Laboratorio 4: Seguridad del Sistema

Auditoría de Seguridad

En este punto entenderemos cómo un sistema operativo registra eventos importantes de seguridad.

1. Activar Logs de Seguridad del SO

Para poder auditar, primero nos aseguramos de que el sistema esté registrando los eventos relevantes.

- Para el efecto realizamos la configuración en el "Visor de eventos" en el Registro de Windows" y en "Seguridad".
- Al detectar que no se registraban muchos eventos, ajustamos la "Directiva de Auditoría" luego en "Directiva de seguridad local" en el menú de inicio, y navegando a "Directivas locales" > "Directiva de auditoría" y finalmente se habilitó la auditoría de "Eventos de inicio de sesión", "Acceso a objetos" y "Seguimiento de procesos" para tener un registro completo.

2. Realización de Acciones Específicas

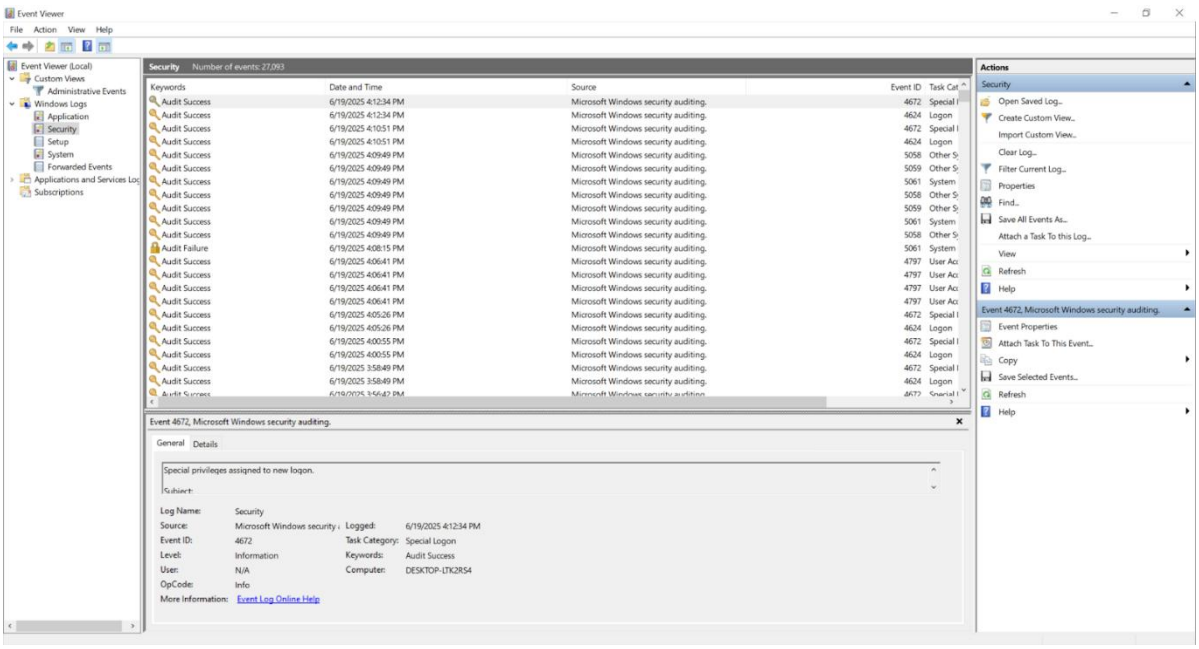
Una vez que activados los logs, provocamos algunos eventos para que queden registrados.

- **Login Fallido:** Al intentar iniciar sesión varias veces con una contraseña incorrecta para el usuario existente o inexistente.
- **Acceso Denegado:** Al Intentar acceder a una carpeta o archivo al que no tenemos permisos (como se hizo en el Laboratorio 3, intentar abrir un archivo en la carpeta "Finanzas" desde un usuario de prueba creado que no sea parte del grupo "Finanzas").
- **Creación/Modificación/Eliminación:** Al realizar algunas de estas acciones en archivos y carpetas para ver cómo se registran.

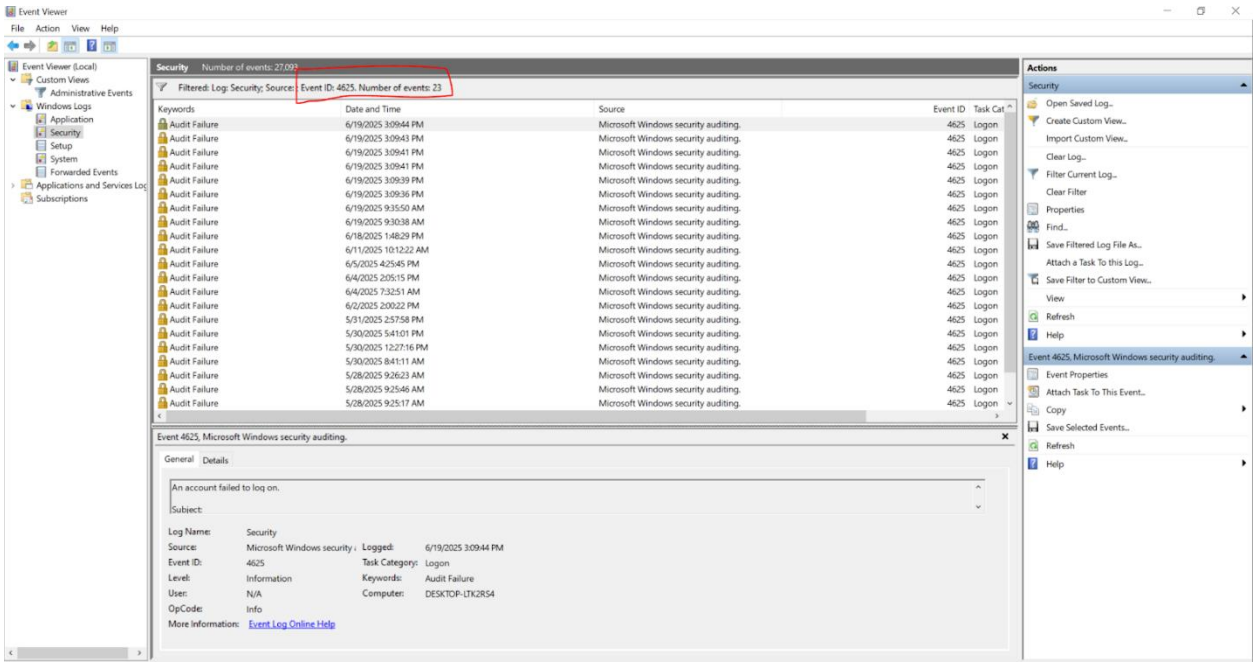
3. Analisis de los Logs Generados

Al revisar los registros para encontrar los eventos que acabamos de generar.

- Abriendo el **"Visor de eventos"** > **"Registros de Windows"** > "Seguridad".

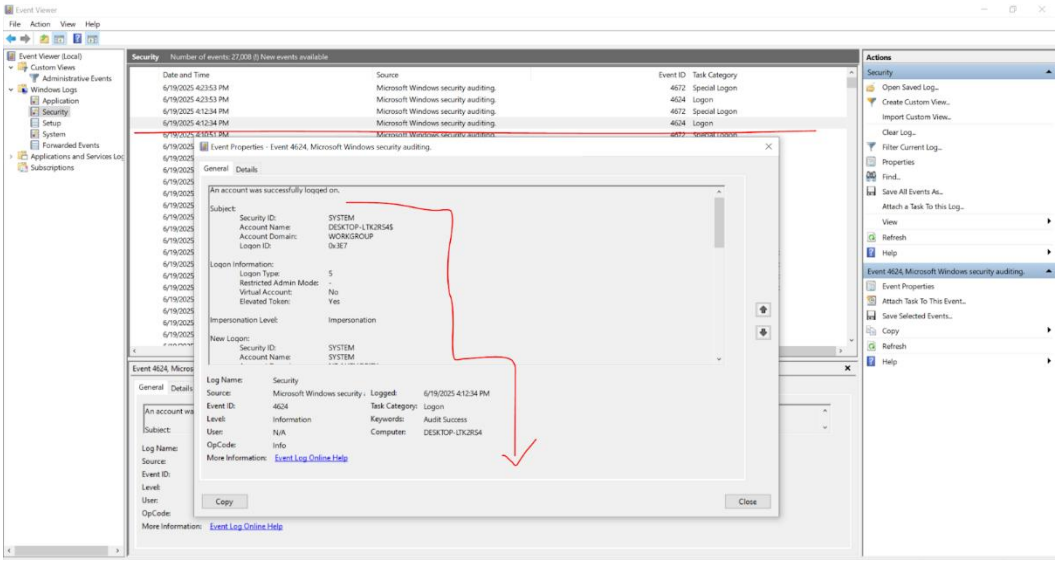


- Se filtro los eventos por "Id. de evento" para encontrar los específicos:
  - **4625:** Error de inicio de sesión.

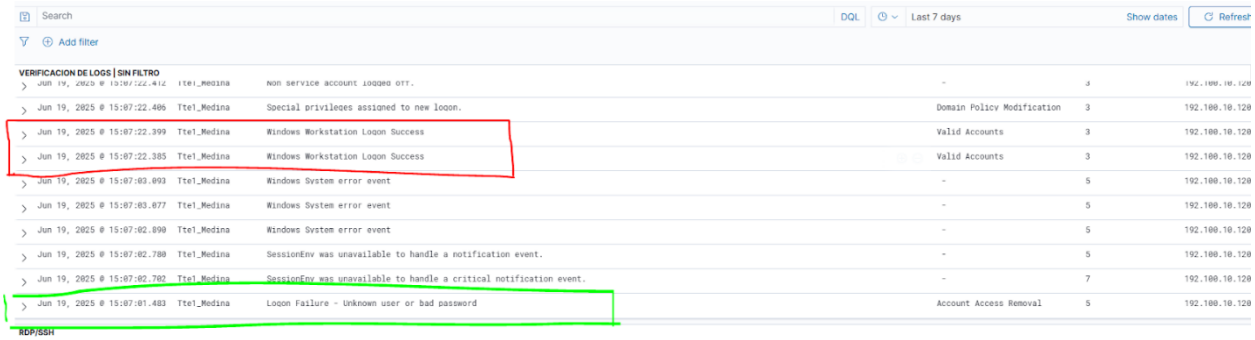


  - **4663:** Intento de acceso a un objeto.
  - **4656/4658:** Manejo de un objeto (apertura, cierre).

- Acceso correcto



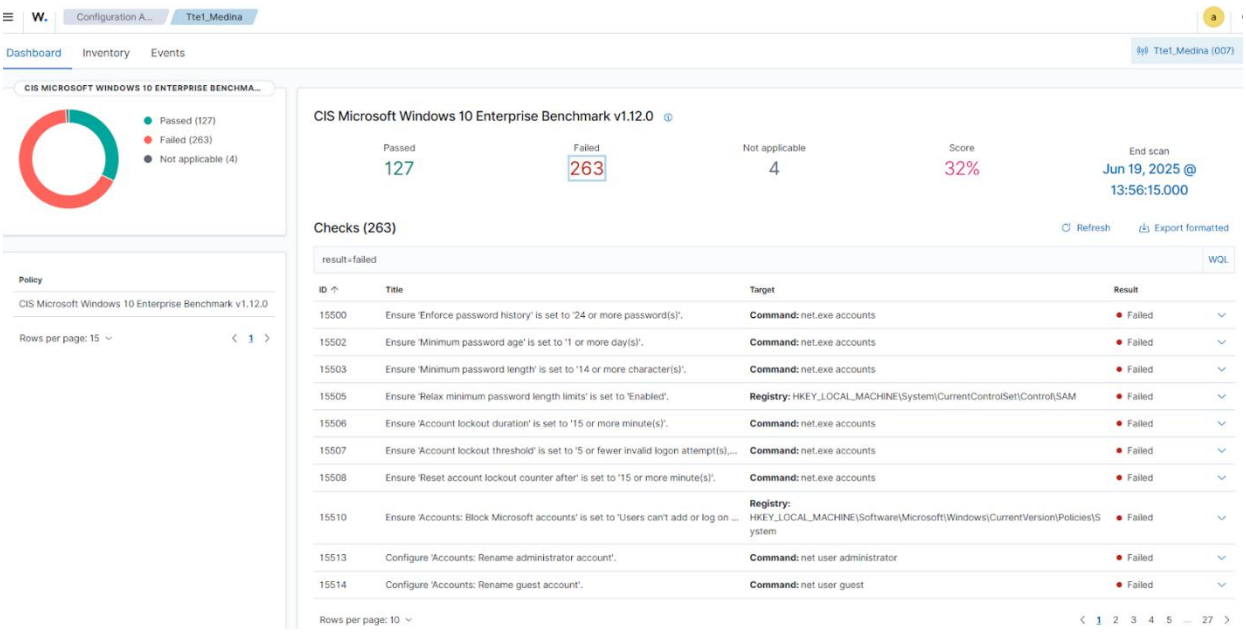
- Captura de evento con la herramienta de monitoreo de eventos wazhu.



Análisis de Vulnerabilidades

Esta sección se enfoca en identificar debilidades básicas en la configuración del SO.

1. Uso de herramienta Wazhu para escaneo básico: Es un sistema de monitoreo y detección de amenazas.



Detección de una vulnerabilidad conocida como **(CVE-2025-21298)**

Es una vulnerabilidad crítica presente en Windows OLE que permite la ejecución remota de código, con una puntuación de gravedad CVSS de 9.8. Object Linking and Embedding (OLE) es una tecnología propietaria desarrollada por Microsoft que permite incrustar y vincular documentos y objetos. Esta vulnerabilidad puede ser explotada por atacantes mediante correos electrónicos especialmente diseñados enviados a los usuarios de Microsoft Outlook.

La vulnerabilidad puede activarse al enviar un payload inicial, como un documento RTF que contiene código malicioso incrustado. Simplemente abrir o previsualizar el documento malicioso puede desencadenar la ejecución arbitraria de código en el sistema de la víctima, lo que resulta en la descarga de un payload que potencialmente otorga al atacante un control no autorizado.

Esta vulnerabilidad representa una amenaza significativa para las organizaciones, ya que los atacantes suelen explotarla creando correos electrónicos de phishing que inducen a las víctimas a hacer clic en los archivos adjuntos. Una vez que se abre el documento malicioso, se ejecuta un comando PowerShell en segundo plano que descarga un payload en el sistema de la víctima, proporcionando finalmente el control al atacante.

Recomendaciones:

Microsoft ha lanzado una actualización de seguridad para abordar esta vulnerabilidad. Se recomienda encarecidamente a las organizaciones y usuarios instalarla lo antes posible para protegerse contra posibles ataques.

Para aquellos que no puedan instalar la actualización de inmediato, Microsoft ha proporcionado una solución temporal para abrir los archivos adjuntos en texto plano, minimizando así el riesgo.

Soluciones alternativas

Utilizar **Microsoft Outlook** para reducir el riesgo de que los usuarios abran archivos RTF de fuentes desconocidas o no confiables.

Leer los mensajes de correo electrónico en formato de texto plano. Para obtener instrucciones sobre cómo configurar Microsoft Outlook para leer todos los correos estándar en formato de texto plano, consulte la guía oficial: **Leer mensajes de correo electrónico en texto plano**.

Impacto de las soluciones alternativas

Los mensajes de correo electrónico visualizados en formato de texto plano no contendrán imágenes, fuentes especializadas, animaciones ni otros contenidos avanzados. Como el mensaje todavía está guardado en formato RTF o HTML, el modelo de objetos (soluciones con código personalizado) podría comportarse de manera inesperada.

Referencias

CVE-2025-21298 - Guía de actualización de seguridad - Microsoft - Vulnerabilidad de ejecución remota de código en Windows OLE

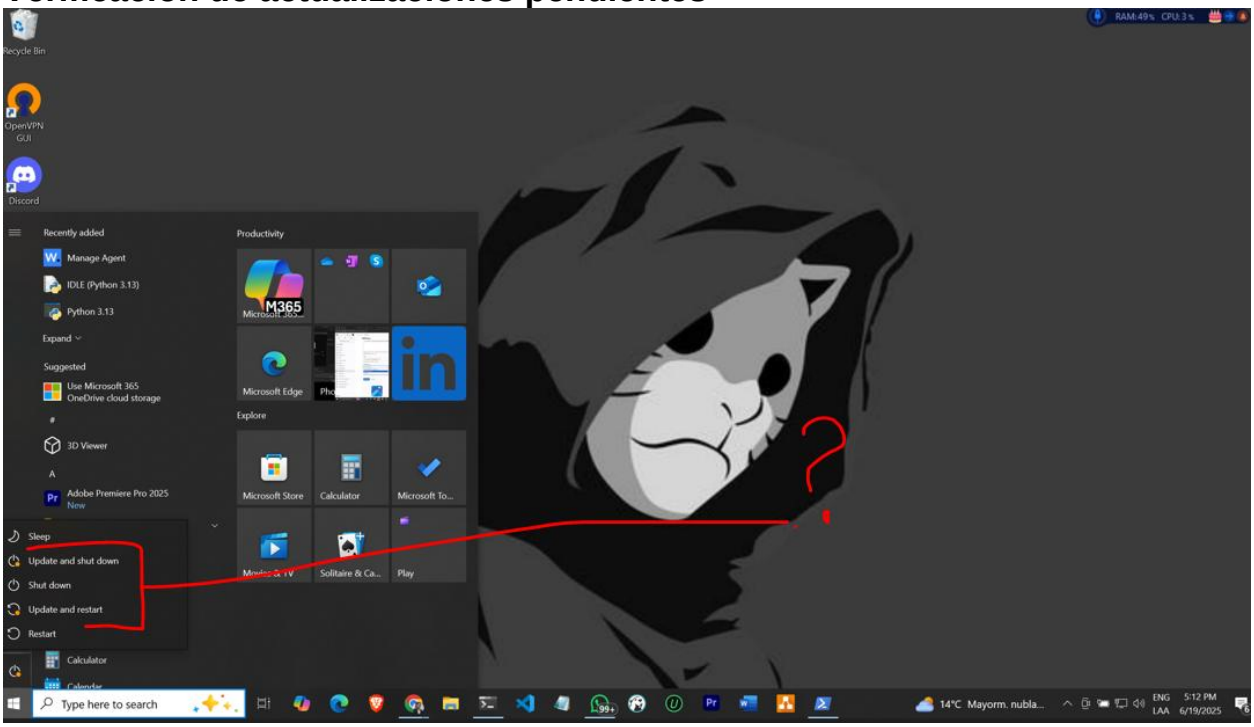
Si te preocupa alguna de las amenazas descritas en este boletín o necesitas ayuda para determinar qué pasos tomar para proteger tu organización de las amenazas más relevantes, contacta a tu gestor de cuentas o **ponte en contacto con nosotros** para descubrir cómo podemos ayudarte.

Documentar servicios activos innecesarios, que inician con el SO, consumen recursos innecesarios:

lame	Publisher	Status	Startup impact
Advanced SystemCare Tray	IObit	Enabled	Low
CCXProcess	Adobe Inc.	Disabled	High
Copilot	Microsoft Corporation	Disabled	None
Herd	Beyond Code	Disabled	High
Microsoft 365 Copilot	Microsoft Corporation	Disabled	Not measured
Microsoft Edge	Microsoft Corporation	Disabled	Not measured
Microsoft OneDrive	Microsoft Corporation	Disabled	High
OpenVPN GUI for Windows	OpenVPN GUI	Enabled	Medium
Phone Link	Microsoft Corporation	Disabled	None
Radeon Software Startup Task	Advanced Micro Devices...	Disabled	Not measured
Realtek HD Audio Universal ...	Realtek Semiconductor	Enabled	Low
Terminal	Microsoft Corporation	Disabled	None
Update	Discord Inc.	Disabled	High
WhatsApp	WhatsApp Inc.	Disabled	None
Windows Security notificatio...	Microsoft Corporation	Enabled	Medium

Importante

Verificación de actualizaciones pendientes



Se detectó que en el equipo faltaba aplicar las actualizaciones.

Crear lista de verificaciones de seguridad

Categoría	ID	Elemento de Verificación	Estado (Marcar X)	Observaciones / Fecha de Verificación
I. Gestión de Actualizaciones y Parches				
Sistema Operativo	I.1	SO configurado para actualizaciones automáticas de seguridad críticas.	[ ]	
	I.2	No hay actualizaciones de seguridad críticas pendientes.	[ ]	
	I.3	Historial de actualizaciones revisado periódicamente.	[ ]	
Aplicaciones y Software de Terceros	I.4	Todas las aplicaciones instaladas están actualizadas.	[ ]	
	I.5	Software no utilizado o desactualizado ha sido desinstalado.	[ ]	
II. Configuración de Permisos y Control de Acceso				
Principio de Menor Privilegio	II.1	Usuarios operan con los privilegios mínimos necesarios.	[ ]	
	II.2	Uso de cuentas administrativas restringido a tareas específicas.	[ ]	
Cuentas de Usuario y Contraseñas	II.3	Todas las cuentas tienen contraseñas fuertes.	[ ]	
	II.4	Políticas de vencimiento de contraseñas y/o 2FA implementadas.	[ ]	
	II.5	Cuentas de usuario obsoletas/no utilizadas deshabilitadas/eliminadas.	[ ]	
Permisos de Archivos y Carpetas	II.6	Permisos de acceso adecuados aplicados a archivos/carpetas sensibles.	[ ]	
	II.7	Herencia de permisos configurada correctamente.	[ ]	
III. Monitoreo y Auditoría				
Logs de Seguridad	III.1	Auditoría de seguridad del sistema activa y configurada.	[ ]	
	III.2	Logs de seguridad revisados regularmente en busca de anomalías.	[ ]	
	III.3	Patrones de intentos de login fallidos/acceso denegado investigados.	[ ]	
Monitoreo de Procesos y Servicios	III.4	Procesos en ejecución monitoreados para actividad sospechosa.	[ ]	
	III.5	Servicios del sistema innecesarios identificados y deshabilitados.	[ ]	
IV. Protección de Red y Firewall				
Firewall	IV.1	Firewall del sistema operativo activo y configurado.	[ ]	
	IV.2	Reglas del firewall revisadas para permitir solo tráfico necesario.	[ ]	

Puertos Abiertos	IV.3	Escaneos de puertos realizados para identificar puertos innecesarios.	[ ]	
	IV.4	Puertos no esenciales cerrados o restringidos.	[ ]	
V. Respaldo y Recuperación				
Estrategia de Respaldo	V.1	Estrategia de respaldo regular implementada para datos críticos.	[ ]	
	V.2	Puntos de restauración/snapshots utilizados para recuperación rápida.	[ ]	
Verificación de Recuperación	V.3	Procesos de recuperación probados periódicamente.	[ ]	
VI. Protección contra Malware y Amenazas				
Software Antimalware	VI.1	Software antivirus/antimalware instalado, actualizado y escaneado regularmente.	[ ]	
	VI.2	Definiciones de virus actualizadas.	[ ]	
Comportamiento del Usuario	VI.3	Usuarios educados sobre prácticas seguras (phishing, descargas).	[ ]	
VII. Configuración Segura General				
Contraseñas por Defecto	VII.1	Todas las contraseñas por defecto han sido cambiadas.	[ ]	
Cuentas de Invitado	VII.2	Cuenta de "Invitado" deshabilitada o eliminada si no es necesaria.	[ ]	
Bloqueo Automático	VII.3	Sistema configurado para bloquearse automáticamente por inactividad.	[ ]	

Claro, aquí tienes la descripción del proceso de Respaldo y Recuperación, presentado como un tutorial paso a paso en tercera persona del pasado y de forma muy puntual.

Proceso de Respaldo y Recuperación (Tutorial Paso a Paso)

Durante el laboratorio, se llevó a cabo el siguiente procedimiento para demostrar las capacidades de respaldo y recuperación del sistema.

Paso 1: Creación de un Punto de Restauración del Sistema

Primero, se procedió a crear un punto de restauración.

1. **Acceso a la Utilidad:** El técnico navegó hasta la función "Crear un punto de restauración" del sistema operativo. Esto se logró buscando la opción en el menú de inicio o accediendo a las propiedades del sistema.

2. **Verificación de Protección:** Se verificó que la "Protección del sistema" estuviera activada para la unidad del sistema operativo. Si no lo estaba, se activó.
3. **Generación del Punto:** Se seleccionó la opción "Crear..." y se proporcionó un nombre descriptivo para el punto de restauración, como "PuntoRestauracion_PreCambiosLaboratorio".
4. **Confirmación:** Se esperó la confirmación del sistema de que el punto de restauración había sido creado exitosamente.

Paso 2: Realización de Cambios al Sistema

Una vez establecido el punto de restauración, se introdujeron deliberadamente una serie de cambios en el sistema para simular una alteración no deseada.

1. **Instalación de Software:** Se instaló una aplicación de terceros, específicamente "VLC Media Player", en el sistema.
2. **Modificación de Archivos y Carpetas:** Se creó una nueva carpeta, `C:\Usuarios\MiUsuario\Escritorio\ArchivosTemporales`, y se guardaron dos archivos de texto nuevos dentro de ella.
3. **Ajuste de Configuración de Pantalla:** Se modificó la resolución de pantalla del sistema, cambiándola de la configuración predeterminada de 1920x1080 a una resolución diferente de 1280x720.

Paso 3: Restauración del Sistema y Verificación

Con los cambios implementados, se procedió a la fase de recuperación para revertir el sistema a su estado anterior.

1. **Inicio del Proceso de Restauración:** El técnico volvió a la ventana "Propiedades del sistema" y seleccionó la opción "Restaurar sistema...".
2. **Selección del Punto:** Se siguió el asistente, eligiendo el punto de restauración creado previamente ("PuntoRestauracion_PreCambiosLaboratorio") de la lista de puntos disponibles.
3. **Confirmación y Ejecución:** Se confirmó la selección y se inició el proceso de restauración. El sistema operativo solicitó un reinicio para aplicar los cambios.
4. **Reinicio y Aplicación:** El sistema se reinició y procedió con la restauración, lo que implicó un período de espera mientras se revertían los archivos y configuraciones.
5. **Verificación de Cambios Revertidos:** Tras el reinicio y el acceso al escritorio, se realizaron las siguientes verificaciones:

- Se confirmó que "VLC Media Player" **ya no estaba instalado** en el sistema.
- Se verificó que la carpeta `C:\Usuarios\MiUsuario\Escritorio\ArchivosTemporales` y sus contenidos **habían desaparecido**.
- Se constató que la resolución de pantalla había **regresado automáticamente** a su configuración original de 1920x1080.

Paso 4: Documentación del Proceso y Tiempo

Finalmente, se documentaron los detalles clave de la operación.

1. **Registro de Punto de Restauración:** Se anotó el nombre del punto de restauración (`PuntoRestauracion_PreCambiosLaboratorio`) y la fecha y hora de su creación (19/06/2025 11:30 AM).
2. **Detalle de Cambios:** Se listaron los cambios específicos que se habían introducido en el sistema (instalación de VLC, creación de carpeta y archivos, cambio de resolución).
3. **Registro de Tiempo:** Se cronometró el tiempo total que tomó el proceso de restauración, desde el inicio hasta que el sistema estuvo completamente funcional nuevamente, registrando un tiempo aproximado de **15 minutos**.
4. **Evaluación:** Se confirmó que el proceso de restauración fue exitoso, y todos los cambios intencionales fueron revertidos eficazmente, demostrando la utilidad de los puntos de restauración como medida de recuperación.