Laboratorio 4: Seguridad del Sistema

Auditoría de Seguridad

Activación de los logs de seguridad

Para iniciar el proceso de auditoría, se accedió al **Visor de eventos** de Windows. Desde allí se habilitaron los registros de seguridad para que se puedan monitorear eventos relevantes, como accesos, intentos fallidos de inicio de sesión y manipulaciones de archivos o carpetas protegidas.

Ejecución de acciones específicas

- **Login fallido**: Se intentó ingresar con una contraseña incorrecta en una cuenta de usuario, provocando el evento con ID **4625**.
- **Acceso denegado**: Se modificaron los permisos de una carpeta para restringir el acceso a determinados usuarios. Luego se intentó ingresar desde otra cuenta sin privilegios, lo que generó el evento con ID **4663** (acceso a objeto denegado).

Análisis de los eventos registrados

Los eventos fueron revisados detalladamente, analizando los siguientes elementos:

- **Hora exacta del suceso**
- **Nombre de la cuenta afectada**
- **Tipo de acceso (fallido, denegado o correcto)**
- **Proceso o archivo implicado**

Esto permitió comprender la trazabilidad de acciones sospechosas o fallidas en el sistema.

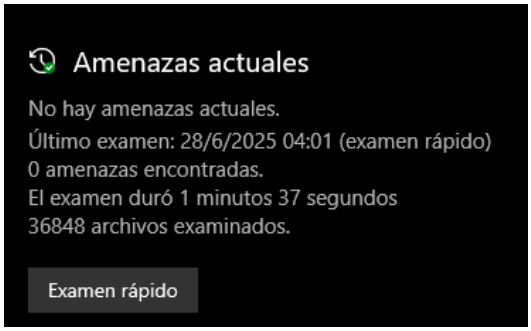
Reporte generado

Se generó un resumen con los eventos ID **4625 y 4663**, incluyendo hora, usuario, y resultado del intento. Este informe puede ser utilizado para auditorías futuras o para revisar comportamientos anómalos.

Análisis de Vulnerabilidades

Escaneo básico

Se utilizó **Windows Defender** como herramienta de análisis de seguridad. Se realizó un escaneo completo, que no arrojó amenazas críticas.



Servicios activos innecesarios

Se identificaron los siguientes servicios como innecesarios en el entorno actual y se procedió a deshabilitarlos:

- Servicio Telefónico
- Telefonía
- WalletService
- Servicio de Directivas de Diagnóstico
- Servicio de Impresora

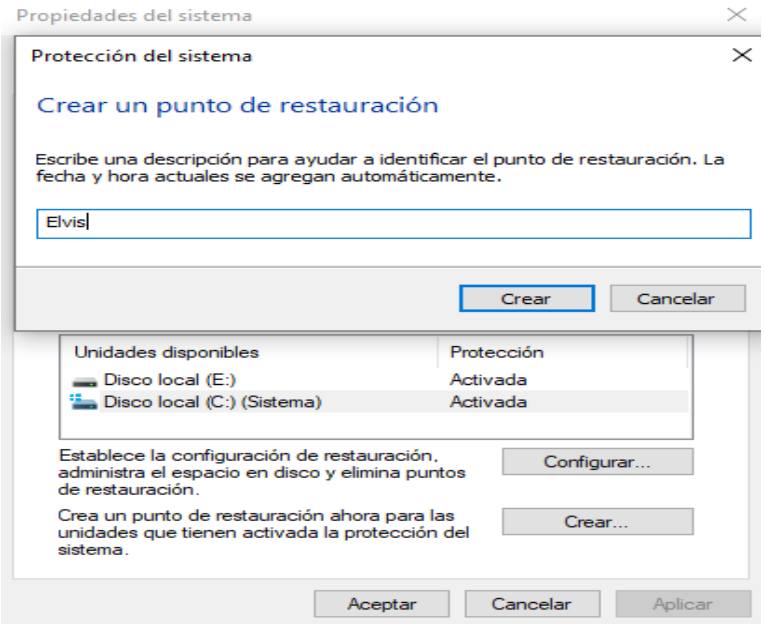
Verificación de actualizaciones

Se accedió a Windows Update, donde se comprobó que el sistema estaba completamente actualizado. Solo se detectó una actualización opcional de calidad, que fue omitida intencionalmente por no ser crítica.

Respaldo y Recuperación

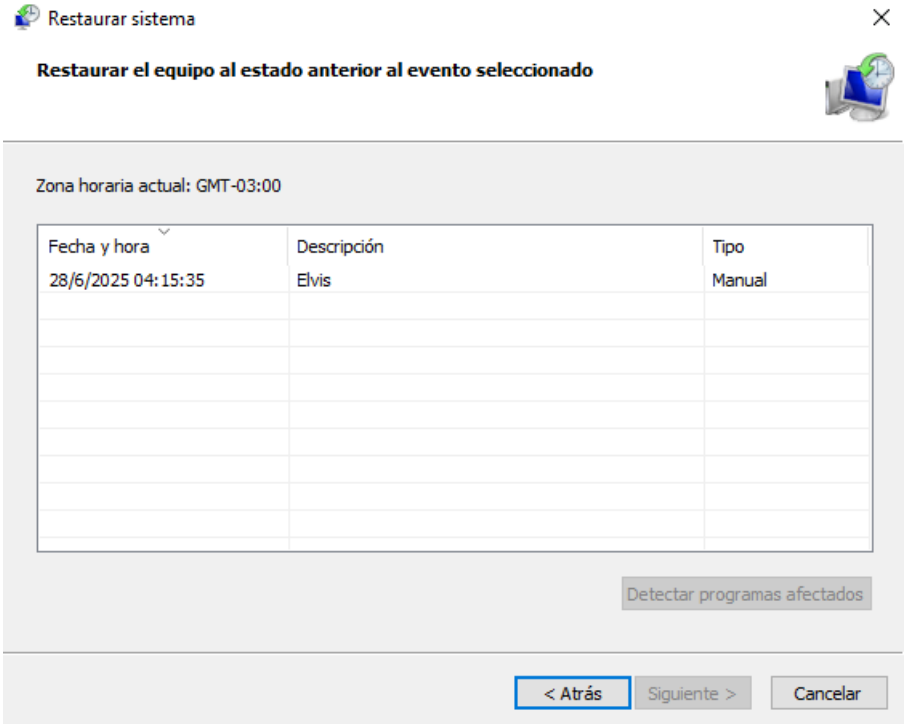
Creación del punto de restauración

Desde la configuración del sistema, se creó un punto de restauración manualmente con fecha y hora específicas.



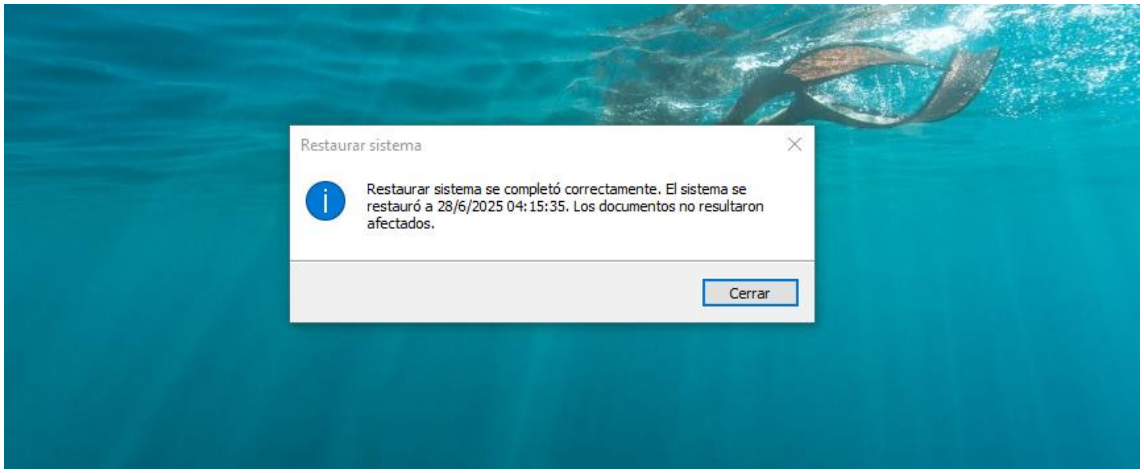
Cambios y restauración

Se hicieron cambios menores al sistema (instalación de software y modificación de configuraciones visuales). Luego se utilizó el punto de restauración previamente creado.



Resultado de la restauración

El proceso de restauración finalizó correctamente. El sistema volvió a su estado anterior sin perder datos personales. La restauración tomó aproximadamente **7 minutos** desde que se inició el proceso hasta el reinicio del equipo.



Conclusión

Este laboratorio permitió explorar aspectos clave de la seguridad en sistemas operativos Windows. Se observaron eventos importantes mediante la auditoría del sistema, se identificaron posibles vulnerabilidades, y se practicó un método seguro de respaldo y recuperación. Estas tareas son fundamentales para mantener un sistema estable, protegido ante amenazas y preparado para recuperarse ante fallos inesperados.