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**.

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).

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.

4) Evaluación

- **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

A1. Inventario inicial

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

En el PDF:

- Captura de las ejecuciones de los programas
- Pantallazo del comanod de PowerShell

A2. Creación de estructura de empresa

Obligatorio en PowerShell:

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**

Entrega:

- Script 'CreacionEstructura.ps1 `

Mini-preguntas (en el PDF)

- ¿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

B1. Configura directiva de contraseñas

En `gpedit.msc`, configura:

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

en el PDF:

- Captura de la pantalla de `gpedit.msc` donde se vea la configuración.

B2. Configura bloqueo de cuenta

Configura:

- 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 en el PDF.

Mini-preguntas en el PDF

- 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

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").

En el PDF:

- 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 en el PDF

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

FASE D — Servicios: estabilidad, inicio y dependencias

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.

En el PDF

- Capturas de pantalla

D3. Cambio controlado (con criterio)

Realiza **un** cambio seguro:

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

En el PDF: justificar y documentar “antes/después”.

FASE E — Memoria virtual y “optimización” realista

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 en el PDF

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

E2. Debate técnico corto (en el PDF)

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

FASE F — Auditoría: Visor de eventos y Monitor de rendimiento

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)

En el PDF:

- 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?

En el PDF:

- Captura del conjunto y de la gráfica/resultados.

FASE G — Optimización de almacenamiento (sin particionado)

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. En el PDF 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 en el PDF explica qué has eliminado (con criterio).

FASE H — Recursos compartidos

Para realizar esta apartado hay que configurar la red de la máquina virtual en modo puente. De esta manera la maquina virtual el anfitrion estarán en la misma red. No es necesario apagar la máquina virtual para cambiar su configuración de red, se puede hacer en caliente.

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

Configura un caso donde se vea la “regla de oro”:

- Permisos de compartición: `GG_Oficina` = Control total

- Permisos NTFS: `GG_Oficina` = Lectura

Prueba:

- En la maquina anfitrion, en el explorador de archivos en el apartado de red actviva la detección de redes e intentar acceder al recurso compartido de la máquina virtual utilizando como credenciales:
-
- `empleado1`
- La contraseña que le hayas puesto

Un vez hayas accedido intenta crear/modificar archivos en la carpeta compartida.

En el PDF

- Documenta el resultado y explica por qué pasa.

H3. Mapear unidad de red

Mapea como `Z:` la carpeta compartida desde el equipo anfitrion.

En el PDF:

- Capturas de permisos, prueba y unidad mapeada.

FASE I — Información del sistema y Registro

I1. Comandos obligatorios

Ejecuta y adjunta salida:

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

Enel PDF:

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

I2. Registro (solo consulta + precaución)

1. Abre `regedit.exe`
2. Eneel PDF 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.