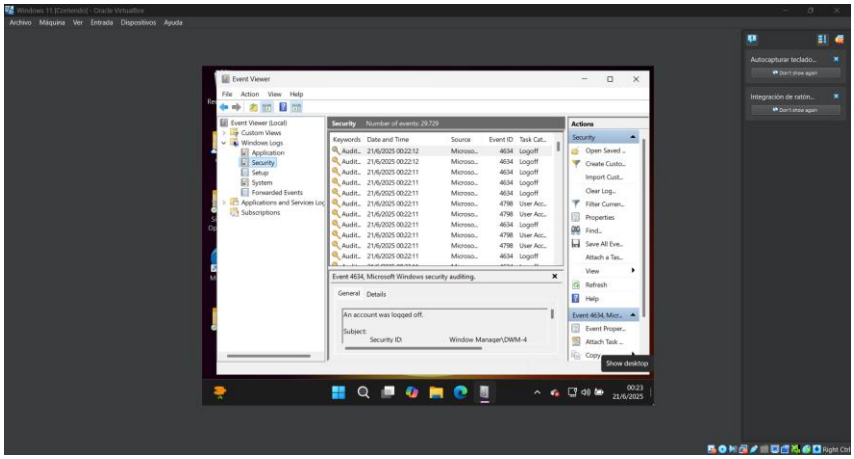
Informe de Auditoría de Seguridad - Laboratorio 4

Este informe presenta los resultados de la auditoría de seguridad realizada en un entorno Windows 11 ejecutado desde una máquina virtual. El objetivo fue activar los registros de seguridad, realizar acciones específicas que generen eventos relevantes, analizarlos y documentarlos.

Eventos de Seguridad Registrados

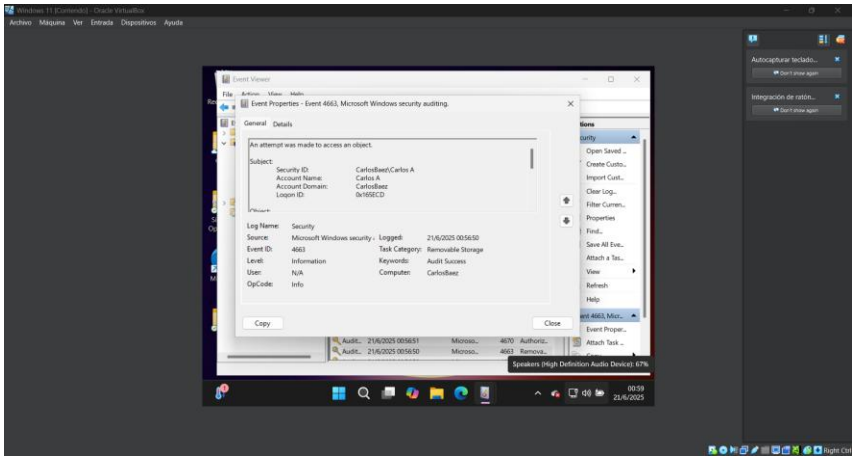
Evento 4634 – Logoff:

Este evento indica que una cuenta de usuario cerró sesión en el sistema. Se registraron múltiples eventos de este tipo durante la sesión de prueba.

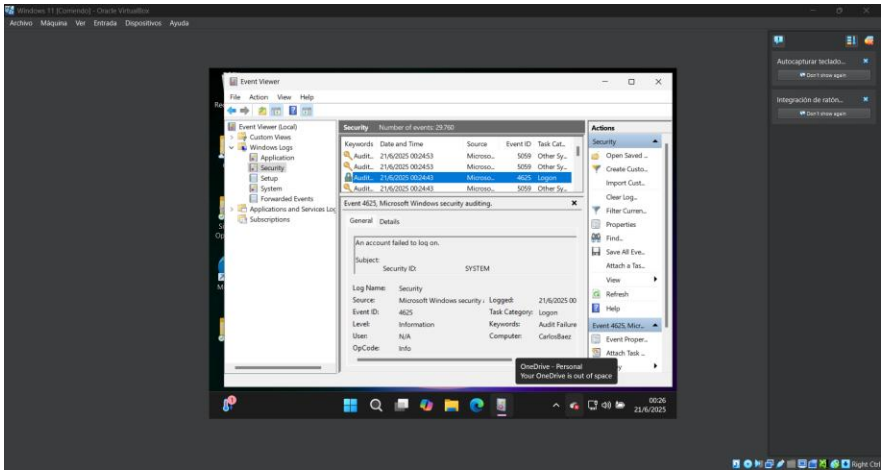


Evento 4663 - Acceso a Objeto:

Este evento se genera cuando un usuario intenta acceder a un archivo o carpeta y se ha configurado la auditoría correspondiente. Aquí se evidencia acceso exitoso a una carpeta protegida.

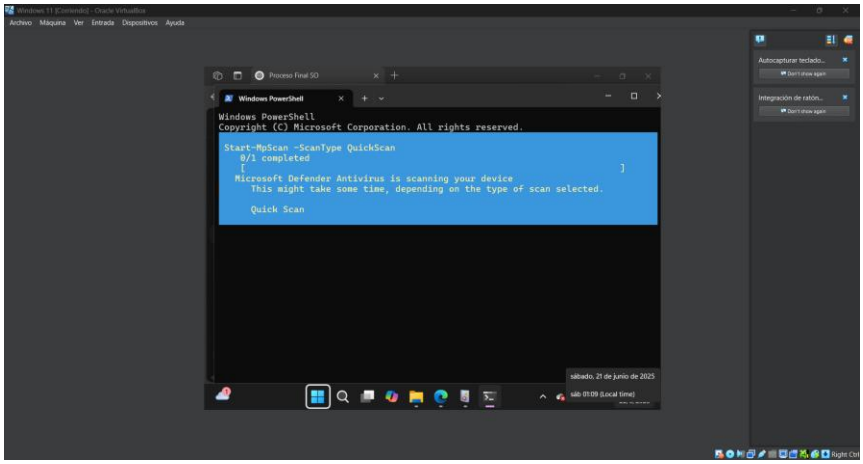


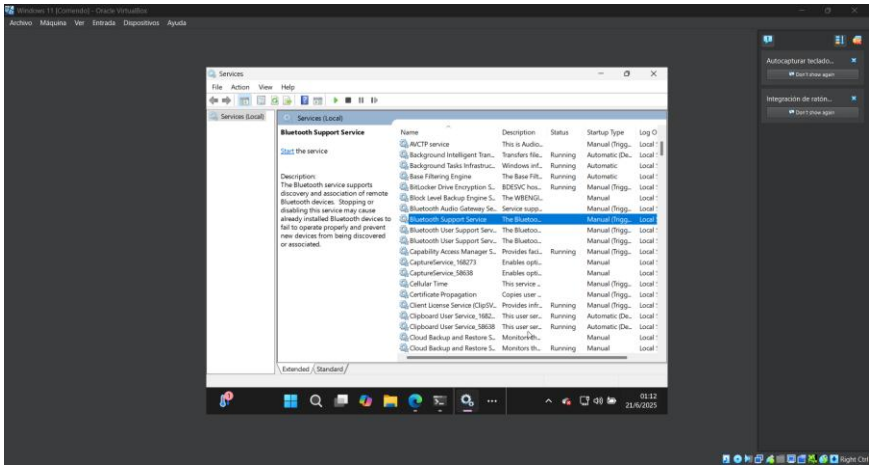
Evento 4625 - Inicio de sesión fallido:
Este evento refleja un intento fallido de inicio de sesión. Fue generado manualmente para verificar el funcionamiento del sistema de auditoría.



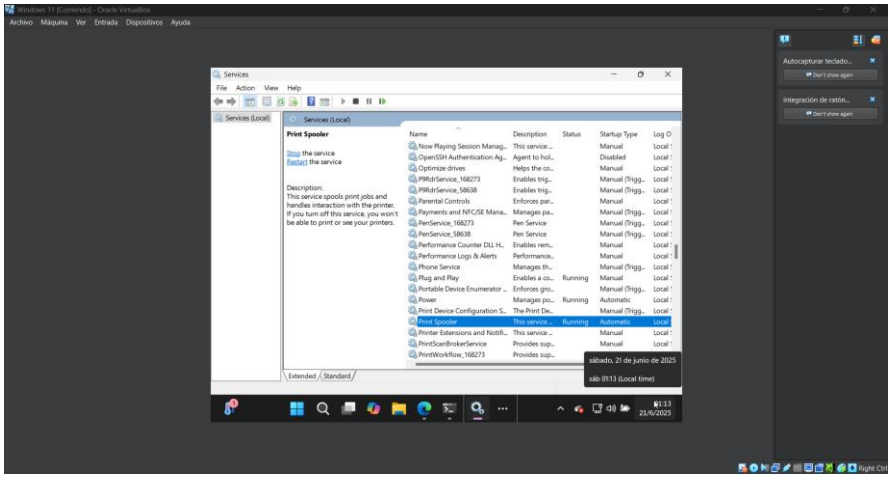
2. Análisis de Vulnerabilidades

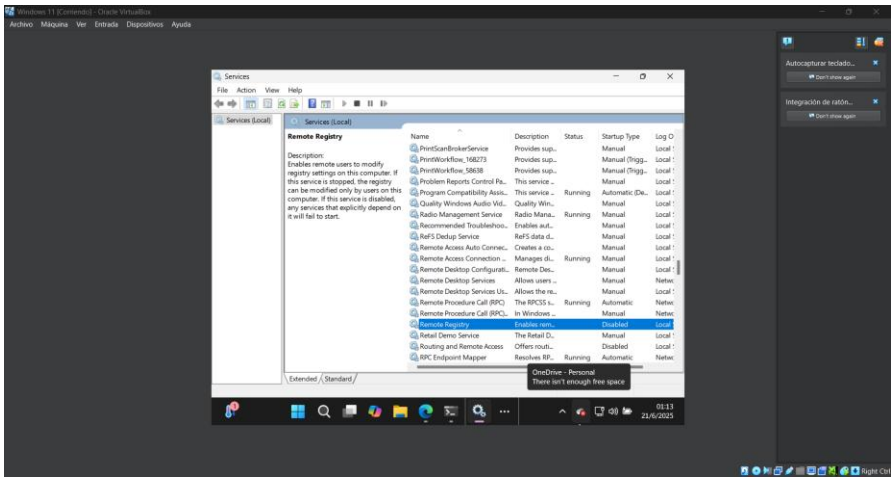
En esta sección se exploraron y modificaron configuraciones de servicios del sistema operativo que pueden representar posibles vulnerabilidades si no se administran correctamente. Por ejemplo, se observó y en algunos casos se desactivó el servicio 'Remote Registry', que permite modificar el registro de Windows de forma remota, lo cual es un riesgo si no se utiliza en un entorno seguro.

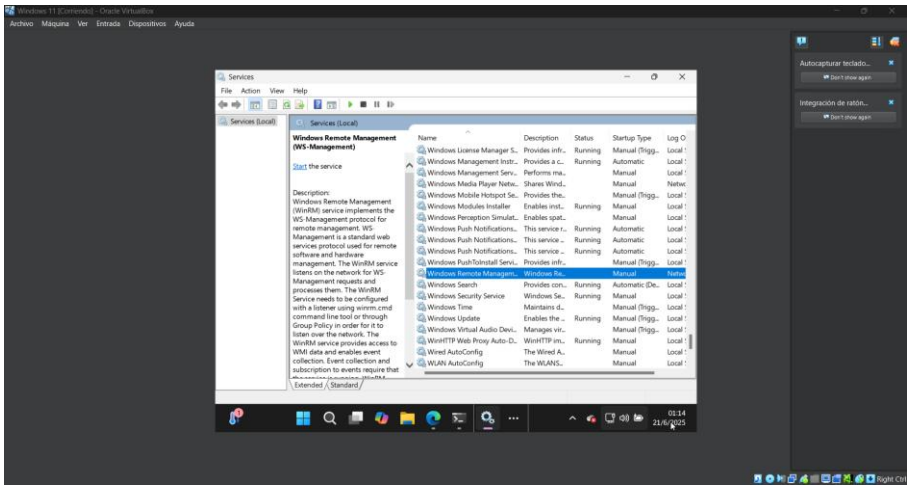




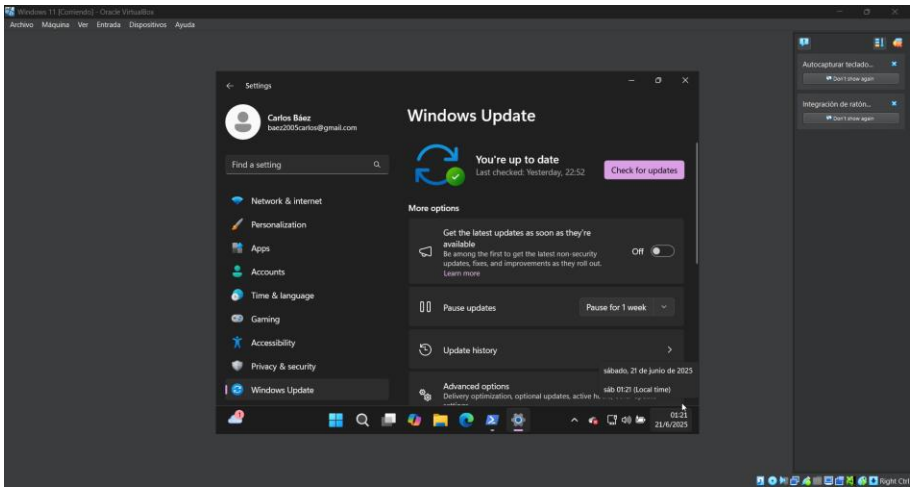
También se exploraron otros servicios como el 'Print Spooler', 'Bluetooth Support Service' y se usó PowerShell para ejecutar un análisis rápido con Microsoft Defender Antivirus para detectar posibles amenazas activas.





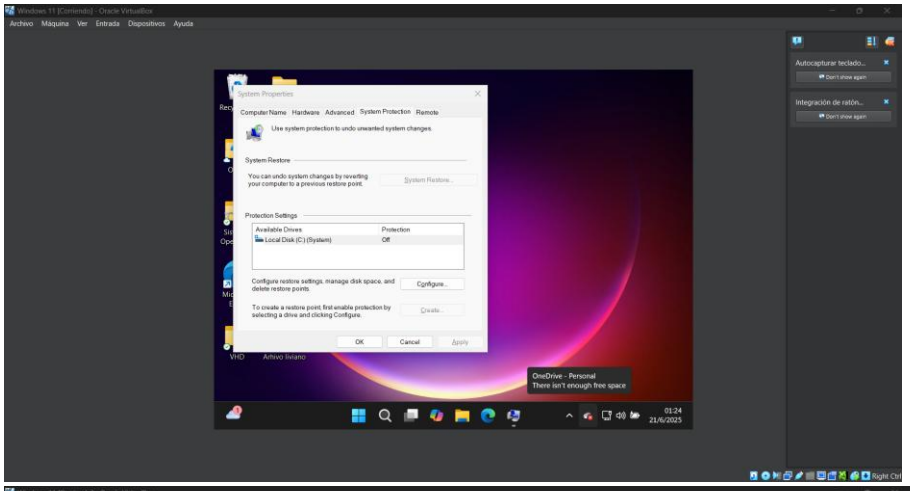


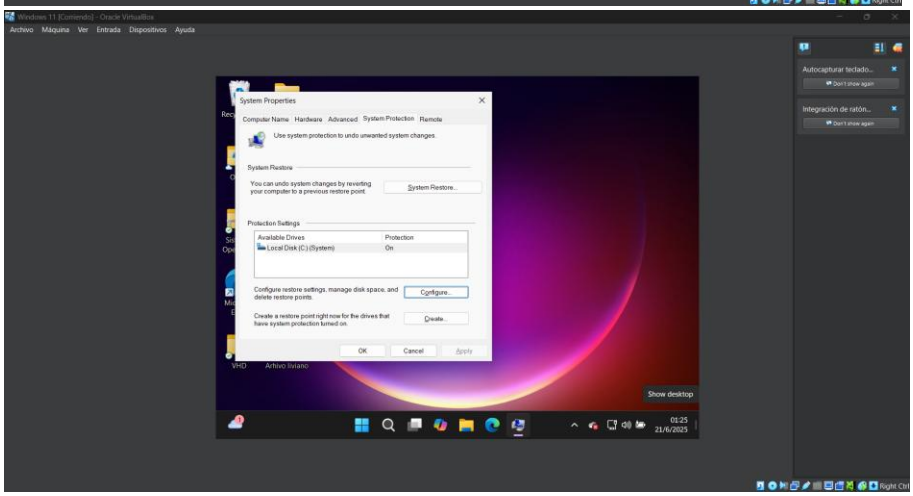
También se realizó la prueba de actualizaciones:

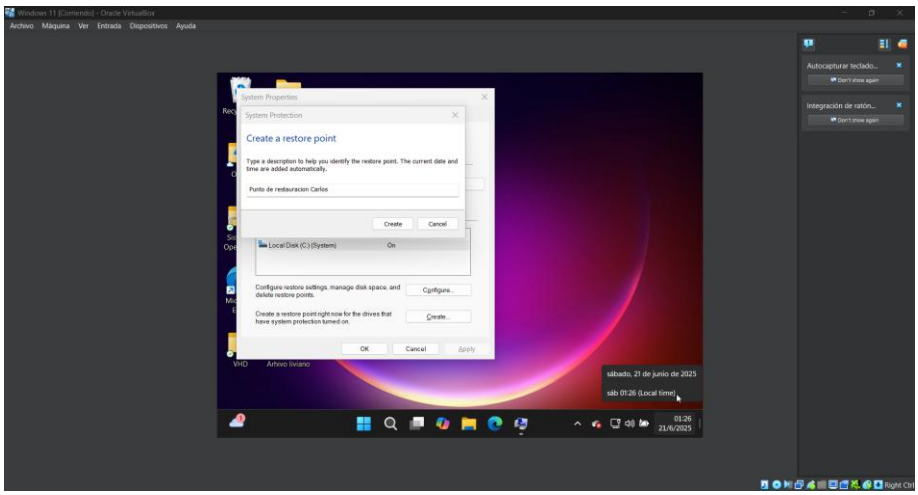


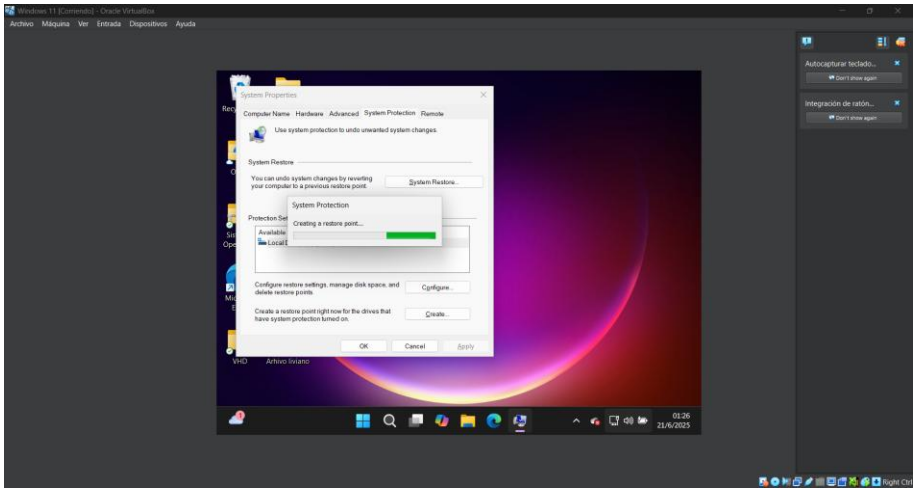
3. Respaldo y Recuperación

La actividad consistió en crear un punto de restauración del sistema antes de realizar cualquier modificación importante. Luego se hicieron cambios en los servicios del sistema como parte del análisis de vulnerabilidades, y finalmente se restauró el sistema al punto guardado para verificar que todo vuelva al estado anterior.

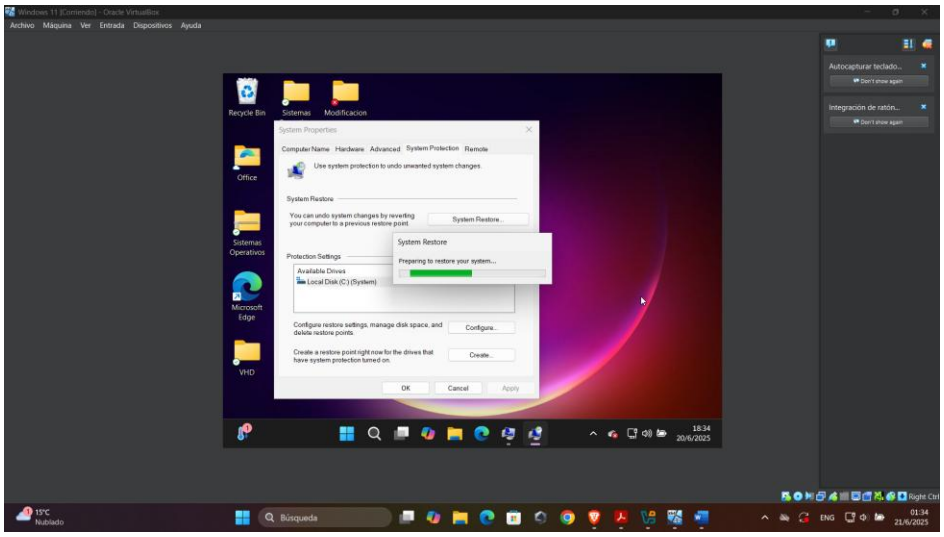

Windows 11 [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
System Properties
Computer Name Hardware Advanced System Protection Remote
Use system protection to undo unwanted system changes.
System Restore
You can undo system changes by reverting your computer to a previous restore point.
System Restore...
Protection Settings
Available Drives Protection
Local Disk (C:) (System) Off
Configure restore settings, manage disk space, and delete restore points.
Configure...
To create a restore point, first enable protection by selecting a drive and clicking Configure.
Create...
OK Cancel Apply
VHD Archivo liviano
Autocapturar teclado...
Don't show again
Integración de ratón...
Don't show again
OneDrive - Personal
There isn't enough free space
01:24
21/6/2025
Right Ctrl


Windows 11 [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
System Properties
Computer Name Hardware Advanced System Protection Remote
Use system protection to undo unwanted system changes.
System Restore
You can undo system changes by reverting your computer to a previous restore point.
System Restore...
Protection Settings
Available Drives Protection
Local Disk (C:) (System) On
Configure restore settings, manage disk space, and delete restore points.
Configure...
Create a restore point right now for the drives that have system protection turned on.
Create...
OK Cancel Apply
VHD Archivo liviano
Autocapturar teclado...
Don't show again
Integración de ratón...
Don't show again
Show desktop
01:25
21/6/2025
Right Ctrl


Windows 11 [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
System Properties
System Protection
Create a restore point
Type a description to help you identify the restore point. The current date and time are added automatically.
Punto de restauracion Carlos
Create Cancel
Local Disk (C:) (System) On
Configure restore settings, manage disk space, and delete restore points.
Configure...
Create a restore point right now for the drives that have system protection turned on.
Create...
OK Cancel Apply
VHD Archivo liviano
Autocapturar teclado...
Don't show again
Integración de ratón...
Don't show again
sábado, 21 de junio de 2025
sáb 01:26 (Local time)
01:26
21/6/2025
Right Ctrl



El proceso de restauración se ejecutó correctamente, iniciando a las 01:34 y finalizando a las 01:47 del 21/06/2025. Esto demostró que el sistema de recuperación es funcional y esencial para mantener la estabilidad del entorno ante fallos o cambios críticos.




Windows 11 [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Autocapturar teclado...
Don't show again
Integración de ratón...
Don't show again
Please wait while your Windows files and settings are being restored
System Restore is initializing...
Right Ctrl


Windows 11 [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Autocapturar teclado...
Don't show again
Integración de ratón...
Don't show again
Recycle Bin
Sistemas Operativos
Modificacion
Office
Google Chrome
Sistemas Operativos
USB CARLOS SO
Microsoft Edge
USB Carlos
VHD
Arhivo liviano
15°C
Nublado
01:47
21/6/2025
Búsqueda
ENG
Right Ctrl

CONCLUSIÓN:

El laboratorio permitió conocer y aplicar herramientas fundamentales de Windows para mantener la seguridad del sistema. La auditoría mostró cómo se pueden detectar accesos y movimientos sospechosos. El análisis de vulnerabilidades destacó la importancia de conocer qué servicios están activos y cómo podrían ser utilizados de forma indebida. Finalmente, el respaldo y la recuperación demostraron ser herramientas clave para prevenir la pérdida de funcionalidad ante fallas. Con estas prácticas, se afianza el conocimiento práctico en seguridad informática dentro del contexto de sistemas operativos.