

### **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:

```
Cristóbal con root - miércoles 28 ene 2020
[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

```
Símbolo del sistema - ssh usu X + v
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

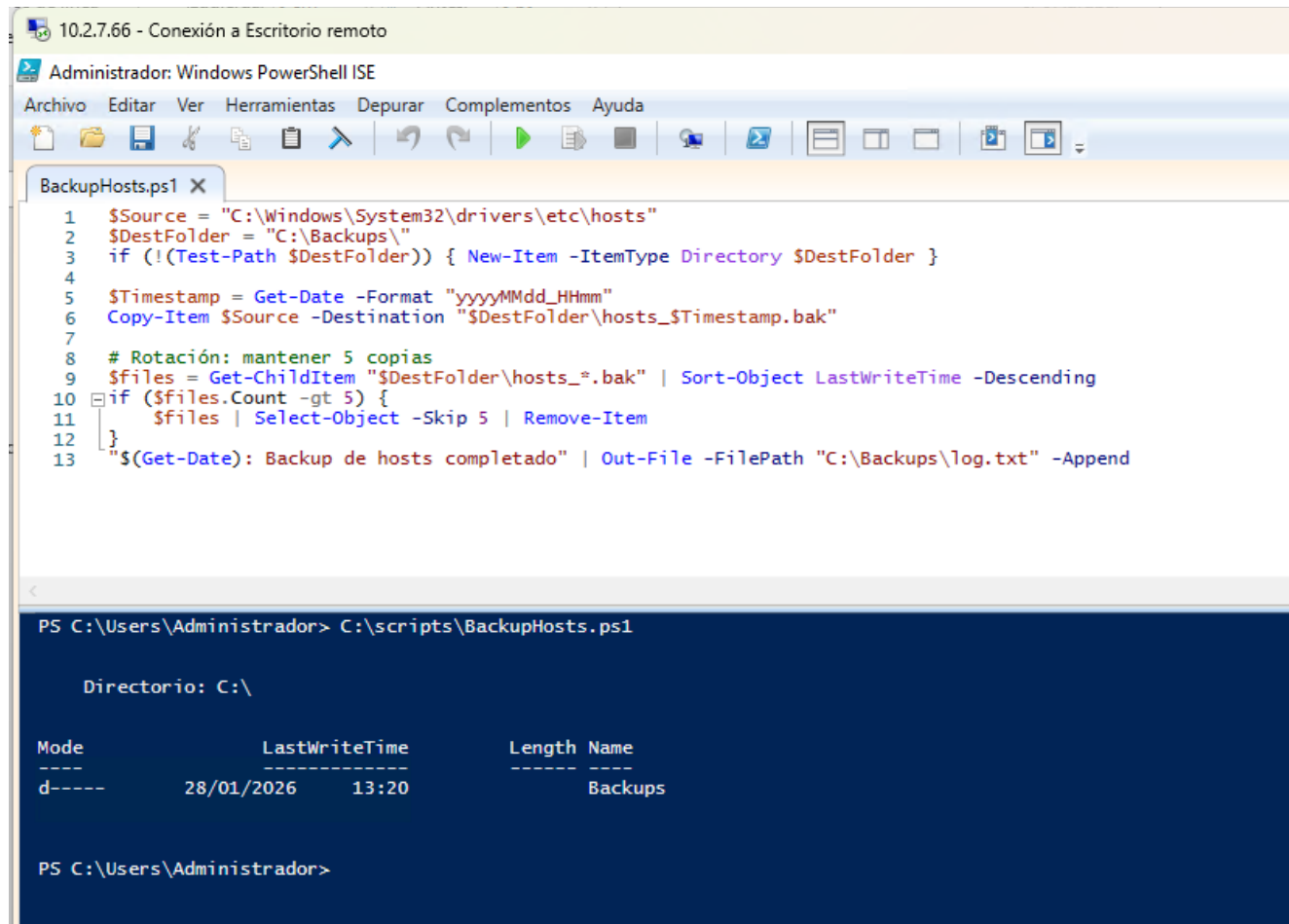
```
0 0 * * * /bin/bash /usr/local/bin/limpieza.sh
0 0 * * * /usr/local/bin/backup_motd.sh
```

Guardamos y salimos:

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

En Windows (hosts):

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



The screenshot shows a remote desktop connection to a Windows machine. The title bar reads "10.2.7.66 - Conexión a Escritorio remoto". The application window is "Administrador: Windows PowerShell ISE". The menu bar includes "Archivo", "Editar", "Ver", "Herramientas", "Depurar", "Complementos", and "Ayuda". The toolbar contains icons for file operations and execution. The script editor shows a file named "BackupHosts.ps1" with the following code:

```
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
```

The console window shows the execution of the script:

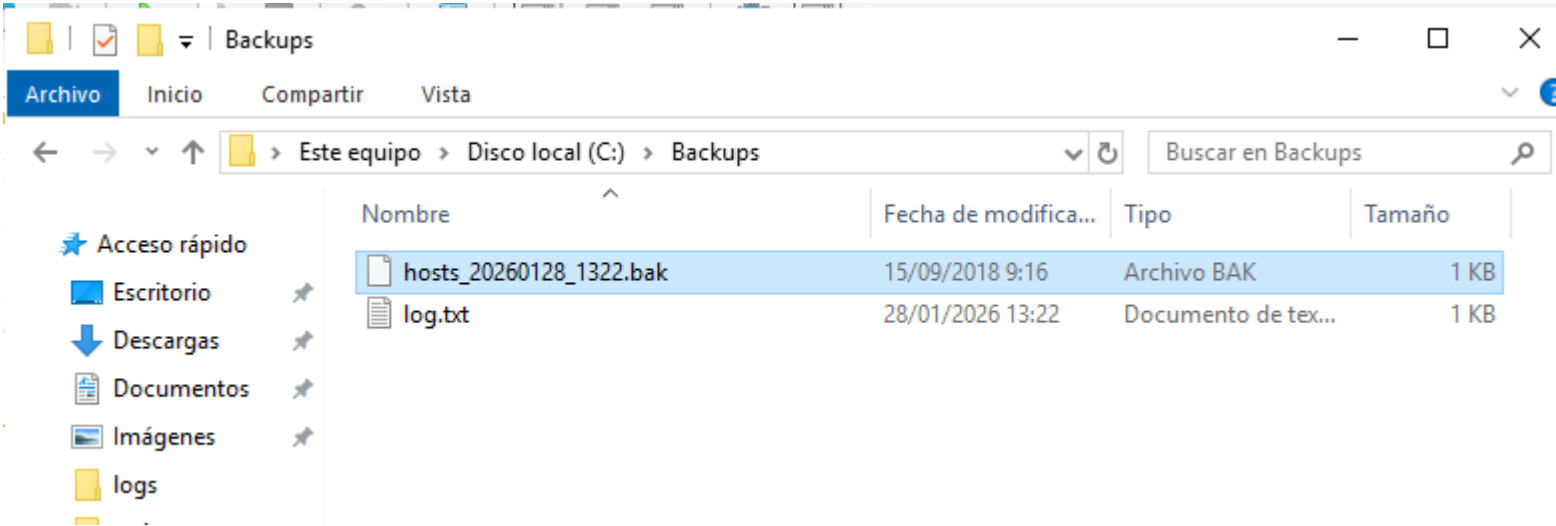
```
PS C:\Users\Administrador> C:\scripts\BackupHosts.ps1

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
Acción	<input type="radio"/> Semanalmente
Finalizar	<input type="radio"/> Mensualmente
	<input type="radio"/> Una vez



Diariamente

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

Crear una tarea básica

Desencadenar ¿Qué acción desea que realice la tarea?

Diariamente

**Acción**

Finalizar

☒ Iniciar un programa

☐ Enviar un correo electrónico (desusado)

☐ Mostrar un mensaje (desusado)

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

Asistente para crear tareas básicas



Iniciar un programa

Crear una tarea básica

Desencadenar Programa o script:

Diariamente

Acción

**Iniciar un programa**

Finalizar

Agregar argumentos (opcional):

Iniciar en (opcional):

Tarea programada:

10.2.7.66 - Conexión a Escritorio remoto

Programador de tareas

Archivo Acción Ver Ayuda

Programador de tareas (local)

Biblioteca del P

Microsoft

Mozilla

Nombre	Estado	Desencadenadores	Hora próxima ejecución	Hora últ
			28/01/2026 15:05:00	10/01/20
			28/01/2026 17:41:24	27/01/20
			29/01/2026 13:25:15	30/11/19
				28/01/20
			29/01/2026 11:40:13	10/01/20
			29/01/2026 3:00:00	29/12/20
			28/01/2026 19:25:45	27/01/20
			30/01/2026 22:00:00	10/01/20

Propiedades de BackupHosts (Equipo local)

General

Desencadenadores

Acciones

Condiciones

Configuración

Historial

Nombre: BackupHosts

Ubicación: \

Autor: EMPRESA\Administrador

Descripción:

Opciones de seguridad

Al ejecutar la tarea, usar esta cuenta de usuario:  
Administrador 

Cambiar usuario o grupo...

☒ Ejecutar solo cuando el usuario haya iniciado sesión

☐ Ejecutar tanto si el usuario inició sesión como si no

☐ No almacenar contraseña. La tarea solo tendrá acceso a los recursos del equipo local.

☐ Ejecutar con los privilegios más altos

☐ Oculta

Configurar para: Windows Vista™, Windows Server™ 2008

Aceptar

Cancelar

Acciones

Biblioteca del Programador de tareas

Crear tarea básica...

Crear tarea...

Importar tarea...

Mostrar todas las tareas en ejec...

Deshabilitar el historial de todas...

Nueva carpeta...

Ver

Actualizar

Ayuda

Elemento seleccionado

Ejecutar

Finalizar

Deshabilitar

Exportar...

Propiedades

Eliminar

Ayuda

13:28

28/01/2026

### **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

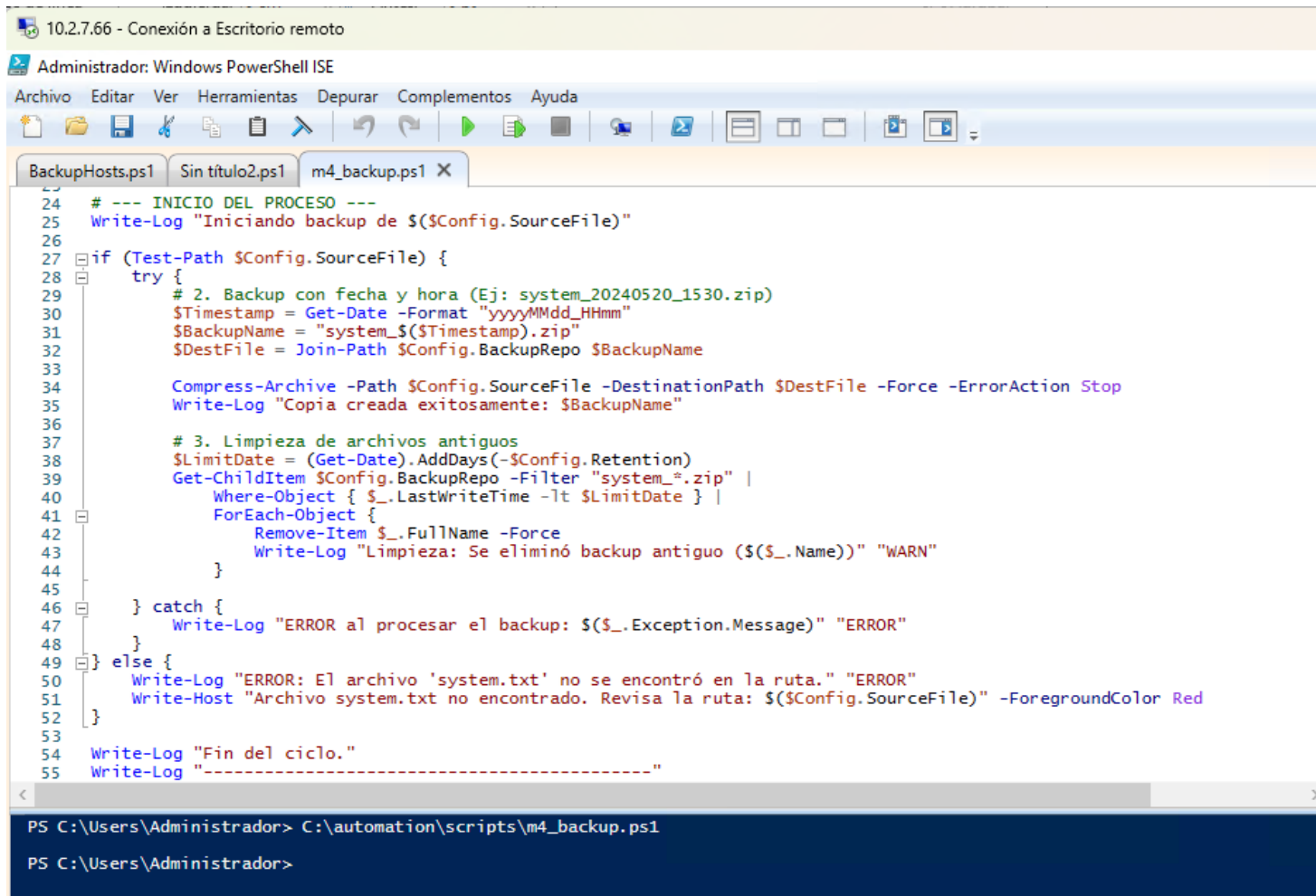
# Backup
tar czf $BACKUP/motd_$DATE.tar.gz $SRC
echo "[$(date)] Copia creada: motd_$DATE.tar.gz" >> $LOG

# 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:



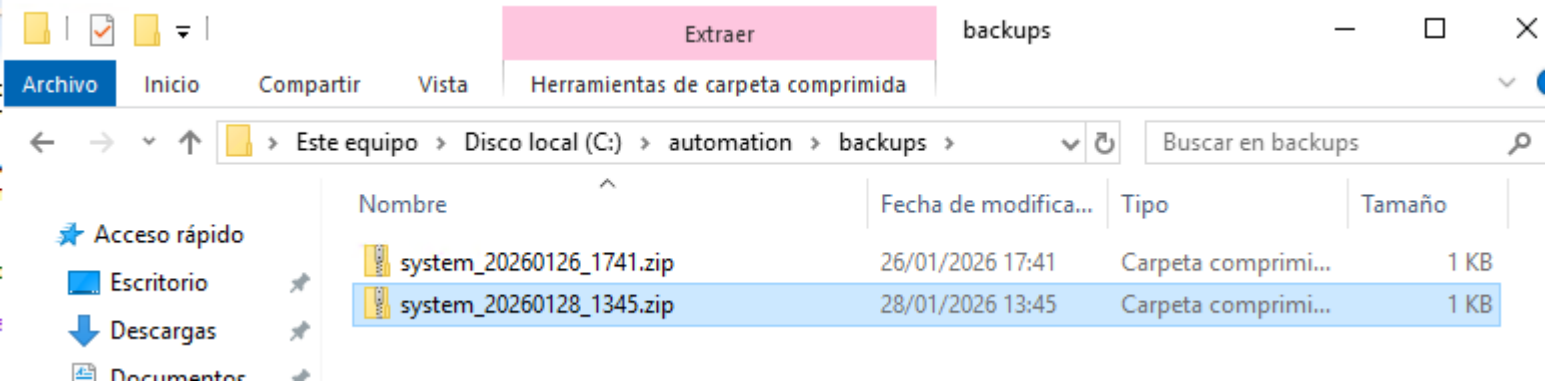
The screenshot displays a remote desktop session titled "10.2.7.66 - Conexión a Escritorio remoto". The main window is the "Administrador: Windows PowerShell ISE", which has three tabs: "BackupHosts.ps1", "Sin título2.ps1", and "m4\_backup.ps1". The "m4\_backup.ps1" tab is active, showing a PowerShell script with line numbers 24 through 55. The script performs a backup of a file specified in a configuration, compresses it into a zip file, and then cleans up old backups based on a retention policy. It includes error handling and logging. Below the ISE window, a terminal window shows the command to execute the script: "PS C:\Users\Administrador> C:\automation\scripts\m4\_backup.ps1".

```
24 # --- INICIO DEL PROCESO ---
25 Write-Log "Iniciando backup de $($Config.SourceFile)"
26
27 if (Test-Path $Config.SourceFile) {
28     try {
29         # 2. Backup con fecha y hora (Ej: system_20240520_1530.zip)
30         $Timestamp = Get-Date -Format "yyyyMMdd_HHmm"
31         $BackupName = "system_{$Timestamp}.zip"
32         $DestFile = Join-Path $Config.BackupRepo $BackupName
33
34         Compress-Archive -Path $Config.SourceFile -DestinationPath $DestFile -Force -ErrorAction Stop
35         Write-Log "Copia creada exitosamente: $BackupName"
36
37         # 3. Limpieza de archivos antiguos
38         $LimitDate = (Get-Date).AddDays(-$Config.Retention)
39         Get-ChildItem $Config.BackupRepo -Filter "system_*.zip" |
40         Where-Object { $_.LastWriteTime -lt $LimitDate } |
41         ForEach-Object {
42             Remove-Item $_.FullName -Force
43             Write-Log "Limpieza: Se eliminó backup antiguo ($($_.Name))" "WARN"
44         }
45     } catch {
46         Write-Log "ERROR al procesar el backup: $($_.Exception.Message)" "ERROR"
47     }
48 } else {
49     Write-Log "ERROR: El archivo 'system.txt' no se encontró en la ruta." "ERROR"
50     Write-Host "Archivo system.txt no encontrado. Revisa la ruta: $($Config.SourceFile)" -ForegroundColor Red
51 }
52
53 Write-Log "Fin del ciclo."
54 Write-Log "-----"
```

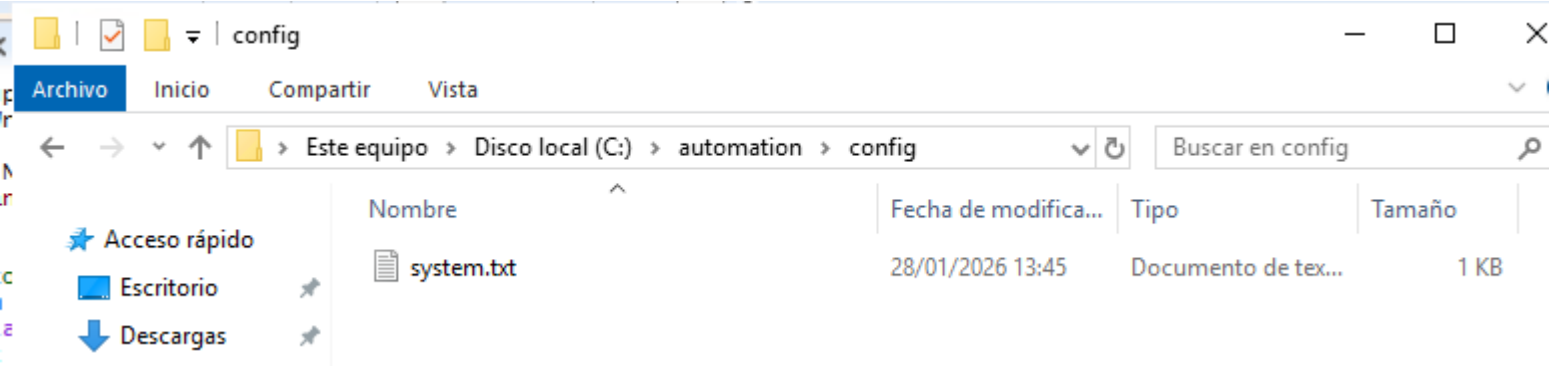
PS C:\Users\Administrador> C:\automation\scripts\m4\_backup.ps1

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 /usr/local/bin/crear_usuario_test.sh
#!/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
```

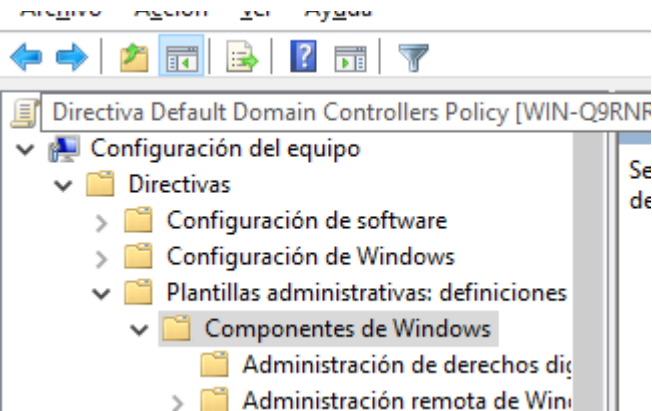
### Tarea 5 – Auditoría y seguridad (Windows)

- 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:



Windows PowerShell:

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

Windows PowerShell

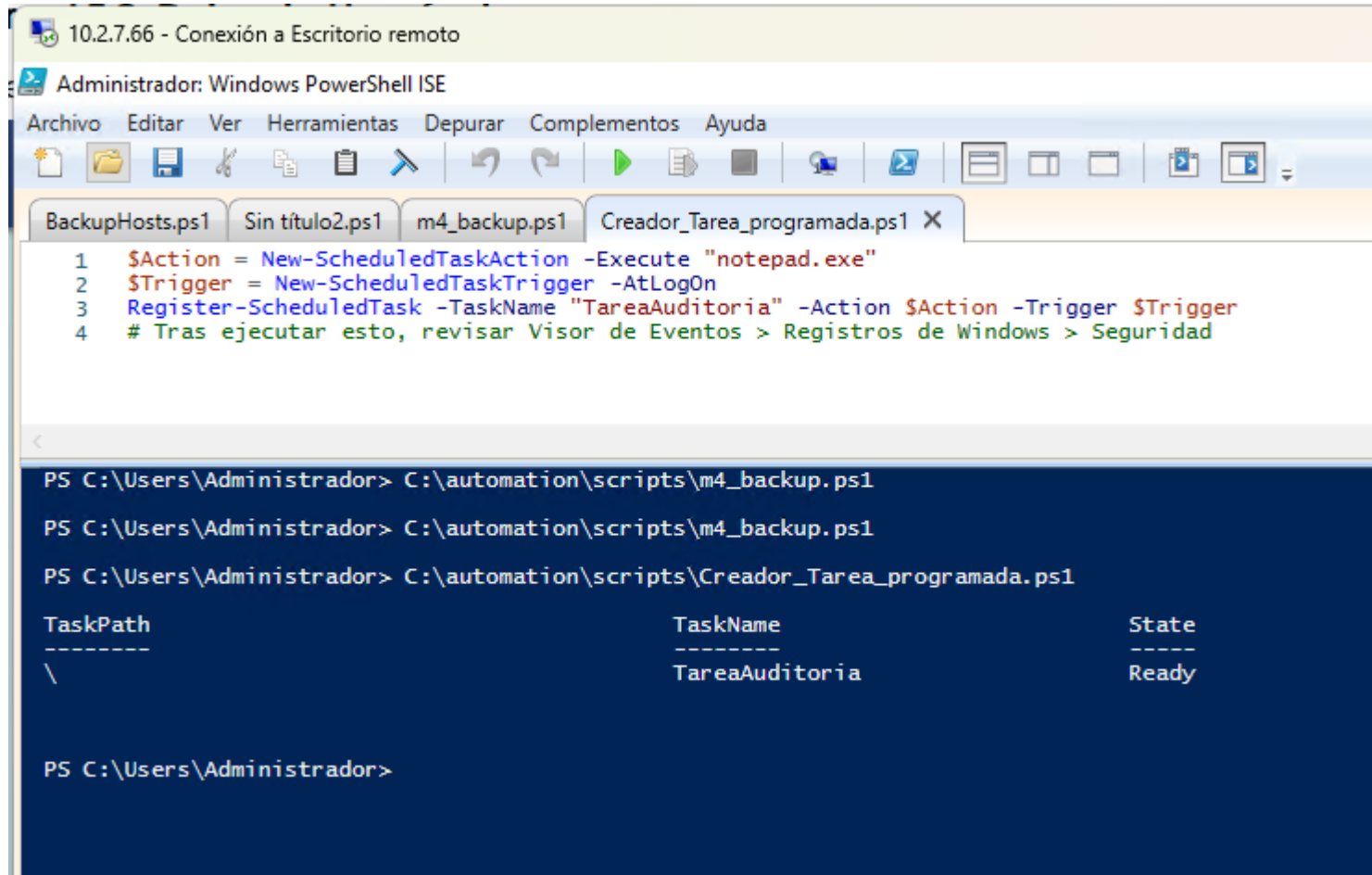
Activar el registro de bloque de script de PowerShell

Editar [configuración de directiva](#)

Requisitos:  
Al menos familia de Microsoft Windows 7 o Windows Server 2008

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 window has a menu bar with "Archivo", "Editar", "Ver", "Herramientas", "Depurar", "Complementos", and "Ayuda". Below the menu bar is a toolbar with various icons. The script editor shows four tabs: "BackupHosts.ps1", "Sin título2.ps1", "m4\_backup.ps1", and "Creador\_Tarea\_programada.ps1". The active tab "Creador\_Tarea\_programada.ps1" contains the following PowerShell script:

```
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
```

The console window below the script editor shows the execution of the script. The prompt is "PS C:\Users\Administrador>". The user enters "C:\automation\scripts\m4\_backup.ps1" twice. Then, the user enters "C:\automation\scripts\Creador\_Tarea\_programada.ps1". The output shows the task details:

TaskPath	TaskName	State
\	TareaAuditoria	Ready

The prompt returns to "PS C:\Users\Administrador>".

Visor de Eventos:

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

10.2.7.66 - Conexión a Escritorio remoto

Visor de eventos

Archivo Acción Ver Ayuda

Visor de eventos (local)

- Vistas personalizadas
- Registros de Windows
  - Aplicación
  - Seguridad
  - Instalación
  - Sistema
  - Eventos reenviados
- Registros de aplicaciones y servicios
- Suscripciones

**Seguridad** Número de eventos: 100.524 (!) Nuevos eventos disponibles

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