CIPFP Mislata

Luis García Bonifaz - l.garciabonifaz@edu.gva.es

SOM T06 - Administración Windows

Actividad 1

Actividad: Auditoría, administración y optimización de un equipo Windows

Contexto (escenario)

Eres el/la técnico/a de una microempresa (8–12 empleados) que ha detectado:

- Usuarios que comparten contraseñas.
- Equipos lentos al arrancar y durante el uso.
- Dudas sobre qué servicios/procesos consumen recursos.
- Necesidad de compartir una carpeta en red con permisos correctos.
- Errores intermitentes (cuelgues) sin causa aparente.

Tu misión será **administrar usuarios**, **mejorar seguridad**, **diagnosticar rendimiento**, **revisar eventos**, **optimizar el sistema** y **configurar compartición en red**.

> **Trabajo recomendado:** parejas (técnico/a A y técnico/a B).
> **Duración recomendada:** 6–8 horas (2–3 sesiones).
> **Requisito:** Windows 10/11 Pro o Enterprise (para `gpedit.msc`). Si no hay Pro, se adapta usando comandos e interfaz donde se pueda.

1) Objetivos de aprendizaje

Al terminar, el alumnado será capaz de:

1. Crear y gestionar **usuarios y grupos locales** desde GUI y desde línea de comandos (CMD/PowerShell).
2. Aplicar **políticas de contraseñas** y **bloqueo de cuenta** (seguridad básica).
3. Identificar procesos problemáticos con **Administrador de tareas** y **Monitor de recursos**.
4. Comprender y gestionar **servicios**, tipos de inicio y **dependencias**.
5. Ajustar/explicar **memoria virtual (pagefile)** y valorar “optimizers” de RAM.
6. Analizar el sistema con **Visor de eventos** y **Monitor de rendimiento**.
7. Aplicar optimización básica de almacenamiento (**TRIM/Desfragmentación + Limpieza de disco**) con criterio.

8. Configurar **carpetas compartidas** y justificar el acceso final (Compartición vs NTFS).
9. Obtener información del sistema con **ipconfig/systeminfo/tasklist** y usar el **Registro** con precaución (consulta y backup).
10. Documentar una auditoría técnica clara y reproducible.

2) Materiales y preparación

- 1 PC o VM por pareja (ideal).
- Cuenta con privilegios de **administrador**.
- Red local o red virtual (para pruebas de compartición).
- Carpeta "EVIDENCIAS" en el Escritorio para capturas y logs.

Normas de seguridad del aula (muy importante)

- No modificar el Registro salvo para **consultar** o con **copia de seguridad previa**.
- No deshabilitar servicios "a ciegas": justificar y registrar cambios.
- Si se cambia configuración (servicios, pagefile, políticas), anotar "antes/después".

---

3) Entregables (lo que entregan)

1. **Informe técnico (PDF o DOCX)** con capturas y conclusiones.
2. **Script PowerShell** (o comandos anotados) usados para gestionar usuarios/grupos.
3. Evidencias:
   - Capturas de `eventvwr.msc`, `perfmon.msc`, `services.msc`, `resmon.exe`
   - Salidas de `ipconfig /all`, `systeminfo`, `tasklist /svc`
4. Tabla final de permisos de la carpeta compartida (quién puede qué y por qué).

---

4) Evaluación (rúbrica sugerida /100)

- **Usuarios y grupos (20 pts):** creación, grupos, membresía, evidencia.
- **Seguridad (20 pts):** políticas de contraseña + bloqueo + pruebas documentadas.
- **Procesos y rendimiento (20 pts):** diagnóstico razonado con tareas/resmon/perfmon.
- **Servicios (15 pts):** cambios justificados + dependencias entendidas.
- **Eventos y logs (15 pts):** filtros, IDs/orígenes, explicación de hallazgos.
- **Compartición y permisos (10 pts):** coherencia "más restrictivo prevalece" + pruebas.

---

5) Desarrollo por fases (guía paso a paso)

FASE A — Identidad y control del equipo: usuarios y grupos (1,5–2 h)

A1. Inventario inicial

1. Ejecuta y captura:
   - `winver`
   - `systeminfo`
2. Lista usuarios locales:
   - GUI: `compmgmt.msc` → Usuarios y grupos locales
   - PowerShell: `Get-LocalUser`

Evidencia: captura o salida de comandos.

A2. Creación de estructura de empresa

Crea estas cuentas locales:

- `admin_soporte` (administrador)
- `empleado1` (estándar)
- `empleado2` (estándar)
- `invitado_temp` (estándar, luego deshabilitar)

Crea estos grupos locales:

- `GG_Soporte`
- `GG_Oficina`

Asigna:

- `admin_soporte` → `Administradores` + `GG_Soporte`
- `empleado1` y `empleado2` → `Usuarios` + `GG_Oficina`
- `invitado_temp` → `GG_Oficina` y después **deshabilitar**

Obligatorio (PowerShell): al menos una parte debe hacerse con cmdlets.
Ejemplos de acciones que deben aparecer en evidencias:

- `New-LocalUser`, `New-LocalGroup`
- `Add-LocalGroupMember`
- `Disable-LocalUser`
- `Get-LocalUser`, `Get-LocalGroup`

Evidencias mínimas:

- Captura de los usuarios creados.
- Captura de membresía de grupos o salida del comando.

A3. Comprobación con CMD (extra de robustez)

Usa (y documenta) al menos:

- `net user`
- `net localgroup`

Mini-preguntas (informe)

- ¿Qué ventajas tiene gestionar permisos por grupos y no por usuario?
- ¿Por qué la cuenta Administrador debe usarse “con precaución”?

FASE B — Seguridad: contraseñas y bloqueo (1–1,5 h)

B1. Configura directiva de contraseñas

En `gpedit.msc`, configura (propuesta):

- Complejidad: **habilitada**
- Longitud mínima: **10**
- Vigencia máxima: **90 días**
- Historial: **5**

Evidencia: captura de la ruta completa y los valores.

B2. Configura bloqueo de cuenta

Configura (propuesta):

- Umbral: **5 intentos**
- Duración: **30 min**
- Restablecer contador: **30 min**

Prueba obligatoria

1. Intenta iniciar sesión con `empleado1` y contraseña incorrecta hasta bloquearlo.
2. Documenta qué ocurre y cómo lo detectas.

Mini-preguntas

- Explica con tus palabras qué ataque reduce el bloqueo de cuenta.
- Propón una alternativa moderna: ¿qué aporta MFA?

FASE C — Diagnóstico de rendimiento: procesos y recursos (1–1,5 h)

C1. Administrador de tareas: análisis guiado

1. Abre el Administrador de tareas.
2. Identifica:
    - Top 3 procesos por CPU
    - Top 3 por Memoria
    - Top 3 por Disco (si aplica)

Acción práctica

- Cambia la **prioridad** de un proceso "de usuario" (por ejemplo, navegador) y describe el impacto esperado (sin usar "Tiempo real").

Evidencia: captura en pestañas Procesos/Rendimiento/Detalles.

C2. Monitor de recursos (`resmon.exe`)

Tareas:

- En CPU: filtra un proceso y mira hilos/uso.
- En Disco: identifica qué archivos está leyendo/escribiendo un proceso "pesado".
- En Red: identifica conexiones activas de un proceso (si hay).

Mini-pregunta

- ¿Qué aporta `resmon` frente al Administrador de tareas?

FASE D — Servicios: estabilidad, inicio y dependencias (1–1,5 h)

D1. Inspección de servicios

En `services.msc`:

1. Elige 3 servicios "bien conocidos" (por ejemplo: Windows Update, Cola de impresión, etc.).
2. Para cada uno, anota:
    - Estado
    - Tipo de inicio
    - Qué función cumple (explicación breve)

D2. Dependencias (obligatorio)

Elige 1 servicio con dependencias visibles:

- Captura la pestaña **Dependencias**
- Explica qué podría pasar si lo detienes.

D3. Cambio controlado (con criterio)

Realiza **un** cambio seguro:

- Cambiar un servicio no crítico a "Manual" o "Inicio retrasado"
- Reiniciar un servicio

Importante: justificar y documentar "antes/después".

FASE E — Memoria virtual y "optimización" realista (45–60 min)

E1. Pagefile (memoria virtual)

1. Localiza la configuración de memoria virtual.
2. Documenta:

    - ¿Está gestionado por el sistema?
    - ¿En qué unidad está?
3. Decide (y justifica) una de estas opciones:
    - Mantener automático (recomendado en la mayoría de casos)
    - Establecer tamaño personalizado (si justificas el escenario)

Mini-preguntas

- ¿Para qué sirve `pagefile.sys`?
- ¿Por qué en SSD se recomienda no obsesionarse con "ajustes agresivos" del pagefile?

E2. Debate técnico corto (en el informe)

- Explica por qué muchos "optimizadores de RAM" pueden ser inútiles o contraproducentes.

FASE F — Auditoría: Visor de eventos y Monitor de rendimiento (1,5–2 h)

F1. Visor de eventos (`eventvwr.msc`)

Tareas obligatorias:

1. En **Sistema**, filtra por:
    - Nivel: Error y Advertencia
    - Rango temporal: "últimas 24 h" (o desde el arranque)
2. Identifica:
    - 2 errores recurrentes o relevantes
    - 2 advertencias relevantes
3. En **Seguridad**, busca:
    - intentos fallidos/exitosos de inicio de sesión (relacionado con la fase de bloqueo)

Evidencia: capturas de filtros y eventos seleccionados.

F2. Monitor de rendimiento (`perfmon.msc`)

1. Añade contadores:
    - CPU
    - Memoria disponible
    - Actividad de disco (básico)
2. Crea un **Conjunto de recopiladores de datos**:
    - duración 3–5 minutos mientras abres varias apps
3. Extrae una conclusión:
    - ¿Dónde estuvo el cuello de botella?

Evidencia: captura del conjunto y de la gráfica/resultados.

FASE G — Optimización de almacenamiento (sin particionado) (45–60 min)

> *Ojo:* aquí **NO** se toca el Administrador de discos ni particiones (eso era del apartado 2).

G1. Optimizar unidades

1. Abre "Desfragmentar y optimizar unidades".
2. Identifica si la unidad es HDD o SSD.
3. Ejecuta:
   - HDD: desfragmentación (si procede)
   - SSD: optimización/TRIM (si procede)
4. Explica por qué **no** se debe desfragmentar un SSD.

G2. Limpieza de disco (`cleanmgr.exe`)

1. Ejecuta limpieza estándar.
2. Si procede, "Limpiar archivos del sistema" y explica qué has eliminado (con criterio).

FASE H — Recursos compartidos: permisos reales (1–1,5 h)

H1. Crear carpeta compartida

1. Crea `C:\Empresa\Compartida`
2. Comparte la carpeta por red y anota la ruta UNC: `\\EQUIPO\Compartida`

H2. Permisos de compartición vs permisos NTFS (obligatorio y clave)

Configura un caso donde se vea la "regla de oro":

- Permisos de compartición: `GG_Oficina` = Control total
- Permisos NTFS: `GG_Oficina` = Lectura

Prueba:

- Inicia sesión como `empleado1` e intenta crear/modificar archivos en la carpeta compartida desde la red.
- Documenta el resultado y explica por qué pasa (prevalece el más restrictivo).

H3. Mapear unidad de red

Mapea como `Z:` la carpeta compartida desde el usuario estándar.

Evidencias: capturas de permisos, prueba y unidad mapeada.

FASE I — Información del sistema y Registro (consulta segura) (45–60 min)

I1. Comandos obligatorios

Ejecuta y adjunta salida:

- `ipconfig /all`
- `tasklist /svc`
- `systeminfo`

Pregunta:

- ¿Qué comando te da más pistas si sospechas problemas de red?

I2. Registro (solo consulta + precaución)

1. Abre `regedit.exe`
2. Explica la diferencia entre HKLM y HKCU.
3. Realiza una **copia de seguridad** de una rama (exportar) **antes** de tocar nada.
4. Consulta una clave (sin modificar) y documenta qué información aporta.

Prohibido: cambios "porque sí".

---

6) Plantilla rápida para el informe (estructura sugerida)

1. **Portada** (nombre, curso, fecha, equipo/VM).
2. **Objetivo del trabajo** (5–6 líneas).
3. **Usuarios y grupos** (capturas + tabla de cuentas y grupos).
4. **Políticas de seguridad** (valores + prueba de bloqueo).
5. **Rendimiento** (tareas/resmon/perfmon: hallazgos).
6. **Servicios** (cambios y dependencias).
7. **Eventos** (errores/advertencias y explicación).
8. **Optimización** (TRIM/defrag según tipo + cleanmgr).
9. **Compartición** (tabla permisos compartición vs NTFS + prueba).
10. **Comandos y registro** (salidas + conclusiones).
11. **Conclusiones y recomendaciones** (5 bullets accionables).