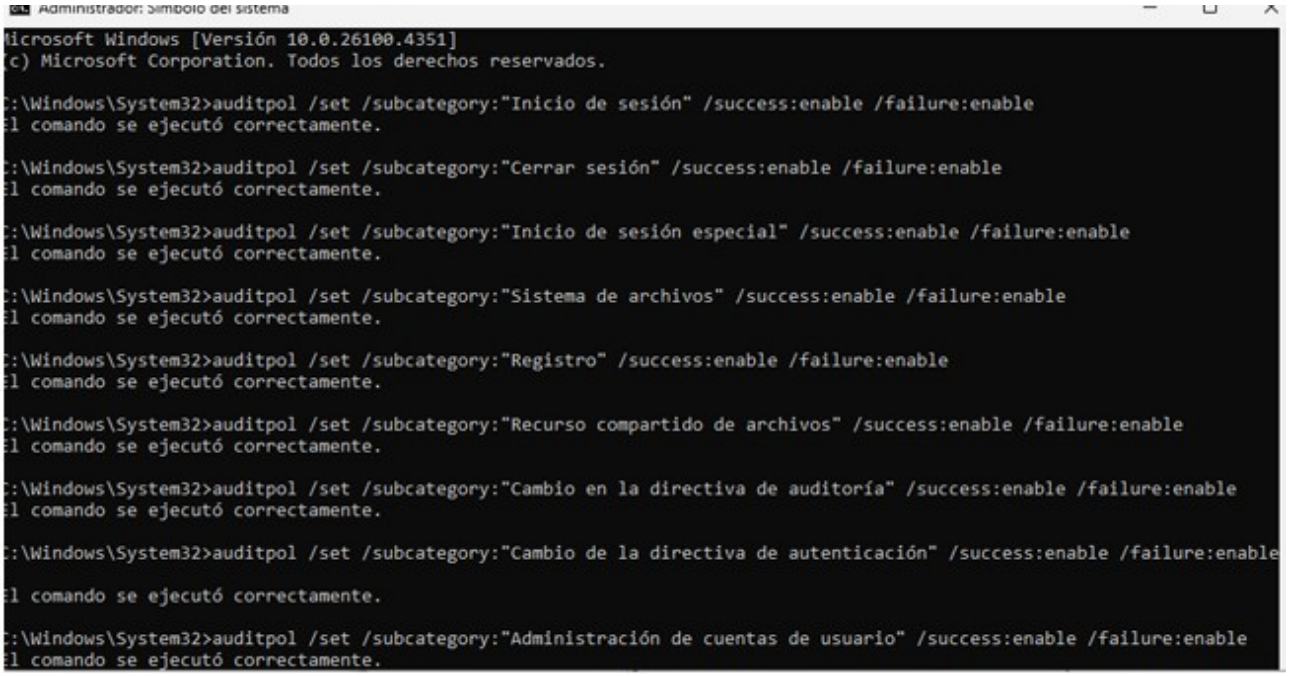
LABORATORIO 4:
SEGURIDAD DEL SISTEMA Auditoría de Seguridad
• Activar logs de seguridad del SO

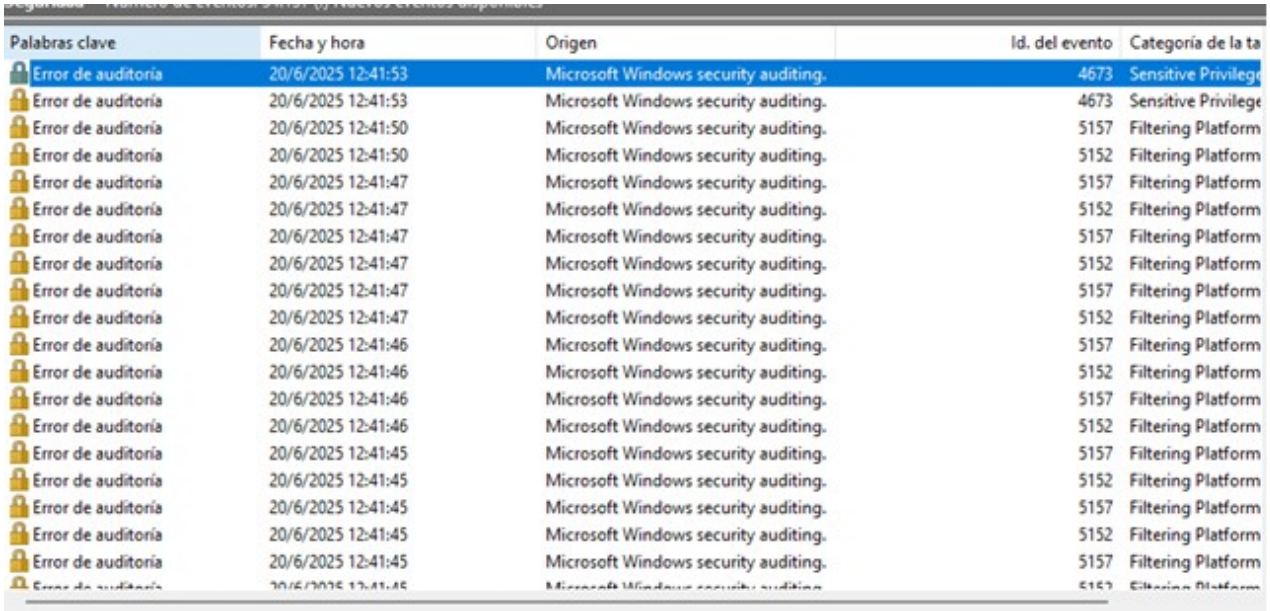


```
icrosoft Windows [Versión 10.0.26100.4351]
(c) Microsoft Corporation. Todos los derechos reservados.

:\Windows\System32>auditpol /set /subcategory:"Inicio de sesión" /success:enable /failure:enable
l comando se ejecutó correctamente.

:\Windows\System32>auditpol /set /subcategory:"Cerrar sesión" /success:enable /failure:enable
l comando se ejecutó correctamente.

:\Windows\System32>auditpol /set /subcategory:"Inicio de sesión especial" /success:enable /failure:enable
l comando se ejecutó correctamente.

:\Windows\System32>auditpol /set /subcategory:"Sistema de archivos" /success:enable /failure:enable
l comando se ejecutó correctamente.

:\Windows\System32>auditpol /set /subcategory:"Registro" /success:enable /failure:enable
l comando se ejecutó correctamente.

:\Windows\System32>auditpol /set /subcategory:"Recurso compartido de archivos" /success:enable /failure:enable
l comando se ejecutó correctamente.

:\Windows\System32>auditpol /set /subcategory:"Cambio en la directiva de auditoría" /success:enable /failure:enable
l comando se ejecutó correctamente.

:\Windows\System32>auditpol /set /subcategory:"Cambio de la directiva de autenticación" /success:enable /failure:enable

l comando se ejecutó correctamente.

:\Windows\System32>auditpol /set /subcategory:"Administración de cuentas de usuario" /success:enable /failure:enable
l comando se ejecutó correctamente.
```

Activa los logs de seguridad desde la MCD.

Al habilitar los registros (logs), el sistema empieza a guardar información sobre todo lo que hacen los usuarios y el propio sistema. Por ejemplo, cada vez que alguien intenta iniciar sesión, realiza un cambio en la configuración o accede a algún recurso, queda un registro con la fecha, la hora y los detalles del evento. Así, es posible saber qué ocurrió y cuándo pasó, lo que sirve para revisar la seguridad y detectar cualquier actividad sospechosa**.**

🕐 Encontrar y analizar los logs generados



Palabras clave	Fecha y hora	Origen	Id. del evento	Categoría de la ta
Error de auditoría	20/6/2025 12:41:53	Microsoft Windows security auditing.	4673	Sensitive Privileg
Error de auditoría	20/6/2025 12:41:53	Microsoft Windows security auditing.	4673	Sensitive Privilege
Error de auditoría	20/6/2025 12:41:50	Microsoft Windows security auditing.	5157	Filtering Platform
Error de auditoría	20/6/2025 12:41:50	Microsoft Windows security auditing.	5152	Filtering Platform
Error de auditoría	20/6/2025 12:41:47	Microsoft Windows security auditing.	5157	Filtering Platform
Error de auditoría	20/6/2025 12:41:47	Microsoft Windows security auditing.	5152	Filtering Platform
Error de auditoría	20/6/2025 12:41:47	Microsoft Windows security auditing.	5157	Filtering Platform
Error de auditoría	20/6/2025 12:41:47	Microsoft Windows security auditing.	5152	Filtering Platform
Error de auditoría	20/6/2025 12:41:47	Microsoft Windows security auditing.	5157	Filtering Platform
Error de auditoría	20/6/2025 12:41:47	Microsoft Windows security auditing.	5152	Filtering Platform
Error de auditoría	20/6/2025 12:41:46	Microsoft Windows security auditing.	5157	Filtering Platform
Error de auditoría	20/6/2025 12:41:46	Microsoft Windows security auditing.	5152	Filtering Platform
Error de auditoría	20/6/2025 12:41:46	Microsoft Windows security auditing.	5157	Filtering Platform
Error de auditoría	20/6/2025 12:41:46	Microsoft Windows security auditing.	5152	Filtering Platform
Error de auditoría	20/6/2025 12:41:45	Microsoft Windows security auditing.	5157	Filtering Platform
Error de auditoría	20/6/2025 12:41:45	Microsoft Windows security auditing.	5152	Filtering Platform
Error de auditoría	20/6/2025 12:41:45	Microsoft Windows security auditing.	5157	Filtering Platform
Error de auditoría	20/6/2025 12:41:45	Microsoft Windows security auditing.	5152	Filtering Platform
Error de auditoría	20/6/2025 12:41:45	Microsoft Windows security auditing.	5157	Filtering Platform

Durante la auditoría de seguridad en Windows, se utilizaron directivas activadas mediante el comando auditpol para registrar eventos críticos del sistema operativo. Estos eventos incluyen accesos con privilegios especiales, intentos de inicio de sesión fallidos y otras acciones importantes que pueden poner en riesgo la seguridad.

Crear reporte de eventos de seguridad

Este reporte resume y analiza los eventos de seguridad detectados en Windows, en particular los errores y advertencias que aparecen en el Visor de eventos. El objetivo es identificar los incidentes que podrían comprometer la seguridad del sistema y proponer recomendaciones para reducir los posibles riesgos.

A	B	C	D	E	F
Fecha y hora	ID del Evento	Categoría	Tipo de Evento	Usuario	Descripción breve
20/05/2025 12:09:09	5157	Filtering Platform Connection	Error de auditoría	No disponible	Evento relacionado con la conexión en la plataforma de filtrado.
20/05/2025 12:09:08	5152	Filtering Platform Packet Drop	Error de auditoría	No disponible	Evento de paquete descartado en la plataforma de filtrado.
20/05/2025 12:41:53	4673	Sensitive Privilege Use	Error de auditoría	No disponible	Uso de privilegios sensibles detectado en el sistema.
20/05/2025 12:41:53	4673	Sensitive Privilege Use	Error de auditoría	No disponible	Uso de privilegios sensibles detectado en el sistema.

Eventos 5157 y 5152 (Filtering Platform):

Estos eventos aparecen cuando hay problemas con la conexión o cuando Windows bloquea o filtra paquetes en la red. Esto suele pasar por reglas del firewall o por configuraciones que bloquean el tráfico.

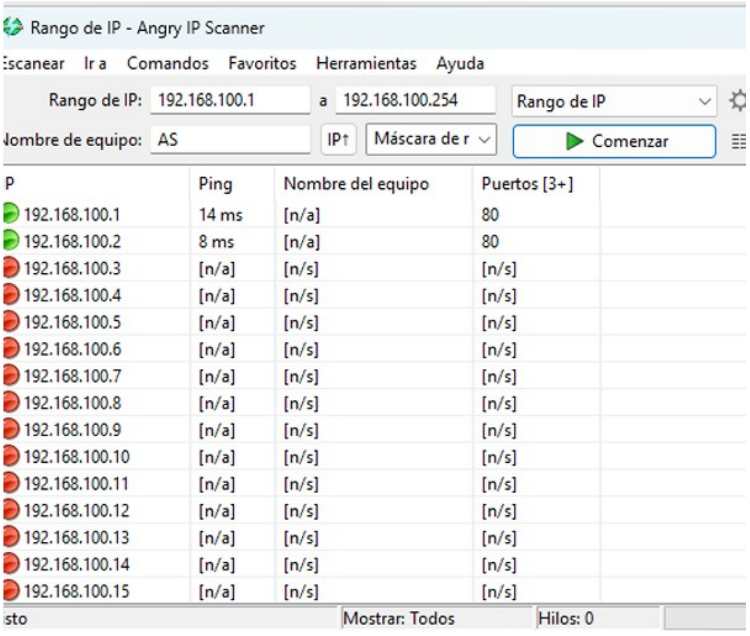
Es importante revisarlos para confirmar que no se esté bloqueando nada que sea válido y que la configuración sea segura para que nadie la aproveche mal.

- **Evento 4673 (Sensitive Privilege Use):**

Este evento se genera cuando un usuario o programa usa privilegios especiales en el sistema. Si sucede muy seguido, puede que sean tareas normales o que alguien esté abusando de permisos que no debería tener. Por eso es clave revisar qué usuarios o procesos están usando estos privilegios y asegurarse de que sea correcto.

Análisis de Vulnerabilidades

• Usar herramienta de escaneo básico



Para el análisis de vulnerabilidades se utilizó la herramienta Angry IP Scanner, una aplicación gratuita y fácil de usar que permite detectar qué dispositivos están activos en la red y qué puertos tienen abiertos.

Documentar servicios activos innecesarios:
Se realizó un escaneo en el rango de IPs de la red local (192.168.100.1 a 192.168.100.254) para identificar dispositivos encendidos y qué servicios tienen activos.

Resultados del escaneo:

- **Hubo respuesta al ping solo en las siguientes direcciones IP:**
  - **192.168.100.1 → probable puerta de enlace o router.**
  - **192.168.100.2 → otro dispositivo activo en la red.**
- **Desde la dirección 192.168.100.3 en adelante no hubo respuesta, lo que indica que no hay más dispositivos activos, que están apagados o que tienen bloqueado el ping.**

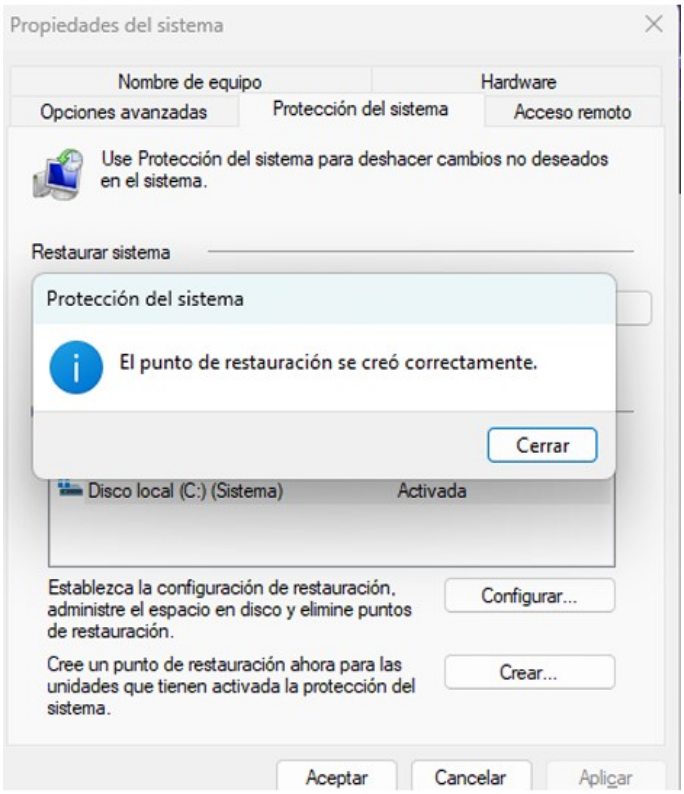
Verificar actualizaciones pendientes:
Es recomendable revisar si tanto el sistema operativo como las aplicaciones y servicios de los dispositivos activos tienen actualizaciones pendientes para evitar posibles vulnerabilidades.

Se ingresó a la configuración de Windows Update para comprobar si existían actualizaciones pendientes en el sistema.
🕐 Al realizar la verificación manual, se puede observar el mensaje de que el sistema está completamente actualizado.
🕐 No se encontraron actualizaciones pendientes al momento del análisis.

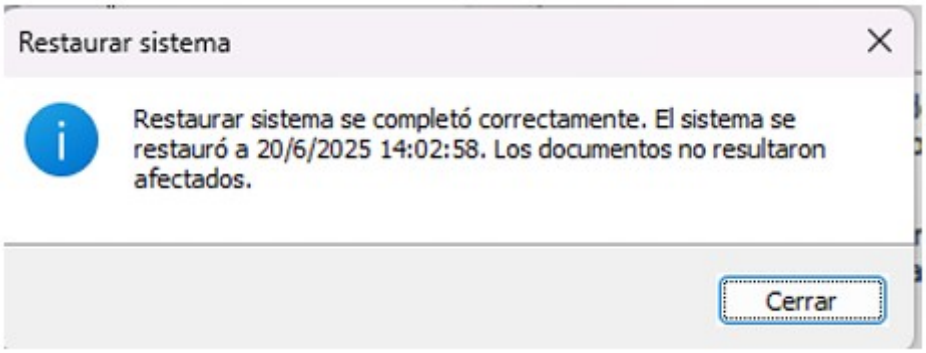
• Crear lista de verificaciones de seguridad

Verificación	Realizado (Sí/No)	Comentarios / Recomendaciones
Sistema operativo actualizado	Sí	Windows Update indicó que el sistema está completamente actualizado.
Escaneo de red realizado	Sí	Se utilizó Angry IP Scanner. Se detectaron 2 dispositivos activos.
Servicios innecesarios identificados	Parcial	Requiere análisis más profundo de puertos y servicios abiertos.
Firewall activado	Sí	Confirmado desde Seguridad de Windows.
Antivirus activo y actualizado	Sí	Microsoft Defender activo y sin amenazas detectadas.
Cuentas de usuario sin contraseñas débiles	Parcial	Se encontró una cuenta de prueba 'arel'; se recomienda revisar su uso y seguridad.
Puertos innecesarios cerrados	Parcial	Falta análisis detallado con Nmap u otra herramienta.
Realización de copias de seguridad	No verificado	Se recomienda configurar backups periódicos del sistema.

Lista de verificaciones de Seguridad Respaldo y Recuperación
• Crear punto de restauración



Se puede observar el mensaje que confirma la correcta creación del punto de restauración en el disco local C:, el cual fue nombrado previamente antes de realizar los cambios • Hacer cambios al sistema



Documentar proceso y tiempo:
Se comprobó que el sistema fue restaurado correctamente a la fecha y hora seleccionadas. No se detectaron daños en los archivos personales ni problemas con la integridad del sistema.