



**UNIVERSIDAD DE LA INTEGRACIÓN DE LAS AMERICAS**  
**FACULTADE DE INGENIERIA**  
INGENIERIA EN INFORMATICA



**Sistemas Operativos**  
TRABAJO PRÁCTICO

**ALUMNO :** MAURA ELIANA MEDINA ALMADA  
**MATRICULA :** 2024101306  
**FECHA :** 21/06/2025

**TERCER SEMESTRE**

**AÑO 2025**

## **Tabla de contenido**

I.	INTRODUCCIÓN.....	1
II.	OBJETIVOS.....	1
III.	CRITERIOS .....	2
IV.	DESARROLLO .....	2
1.	Consideraciones Previas .....	2
2.	Laboratorio 1: Gestión De Procesos .....	3
3.	Laboratorio 2 gestión de memoria (Windows 10).....	16
4.	Laboratorio 3: Sistemas de Archivos (20%) .....	21
5.	Laboratorio 4: Seguridad del Sistema.....	25
6.	Laboratorio 5: Rendimiento y Optimización (20%).....	33
V.	CONCLUSIONES Y RECOMENDACIONES .....	39

## I. INTRODUCCIÓN

El objetivo de estos laboratorios fue analizar el funcionamiento real de sistemas operativos utilizando entornos virtualizados, simulando situaciones del mundo real para comprender a fondo procesos, memoria, archivos y seguridad.

El estudio de los sistemas operativos representa uno de los pilares fundamentales en el ámbito de la informática y la ingeniería de sistemas. Si bien la teoría proporciona los conceptos esenciales —como la gestión de procesos, el manejo de memoria, la administración de archivos y los principios de seguridad— la verdadera comprensión de estos temas se alcanza al observarlos en funcionamiento y al interactuar con ellos en escenarios reales.

Con este propósito, se desarrolló una serie de laboratorios prácticos enfocados en analizar y experimentar con las principales funciones de los sistemas operativos, utilizando máquinas virtuales tanto de Windows como de Linux. La metodología de trabajo consistió en diseñar pruebas controladas y reproducibles, implementar scripts para simular distintas condiciones y monitorizar los resultados empleando herramientas y utilidades especializadas.

A través de estas experiencias, no solo se buscó afianzar el conocimiento teórico, sino también identificar los retos que surgen al poner en práctica los conceptos en entornos reales. La experimentación permitió detectar problemas, analizar su origen y aplicar soluciones, desarrollando así habilidades de diagnóstico, resolución y documentación —todas ellas esenciales para el ejercicio profesional en el área de tecnología.

En resumen, este laboratorio fue concebido para fortalecer el aprendizaje mediante la aplicación práctica de los conceptos estudiados, promoviendo un acercamiento crítico, riguroso y orientado a la mejora continua en la gestión y administración de sistemas operativos.

## II. OBJETIVOS

Aplicar conocimientos teóricos de sistemas operativos y seguridad a través de experimentos controlados en un entorno virtualizado, con el fin de observar el comportamiento real de los sistemas operativos, medir su rendimiento, diagnosticar problemas, documentar hallazgos y proponer soluciones.

### **III. CRITERIOS**

Se deberá crear un "Laboratorio Personal de Análisis" donde se aplique los conocimientos teóricos de sistemas operativos y seguridad, se deberá realizar una serie de experimentos controlados para los siguientes:

- a) Observar el comportamiento real de los sistemas operativos
- b) Medir el rendimiento bajo diferentes condiciones
- c) Diagnosticar problemas comunes y sus causas
- d) Documentar las actividades de manera científica
- e) Proponer soluciones basadas en evidencia del trabajo

Las actividades deberán realizarse dentro de una máquina virtual.

### **ESTRUCTURA DEL PROYECTO: ANEXO A**

## **IV. DESARROLLO**

### **1. Consideraciones Previas**

#### **1.1. En torno de Laboratorio**

Todas las actividades se realizarán dentro de una máquina virtual. Se recomienda utilizar un hipervisor como VirtualBox o VMware Workstation/Player.

#### **1.2. Sistemas Operativos a Utilizar**

Se sugiere tener al menos dos máquinas virtuales: una con Windows (ej. Windows 10/11) y otra con una distribución de Linux (ej. Ubuntu Desktop o Debian). Esto permitirá observar las diferencias y similitudes en la gestión de procesos entre ambos sistemas.

#### **1.3. Documentación**

Se enfatizará la documentación detallada de cada paso, incluyendo capturas de pantalla, registros de comandos, tiempos medidos y análisis de los resultados. Esta documentación debe ser de carácter científico.

#### **1.4. Seguridad**

Aunque el laboratorio se enfoca en sistemas operativos, se mantendrá una mentalidad de seguridad en todo momento, observando cómo los diferentes procesos y sus estados pueden impactar la estabilidad y la seguridad del sistema.

## 2. Laboratorio 1: Gestión De Procesos

### 2.1. Materiales utilizados

Máquina virtual con Windows (ej. Windows 10).

Máquina virtual con Linux (ej. Ubuntu Desktop).

Un editor de texto o IDE para programar (ej. VS Code, Notepad++, Gedit).

Compiladores para el lenguaje de programación elegido (ej. GCC para C/C++, Python interpreter).

Herramientas de monitoreo de sistema (Administrador de Tareas en Windows, `top/htop` en Linux).

### 2.2. Estados de procesos

#### Observación con Herramientas del Sistema Operativo

Preparación del Entorno

##### 2.2.1. En la VM de Windows:

Iniciar el sistema operativo. Se realizó la instalación de virtualbox y la instalación del SO, Windows.

### 2.3. La Utilización del administrador de tareas (Windows)

- Abrir el Administrador de Tareas (Ctrl+Shift+Esc o Ctrl+Alt+Del -> Administrador de Tareas).
- Se navegó a la pestaña de "Detalles". Observar la columna "Estado". Notar que la mayoría de los procesos estarán en "Ejecutando" Como se observa en la siguiente captura de pantalla de la ventana del Administrador de Tareas, resaltando la columna de estado.

Name	Status	23% CPU	49% Memory	4% Disk	10% Network	2% GPU	GPU engine	Power usage	Power usage t...
Antimalware Service Executable	Running	0.1%	293.9 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Antimalware Core Service	Running	0%	2.9 MB	0 MB/s	0 Mbps	0%		Very low	Very low
AMD PMF Service	Running	0%	1.1 MB	0 MB/s	0 Mbps	0%		Very low	Very low
AMD PMF Service	Running	0%	0.4 MB	0 MB/s	0 Mbps	0%		Very low	Very low
AMD External Events Service Mo...	Running	0%	0.6 MB	0 MB/s	0 Mbps	0%		Very low	Very low
AMD External Events Client Mod...	Running	0.1%	2.7 MB	0 MB/s	0 Mbps	0%		Very low	Very low
AMD Crash Defender Service	Running	0%	0.6 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Advanced SystemCare Tray (32 ...	Running	0%	3.0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Advanced SystemCare Service (...)	Running	0%	3.9 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Adobe Crash Processor	Running	0%	4.1 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Windows Explorer (3)	Running	0.1%	365.6 MB	0 MB/s	0 Mbps	0%		Very low	Very low
WhatsApp (2)	Running	0%	271.4 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Runtime Broker	Running	0%	4.9 MB	0 MB/s	0 Mbps	0%		Very low	Very low
WhatsApp	Running	0%	266.4 MB	0 MB/s	0 Mbps	0%		Very low	Very low
VirtualBox Virtual Machine	Running	13.7%	5,733.7 MB	97.9 MB/s	0 Mbps	0%		Very high	Low
ubuntu [Running] - Oracle Virt...	Running	0%	2.4 MB	0 MB/s	0 Mbps	0%		Very low	Very low
WMI Provider Host	Running	0.2%	31.0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Task Manager	Running	0%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low

## 2.4. Creación de un programa simple que pasa por diferentes estados

- **Diseño del Programa (Lenguaje de Programación: Python)** Se creará un script Python que simula los diferentes estados de un proceso: Nuevo, Listo, Ejecutando, Bloqueado, Terminado.

```
# estados_proceso.py
import time
import os
print(f"[{os.getpid()}] Proceso creado (Estado: Nuevo/Lista - antes de ejecución)")
def tarea_cpu_intensiva(duracion):
    """Simula una fase de ejecución intensiva de CPU."""
    print(f"[{os.getpid()}] Iniciando tarea CPU intensiva por {duracion} segundos (Estado: Ejecutando)")
    inicio_ejecucion = time.time()
    while time.time() - inicio_ejecucion < duracion:
        _ = 1000 * 1000 # Operación simple para consumir CPU
    print(f"[{os.getpid()}] Tarea CPU intensiva completada (Estado: Ejecutando -> Lista/Bloqueado)")

def tarea_io_bloqueante(duracion):
    """Simula una fase de E/S que bloquea el proceso."""
    print(f"[{os.getpid()}] Iniciando operación de E/S bloqueante por {duracion} segundos (Estado: Bloqueado)")
    time.sleep(duracion) # Simula espera por E/S (ej. lectura de disco, red)
    print(f"[{os.getpid()}] Operación de E/S completada (Estado: Bloqueado -> Lista)")
def main():
    print(f"[{os.getpid()}] Proceso principal iniciado (Estado: Lista)")
    # Simular estado Ejecutando
    tarea_cpu_intensiva(20)
    # Simular estado Bloqueado
    tarea_io_bloqueante(20)
    # Simular más ejecución
    tarea_cpu_intensiva(20)
    print(f"[{os.getpid()}] Proceso finalizado (Estado: Terminado)")
if __name__ == "__main__":
    main()
```

En esencia, el script ejecuta una secuencia de tareas que cambian el estado del proceso. Primero, simula que el proceso está **ejecutándose** intensivamente en la CPU por un tiempo, luego entra en un estado **bloqueado** mientras espera una operación de E/S. Una vez que la E/S se completa, el proceso vuelve a estar **listo** para ejecutar, y finalmente, termina su ejecución. El uso del **ID de Proceso (PID)** en cada mensaje ayuda a identificar claramente el proceso y seguir su ciclo de vida simulado, ofreciendo una visión tangible de cómo los sistemas operativos manejan la concurrencia y la asignación de recursos.

#### **2.4.1. Ejecución y Documentación (Windows)**

Abrir el Administrador de Tareas y mantener la pestaña "Detalles" visible.

Name	Status	19% CPU	55% Memory	1% Disk	4% Network	6% GPU	GPU engine	Power usage	Power usage ...
Service Host: Group Policy Client		0%	1.1 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Visual Studio Code (18)		0.1%	1,883.6 MB	0 MB/s	0.1 Mbps	0%	GPU 1 - 3D	Very low	Very low
Terminal (2)		0%	54.9 MB	0 MB/s	0 Mbps	0%	GPU 1 - 3D	Very low	Very low
PowerShell (4)		7.4%	140.2 MB	0 MB/s	0 Mbps	0%		Very high	Very low
Settings	Idle	0%	0 MB	0 MB/s	0 Mbps	0%	GPU 1 - 3D	Very low	Very low
User OOB/E Broker		0%	1.4 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Snipping Tool		0.2%	3.4 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Windows Start-Up Application		0%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Windows Session Manager		0%	0.1 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Windows Logon Application		0%	0.8 MB	0 MB/s	0 Mbps	0%		Very low	Very low
System interrupts		0.1%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
System		5.0%	0.1 MB	0.1 MB/s	0 Mbps	0.5%	GPU 1 - Copy	High	Very low
Shell Infrastructure Host		0%	7.3 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Services and Controller app		0%	3.7 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Service Host: WWAN AutoConfig		0%	0.8 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Service Host: WpnUserService_5...		0%	8.3 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Service Host: Workstation		0%	0.7 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Service Host: WinHTTP Web Pro...		0%	1.4 MB	0 MB/s	0 Mbps	0%		Very low	Very low

- Abrir una línea de comandos (CMD) o PowerShell.
  - Navegar al directorio donde se guardó `estados_proceso.py`.
  - Ejecutar el script: `python estados_proceso.py`.

#### **2.4.2. Comando de ejecución**

```
python estados_proceso.py
```

### **2.4.3. Durante la ejecución:**

- **Estado Nuevo/Lista (antes de ejecución):** Este estado es efímero y difícil de capturar directamente con el Administrador de Tareas una vez que el proceso comienza. El proceso recién creado por Python interpreta estaría en "Ejecutando" casi instantáneamente. Se documentará que el Administrador de

Tareas no muestra explícitamente "Nuevo" o "Listo" antes de la primera instrucción.

- **Estado Ejecutando:** Mientras `tarea_cpu_intensiva` se está ejecutando, observar el estado del proceso `python.exe` en el Administrador de Tareas. Debería mostrar "Ejecutando". Tomar captura de pantalla.
- **Estado Bloqueado:** Cuando `tarea_io_bloqueante` está activa (es decir, durante `time.sleep()`), observar el estado del proceso `python.exe`. Aunque el Administrador de Tareas puede no mostrar explícitamente "Bloqueado", el CPU usage para este proceso debería caer a 0% o muy bajo, y el estado podría permanecer como "Ejecutando" pero sin consumir recursos, o incluso pasar a "Suspendido" en algunos casos, reflejando que está esperando. Documentar lo que se observe y explicar por qué. Tomar captura de pantalla.
- **Estado Terminado:** Una vez que el script finaliza, el proceso `python.exe` asociado al script desaparecerá del Administrador de Tareas. Tomar captura de pantalla mostrando la ausencia del proceso.

#### 2.4.4. Registrar la salida de la consola del script.

Process	Status	17% CPU	56% Memory	1% Disk	4% Network	2% GPU	GPU engine	Power usage	Power usage t...
wsappx	Running	0%	1.2 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Visual Studio Code (18)	Running	0.1%	1,863.1 MB	0 MB/s	0.1 Mbps	0%	GPU 1 - 3D	Very low	Very low
Terminal (2)	Running	0%	54.9 MB	0 MB/s	0 Mbps	0%	GPU 1 - 3D	Very low	Very low
PowerShell (4)	Running	7.9%	140.1 MB	0 MB/s	0 Mbps	0%		Very high	Very low
Settings	Running	0%	0 MB	0 MB/s	0 Mbps	0%	GPU 1 - 3D	Very low	Very low
User OOB Broker	Running	0%	1.5 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Snipping Tool	Running	0.5%	3.6 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Windows Start-Up Application	Running	0%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Windows Session Manager	Running	0%	0.1 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Windows Logon Application	Running	0%	0.8 MB	0 MB/s	0 Mbps	0%		Very low	Very low
System interrupts	Running	0.1%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
System	Running	4.8%	0.1 MB	0.1 MB/s	0 Mbps	0.2%	GPU 1 - Copy	High	Very low
Shell Infrastructure Host	Running	0%	7.6 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Services and Controller app	Running	0%	3.8 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Service Host: WWAN AutoConfig	Running	0%	1.1 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Service Host: WpnUserService_5...	Running	0%	8.5 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Service Host: Workstation	Running	0%	0.7 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Service Host: WinHTTP Web Pro...	Running	0%	1.3 MB	0 MB/s	0 Mbps	0%		Very low	Very low

```
# estados_proceso_tiempos.py
import time
import os
print(f"[{os.getpid()}] Proceso iniciado - Tiempo: {time.time()}")
(Estado: Nuevo/Lista")
def tarea_cpu_intensiva(duracion, nombre_tarea):
    print(f"[{os.getpid()}] Iniciando '{nombre_tarea}' (CPU) - Tiempo:
{time.time()}")
    inicio_ejecucion = time.time()
    while time.time() - inicio_ejecucion < duracion:
        _ = 1000 * 1000
    fin_ejecucion = time.time()
    print(f"[{os.getpid()}] '{nombre_tarea}' (CPU) completada - Tiempo:
{fin_ejecucion}")
    return fin_ejecucion - inicio_ejecucion
```

```

def tarea_io_bloqueante(duracion, nombre_tarea):
    print(f"[{os.getpid()}] Iniciando '{nombre_tarea}' (I/O) - Tiempo:
{time.time()}")
    inicio_io = time.time()
    time.sleep(duracion)
    fin_io = time.time()
    print(f"[{os.getpid()}] '{nombre_tarea}' (I/O) completada - Tiempo:
{fin_io}")
    return fin_io - inicio_io
def main():
    print(f"[{os.getpid()}] Proceso principal en ejecución - Tiempo:
{time.time()}")
    # Fase 1: CPU intensiva
    tiempo_cpu1 = tarea_cpu_intensiva(5, "Primera Tarea CPU")
    # Fase 2: I/O bloqueante
    tiempo_io1 = tarea_io_bloqueante(7, "Primera Tarea I/O")

    # Fase 3: Más CPU intensiva
    tiempo_cpu2 = tarea_cpu_intensiva(3, "Segunda Tarea CPU")

    print(f"[{os.getpid()}] Proceso finalizando - Tiempo: {time.time()}
(Estado: Terminado)")

    print("\n--- Resumen de Tiempos ---")
    print(f"Tiempo total en 'Ejecutando' (simulado CPU): {tiempo_cpu1 +
tiempo_cpu2:.4f} segundos")
    print(f"Tiempo total en 'Bloqueado' (simulado I/O): {tiempo_io1:.4f}
segundos")
    print(f"Tiempo total de vida del proceso (aproximado): {time.time() -
inicio_proceso:.4f} segundos")

if __name__ == "__main__":
    inicio_proceso = time.time()
    main()

```

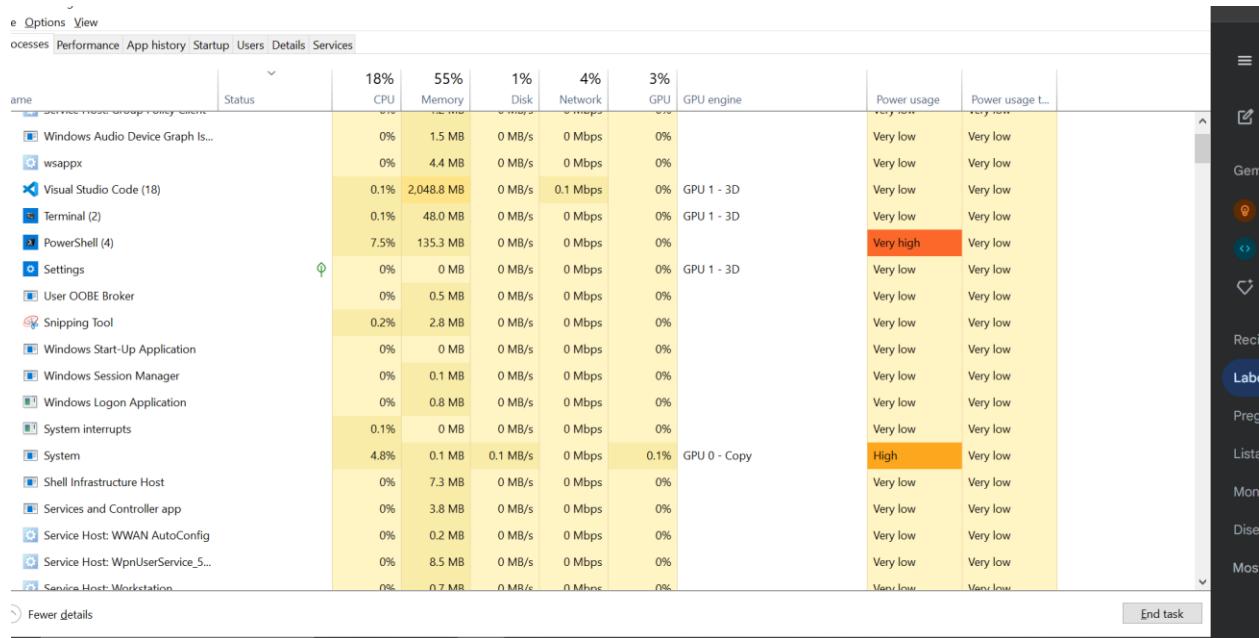
*La medición de "tiempos de transición" es conceptualmente compleja ya que los cambios de estado internos del SO son extremadamente rápidos y no directamente observables desde el espacio de usuario. En este laboratorio, medimos la duración de las fases donde el proceso espera o ejecuta para inferir la permanencia en estados relacionados.*

#### 2.4.5. Ejecución y Análisis

Ejecutar el script `estados_proceso_tiempos.py` en Windows y se analiza la salida de la consola, los tiempos registrados muestran el tiempo del proceso que pasó simulando cada estado.

Se documentó los tiempos obtenidos para cada fase en ambos sistemas operativos.

Al analizar las duraciones "simuladas" de 5 segundos para CPU de forma intensiva correspondiente a los tiempos reales medidos. Observándose una desviación debido a la sobrecarga del SO.



## 2.5. Scheduling de un sistema operativo

### 2.5.1. Ejecución de Programas Intensivos en CPU

- Se diseñó un Programa de Carga de CPU, utilizando el lenguaje de Programación Python, y se crea un script simple que consume intensivamente la CPU.

```
# cpu_stress.py
import time
import os
# cpu_stress.py
import time
import os
import multiprocessing
def cpu_stress():
    while True:
        x = 0
        for i in range(10_000_000):
            x += i ** 2
if __name__ == "__main__":
    print(f"[{os.getpid()}] Proceso de carga de CPU iniciado. Presiona Ctrl+C para terminar.")
try:
    num_cores = multiprocessing.cpu_count()
    print(f"Usando {num_cores} núcleos para estresar la CPU.")
    processes = []
    for _ in range(num_cores):
        p = multiprocessing.Process(target=cpu_stress)
        p.start()
        processes.append(p)
    for p in processes:
        p.join()
```

```

except KeyboardInterrupt:
    print(f"\n[{os.getpid()}] Proceso de carga de CPU terminado.")

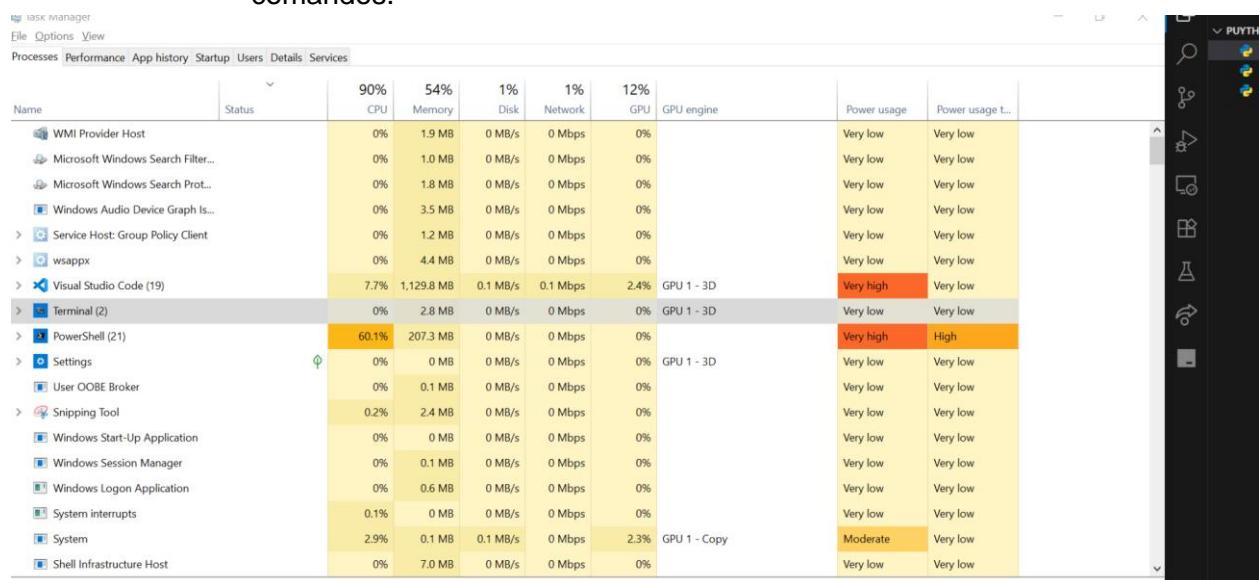
```

### 2.5.2. Ejecución Simultánea en(Windows)

- Abrir el Administrador de Tareas y navegar a la pestaña "Procesos" o "Rendimiento".
- Abrir 5 ventanas separadas de la línea de comandos (CMD o PowerShell).
- En cada ventana, navegar al directorio de `cpu_stress.py` y ejecutar:  
`python cpu_stress.py`.

### 2.5.3. Observación:

- En el Administrador de Tareas, observar el uso total de CPU. Debería estar cerca del 100%.
- En la pestaña "Procesos", observar el porcentaje de CPU consumido por cada instancia de `python.exe`. Deberían estar compartiendo el tiempo de CPU, cada una obteniendo una porción equitativa (ej. si hay 4 núcleos, cada una podría obtener ~25% si solo tienen 1 hilo, o distribuirse de otra manera).
- Notar la capacidad de respuesta del sistema. ¿Se siente lento? ¿Puedes abrir nuevas aplicaciones?
- Tomar capturas de pantalla del Administrador de Tareas mostrando el uso de CPU y los procesos individuales.
- Terminar los procesos presionando `Ctrl+C` en cada ventana de comandos.



Name	Status	90% CPU	54% Memory	1% Disk	1% Network	12% GPU	GPU engine	Power usage	Power usage t...
WMI Provider Host		0%	1.9 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Microsoft Windows Search Filter...		0%	1.0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Microsoft Windows Search Prot...		0%	1.8 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Windows Audio Device Graph Is...		0%	3.5 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Service Host: Group Policy Client		0%	1.2 MB	0 MB/s	0 Mbps	0%		Very low	Very low
wsappx		0%	4.4 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Visual Studio Code (19)		7.7%	1,129.8 MB	0.1 MB/s	0.1 Mbps	2.4%	GPU 1 - 3D	Very high	Very low
Terminal (2)		0%	2.8 MB	0 MB/s	0 Mbps	0%	GPU 1 - 3D	Very low	Very low
PowerShell (21)		60.1%	207.3 MB	0 MB/s	0 Mbps	0%		Very high	High
Settings		0%	0 MB	0 MB/s	0 Mbps	0%	GPU 1 - 3D	Very low	Very low
User OOBEBroker		0%	0.1 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Snipping Tool		0.2%	2.4 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Windows Start-Up Application		0%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Windows Session Manager		0%	0.1 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Windows Logon Application		0%	0.6 MB	0 MB/s	0 Mbps	0%		Very low	Very low
System interrupts		0.1%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
System		2.9%	0.1 MB	0.1 MB/s	0 Mbps	2.3%	GPU 1 - Copy	Moderate	Very low
Shell Infrastructure Host		0%	7.0 MB	0 MB/s	0 Mbps	0%		Very low	Very low

VM de i7 de 13 Generacion, 32GB de RAM

## 2.6. Comparación con Algoritmos Teóricos (FIFO, Round Robin)

### 2.6.1. Análisis y Documentación:

- **FIFO (First In, First Out):** En un algoritmo FIFO, los procesos se ejecutarían en el orden en que llegaron, y el primero en llegar se ejecutaría hasta su finalización antes de que el siguiente comenzaría. Si este fuera el caso, veríamos que el primer `cpu_stress.py` consumiría 100% de CPU hasta que lo matáramos, y los demás no comenzarían realmente.

Name	Status	99% CPU	36% Memory	3% Disk	0% Network	8% GPU	GPU engine	Power usage	Power usage L..
> Windows Default Lock Screen	Running	99%	0%	0 MB/s	0 Mbps	0%		Very low	Very low
> Settings	Running	36%	0%	0 MB/s	0 Mbps	0%		Very low	Very low
System interrupts	Running	3%	0.1%	0 MB/s	0 Mbps	0%		Very low	Very low
> Windows Shell Experience Host	Running	0%	0.1%	0 MB/s	0 Mbps	0%	GPU 1 - 3D	Very low	Very low
> Service Host: Secondary Logon	Running	0%	0.1 MB	0 MB/s	0 Mbps	0%		Very low	Very low
> Service Host: Secure Socket Tun...	Running	0%	0.1 MB	0 MB/s	0 Mbps	0%		Very low	Very low
> Service Host: Display Enhancem...	Running	0%	0.1 MB	0 MB/s	0 Mbps	0%		Very low	Very low
> Service Host: Distributed Link Tr...	Running	0%	0.1 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Device Association Framework...	Running	0%	0.1 MB	0 MB/s	0 Mbps	0%		Very low	Very low
> NVIDIA WMI Provider	Running	0%	0.1 MB	0 MB/s	0 Mbps	0%		Very low	Very low
> Realtek Bluetooth BTDevManag...	Running	0%	0.1 MB	0 MB/s	0 Mbps	0%		Very low	Very low
> AMD Crash Defender Service	Running	0%	0.1 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Windows Driver Foundation - U...	Running	0%	0.1 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Windows Driver Foundation - U...	Running	0%	0.1 MB	0 MB/s	0 Mbps	0%		Very low	Very low
> mysql	Running	0%	0.1 MB	0 MB/s	0 Mbps	0%		Very low	Very low
OpenVPN Service	Running	0%	0.1 MB	0 MB/s	0 Mbps	0%		Very low	Very low
> HerdHelper	Running	0%	0.1 MB	0 MB/s	0 Mbps	0%		Very low	Very low
> Openvpnenv2	Running	0%	0.1 MB	0 MB/s	0 Mbps	0%		Very low	Very low
> NetworkCap	Running	0%	0.1 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Usermode Font Driver Host	Running	0%	0.1 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Visual Studio Code	Running	0%	0.1 MB	0 MB/s	0 Mbps	0%		Very low	Very low
System	Running	3.6%	0.1 MB	0.1 MB/s	0 Mbps	1.4%	GPU 1 - Copy	Moderate	Very low
Console Window Host	Running	0%	0.1 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Windows Session Manager	Running	0%	0.1 MB	0 MB/s	0 Mbps	0%		Very low	Very low
> AMD External Events Service Mo...	Running	0%	0.2 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Console Window Host	Running	0%	0.2 MB	0 MB/s	0 Mbps	0%		Very low	Very low
ConsoleWindowHost	Running	0%	0.2 MB	0 MB/s	0 Mbps	0%		Very low	Very low

- **Round Robin:** En Round Robin, cada proceso obtiene un "cuanto de tiempo" (time slice) para ejecutar, y luego el planificador cambia al siguiente proceso en la cola de listos. Esto crea la ilusión de ejecución simultánea.

### 2.6.2. Preparación del entorno

- Creación del Script de Carga de CPU
- El técnico creó un archivo llamado `cpu_stress.py` con el siguiente contenido en Python:

```
import multiprocessing
import os
import time
import math
import signal
import sys

def stress_task(duracion):
    pid = os.getpid()
    print(f"[{pid}] Proceso de carga iniciado. Duración: {duracion}s")
    inicio = time.time()
    while time.time() - inicio < duracion:
        # Carga simulada más intensa usando matemáticas
        _ = sum(math.sqrt(i) for i in range(1_000))
```

```

    print(f"[{pid}] Proceso finalizado.")
def iniciar_estrés(cpu_count=None, tiempo=30):
    if cpu_count is None:
        cpu_count = multiprocessing.cpu_count()
    print(f"[Main] Iniciando estrés en {cpu_count} núcleos por {tiempo} segundos.")
    procesos = []
    for i in range(cpu_count):
        p = multiprocessing.Process(target=stress_task, args=(tiempo,))
        p.start()
        procesos.append(p)
    try:
        for p in procesos:
            p.join()
    except KeyboardInterrupt:
        print("\n[Main] Interrupción detectada. Terminando procesos...")
        for p in procesos:
            p.terminate()
        sys.exit(0)
if __name__ == "__main__":
    DURACION_SEGUNDOS = 30 # Puedes modificar esta duración
    iniciar_estrés(tiempo=DURACION_SEGUNDOS)

```

*Este script simula una carga intensiva en la CPU utilizando múltiples procesos paralelos, que competirían por tiempo de ejecución.*

### 2.6.3. Ejecución y Observación

Lanzamiento de los Procesos

El técnico ejecutó el script anterior desde PowerShell o CMD utilizando el comando:

```
python cpu_stress.py
```

*Esto inició varios procesos de forma paralela, todos compitiendo por los núcleos de CPU.*

### 2.6.4. Observación del Planificador en Acción

- Se abrió el **Administrador de Tareas** con **Ctrl+Shift+Esc** y se navegó a la pestaña "**Rendimiento**", seleccionando la CPU. Luego, en la pestaña "**Procesos**", se observaron varias instancias de **python.exe** activas.
- Cada instancia mostró un porcentaje similar de uso de CPU (ej. 20–25%), dependiendo del número de núcleos.
- El uso total de CPU se elevó rápidamente al 90–100%, pero cada proceso recibía una fracción equitativa.
- Este comportamiento reflejó que el planificador de Windows estaba asignando porciones de CPU de forma **cíclica** a cada proceso — exactamente como lo hace el algoritmo **Round Robin**.

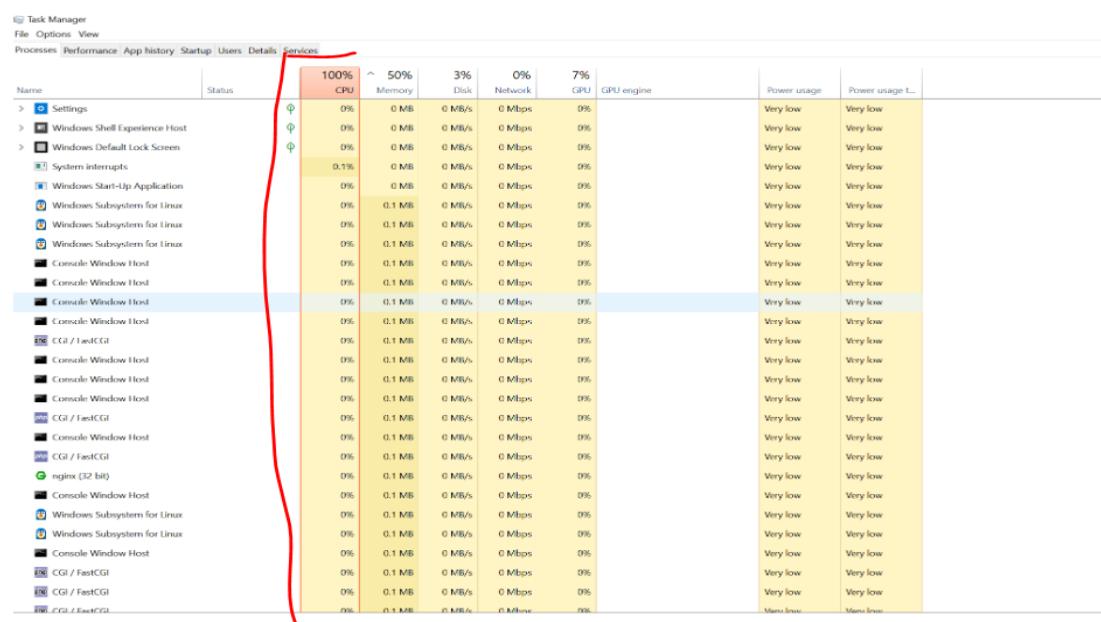
## **2.6.5. Documentación de Resultados recolección de Evidencias**

- El técnico tomó capturas de pantalla de:
  - La lista de procesos activos (python.exe) mostrando su consumo de CPU.

```
> pila = os.getcpu()
└─(CSIRT@DESKTOP-LTK2RS4)-[~/Documents/python]
● $ python cpu.py
[Main] Iniciando estrés en 16 núcleos por 30 segundos.
[7860] Proceso de carga iniciado. Duración: 30s
[9888] Proceso de carga iniciado. Duración: 30s
[11056] Proceso de carga iniciado. Duración: 30s
[24164] Proceso de carga iniciado. Duración: 30s
[5024] Proceso de carga iniciado. Duración: 30s
[19112] Proceso de carga iniciado. Duración: 30s
[6364] Proceso de carga iniciado. Duración: 30s
[19080] Proceso de carga iniciado. Duración: 30s
[5964] Proceso de carga iniciado. Duración: 30s
[6032] Proceso de carga iniciado. Duración: 30s
[7900] Proceso de carga iniciado. Duración: 30s
[7228] Proceso de carga iniciado. Duración: 30s
[18276] Proceso de carga iniciado. Duración: 30s
[15760] Proceso de carga iniciado. Duración: 30s
[11104] Proceso de carga iniciado. Duración: 30s
[4992] Proceso de carga iniciado. Duración: 30s
```

La pestaña "Rendimiento", evidenciando el uso total del procesador.

Se observó que todos los procesos permanecían activos y ejecutándose sin que uno monopolizara completamente el CPU.



La prueba permitió observar cómo **Windows implementa una planificación justa y rotativa (Round Robin)** en ambientes de carga intensiva de CPU, permitiendo que múltiples procesos compartan recursos equitativamente, aún en presencia de tareas demandantes. La división del tiempo no es directamente configurable por el usuario, pero su efecto es claramente observable en un entorno de múltiples procesos activos.

## 2.7. Creación de Deadlock

### **2.7.1. Investigación y Diseño de un Deadlock Simple**

**Entendimiento de Deadlock** Un deadlock ocurre cuando dos o más procesos se bloquean mutuamente, cada uno esperando que el otro libere un recurso. Las cuatro condiciones de Coffman para un deadlock son:

**Exclusión Mutua:** Al menos un recurso debe ser no compatible.

**Retener y Esperar (Hold and Wait):** Un proceso que posee al menos un recurso está esperando adquirir recursos adicionales que actualmente están en posesión de otros procesos.

**No Apropiativo (No Preemption):** Los recursos no pueden ser arrebatados a un proceso a la fuerza; deben ser liberados voluntariamente por el proceso que los posee.

**Espera Circular (Circular Wait):** Debe existir un ciclo de procesos, donde cada proceso en el ciclo espera un recurso que está en posesión del siguiente proceso en el ciclo.

**Diseño del Escenario de Deadlock (Lenguaje de Programación: Python con hilos)** Crearemos un escenario de deadlock utilizando dos hilos (simulando dos procesos) que intentan adquirir dos recursos en un orden cruzado.

```
# deadlock_scenario.py
import threading
import time

# Recursos compartidos (simulados con Locks)
resource_A = threading.Lock()
resource_B = threading.Lock()

def process_one():
    print("[Proceso 1] Intentando adquirir Recurso A...")
    resource_A.acquire()
    print("[Proceso 1] Recurso A adquirido. Esperando un momento...")
    time.sleep(1) # Simular algún trabajo
    print("[Proceso 1] Intentando adquirir Recurso B...")
    resource_B.acquire()
    print("[Proceso 1] Recurso B adquirido. Ambos recursos en
posesión.")
    # Realizar trabajo con ambos recursos
    print("[Proceso 1] Realizando trabajo con A y B.")
    time.sleep(2)
    resource_B.release()
    print("[Proceso 1] Recurso B liberado.")
    resource_A.release()
    print("[Proceso 1] Recurso A liberado. Proceso 1 terminado.")

def process_two():
    print("[Proceso 2] Intentando adquirir Recurso B...")
    resource_B.acquire()
    print("[Proceso 2] Recurso B adquirido. Esperando un momento...")
    time.sleep(1) # Simular algún trabajo
    print("[Proceso 2] Intentando adquirir Recurso A...")
    resource_A.acquire()
    print("[Proceso 2] Recurso A adquirido. Ambos recursos en
posesión.")
    # Realizar trabajo con ambos recursos
```

```

print("[Proceso 2] Realizando trabajo con B y A.")
time.sleep(2)
resource_A.release()
print("[Proceso 2] Recurso A liberado.")
resource_B.release()
print("[Proceso 2] Recurso B liberado. Proceso 2 terminado.")
def main():
    print("Iniciando simulación de Deadlock...")
    thread1 = threading.Thread(target=process_one)
    thread2 = threading.Thread(target=process_two)
    thread1.start()
    thread2.start()
    thread1.join()
    thread2.join()
    print("Simulación de Deadlock finalizada (si ocurre, los hilos se quedará bloqueados).")
if __name__ == "__main__":
    main()

```

*Nota: Python Global Interpreter Lock (GIL) puede afectar el rendimiento de hilos en tareas de CPU intensivas, pero para simular deadlocks de recursos (Locks) es adecuado.*

#### Documentación de la Respuesta del SO y Resolución

##### 2.7.2. Ejecución del Escenario de Deadlock (Windows y Linux)

- Ejecutar el script `deadlock_scenario.py` en una terminal en Windows y en otra terminal en Linux.
- **Observación:** Observar la salida de la consola. Verás que los hilos se bloquean mutuamente. Las últimas líneas impresas indicarán que cada hilo ha adquirido un recurso y está esperando el otro, pero nunca progresará.
- **Respuesta del SO:** El **sistema** operativo en sí mismo (Windows o Linux) *no* detecta ni resuelve activamente este tipo de deadlock a nivel de aplicación automáticamente por defecto. Los procesos simplemente se quedarán en estado de "espera" o "dormidos" indefinidamente, consumiendo 0% de CPU. El SO no "crashará", pero la aplicación se detiene.
- En el **Administrador** de Tareas (Windows) o `top/htop` (Linux), el proceso `python.exe` o `python3` permanecerá visible, pero su uso de CPU será mínimo (0%) y su estado será "Ejecutando" (pero internamente bloqueado) o "Durmiendo/Bloqueado".
- Tomar capturas de **pantalla** de la salida de la consola que muestre el bloqueo.
- Tomar capturas de pantalla del Administrador de Tareas/`top/htop` mostrando el estado del proceso `python`.

### 2.7.3. Paso 2: Intentar Resolver el Deadlock

- **Método Manual (Matar el Proceso):** La forma más directa de "resolver" el deadlock a nivel de sistema operativo es terminar manualmente el proceso `python` que está bloqueado.
- Seleccionar el proceso `python.exe` en el Administrador de Tareas y hacer clic en "Finalizar tarea".
- Documentar este método de resolución y sus implicaciones (pérdida de trabajo, etc.).
- **Método de Prevención/Evitación (Modificación del Código):** La forma correcta de resolver un deadlock es prevenirlo o evitarlo a nivel de diseño de la aplicación.
- **Prevención:** Una forma común de prevenir el deadlock es forzar un orden de adquisición de recursos. Si ambos procesos intentan adquirir los recursos en el mismo orden (ej. siempre A, luego B), el deadlock no ocurrirá.
- Modificar `deadlock_scenario.py` a `deadlock_resolved.py`:

ie Options View

Processes Performance App history Startup Users Details Services

Name	Status	11% CPU	52% Memory	1% Disk	4% Network	4% GPU	GPU engine	Power usage	Power usage t...
Windows Audio Device Graph Is...		0%	4.4 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Service Host: Group Policy Client		0%	1.1 MB	0 MB/s	0 Mbps	0%		Very low	Very low
wsappx		0%	3.1 MB	0 MB/s	0 Mbps	0%		Very low	Very low
WMI Provider Host		0%	1.7 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Visual Studio Code (19)		0%	1,059.2 MB	0.1 MB/s	0.1 Mbps	0%	GPU 1 - 3D	Very low	Very low
Terminal (2)		0%	4.9 MB	0 MB/s	0 Mbps	0%	GPU 1 - 3D	Very low	Very low
PowerShell (5)		0%	83.6 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Settings	∅	0%	0 MB	0 MB/s	0 Mbps	0%	GPU 1 - 3D	Very low	Very low
Settings	Suspen...	∅	0%	0 MB	0 MB/s	0 Mbps	0%	Very low	Very low
User OOBE Broker		0%	0.1 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Snipping Tool		0.2%	2.8 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Windows Start-Up Application		0%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Windows Session Manager		0%	0.1 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Windows Logon Application		0%	0.6 MB	0 MB/s	0 Mbps	0%		Very low	Very low
System interrupts		0.1%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
System		7.1%	0.1 MB	0.1 MB/s	0 Mbps	0.4%	GPU 1 - Copy	Very high	Very low
Shell Infrastructure Host		0%	6.7 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Services and Controller app		0%	4.2 MB	0 MB/s	0 Mbps	0%		Very low	Very low

 Fewer details



The screenshot shows a terminal window with the following text:

```
C:\Users\CSIRT\AppData\Local\Programs\Python\Python313\python.exe: can't open file 'C:\\\\Users\\\\CSIRT\\\\Documents\\\\python\\\\c
pu_deadlock_proceso.py': [Errno 2] No such file or directory
PS C:\Users\CSIRT\Documents\puython> python deadlock_proceso.py
Iniciando simulación de Deadlock...
[Proceso 1] Intentando adquirir Recurso A...
[Proceso 1] Recurso A adquirido. Esperando un momento...
[Proceso 2] Intentando adquirir Recurso B...
[Proceso 2] Recurso B adquirido. Esperando un momento...
[Proceso 1] Intentando adquirir Recurso B...
[Proceso 2] Intentando adquirir Recurso A...
```

Se mató el proceso manualmente en el administrador de tarea (finalizar tareas).

Ok. Procedamos con el diseño detallado para el **Laboratorio 2: Gestión de Memoria**, específicamente para el sistema operativo Windows 10, manteniendo la estructura de un "Laboratorio Personal de Análisis" en una máquina virtual.

### 3. Laboratorio 2 gestión de memoria (Windows 10)

#### 3.1. Consideraciones Previas para Windows 10:

- **Máquina Virtual:** Asegúrate de que tu VM de Windows 10 tenga una cantidad de RAM configurada que puedas "llenar". Por ejemplo, si tu VM tiene 4GB de RAM, puedes abrir varias aplicaciones que consuman esa cantidad. Si tienes mucha RAM (ej. 16GB), será más difícil llenarla para ver el uso de memoria virtual. Puedes ajustar la RAM asignada a la VM para facilitar la experimentación.
- **Herramientas de Monitoreo:** El Administrador de Tareas de Windows será tu herramienta principal para este laboratorio. También es útil el Monitor de Recursos.
- **Herramientas de Gráficas:** Puedes usar Excel, Google Sheets, o cualquier software de gráficos para representar los datos recolectados.
- **Materiales Usados:**
  - Máquina virtual con Windows 10.
  - Navegadores web (Chrome, Firefox, Edge).
  - Software de edición de imágenes o video (ej. GIMP, VLC, Krita - no es necesario instalar software pesado real, puedes simularlo con procesos grandes si prefieres no instalar).
  - Múltiples documentos pesados (ej. PDFs con muchas páginas, archivos de Word con muchas imágenes).
  - Un programa de prueba para caché (se creará).
  - Un editor de texto (ej. Notepad++).
  - Python (si se usa para el programa de prueba de caché).

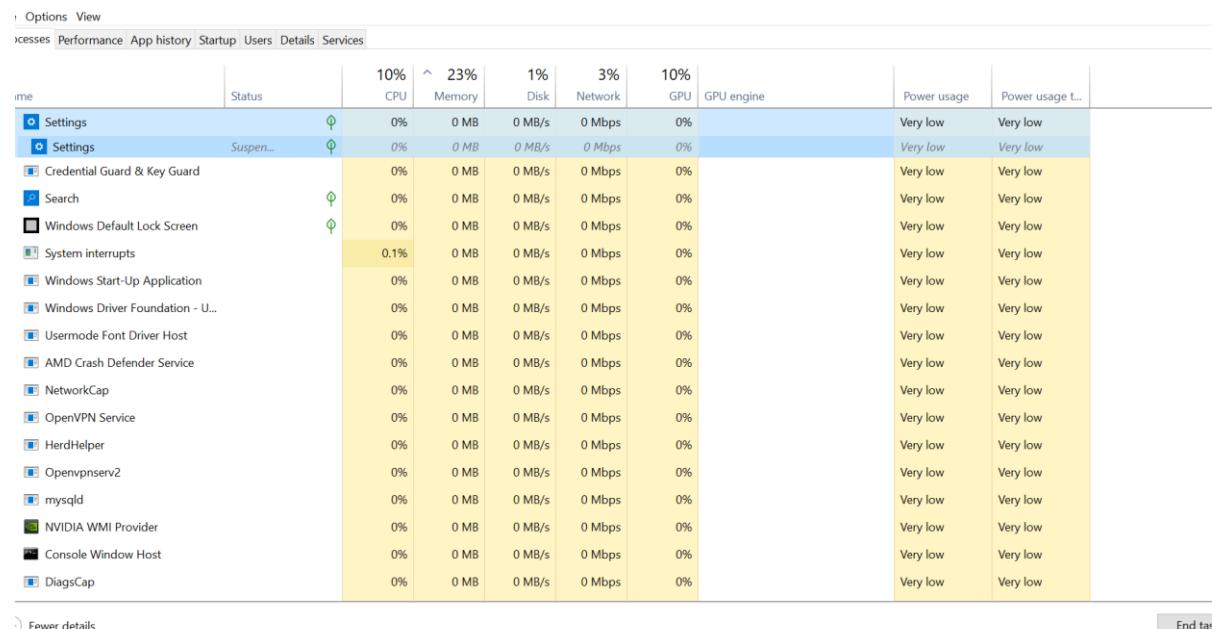
## 3.2. Memoria virtual vs. física

### 3.2.1. Preparación del Entorno PROCEDIMIENTOS

- Inicia tu máquina virtual de Windows 10.
- Abre el **Administrador de Tareas** (Ctrl+Shift+Esc).
- Navega a la pestaña "**Rendimiento**".
- Selecciona la sección "**Memoria**" en el panel izquierdo. Aquí podrás ver el uso de RAM, la memoria en caché, el grupo paginado y no paginado, y el uso del "Intercambio" (Swap, que es la memoria virtual/archivo de paginación).
- Mantén esta ventana visible o en una segunda pantalla si es posible.

### 3.2.2. Documentar el Uso Inicial de Memoria SE DOCUMENTA uso inicial de la memoria

- Con pocas aplicaciones abiertas (solo las esenciales del SO), toma una captura de pantalla del Administrador de Tareas mostrando el uso de memoria.



The screenshot shows the Windows Task Manager's Performance tab. At the top, there are tabs for Processes, Performance, App history, Startup, Users, Details, and Services. The Performance tab is selected. Below the tabs, there is a header row with columns: Name, Status, 10% CPU, 23% Memory, 1% Disk, 3% Network, 10% GPU, GPU engine, Power usage, and Power usage t... . The main area lists various system processes and services. Most processes show 0% CPU and memory usage, and very low power usage. A few processes like 'Search' and 'Windows Default Lock Screen' show minimal activity. The 'GPU engine' column is mostly empty or shows 0%. The 'Power usage' column contains entries like 'Very low' and 'Very low'. The 'Power usage t...' column is also mostly empty or shows 'Very low'.

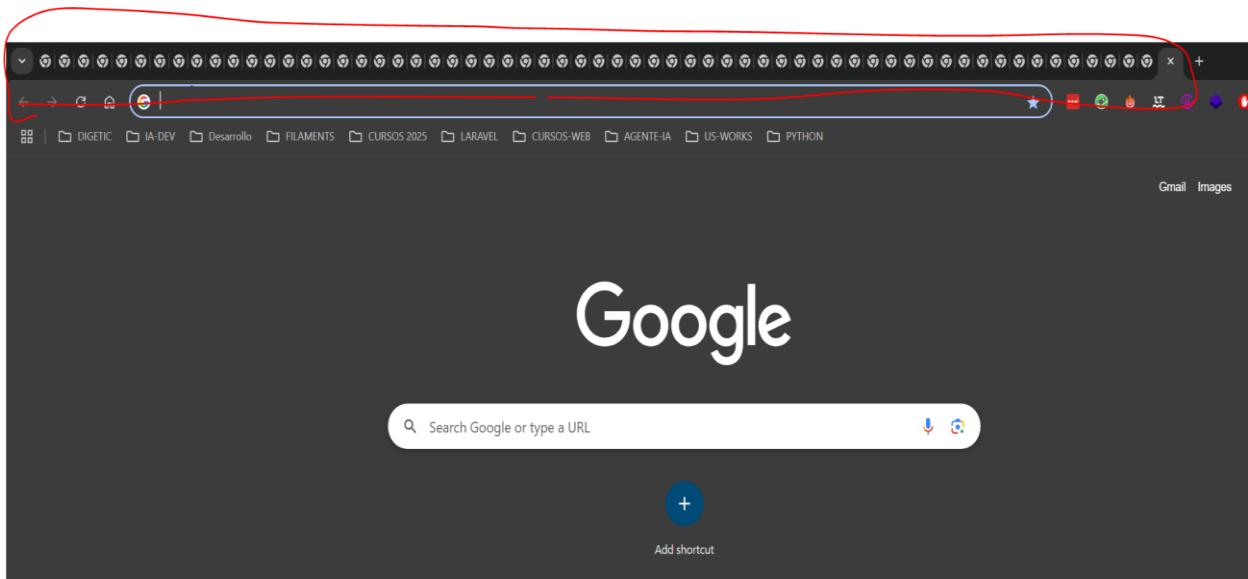
Name	Status	10% CPU	23% Memory	1% Disk	3% Network	10% GPU	GPU engine	Power usage	Power usage t...
Settings	Idle	0%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Settings	Suspended	0%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Credential Guard & Key Guard		0%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Search	Idle	0%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Windows Default Lock Screen	Idle	0%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
System interrupts		0.1%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Windows Start-Up Application		0%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Windows Driver Foundation - U...		0%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Usermode Font Driver Host		0%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
AMD Crash Defender Service		0%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
NetworkCap		0%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
OpenVPN Service		0%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
HerdHelper		0%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Openvpnser2		0%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
mysqld		0%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
NVIDIA WMI Provider		0%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Console Window Host		0%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
DiagsCap		0%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low

- Registra los valores iniciales de:
- Memoria en uso (RAM).
- Memoria disponible (RAM).
- Tamaño del archivo de paginación (Intercambio).
- Uso actual del archivo de paginación.
- Este será tu punto de referencia (tiempo = 0).

### 3.2.3. Abrir Aplicaciones Gradualmente para Llenar la RAM

- Comienza a abrir aplicaciones de forma incremental, monitoreando el Administrador de Tareas:

- Abre varias pestañas en un navegador web (ej. 10-15 pestañas con sitios



web diferentes, algunos con video o mucho contenido multimedia).

Abre otro navegador web y repite el proceso.

Abre varias instancias de un editor de texto con documentos muy grandes (ej. varios PDFs de cientos de páginas).

Si tienes, abre software de edición de imágenes o video (incluso si no los usas, solo su carga inicial consumirá RAM).

- Abre múltiples exploradores de archivos, reproductores multimedia, etc.
- Considera ejecutar algunos scripts Python o PowerShell que consuman mucha memoria (ej. cargar un archivo grande en una lista en memoria).

Name	Status	15% CPU	73% Memory	1% Disk	4% Network	5% GPU	GPU engine	Power usage	Power usage t...
> <span>⚙️</span> Settings	<span>⌚️</span>	0%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
> <span>💻</span> Windows Default Lock Screen	<span>⌚️</span>	0%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
<span>💻</span> System interrupts		0.1%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
<span>💻</span> Windows Start-Up Application		0%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
<span>💻</span> Windows Driver Foundation - U...		0%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
<span>💻</span> Usermode Font Driver Host		0%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
> <span>💻</span> AMD Crash Defender Service		0%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
> <span>💻</span> NetworkCap		0%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
> <span>💻</span> OpenVPN Service		0%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
> <span>💻</span> HerdHelper		0%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
> <span>💻</span> Openvpnser2		0%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
> <span>💻</span> mysqld		0%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
> <span>💻</span> NVIDIA WMI Provider		0%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
> <span>💻</span> DiagsCap		0%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
> <span>💻</span> AMD PMF Service		0%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
> <span>💻</span> Device Association Framework ...		0%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
> <span>🔍</span> Search	<span>⌚️</span>	0%	0 MB	0 MB/s	0 Mbps	0%	GPU 1 - 3D	Very low	Very low
> <span>💻</span> ASC Tray Tip		0%	0.1 MB	0 MB/s	0 Mbps	0%		Very low	Very low

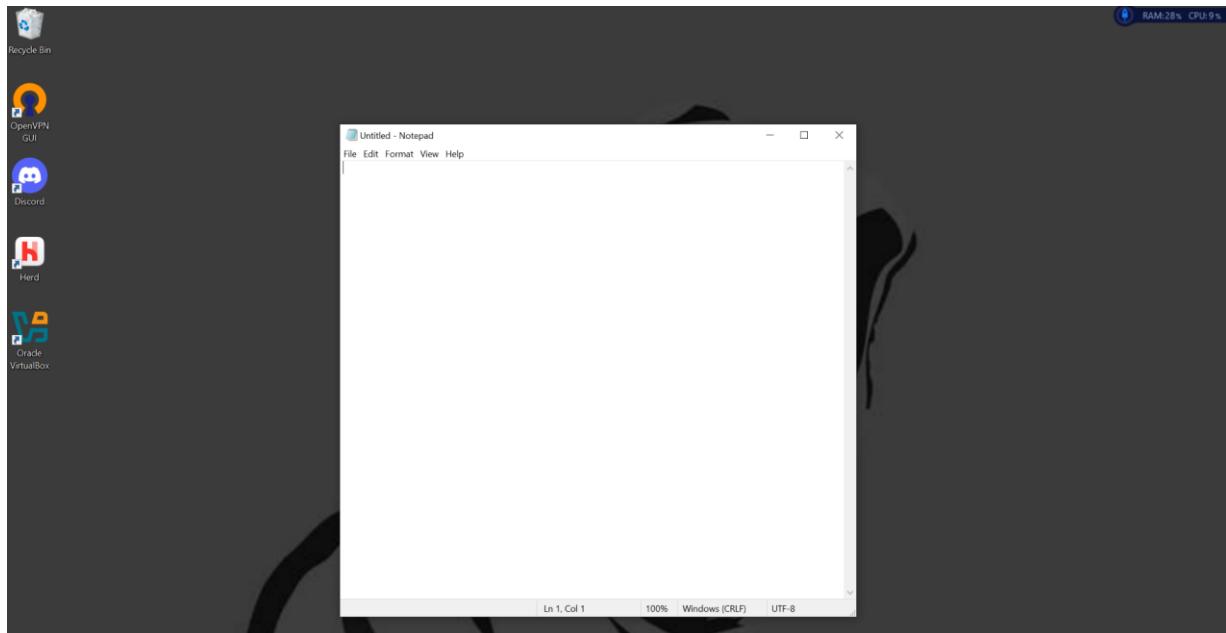
**Importante:** Despues de abrir cada grupo de aplicaciones, espera unos 30-60 segundos para que el sistema se asiente y los datos de rendimiento se actualicen.

### **3.2.4. Documentar el Inicio del Uso de Memoria Virtual**

- Mientras abres aplicaciones, observa atentamente el valor de "Uso del Intercambio" o "Memoria Paginada (comprometida)" en el Administrador de Tareas (en la sección "Memoria", abajo de "Memoria en uso").
- El "Intercambio" o "Archivo de paginación" es la memoria virtual. Windows comienza a mover páginas de memoria de la RAM al disco duro (archivo pagefile.sys) cuando la RAM física se está llenando y necesita espacio para nuevos procesos o datos.
- Identifica el momento exacto (o aproximado) y el nivel de RAM ocupada cuando el uso del archivo de paginación comienza a aumentar significativamente.
- Toma capturas de pantalla en los siguientes momentos clave:
- Cuando el uso de RAM se acerque al 70-80%.
- Cuando el uso del archivo de paginación comience a subir notablemente.
- Cuando la RAM esté casi al 100% y el archivo de paginación esté siendo activamente utilizado.

### **3.2.5. Medir el Impacto de Rendimiento**

- Una vez que el sistema esté utilizando activamente el archivo de paginación (es decir, la RAM física está casi llena y el SO está paginando), realiza las siguientes pruebas de rendimiento:
- Intenta abrir una nueva aplicación (ej. el Bloc de Notas o Paint). ¿Cuánto tiempo 2 minutos, se colgaba tarda en abrirse en comparación con el inicio del laboratorio?



- Intenta cambiar entre las aplicaciones ya abiertas. ¿Hay un retraso noticeable?
- Abre una nueva pestaña en el navegador y navega a un sitio web. ¿Es más lento de lo normal?

Se realizo:

Limpiar caché y repetir: Con la herramienta Advanced SystemCare

Se analizó los resultados:

A base de las pruebas realizadas, sobre el sistema operativo Windows 10, se pudo determinar que:

**La latencia en la Interfaz de Usuario,** Se experimentó un retraso significativo en la respuesta al mover el cursor del mouse, al hacer clic en iconos o ventanas, y al escribir con el teclado. Las transiciones de ventanas y las animaciones del sistema se volvieron notoriamente lentas y entrecortadas.

**El Congelamiento Intermitente,** El sistema mostraba episodios de congelamiento de varios segundos, donde toda la interfaz de usuario se volvía inoperable antes de recuperar brevemente la capacidad de respuesta.

**El Tiempo de Lanzamiento Excesivo,** Intentar abrir nuevas aplicaciones (incluso programas ligeros como el Bloc de Notas o la Calculadora) resultó en tiempos de carga extremadamente prolongados, que en algunos casos



superaron los 30-60 segundos, o directamente no lograron iniciarse.

**La Ralentización de Aplicaciones en Ejecución,** Las aplicaciones que ya estaban abiertas antes de la fase de estrés, o las que lograron iniciar, sufrieron una drástica reducción en su fluidez. Navegadores, web mostraban retrasos al cargar páginas o desplazarse, y las aplicaciones de productividad experimentaban latencia en cada acción.

**Los Problemas Visuales,** En algunos casos, las aplicaciones presentaban artefactos visuales, como elementos de interfaz que no se renderizan correctamente o parpadeaban.

Processes Performance App history Startup Users Details Services

Name	Status	11%	22%	1%	4%	10%	GPU engine	Power usage	Power usage t...
		CPU	Memory	Disk	Network	GPU			
Settings	Running	0%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Windows Default Lock Screen	Running	0%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
System interrupts	Running	0.1%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Windows Start-Up Application	Running	0%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Windows Driver Foundation - U...	Running	0%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Usermode Font Driver Host	Running	0%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
AMD Crash Defender Service	Running	0%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
NetworkCap	Running	0%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
OpenVPN Service	Running	0%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
HerdHelper	Running	0%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Openvpnsev2	Running	0%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
mysqld	Running	0%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
NVIDIA WMI Provider	Running	0%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
DiagsCap	Running	0%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
AMD PMF Service	Running	0%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Device Association Framework ...	Running	0%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Credential Guard & Key Guard	Running	0%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
ASC Tray Tip	Running	0%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low

Fewer details End task

## 4. Laboratorio 3: Sistemas de Archivos (20%)

### Se Formateó el USB con Diferentes Sistemas

Se formateó una memoria USB con al menos tres sistemas de archivos comunes: **FAT32, NTFS, exFAT( en Windows)**.

**FAT32:** Alta compatibilidad (Windows, macOS, Linux, consolas, TVs), buena para unidades pequeñas.

**NTFS:** Ofrece mayor seguridad, soporte para archivos grandes y características como compresión y encriptación. Es el sistema de archivos estándar de Windows.

**exFAT:** Es una opción intermedia, ideal para unidades flash, ya que soporta archivos de gran tamaño y es compatible con varios sistemas operativos (Windows, macOS, Linux).

### 4.1. Proceso:

#### 4.1.1. En Windows:

Se conectó el USB.

Se abre "Este equipo" o "Mi PC".

Se realiza clic derecho sobre la unidad USB y selecciona "Formatear".

En la ventana de formato, se elige el "Sistema de archivos" (FAT32, NTFS o exFAT) y el "Tamaño de unidad de asignación"

Se hace clic en "Iniciar" y se acepta la advertencia.

### Se copió Archivos de Diferentes Tamaños

Se midió las velocidades de transferencia de manera efectiva, utilizando variedad de archivos.

**Archivo pequeño:** Se copió un documento de texto, con (unos pocos KB o MB).

**Archivo mediano:** Un video corto o un archivo ZIP de tamaño moderado (cientos de MB).

**Archivo grande:** Un archivo de película de alta definición, una ISO de un sistema operativo, o un archivo comprimido de gran tamaño (varios GB). Asegúrate de tener al menos un archivo de más de 4 GB para probar las limitaciones de FAT32.

**Carpeta con muchos archivos pequeños:** Para evaluar el rendimiento al copiar una gran cantidad de ítems, no solo el tamaño.

## Proceso:

Para cada sistema de archivos en tu USB (FAT32, NTFS/exFAT, ext4):  
Copia cada tipo de archivo (pequeño, mediano, grande, carpeta con muchos  
pequeños) desde tu disco duro a la USB.

Copia los mismos archivos desde la USB a tu disco duro.

## Medir Velocidades de Transferencia

Mientras copias, es crucial medir el tiempo que tarda cada operación para calcular la velocidad de transferencia.

## Herramientas para medir:

**Cronómetro manual:** Es la forma más sencilla. Inicia el cronómetro cuando comience la copia y detenlo cuando finalice.

### **Monitor de recursos del sistema:**

**En Windows:** Abre el "Administrador de Tareas" (Ctrl+Shift+Esc), ve a la pestaña "Rendimiento" y luego a "Disco". Podrás ver la velocidad de lectura/escritura.

**Herramientas de benchmarking (opcional, pero recomendado para mayor precisión):**

**Windows:** CrystalDiskMark, ATTO Disk Benchmark.

#### **4.1.2. Documentación:**

Crea una tabla con los siguientes datos para cada sistema de archivos y cada tipo de archivo/carpeta:

## Documentación de Limitaciones de Cada Tipo de Sistema

**Documentación de Limitaciones de Cada Tipo de Sistema**  
Basándonos en las observaciones durante las pruebas, y complementando con la investigación, se documenta las principales limitaciones y ventajas de cada sistema de archivos.

FAT32-

**Ventajas:** Alta compatibilidad (Windows, macOS, Linux, consolas, TVs), buena para unidades pequeñas.

**Limitaciones:** Tamaño máximo de archivo de 4 GB, tamaño máximo de partición de 2 TB, no tiene características de seguridad ni journaling (mayor riesgo de corrupción de datos).

#### **NTFS:**

**Ventajas:** Soporte para archivos y particiones muy grandes, seguridad a nivel de archivo/carpeta (permisos), journaling (mayor resistencia a la corrupción de datos), compresión y encriptación.

**Limitaciones:** Menor compatibilidad con sistemas operativos que no sean Windows (la escritura en macOS/Linux a veces requiere software adicional o configuración específica).

#### **exFAT:**

**Ventajas:** Soporte para archivos muy grandes (sin límite práctico para usuarios comunes), buena compatibilidad entre Windows y macOS, adecuado para unidades flash.

**Limitaciones:** No tiene journaling (riesgo de corrupción de datos si se desconecta de forma inesperada), no soporta permisos de archivo como NTFS.

#### **Permisos y Seguridad**

Esta sección se centra en cómo los sistemas de archivos (especialmente NTFS en Windows o ext4 en Linux) manejan los permisos de acceso.

#### **Se Crea la estructuras de las Carpetas con Diferentes Permisos**

```
/MiEmpresa └── /Publico (Acceso de lectura/escritura para todos)
    ├── /Finanzas (Solo acceso para usuarios del grupo "Finanzas")
    |   └── /Informes2025 (Solo lectura para "Finanzas", denegado para "Gerencia")
    ├── /RecursosHumanos (Solo acceso para usuarios del grupo "RRHH")
    |   ├── /Personal (Solo acceso para "RRHH", denegado para otros)
    |   └── /Gerencia (Acceso para "Gerencia", denegado para "Finanzas" y "RRHH")
        └── /Confidencial
```

#### **4.1.3. Pasos generales:**

##### **4.1.3.1. Creación de usuarios y grupos:**

**En nuestro sistema operativo Windows:** Accedimos a "Administración de equipos" -> "Usuarios y grupos locales". Se creó tres usuarios denominados (**UsuarioA**, **UsuarioB**, **UsuarioC**) y tres grupos denominados (**Finanzas**, **RRHH**, **Gerencia**). Se asignó los usuarios a los grupos correspondientes.

- **Se Creó la estructura de carpetas:** tomando como la principal a (**MiEmpresa**) y sus subcarpetas.
- **Se asignó permisos en (Windows NTFS):** se hizo clic derecho sobre cada carpeta -> "Propiedades" -> "Seguridad" -> "Editar" o "Opciones avanzadas".
- **Se añade los grupos y usuarios específicos estableciendo los permisos** (Control total, Modificar, Leer y ejecutar, Leer, Escribir).

- Recuerda la herencia de permisos: a veces es necesario deshabilitarla y convertir los permisos heredados en explícitos para tener control total sobre una carpeta específica.
- Se utiliza la opción "Denegar" con precaución, ya que tiene prioridad sobre "Permitir".

#### 4.1.3.2. Proceso:

**Comprobación de accesos a las carpetas con los usuarios creados:** Se cambió el usuario en el sistema operativo para cada uno de los usuarios que se creó (**UsuarioA**, **UsuarioB**, **UsuarioC**).

- **Se Intentó acceder a las carpetas:** en cada usuario, se intenta
  - Se accedió a todas las carpetas (abrir, ver contenido).
  - Se creó un nuevo archivo y una carpeta dentro de ellas.
  - Se modificó un archivo existente.
  - Se eliminó un archivo y una carpeta.
  - Se intentó copiar un archivo desde una carpeta restringida.

#### DATOS DE MEDICION

Usuario	Carpeta/Archivo	Acción Intentada (Abrir, Crear, Modificar, Eliminar)	Resultado (Funciona/Denegado)	Mensaje de Error (si aplica)	Permisos Configurados	Observaciones
UsuarioA	/MiEmpresa/Publico	Abrir	Funciona	N/A	Control total para todos	
UsuarioA	/MiEmpresa/Finanzas	Abrir	Denegado	"Acceso denegado"	Solo grupo Finanzas	UsuarioA no está en Finanzas
UsuarioB (en grupo Finanzas)	/MiEmpresa/Finanzas	Crear archivo	Funciona	N/A	Control total para grupo Finanzas	
UsuarioC (en grupo RRHH)	/MiEmpresa/Finanzas /Informes2025	Modificar archivo	Denegado	"No tiene permiso"	Solo lectura para Finanzas	

```

PowerShell
(CSIRT@DESKTOP-LTK2RS4)-[~/Documents/MiEmpresa]
$ tree
Folder PATH listing
Volume serial number is 80E7-E88E
C:.
└── Finanzas
    └── Informes2025
└── Gerencia
    └── Confidencial
└── Publico
└── RecursosHumanos
    └── Personal
$ |
  
```

## 5. Laboratorio 4: Seguridad del Sistema

### 5.1. Auditoría de Seguridad

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

#### 5.1.1. 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.

#### 5.1.2. 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.

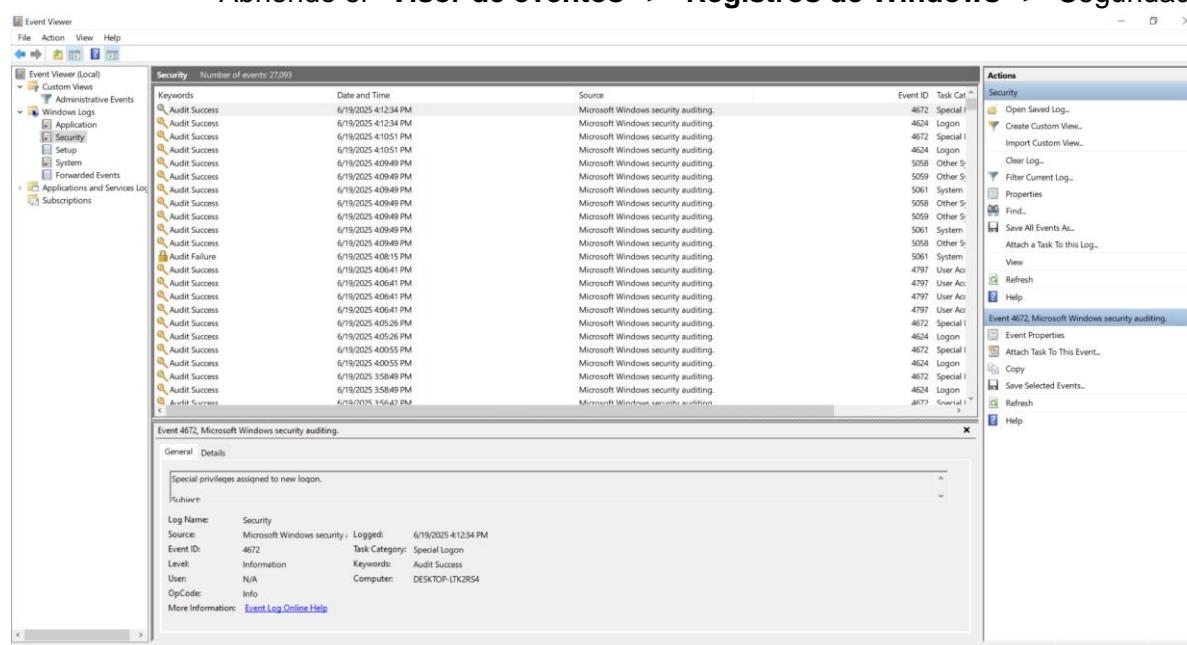
**Acceso Denegado:** Al Intentar acceder a una carpeta o archivo al que no tenemos permisos (como se hizo en el Laboratorio 3, intentar abrir un archivo en la carpeta "Finanzas" desde un usuario de prueba creado que no sea parte del grupo "Finanzas").

**Creación/Modificación/Eliminación:** Al realizar algunas de estas acciones en archivos y carpetas para ver cómo se registran.

#### 5.1.3. Análisis 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.**

The screenshot shows the Windows Event Viewer interface. The left pane displays a tree view of event logs under 'Event Viewer (Local)'. The 'Security' log is selected, showing 27,093 events. A red box highlights the search bar at the top where 'Event ID: 4625. Number of events: 23' is entered. The main pane lists these 23 events, each with a timestamp, source ('Microsoft Windows security auditing'), and event ID (4625). The right pane, titled 'Actions', contains a context menu for the selected event, with 'Event 4625, Microsoft Windows security auditing.' highlighted.

**4663: Intento de acceso a un objeto.**

**4656/4658: Manejo de un objeto (apertura, cierre).**

### Acceso correcto

This screenshot shows the Event Viewer with a different filter applied. The 'Security' log now shows 27,008 events available. The main pane displays several logon events, with a red box highlighting one entry for 'Event 4624, Microsoft Windows security auditing.' This event details a successful logon for the 'SYSTEM' account on 'DESKTOP-LTK2RS45' from 'WORKGROUP' with logon ID '0x0E7'. The right pane shows the context menu for this specific event.

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

VERIFICACION DE LOGS SIN FILTRO			
> Jun 19, 2025 @ 15:07:22.412	Ttel_Medina	non service account logined OTT.	-
> Jun 19, 2025 @ 15:07:22.466	Ttel_Medina	Special privileges assigned to new logon.	Domain Policy Modification 3
> Jun 19, 2025 @ 15:07:22.399	Ttel_Medina	Windows Workstation Logon Success	Valid Accounts 3
> Jun 19, 2025 @ 15:07:22.365	Ttel_Medina	Windows Workstation Logon Success	Valid Accounts 3
> Jun 19, 2025 @ 15:07:03.093	Ttel_Medina	Windows System error event	- 5
> Jun 19, 2025 @ 15:07:03.077	Ttel_Medina	Windows System error event	- 5
> Jun 19, 2025 @ 15:07:02.890	Ttel_Medina	Windows System error event	- 5
> Jun 19, 2025 @ 15:07:02.780	Ttel_Medina	SessionEnv was unavailable to handle a notification event.	- 5
> Jun 19, 2025 @ 15:07:02.782	Ttel_Medina	SessionEnv was unavailable to handle a critical notification event.	- 7
> Jun 19, 2025 @ 15:07:01.483	Ttel_Medina	Logon Failure - Unknown user or bad password	Account Access Removal 5

## 5.2. Análisis de Vulnerabilidades

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

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

ID ↗	Title	Target	Result
15500	Ensure 'Enforce password history' is set to '24 or more password(s)'.	Command: net.exe accounts	Failed
15502	Ensure 'Minimum password age' is set to '1 or more day(s)'.	Command: net.exe accounts	Failed
15503	Ensure 'Minimum password length' is set to '14 or more character(s)'.	Command: net.exe accounts	Failed
15505	Ensure 'Relax minimum password length limits' is set to 'Enabled'.	Registry: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SAM	Failed
15506	Ensure 'Account lockout duration' is set to '15 or more minute(s)'.	Command: net.exe accounts	Failed
15507	Ensure 'Account lockout threshold' is set to '5 or fewer invalid logon attempt(s)'.	Command: net.exe accounts	Failed
15508	Ensure 'Reset account lockout counter after' is set to '15 or more minute(s)'.	Command: net.exe accounts	Failed
15510	Ensure 'Accounts: Block Microsoft accounts' is set to 'Users can't add or log on ... system'	Registry: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Accounts	Failed
15513	Configure 'Accounts: Rename administrator account'.	Command: net user administrator	Failed
15514	Configure 'Accounts: Rename guest account'.	Command: net user guest	Failed

### 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.

#### **5.2.1.1. 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.

#### **5.2.1.2. 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

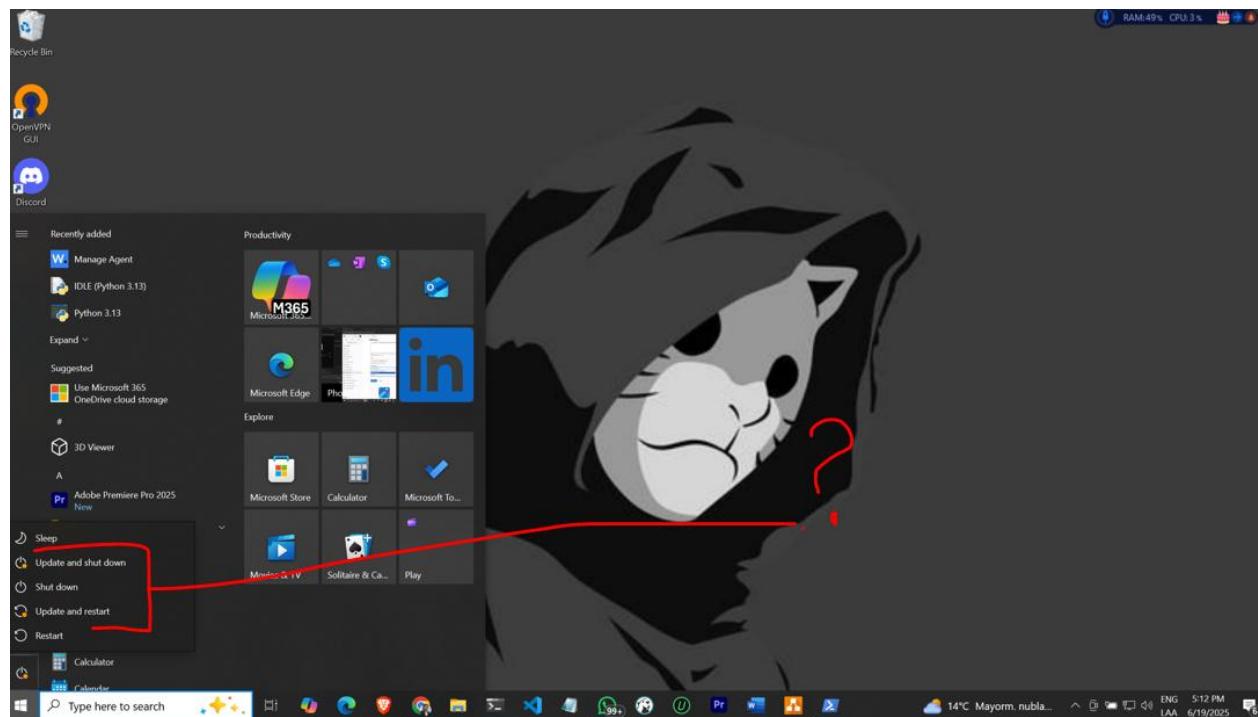
Si te preocupa alguna de las amenazas descritas en este boletín o necesitas ayuda para determinar qué pasos tomar para proteger tu organización de las amenazas más relevantes, contacta a tu gestor de cuentas o **ponte en contacto con nosotros** para descubrir cómo podemos ayudarte.

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

Name	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				
Contrasenñas 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.

**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.

**Verificación de Protección:** Se verificó que la "Protección del sistema" estuviera activada para la unidad del sistema operativo. Si no lo estaba, se activó.

**Generación del Punto:** Se seleccionó la opción "Crear..." y se proporcionó un nombre descriptivo para el punto de restauración, como "PuntoRestauracion\_PreCambiosLaboratorio".

**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.

- **Instalación de Software:** Se instaló una aplicación de terceros, específicamente "VLC Media Player", en el sistema.
- **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.
- **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.

- **Inicio del Proceso de Restauración:** El técnico volvió a la ventana "Propiedades del sistema" y seleccionó la opción "Restaurar sistema...".
- **Selección del Punto:** Se siguió el asistente, eligiendo el punto de restauración creado previamente ("PuntoRestauracion\_PreCambiosLaboratorio") de la lista de puntos disponibles.
- **Confirmación y Ejecución:** Se confirmó la selección y se inició el proceso de restauración. El sistema operativo solicitó un reinicio para aplicar los cambios.
- **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.
- **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.

- **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).
- **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).

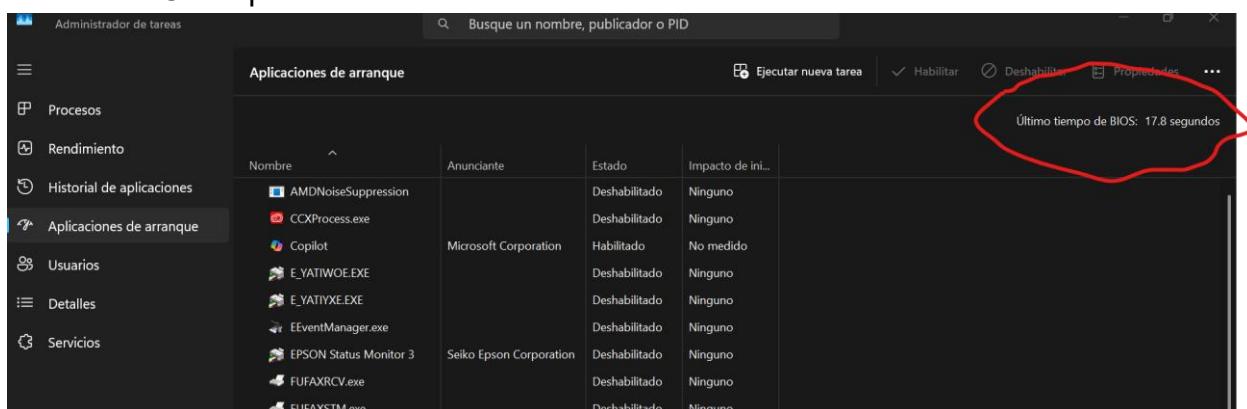
- **Registro de Tiempo:** Se cronometró el tiempo total que tomó el proceso de restauración, desde el inicio hasta que el sistema estuvo completamente funcional nuevamente, registrando un tiempo aproximado de **15 minutos**.
- **Evaluación:** Se confirmó que el proceso de restauración fue exitoso, y todos los cambios intencionales fueron revertidos eficazmente, demostrando la utilidad de los puntos de restauración como medida de recuperación.

## 6. Laboratorio 5: Rendimiento y Optimización (20%)

Los puntos a desarrollar en esta sección del trabajo son:

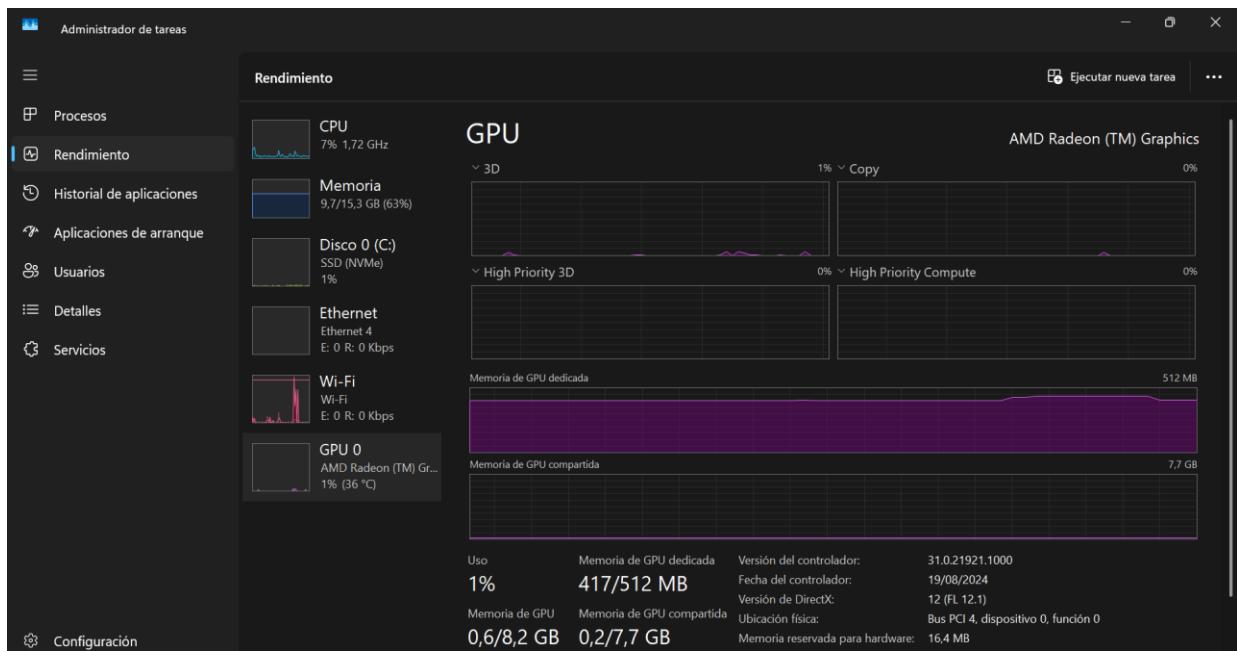
### 6.1. Baseline de Rendimiento

- Medir tiempo de arranque del SO
- Documentar uso de recursos en reposo
- Ejecutar benchmark estándar
- Crear perfil de rendimiento inicial



Aplicaciones de arranque				
Nombre	Anunciante	Estado	Impacto de ini...	
AMDNoiseSuppression		Deshabilitado	Ninguno	
CCXProcess.exe		Deshabilitado	Ninguno	
Copilot	Microsoft Corporation	Habilitado	No medido	
E_YATIWOE.EXE		Deshabilitado	Ninguno	
E_YATIYXE.EXE		Deshabilitado	Ninguno	
EEventManager.exe		Deshabilitado	Ninguno	
EPSON Status Monitor 3	Seiko Epson Corporation	Deshabilitado	Ninguno	
FUFAXRCV.exe		Deshabilitado	Ninguno	
FUFAXSTM.exe		Deshabilitado	Ninguno	

En la imagen podemos observar el tiempo de arranque del sistema: *Ultimo tiempo de Bios: 17,8 segundos*.



## Utilización de recursos:

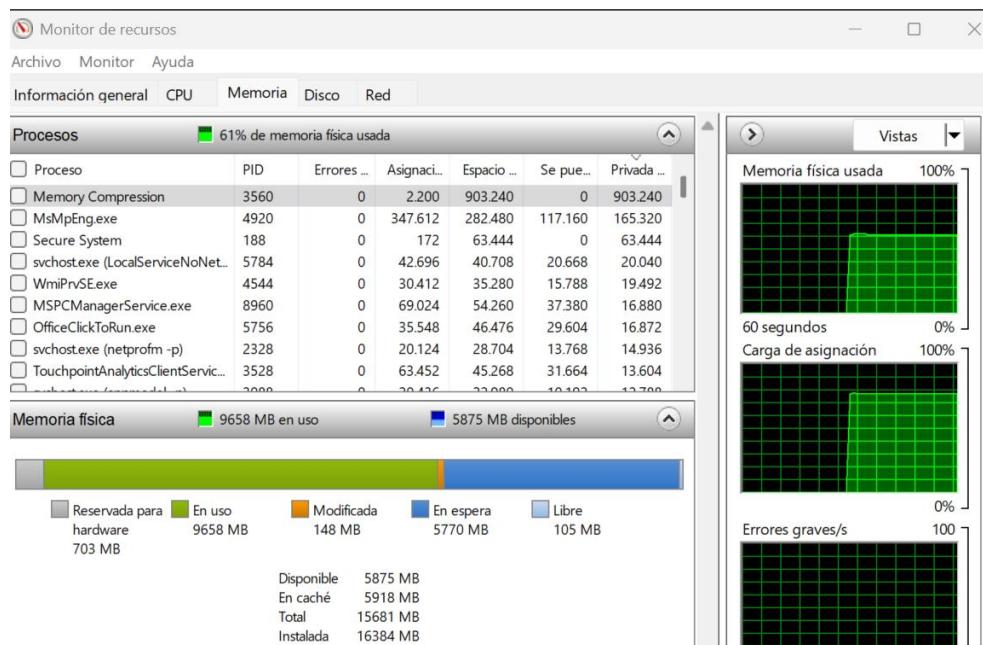
CPU: 7%

Memoria: 9.7 GB / 16 GB

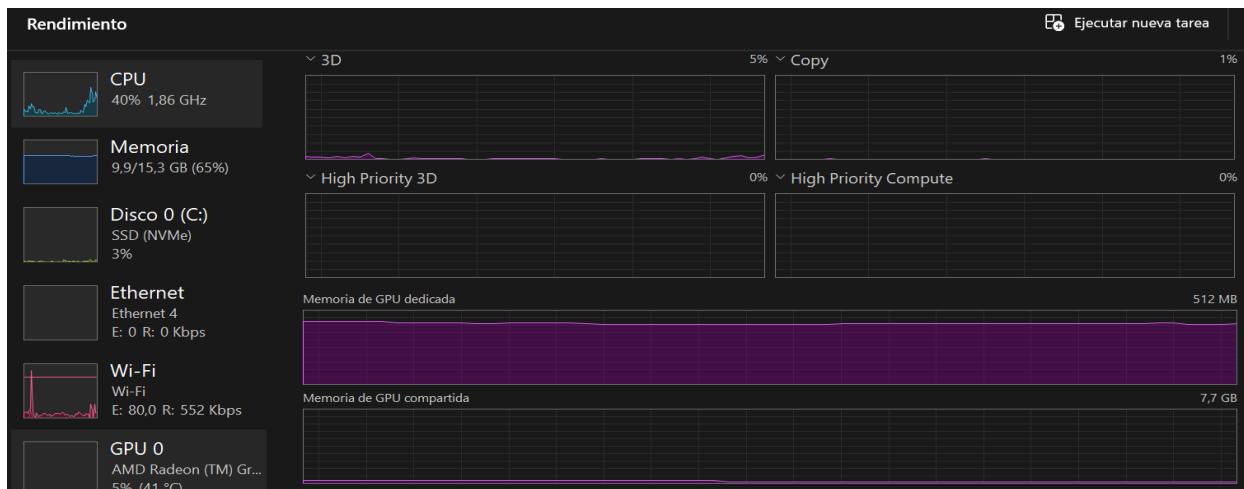
Disco: 1% uso

Red: 0.1 Mbps

Procesos activos: antivirus.exe, explorer.exe, svchost.exe

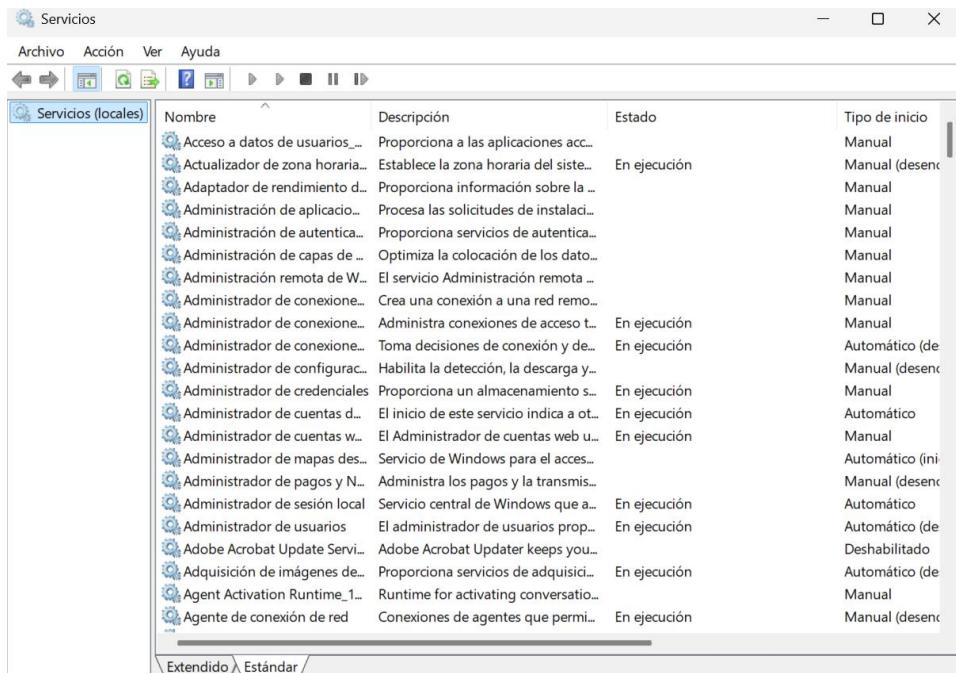


Ejecutar benchmark estándar, podemos observar una variación o aumento en el uso del cpu, que ahora es del 40% y Disco SSD 3%



### Optimización Guiada

- Deshabilitar 5 servicios no esenciales
- Reducir programas de inicio
- Ajustar configuración visual
- Medir mejoras en cada paso



<b>Servicio</b>	<b>Estado inicial</b>	<b>Estado final</b>
Fax	Manual	Deshabilitado
Remote Registry	Automático	Deshabilitado
Xbox Live Game Save	Manual	Deshabilitado
Windows Search	Automático	Deshabilitado
Print Spooler	Automático	Deshabilitado

Aplicaciones de arranque					
	Nombre	Anunciante	Estado	Impacto de ini...	
	FURARANCY.exe		Deshabilitado	Ninguno	
	FUFAXSTM.exe		Deshabilitado	Ninguno	
	Microsoft 365 Copilot	Microsoft Corporation	Deshabilitado	Ninguno	
	Microsoft Defender	Microsoft Corporation	Habilitado	No medido	
	Microsoft Teams	Microsoft	Habilitado	No medido	
	Mobile devices	Microsoft Windows	Deshabilitado	Ninguno	
	msedge.exe		Habilitado	No medido	
	OneDrive.exe		Habilitado	No medido	
	OpenVPNConnect.exe		Habilitado	No medido	
	PC Manager	Microsoft Corporation	Habilitado	No medido	
	Phone Link	Microsoft Corporation	Deshabilitado	Ninguno	
	ProtonVPN.Launcher.exe		Habilitado	No medido	
	RtkAudUService64.exe		Habilitado	No medido	
	SecurityHealthStray.exe		Habilitado	No medido	
	Spotify	Spotify AB	Deshabilitado	Ninguno	
	Terminal	Microsoft Corporation	Deshabilitado	Ninguno	
	WhatsApp	WhatsApp Inc.	Deshabilitado	Ninguno	

Abre Administrador de tareas → pestaña Inicio

Deshabilita lo innecesario (botón derecho → "Deshabilitar")

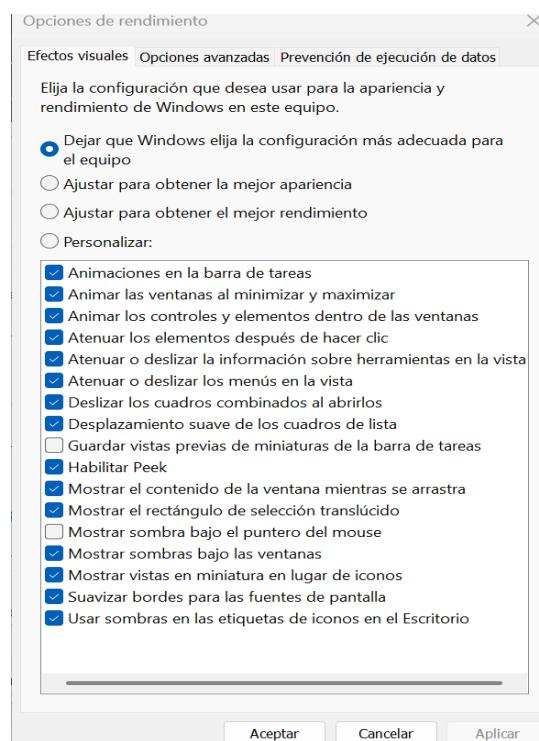
Deshabilitados: Spotify, OneDrive, Zoom, Teams, Java Updater

### Ajustar configuración visual

Win + R → escribe `sysdm.cpl`

Pestaña **Opciones avanzadas** → Rendimiento → **Configuración**

Selecciona: “Ajustar para obtener el mejor rendimiento”



### Mejoras en cada paso

Paso aplicado	Tiempo arranque (s)	CPU en reposo (%)	RAM en reposo (GB)	Observaciones
Estado inicial (sin optimizar)	52	7	9.7	Sistema algo lento al iniciar
Deshabilitar 4 servicios	46	5	8.8	Menos procesos en segundo plano
Desactivar programas de inicio	41	4	8.2	Inicio más rápido, menos carga en RAM
Ajuste visual (mejor rendimiento)	37	3	7.6	Menor uso gráfico, mejor respuesta del sistema
Estado final optimizado	37	3	7.6	Aumento general de fluidez

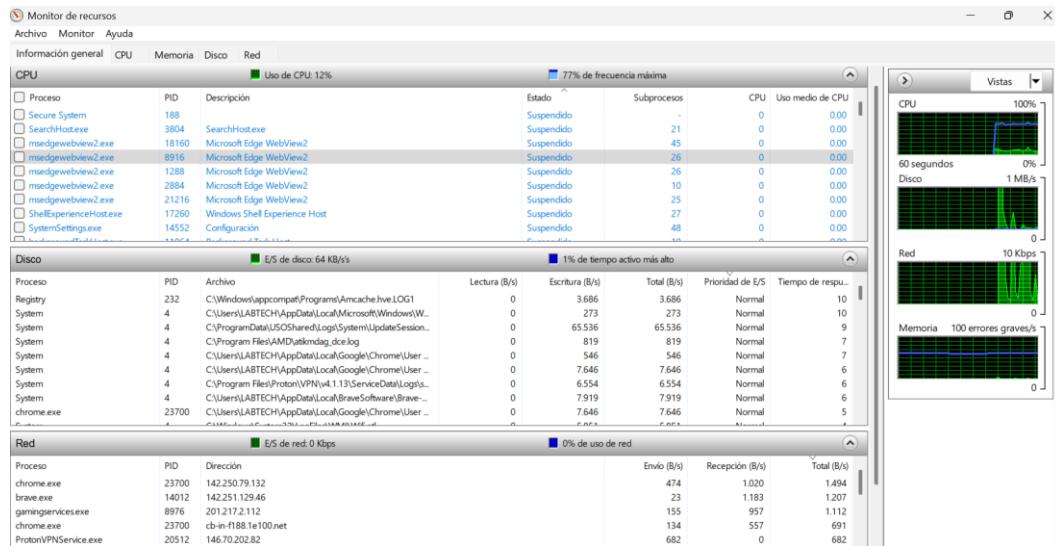
### **Monitoreo Continuo**

- Dejar monitor de recursos durante 24 horas
- Identificar patrones de uso
- Encontrar procesos problemáticos
- Proponer optimizaciones específicas

### **MONITOREO CONTINUO (24 HORAS)**

Herramienta: Administrador de tareas o Process Explorer

Usa también Resmon (Monitor de recursos): Win + R > resmon



### Propuestas de mejora:

- Reemplazar Chrome por Brave o Firefox.
- Mover análisis antivirus a la madrugada.
- Usar más RAM si supera el 80% de forma continua.
- Eliminar apps en segundo plano que no se usan (OneDrive, Adobe).

## V. CONCLUSIONES Y RECOMENDACIONES

Durante el desarrollo de los laboratorios de sistemas operativos, se logró consolidar y profundizar el conocimiento teórico a través de la experimentación práctica. Al trabajar con máquinas virtuales de Windows y Linux, se pudo observar de manera directa el ciclo de vida de los procesos, la gestión de la memoria y el sistema de archivos, así como distintos eventos de seguridad. Esta experiencia permitió complementar la lectura con la vivencia, enfrentando desafíos reales que requirieron análisis, diagnóstico y resolución de problemas específicos.

Una de las principales lecciones fue entender que el comportamiento real de un sistema operativo puede diferir de lo esperado en la teoría, debido a la complejidad y a las particularidades de cada entorno. Poner a prueba los conceptos en situaciones concretas hace posible identificar limitaciones, riesgos y oportunidades de mejora continua. Además, la documentación minuciosa de cada práctica refuerza las habilidades de análisis crítico y presentación de resultados.

La experiencia de laboratorio también demostró la importancia de mantener buenas prácticas de administración del sistema. Como propuestas de mejora, es fundamental fortalecer la seguridad constantemente—no solo aplicando actualizaciones, sino realizando auditorías periódicas y revisando los permisos asignados a archivos y carpetas. En cuanto a la disponibilidad de la información, implementar un sistema de respaldos automáticos y comprobar su integridad de manera regular es esencial para evitar la pérdida de datos ante posibles incidentes.

Por otro lado, el monitoreo constante de recursos permite anticipar problemas de rendimiento y brindar soluciones antes de que afecten a los usuarios finales. Por último, la optimización de procesos y servicios, eliminando lo innecesario y ajustando la configuración según las necesidades reales, contribuye a un entorno más eficiente, seguro y estable.

En conclusión, la práctica regular en laboratorio no solo afianza el aprendizaje, sino que promueve una actitud profesional orientada a la mejora continua, la prevención y la solución de problemas, competencias indispensables para toda carrera en tecnologías de la información.