

Tarea 1 – Limpieza automatizada (Linux)

- Crear un script que limpie /tmp y comprima logs antiguos de /var/log con más de 7 días.
- Programar ejecución diaria usando *cron* o *systemd timer*.
- Registrar en log qué archivos se han eliminado o comprimido.

```
nano /usr/local/bin/limpieza.sh
```

```
GNU nano 6.2
#!/bin/bash
LOG_FILE="/var/log/limpieza_automatizada.log"
echo "--- Inicio de limpieza: $(date) ---" >> $LOG_FILE

# Limpiar /tmp (archivos de más de 1 día para evitar borrar archivos en uso)
find /tmp -type f -atime +1 -delete -print >> $LOG_FILE

# Comprimir logs de más de 7 días en /var/log
find /var/log -name "*.log" -mtime +7 -exec gzip {} \; -print >> $LOG_FILE

echo "--- Fin de limpieza ---" >> $LOG_FILE
```

Programación (Cron): Ejecutar crontab -e y añadir la línea para que corra cada día a las 00:00

```
0 0 * * * /bin/bash /usr/local/bin/limpieza.sh
```

```
0 0 * * * /bin/bash /usr/local/bin/limpieza.sh
```

Guardamos y salimos:

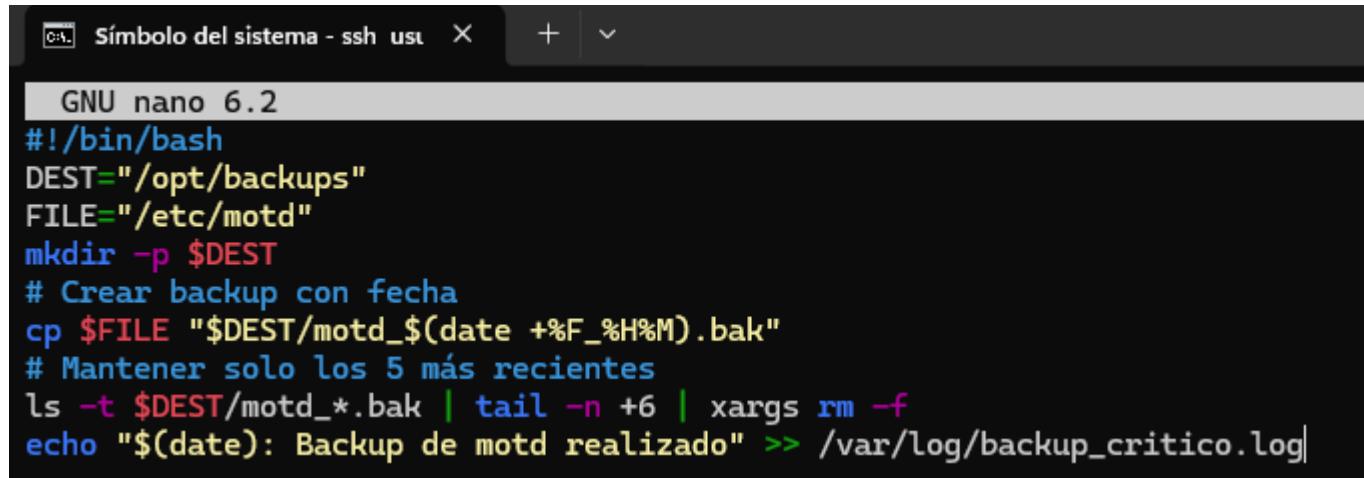
```
[root@server2asir usuario]$crontab -e
crontab: installing new crontab
```

Tarea 2 – Copias de seguridad de archivos críticos (Linux/Windows)

- Crear un script que haga backup de un archivo crítico en cada sistema:
 - Linux: /etc/motd
 - Windows: C:\Windows\System32\drivers\etc\hosts
- Guardar backups con fecha en el nombre.
- Conservar solo las últimas 5 copias y registrar logs de la operación.
- Programar ejecución diaria: Linux → cron/systemd timer, Windows → Task Scheduler.

En Linux (/etc/motd):

/usr/local/bin/backup_motd.sh



The screenshot shows a terminal window titled "Símbolo del sistema - ssh user". It displays a file named "GNU nano 6.2" containing a bash script. The script defines variables \$DEST and \$FILE, creates a directory \$DEST if it doesn't exist, creates a backup of \$FILE with a timestamp, keeps only the 5 most recent backups, and logs the backup completion to /var/log/backup_critico.log.

```
GNU nano 6.2
#!/bin/bash
DEST="/opt/backups"
FILE="/etc/motd"
mkdir -p $DEST
# Crear backup con fecha
cp $FILE "$DEST/motd_$(date +%F_%H%M).bak"
# Mantener solo los 5 más recientes
ls -t $DEST/motd_*.bak | tail -n +6 | xargs rm -f
echo "$(date): Backup de motd realizado" >> /var/log/backup_critico.log
```

Programación (Cron): Ejecutar crontab -e y añadir la línea para que corra cada día a las 00:00

0 0 * * * /usr/local/bin/backup_motd.sh

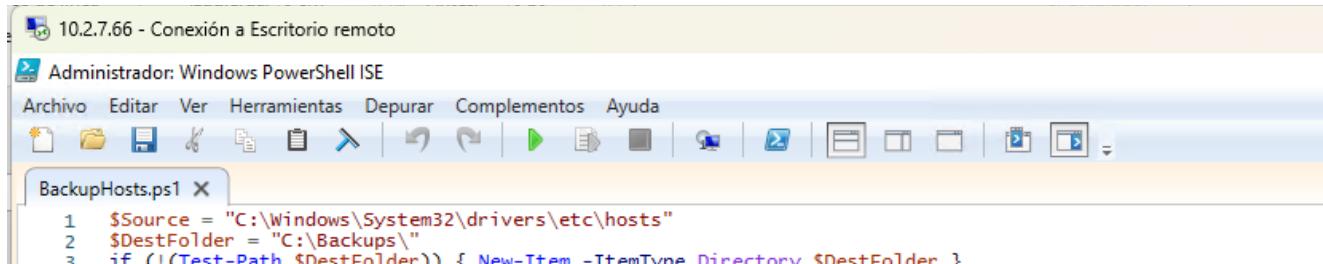
```
0 0 * * * /bin/bash /usr/local/bin/limpieza.sh
0 0 * * * /usr/local/bin/backup_motd.sh
```

Guardamos y salimos:

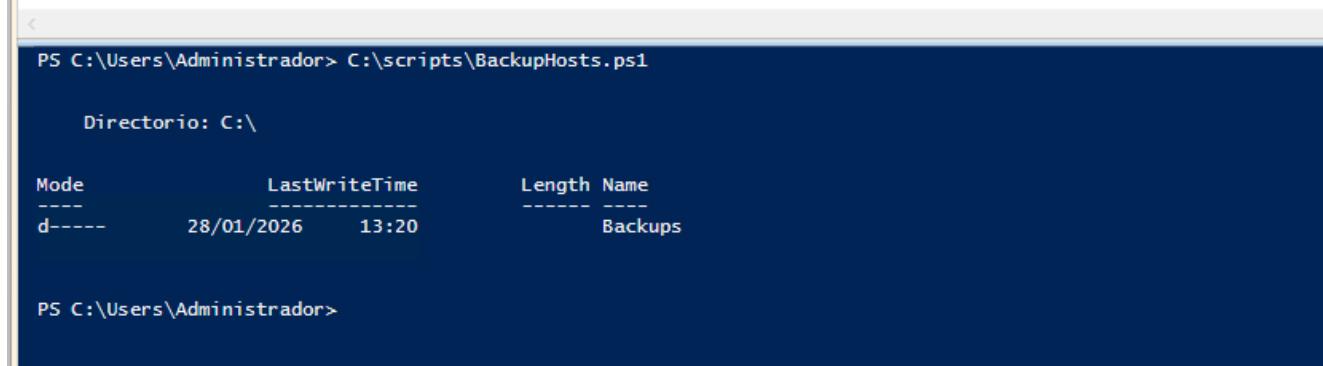
```
[root@server2asir usuario]$crontab -e
crontab: installing new crontab
Cristobal CON ROOT miércoles 28 enero
```

En Windows (hosts):

Script PowerShell (C:\Scripts\BackupHosts.ps1):



```
1 $Source = "C:\Windows\System32\drivers\etc\hosts"
2 $DestFolder = "C:\Backups\
3 if (!(Test-Path $DestFolder)) { New-Item -ItemType Directory $DestFolder }
4
5 $Timestamp = Get-Date -Format "yyyyMMdd_HHmm"
6 Copy-Item $Source -Destination "$DestFolder\hosts_$Timestamp.bak"
7
8 # Rotación: mantener 5 copias
9 $files = Get-ChildItem "$DestFolder\hosts_*.bak" | Sort-Object LastWriteTime -Descending
10 if ($files.Count -gt 5) {
11     $files | Select-Object -Skip 5 | Remove-Item
12 }
13 "$(Get-Date): Backup de hosts completado" | Out-File -FilePath "C:\Backups\log.txt" -Append
```

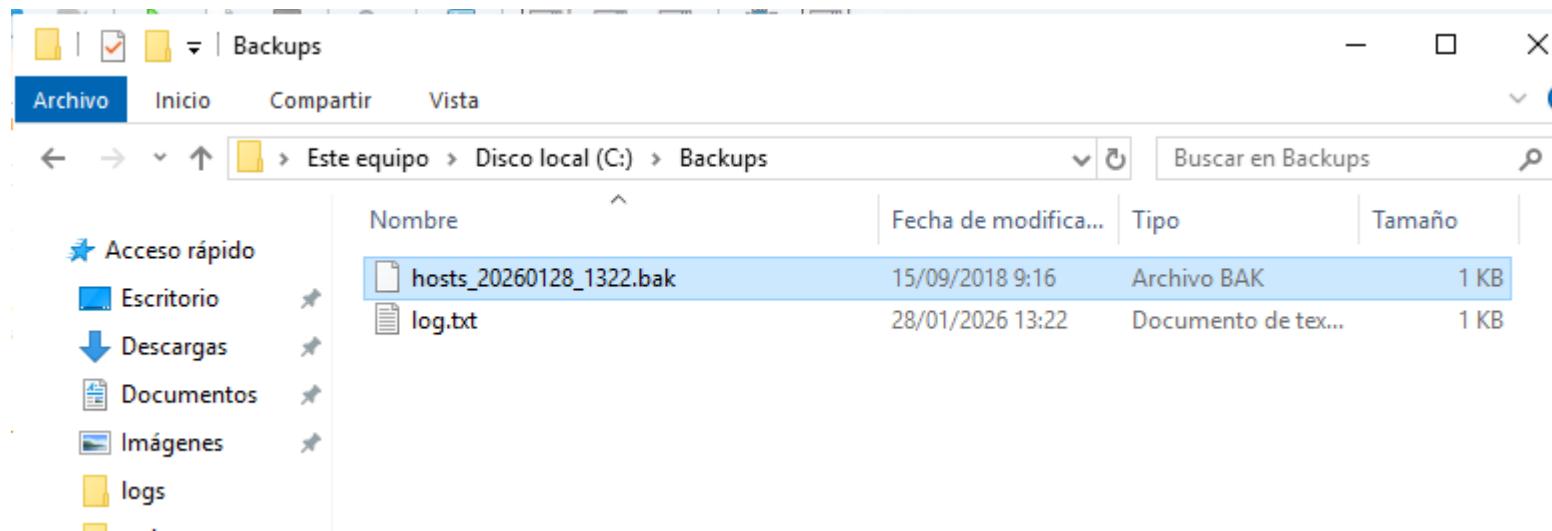
```
PS C:\Users\Administrador> C:\scripts\BackupHosts.ps1

Directorio: C:\

Mode          LastWriteTime      Length Name
----          -----          ---- 
d---  28/01/2026    13:20           Backups

PS C:\Users\Administrador>
```

Logs y copia generada:



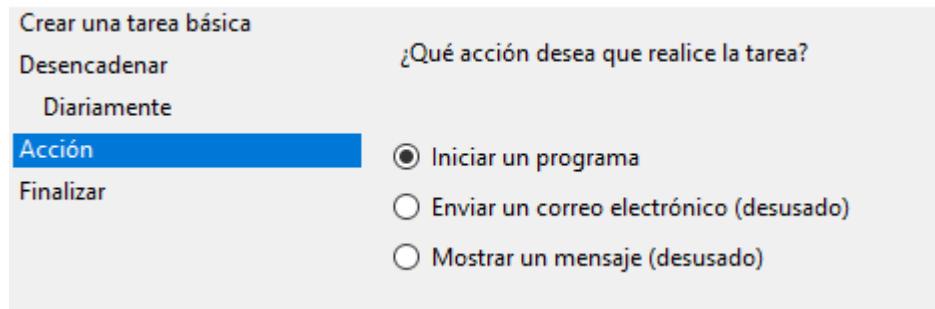
Programador de Tareas → Crear una tarea básica:

Crear una tarea básica	¿Cuándo desea que se inicie la tarea?
Desencadenar	<input checked="" type="radio"/> Diariamente <input type="radio"/> Semanalmente <input type="radio"/> Mensualmente <input type="radio"/> Una vez
Acción	
Finalizar	

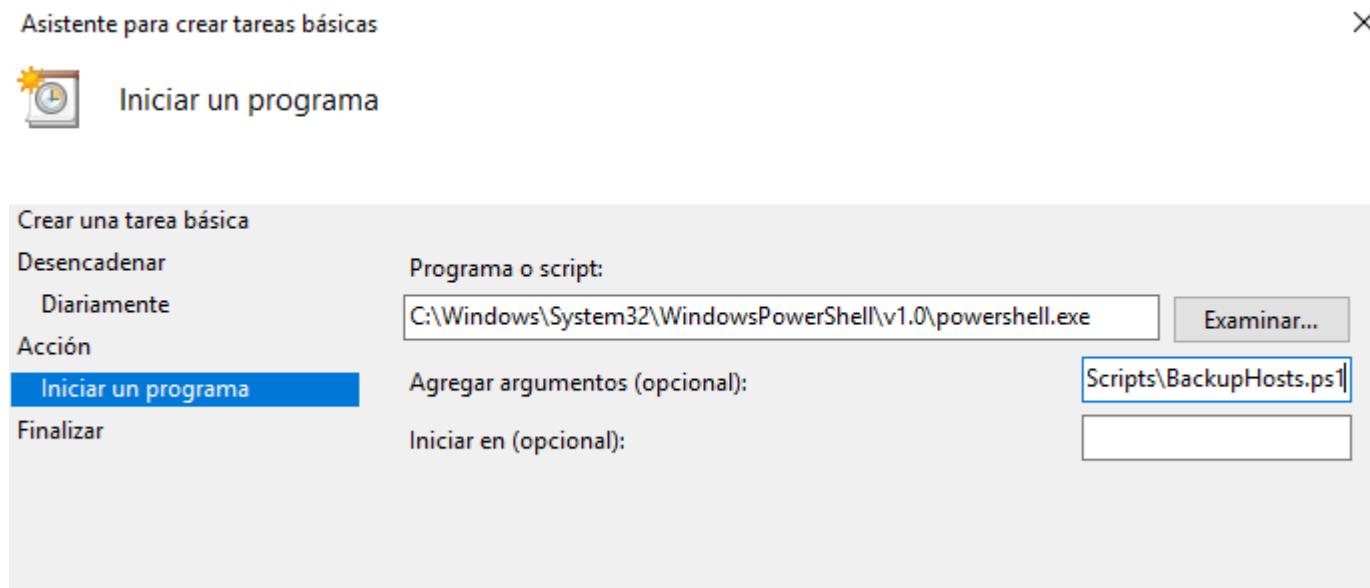


Diariamente

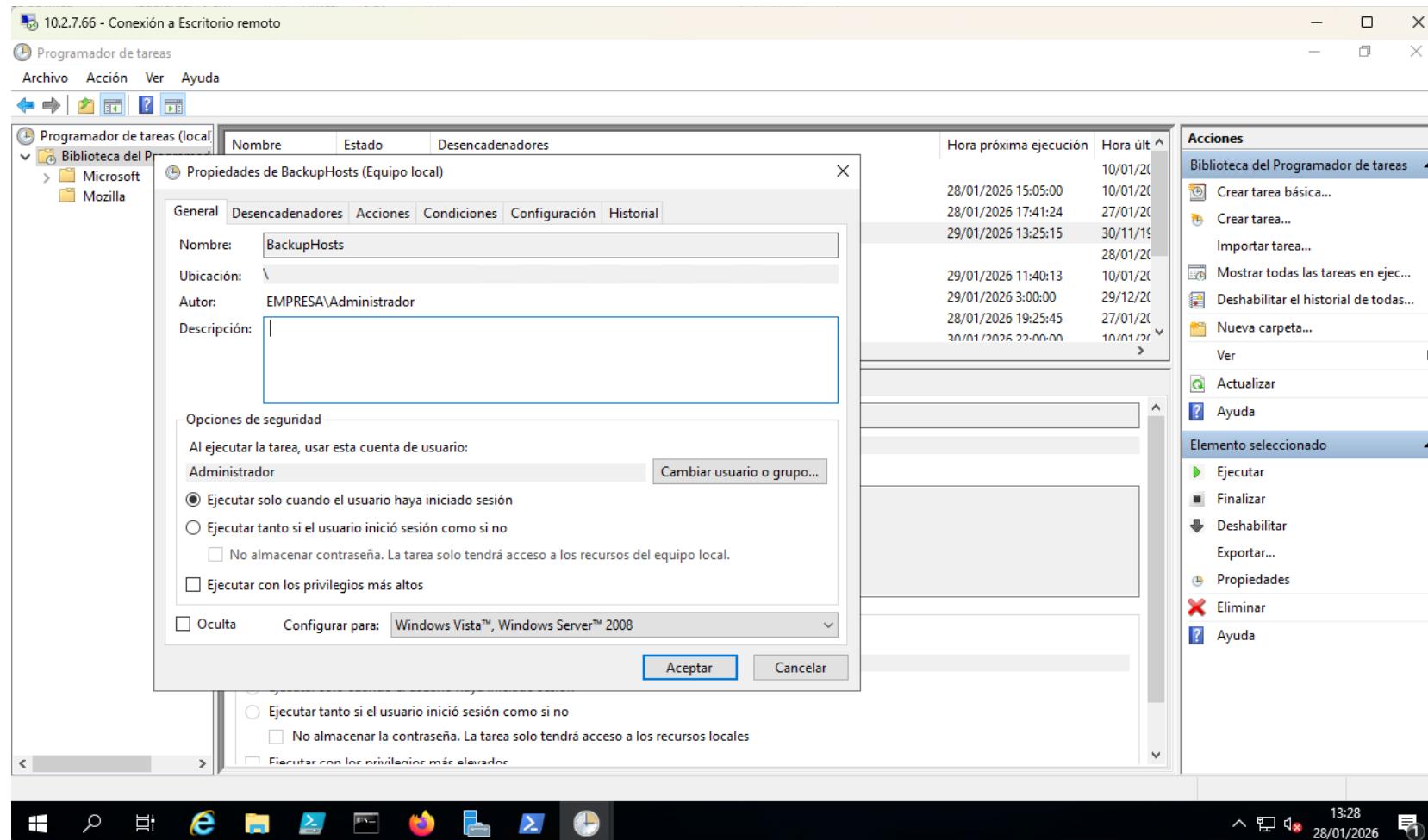
Crear una tarea básica	Inicio: 28/01/2026	<input type="button" value="..."/>	13:25:15	<input type="button" value="..."/>	<input type="checkbox"/> Sincronizar zonas horarias
Desencadenar	Repetir cada:	<input type="text" value="1"/>	días		
Diariamente					
Acción					
Finalizar					



Elegimos PowerShell y la opción: “-File C:\Scripts\BackupHosts.ps1”



Tarea programada:



Tarea 3 – Restauración de archivo congelado (Linux/Windows)

- Modificar manualmente el archivo crítico y comprobar que el script restaura al último backup válido.

En Linux: nano /opt/automation/backup_restore.sh

Este lo genera si la copia ya está hecha de antes.

```
[1/1]
#!/bin/bash

SRC="/etc/motd"
BACKUP="/opt/backups"
LOG="/var/log/automation_backup.log"
DATE=$(date +%F)

mkdir -p $BACKUP

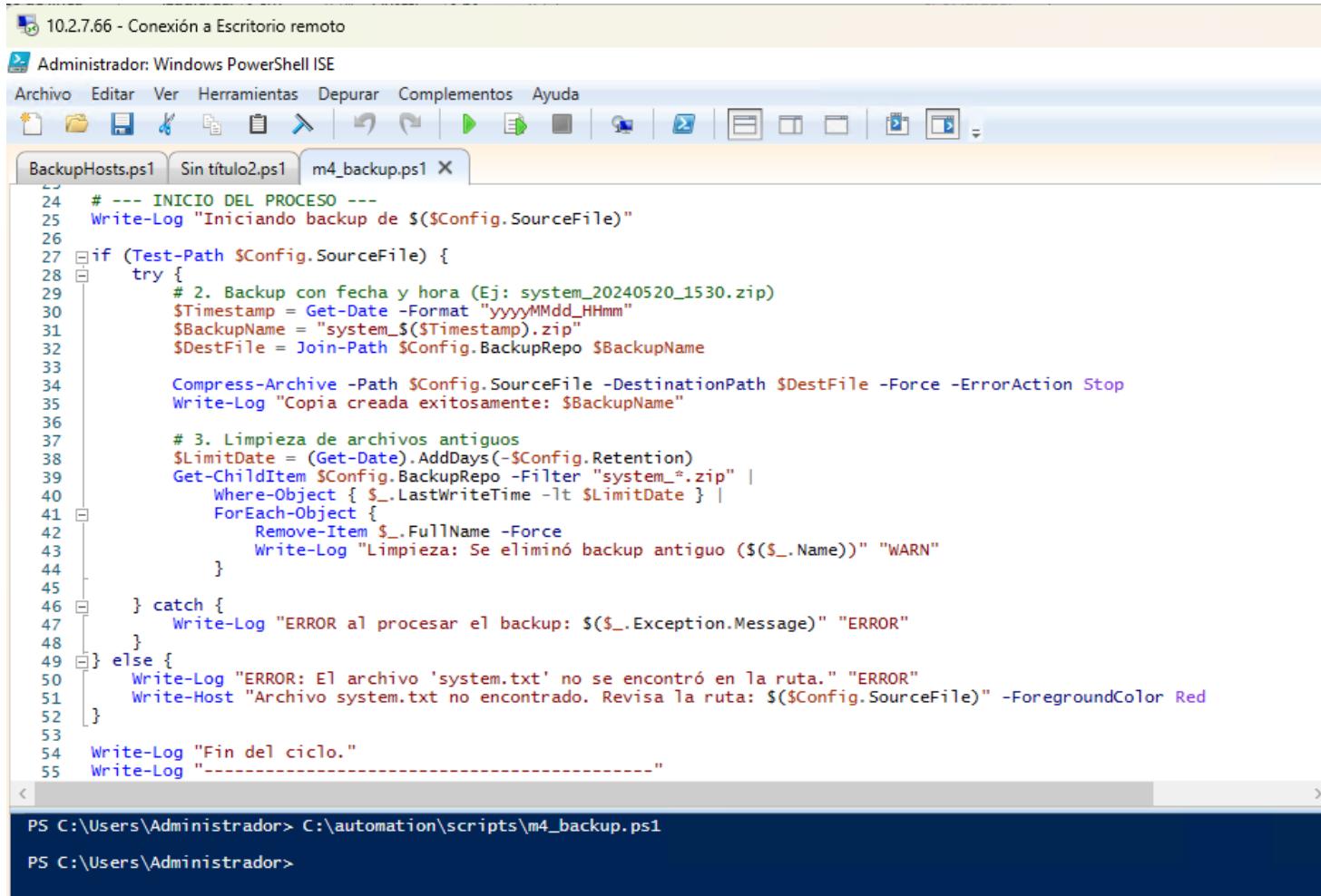
# Backup
tar czf $BACKUP/motd_${DATE}.tar.gz $SRC
echo "[$(date)] Copia creada: motd_${DATE}.tar.gz" >> $LOG

# Eliminar antiguos (>7 días)
find $BACKUP -type f -mtime +7 -delete
echo "[$(date)] Copias antiguas eliminadas" >> $LOG

# Restaurar copia anterior
YESTERDAY=$(date -d "yesterday" +%F)
tar xzf $BACKUP/motd_${YESTERDAY}.tar.gz -C /
echo "[$(date)] motd restaurado" >> $LOG
```

En Windows: C:\automation\scripts\m4_backup.ps1

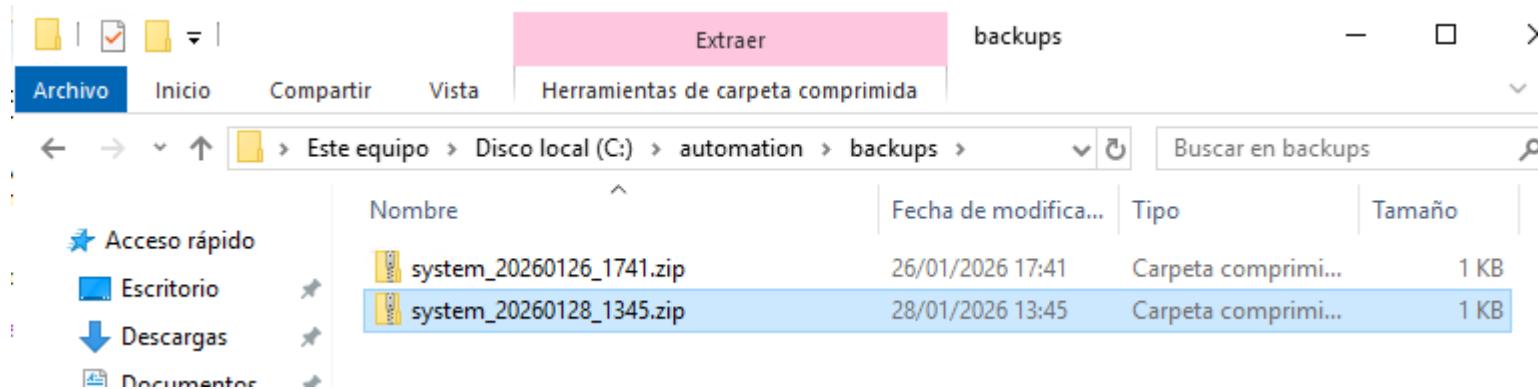
Script ejecutado:



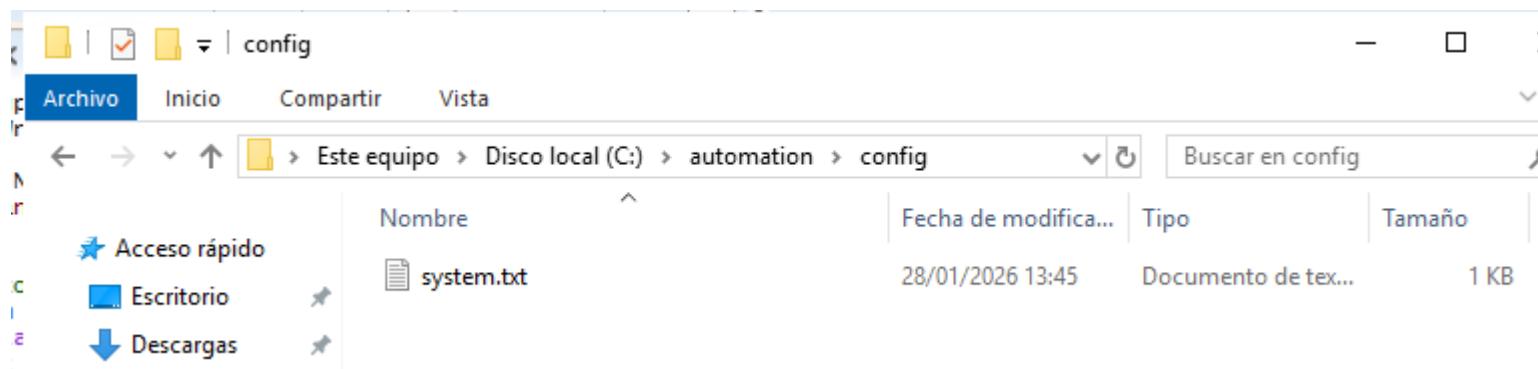
The screenshot shows the Windows PowerShell ISE interface. The title bar reads "10.2.7.66 - Conexión a Escritorio remoto" and "Administrador: Windows PowerShell ISE". The menu bar includes Archivo, Editar, Ver, Herramientas, Depurar, Complementos, Ayuda. The toolbar has standard file operations like Open, Save, Copy, Paste, etc. The tabs at the top show "BackupHosts.ps1", "Sin título2.ps1", and "m4_backup.ps1" (which is the active tab). The code editor displays the PowerShell script "m4_backup.ps1" with syntax highlighting. The script performs a backup process, compresses files, and handles errors. The bottom pane shows the command prompt output:

```
PS C:\Users\Administrador> C:\automation\scripts\m4_backup.ps1
PS C:\Users\Administrador>
```

Imagen del backup realizado.



Archivo restaurado



Tarea 4 – Automatización de cuentas (Linux)

- Crear un script que automatice la creación de un usuario de prueba con permisos mínimos.
- Registrar creación en un log con fecha, hora y usuario que ejecuta la tarea.

/usr/local/bin/crear_usuario_test.sh

```
GNU nano 6.2
#!/bin/bash
USER_NAME="user_test_$(date +%s)"
# Crear usuario con permisos mínimos y sin carpeta home personal accesible
useradd -m -s /usr/sbin/nologin $USER_NAME
echo "$(date) - Usuario $USER_NAME creado por $(whoami)" >> /var/log/gestion_usuarios.log
```

```
aperez:x:1004:1004:Ana Perez:/home/aperez:/bin/sh
#username:x:1015:1015:nombre apellido:/home/#username:/bin/sh
svc_auto:x:996:996::/home/svc_auto:/bin/bash
user_test_1769604544:x:1016:1016::/home/user_test_1769604544:/usr/sbin/nologin
Cristobal CON ROOT miércoles 28 enero 2026 12:49
[root@server2asir usuario]$
```

```
Cristobal CON ROOT miércoles 28 enero 2026 12:49
[root@server2asir usuario]$cat /var/log/gestion_usuarios.log
mié 28 ene 2026 12:49:04 UTC - Usuario user_test_1769604544 creado por root
Cristobal CON ROOT miércoles 28 enero 2026 12:49
```

Tarea 5 – Auditoría y seguridad (Windows)

- Activar **PowerShell Transcription** y **ScriptBlockLogging**.
- Ejecutar un script de prueba que cree una tarea programada en Task Scheduler.
- Comprobar en el **Visor de eventos** que aparecen los eventos 4698 y 4701.

Rúbrica de evaluación:

Sub-tarea	Peso	Criterios RA cubiertos	Indicadores de éxito
Limpieza automatizada (Linux)	20%	a, b, c, d, f, h	Script correcto, cron/systemd timer configurado, logs generados
Backup automatizado	25%	a, b, c, d, e, f, h	Backups creados, logs completos, solo últimas 5 copias conservadas
Restauración	15%	a, e, f, h	Archivo restaurado correctamente, log documentado
Automatización de cuentas	15%	a, g, h	Usuario creado con permisos mínimos, log documentado
Auditoría y seguridad	25%	a, e, h	Transcripción y ScriptBlockLogging activados, eventos correctos registrados

En las directivas de grupo del servidor:

The screenshot shows the Group Policy Management Editor interface. A tree view on the left lists policy components under 'Directiva Default Domain Controllers Policy [WIN-Q9RNF]'. The 'Configuración del equipo' node is expanded, showing 'Directivas' which further branches into 'Configuración de software', 'Configuración de Windows', 'Plantillas administrativas: definiciones', and 'Componentes de Windows'. 'Componentes de Windows' is also expanded, showing 'Administración de derechos digitales' and 'Administración remota de Windows'.

Windows PowerShell:

Habilitar **Activación de la transcripción de PowerShell** y **Activación del registro de bloques de scripts**.

The screenshot shows the configuration page for the 'Activar el registro de bloque de script de PowerShell' policy setting. On the left, there's a sidebar with 'Activar el registro de bloque de script de PowerShell' selected. The main area has a table with four columns: 'Configuración', 'Estado', and 'Comentario'. There are five rows in the table:

Configuración	Estado	Comentario
Activar registro de módulos	No configurada	No
Activar el registro de bloque de script de PowerShell	Habilitada	No
Activar la ejecución de scripts	No configurada	No
Activar la transcripción de PowerShell	Habilitada	No
Establecer la ruta de acceso de origen de Update-Help	No configurada	No

Script creador de tarea:

The screenshot shows a Windows PowerShell ISE window titled "10.2.7.66 - Conexión a Escritorio remoto". The menu bar includes Archivo, Editar, Ver, Herramientas, Depurar, Complementos, and Ayuda. The toolbar contains various icons for file operations. The tabs at the top show BackupHosts.ps1, Sin título2.ps1, m4_backup.ps1, and Creador_Tarea_programada.ps1 (which is currently selected). The code in the editor is as follows:

```
1 $Action = New-ScheduledTaskAction -Execute "notepad.exe"
2 $Trigger = New-ScheduledTaskTrigger -AtLogOn
3 Register-ScheduledTask -TaskName "TareaAuditoria" -Action $Action -Trigger $Trigger
4 # Tras ejecutar esto, revisar Visor de Eventos > Registros de Windows > Seguridad
```

Below the editor, the PowerShell console displays the execution of the script:

```
PS C:\Users\Administrador> C:\automation\scripts\m4_backup.ps1
PS C:\Users\Administrador> C:\automation\scripts\m4_backup.ps1
PS C:\Users\Administrador> C:\automation\scripts\Creador_Tarea_programada.ps1
TaskPath          TaskName          State
-----          -----          -----
\\              TareaAuditoria      Ready
```

The final prompt shows the user has finished interacting with the console.

Visor de Eventos:

Evento 4698: Se genera al crear una tarea programada (Aparece en el registro de Seguridad).

The screenshot shows the Windows Event Viewer interface. The title bar includes buttons for 'Serie de linea', 'Izquierda: 10 cm', 'Antes', 'Desplazar', and 'Deshacer'. Below the title bar, the status bar shows '10.2.7.66 - Conexión a Escritorio remoto' and 'Visor de eventos'. The main window has a toolbar with icons for Back, Forward, Refresh, Search, and Help. The menu bar includes 'Archivo', 'Acción', 'Ver', and 'Ayuda'. The left pane is a navigation tree with 'Visor de eventos (local)', 'Vistas personalizadas', 'Registros de Windows' (selected), 'Aplicación', 'Seguridad' (selected), 'Instalación', 'Sistema', 'Eventos reenviados', 'Registros de aplicaciones y s...', and 'Suscripciones'. The right pane displays a table titled 'Seguridad' with the message 'Número de eventos: 100.524 (!) Nuevos eventos disponibles'. The table columns are 'Palabras clave', 'Fecha y hora', 'Origen', 'Id. del evento', and 'Categoría de la tarea'. The table lists several events, all of which are 'Auditoría correcta' from 'Microsoft Windows sec...' at various dates and times. The event with ID 4648 on 27/01/2026 19:16:12 is highlighted with a blue selection bar.

Palabras clave	Fecha y hora	Origen	Id. del evento	Categoría de la tarea
Auditoría correcta	29/12/2025 12:55:00	Microsoft Windows sec...	4647	Logoff
Auditoría correcta	18/01/2026 18:47:51	Microsoft Windows sec...	4647	Logoff
Auditoría correcta	27/01/2026 19:16:12	Microsoft Windows sec...	4648	Logon
Auditoría correcta	13/01/2026 10:52:40	Microsoft Windows sec...	4648	Logon
Auditoría correcta	13/01/2026 11:08:01	Microsoft Windows sec...	4648	Logon
Auditoría correcta	29/12/2025 12:26:34	Microsoft Windows sec...	4648	Logon
Auditoría correcta	29/12/2025 12:26:35	Microsoft Windows sec...	4648	Logon
Auditoría correcta	13/01/2026 17:20:00	Microsoft Windows sec...	4648	Logon
Auditoría correcta	16/01/2026 18:21:21	Microsoft Windows sec...	4648	Logon
Auditoría correcta	13/01/2026 17:30:00	Microsoft Windows sec...	4648	Logon
Auditoría correcta	16/12/2025 18:20:18	Microsoft Windows sec...	4648	Logon