento	Categoría de la tarea
Error de auditoría	19/6/2025 16:34:41	Microsoft Windows ...	4656	File System
Auditoría correcta	19/6/2025 16:34:41	Microsoft Windows ...	4658	File System
Auditoría correcta	19/6/2025 16:34:41	Microsoft Windows ...	4656	File System
Auditoría correcta	19/6/2025 16:34:41	Microsoft Windows ...	4658	File System
Auditoría correcta	19/6/2025 16:34:41	Microsoft Windows ...	4690	Handle Manipulation
Error de auditoría	19/6/2025 16:34:41	Microsoft Windows ...	4656	File System
Error de auditoría	19/6/2025 16:34:41	Microsoft Windows ...	4656	File System
Error de auditoría	19/6/2025 16:34:06	Microsoft Windows ...	5152	Filtering Platform Pa...
Error de auditoría	19/6/2025 16:33:06	Microsoft Windows ...	5152	Filtering Platform Pa...
Error de auditoría	19/6/2025 16:32:47	Microsoft Windows ...	5152	Filtering Platform Pa...

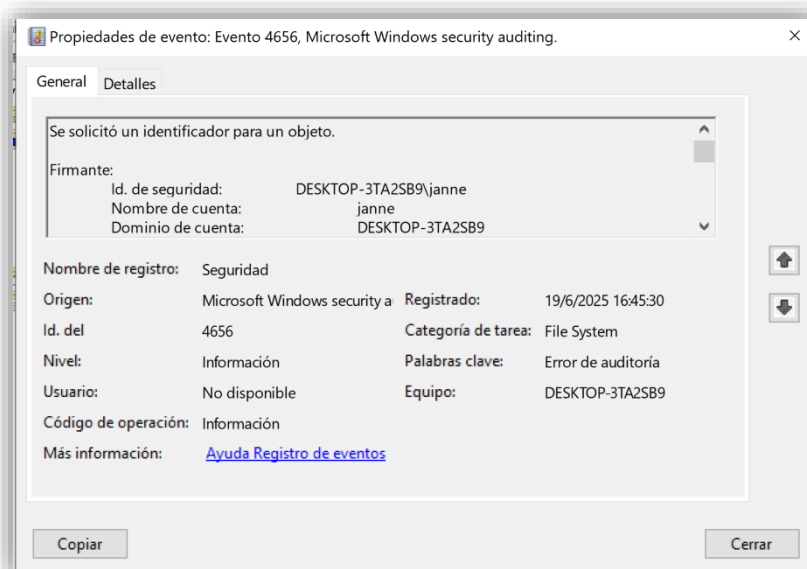


Figura 1. Detalle del evento de acceso denegado registrado correctamente.

Eventos Analizados en la Auditoría.

Evento 1: Intento de Inicio de Sesión Fallido.

- **Acción Realizada:** Se intentó iniciar sesión en el sistema con una contraseña incorrecta para un usuario válido.
- **ID del Evento Registrado:** 4625 (Error de auditoría).
- **Análisis:** El Visor de Eventos de Windows registró correctamente la falla. El análisis del evento mostró la hora exacta, la cuenta de usuario implicada y la razón del fallo (contraseña incorrecta). Esto confirma que la política de "Auditar eventos de inicio de sesión de cuenta" está funcionando como se esperaba.

Evento 2: Intento de Acceso a Objeto Denegado.

- **Acción Realizada:** El usuario estándar "janne" intentó acceder a la carpeta C:\PROYECTO_PERMISOS\Acceso_Denegado, para la cual no tenía permisos.
- **ID del Evento Registrado:** 4656 (Error de auditoría).
- **Análisis:** La auditoría de acceso a objetos funcionó a la perfección. El sistema generó un evento que identificó de manera precisa tanto al sujeto que realizó la acción (SubjectUserName: janne) como el objeto específico al que se intentó acceder (ObjectName: C:\PROYECTO_PERMISOS\Acceso_Denegado).

El sistema de auditoría y registro de eventos de Windows 10 demostró ser una herramienta robusta y fiable para el monitoreo de la seguridad. Los eventos generados proporcionan la información necesaria para realizar un análisis forense básico y detectar actividades potencialmente maliciosas en el sistema.

Análisis de Vulnerabilidades.

- **Servicios Innecesarios:** Se identificaron servicios en ejecución no esenciales para el entorno de laboratorio, como "Cola de Impresión" y "Windows Search". Se concluye que mantener activos estos servicios amplía innecesariamente la superficie de ataque del sistema.
- **Verificación de Actualizaciones:** Se utilizó el panel de Windows Update para confirmar que el sistema operativo contaba con los últimos parches de seguridad, una medida fundamental para la protección contra vulnerabilidades conocidas.

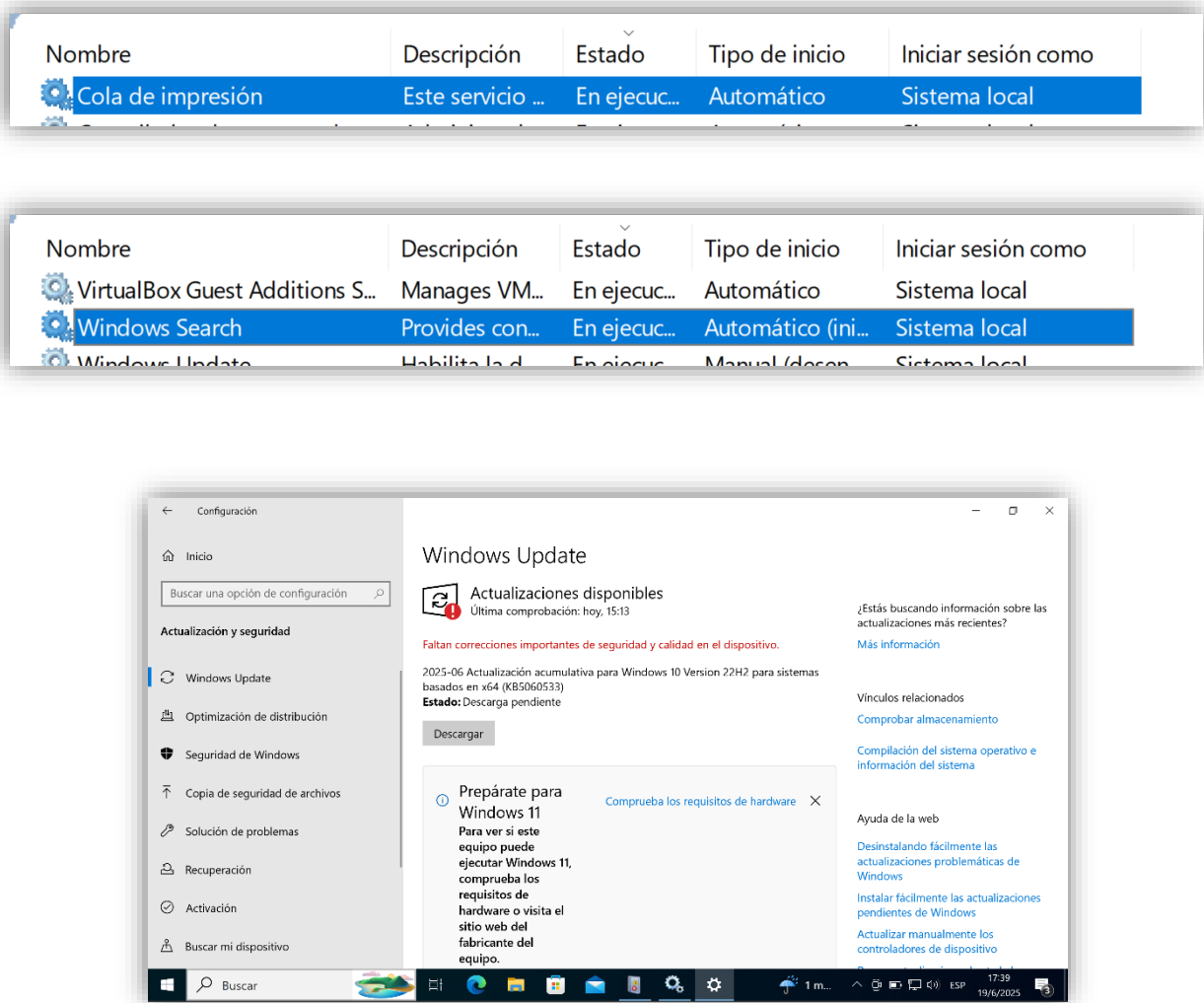


Figura 2, 3 y 4. Verificación del estado de las actualizaciones del sistema.

Respaldo y Recuperación.

- **Procedimiento:** Se creó un punto de restauración del sistema, un proceso que tomó aproximadamente 15 segundos. Posteriormente, se realizaron cambios controlados en el sistema (creación de una carpeta en el escritorio y modificación del fondo de pantalla).
- **Resultados y Análisis:** Se inició el proceso de "Restaurar sistema" utilizando el punto de restauración creado. La operación se completó exitosamente en aproximadamente 8 minutos, tras lo cual el sistema se reinició automáticamente. Al volver a iniciar sesión, un mensaje confirmó el éxito de la restauración. Se verificó que los cambios realizados (la carpeta en el escritorio y el fondo de pantalla) habían sido revertidos correctamente, devolviendo el sistema a su estado anterior.
- **Conclusión de la prueba:** La herramienta "Restaurar Sistema" de Windows demostró ser un mecanismo eficaz y fiable para deshacer cambios no deseados en la configuración del sistema y recuperarse de problemas menores.

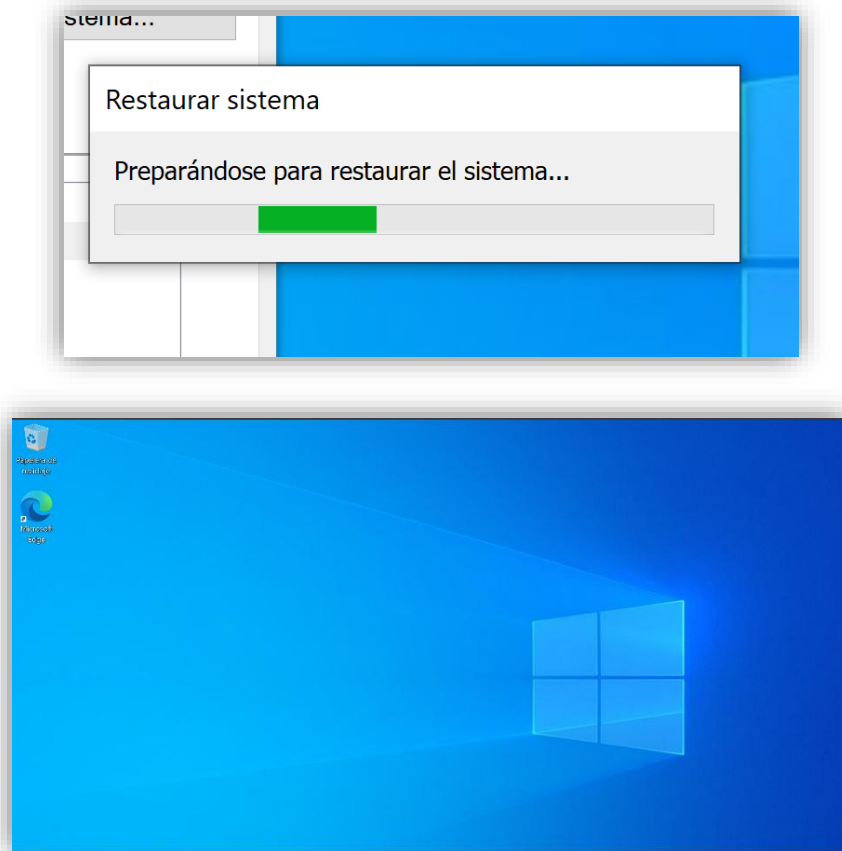


Figura 5. Confirmación de restauración exitosa del sistema.

Conclusión.

Este laboratorio permitió validar de forma práctica la efectividad de las herramientas de seguridad y recuperación integradas en Windows. Se comprobó que el sistema de auditoría es capaz de registrar eventos críticos de forma precisa, el análisis de vulnerabilidades es un paso esencial para el fortalecimiento del sistema, y la función de restauración es un mecanismo fiable para garantizar la integridad y estabilidad del entorno operativo.