LABORATORIO 4 – SEGURIDAD DEL SISTEMA

Axel Amarilla
Ingeniería en Sistemas
Sistemas Operativos
2025

Objetivo del laboratorio

Aprender a aplicar medidas básicas de seguridad en el sistema operativo, como auditoría, análisis de vulnerabilidades y recuperación ante cambios.

Auditoría de Seguridad

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

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

C:\Windows\System32>
```

Se activaron los logs de auditoría del sistema para registrar intentos de inicio de sesión exitosos y fallidos.

Se simuló un intento fallido de inicio de sesión.

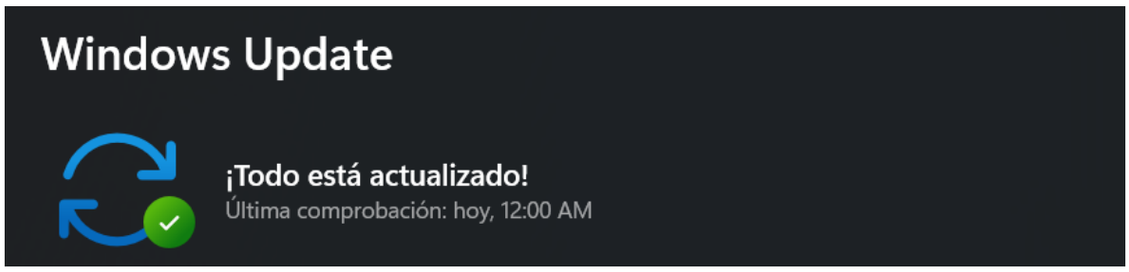
Se accedió al Visor de eventos para verificar los logs generados.

Análisis de Vulnerabilidades

Se analizó el sistema para encontrar vulnerabilidades dentro del mismo, como se presentan en la captura de arriba.

Cliente DNS	El servicio Cli...	En ejecu...	Automático (d...	Servicio de red
Cola de impresión	Este servicio ...	En ejecu...	Automático	Sistema local
Compilador de extremo de a...	Administra l...	En ejecu...	Automático	Sistema local
Configuración automática d...	El servicio W...	En ejecu...	Automático	Sistema local
Contenedor de Microsoft Pa...	Administra cl...	En ejecu...	Manual (desen...	Servicio local
CoreMessaging	Manages co...	En ejecu...	Automático	Servicio local
Datos de contactos_18b475	Indiza los da...	En ejecu...	Manual	Sistema local
Detección de hardware shell	Proporciona ...	En ejecu...	Automático	Sistema local
Detección SSDP	Detecta disp...	En ejecu...	Manual	Servicio local
DevicesFlow_18b475	Permite que ...	En ejecu...	Manual	Sistema local
DtsApo4Service		En ejecu...	Automático	Sistema local
Energía	Administra l...	En ejecu...	Automático	Sistema local
Epson Scanner Service		En ejecu...	Automático	Sistema local
Estación de trabajo	Crea y manti...	En ejecu...	Automático	Servicio de red

Se encontraron servicios activos no utilizados, como servicios de impresoras en ejecución.

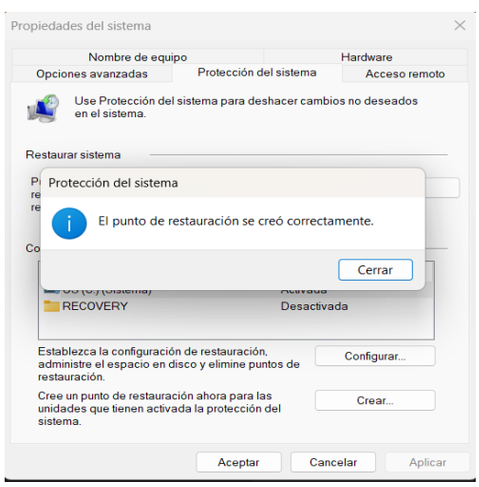


Se verificaron actualizaciones pendientes mediante Windows Update y se encontró que todo está en orden.

Verificación	Estado
Servicios innecesarios deshabilitados	Si
Actualizaciones del sistema al día	Si
Antivirus activo	Si
Firewall de Windows habilitado	Si
Cuentas sin contraseña deshabilitadas	Si
Inicio de sesión remoto deshabilitado	Si

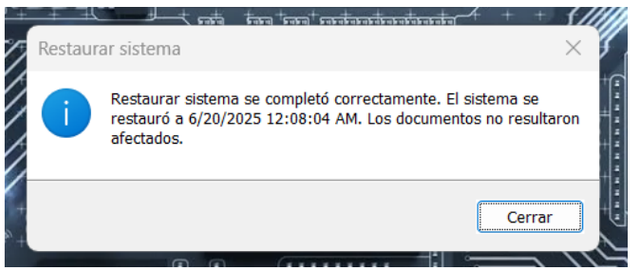
Se hizo una lista en Excel con los puntos que se revisaron para mejorar la seguridad del sistema. Sirvió como guía durante el trabajo.

Respaldo y Recuperación



Se creó un punto de restauración del sistema dentro del disco local C, llamado Respaldo_Lab4.

Se realizaron cambios en la resolución de la pantalla para probar la restauración.



Se restauró el sistema al punto guardado y se verificó que la el sistema y su resolución de pantalla volviera a su estado anterior.

Conclusión

Este laboratorio mostró que proteger el sistema no depende solo de programas externos, sino también de saber usar las herramientas que Windows ya ofrece. Con simples acciones, como auditar eventos o crear puntos de restauración, se puede prevenir y responder ante fallos o riesgos sin complicaciones.