



Administración de Sistemas Operativos Libres

El arte de la arquitectura, seguridad y optimización en entornos UNIX/Linux.

› _
Unidad 7: Herramientas esenciales para asegurar la estabilidad, seguridad y eficiencia de la infraestructura.
› █

Los Cimientos: Filosofía UNIX



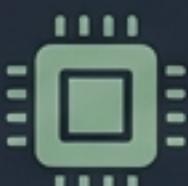
Multitarea y Multiusuario:
Ejecución simultánea de procesos y usuarios.



Estructura Modular:
Herramientas sencillas combinadas para tareas complejas.



Sistema de Archivos Jerárquico: Organización en árbol.



Portabilidad: Adaptable a diferente hardware.



La Potencia del CLI (Línea de Comandos)

- **Eficiencia:** Sin navegación por menús visuales.
- **Automatización:** Creación de scripts para tareas repetitivas.
- **Control Total:** Acceso profundo a la configuración.

Quick Reference

<code>ls</code>	// Listar archivos
<code>cd</code>	// Cambiar directorio
<code>mkdir</code>	// Crear directorio
<code>rm</code>	// Eliminar archivo

Gestión de Identidad: Usuarios y Grupos

Creación:

- Fira Code - `adduser` (crear usuario)
- Fira Code - `passwd` (establecer contraseña)
- Fira Code - `groupadd` (crear grupo)

Modificación:

- Fira Code - `usermod` (asignar usuario a grupo)
- Fira Code - `groupmod` (cambiar nombre de grupo)

Eliminación:

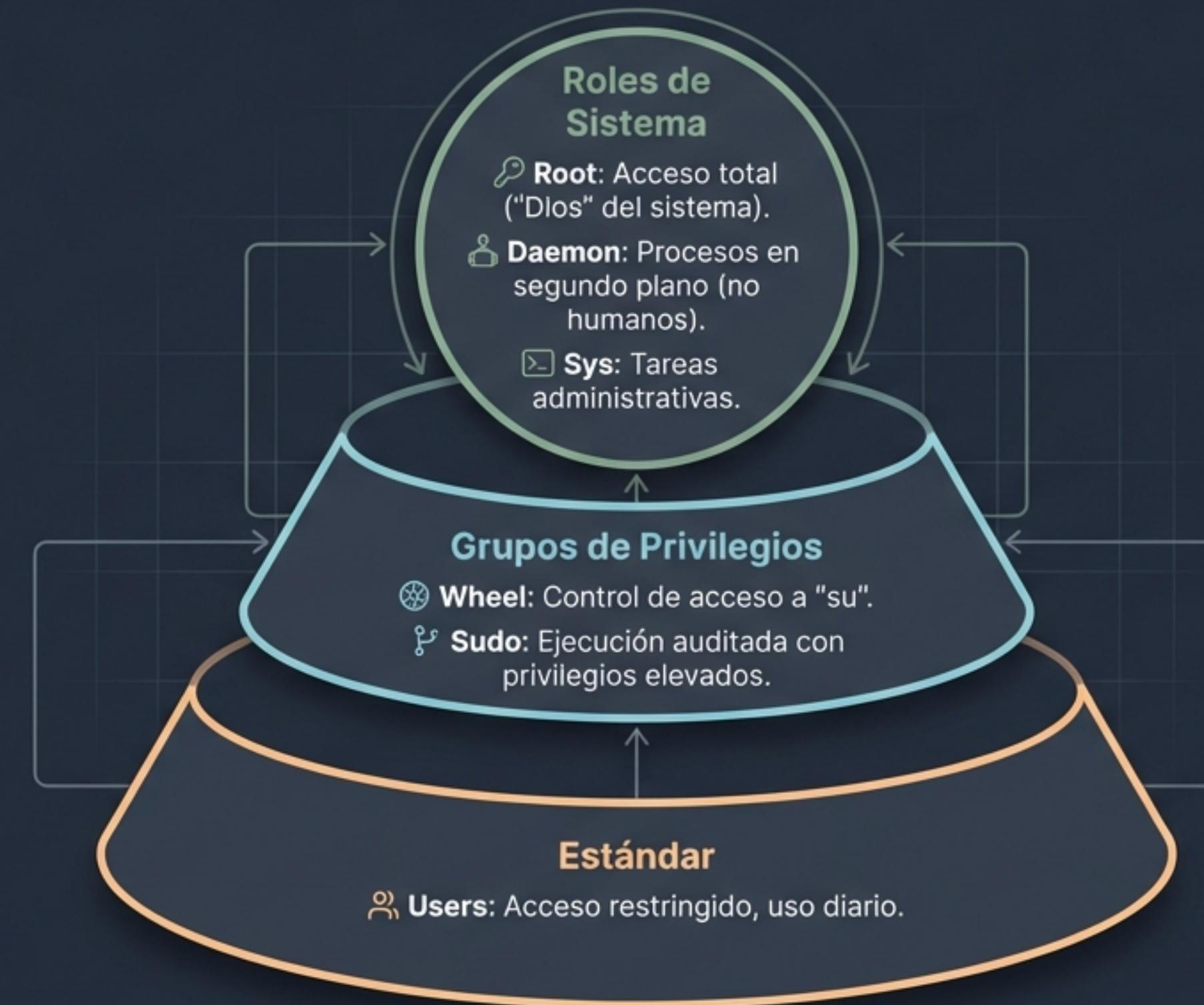
- Fira Code - `userdel` (borrar usuario)
- Fira Code - `groupdel` (borrar grupo)

```
tic1@Green-Corzas:~$ sudo adduser pepito
[sudo] contraseña para tic1:
Lo sentimos, vuelva a intentarlo.
[sudo] contraseña para tic1:
Añadiendo el usuario 'pepito' ...
Añadiendo el nuevo grupo 'pepito' (1002) ...
Añadiendo el nuevo usuario 'pepito' (1002) con grupo 'pepito' ...
Creando el directorio personal '/home/pepito' ...
Copiando los ficheros desde '/etc/skel' ...

Nueva contraseña:
Vuelva a escribir la nueva contraseña:
passwd: contraseña actualizada correctamente
Cambiando la información de usuario para pepito
Introduzca el nuevo valor, o presione INTRO para el predeterminado
    Nombre completo []: Pepe
    Número de habitación []: TIC II
    Teléfono del trabajo []:
    Teléfono de casa []:
    Otro []:
¿Es correcta la información? [S/n] s
tic1@Green-Corzas:~$
```

Nota Crítica: Cada usuario y grupo posee un identificador único (UID/GID). El superusuario (Root) siempre posee el UID 0.

La Jerarquía Predeterminada



El Escudo: Permisos y Elevación

Herramientas de Control

chmod

Cambiar modo/permisos (Change Mode).

chown

Cambiar propietario (Change Owner).

chgrp

Cambiar grupo (Change Group).

La Doctrina Sudo

Sudo permite ejecutar comandos sin cambiar a la cuenta root.

- **Beneficio:** Registro de auditoría y seguridad por contraseña.
- **Configuración:** Archivo 'sudoers' (editar con 'visudo').

Matriz de Permisos

	Read (r)	Write (w)	Execute (x)
Propietario	✓	✓	✓
Grupo	✓		✓
Otros	✓		✓

Fortificación del Almacenamiento

Gestión de Particiones

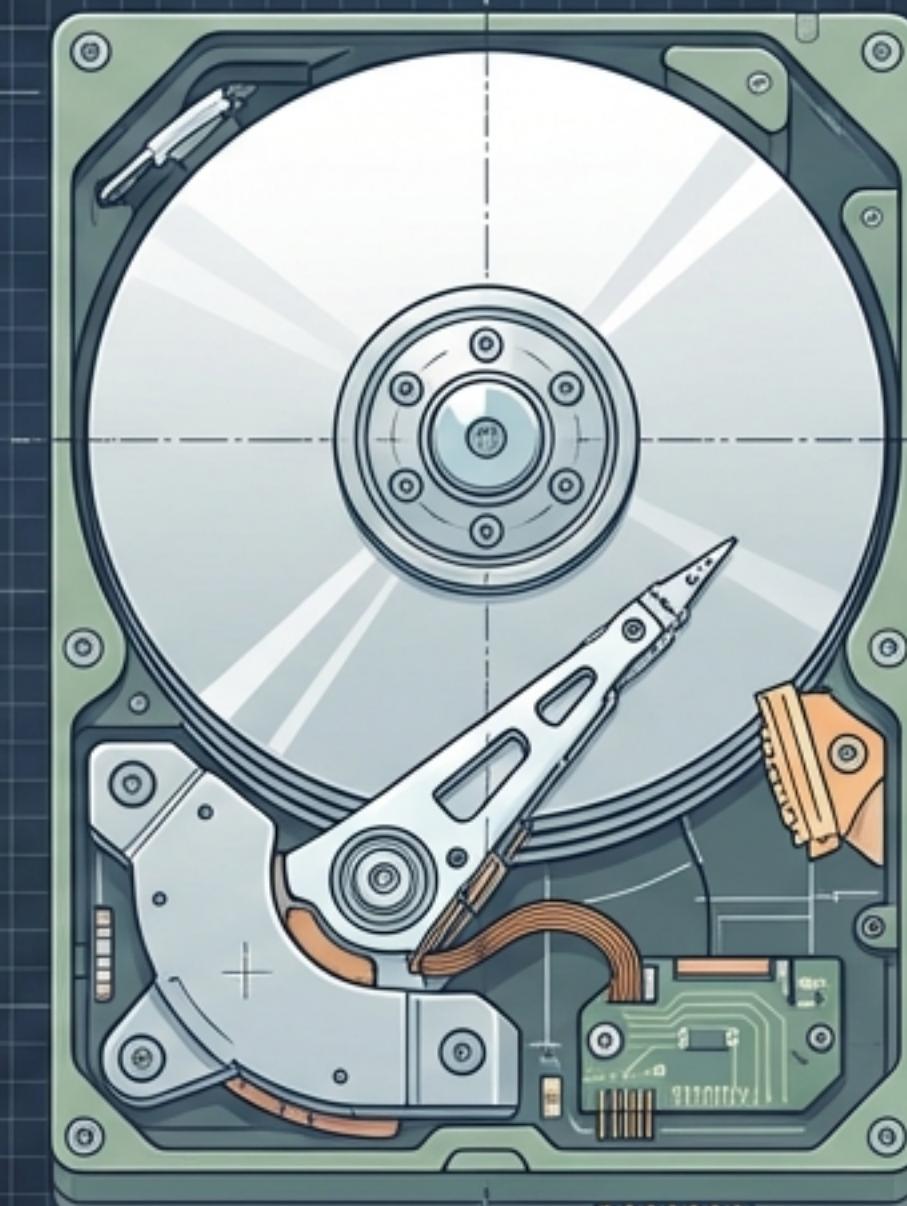
Herramientas:

- GParted (Gráfico)
- fdisk (Línea de comandos)
- lsblk (Listar dispositivos)

Estrategia de Cifrado

- LUKS: Estándar para cifrado de disco completo.
- eCryptfs: Cifrado a nivel de directorio (ej. /home).

Buenas Prácticas: Contraseñas fuertes y copias de seguridad de claves.



Políticas de Seguridad y Cuentas de Servicio

Principio de Mínimos Privilegios



Cuentas de Servicio

- Ejecución aislada de aplicaciones.
- Una cuenta por servicio (Segregación).
- Sin acceso para humanos.

Reglas de Hardening

- Directorios privados: Permisos 700 (Solo propietario).
- Archivos públicos: Permisos 755.
- Higiene Sudo: Evitar `sudo` en scripts; registrar toda actividad.

Vigilancia: Auditoría y Monitorización

The Watchdog (auditd)

Demonio que registra eventos de seguridad.

```
auditctl -w  
/path/to/file -p rwxa
```

The Log

/var/log/audit/audit.log

The Analyst (ausearch & aureport)

- **ausearch**: Análisis de logs.
- **aureport**: Generación de resúmenes.

Gestión de Energía en Portátiles

1. TLP (Gestión Avanzada)

- Filosofía: 'Set and forget'
(Instalar y olvidar).

- Comando Instalar:

```
'sudo apt install tlp tlp-rdw'
```

o [quir](#) de tlp-rdw

- Comando Activar:

```
'sudo systemctl enable tlp'
```



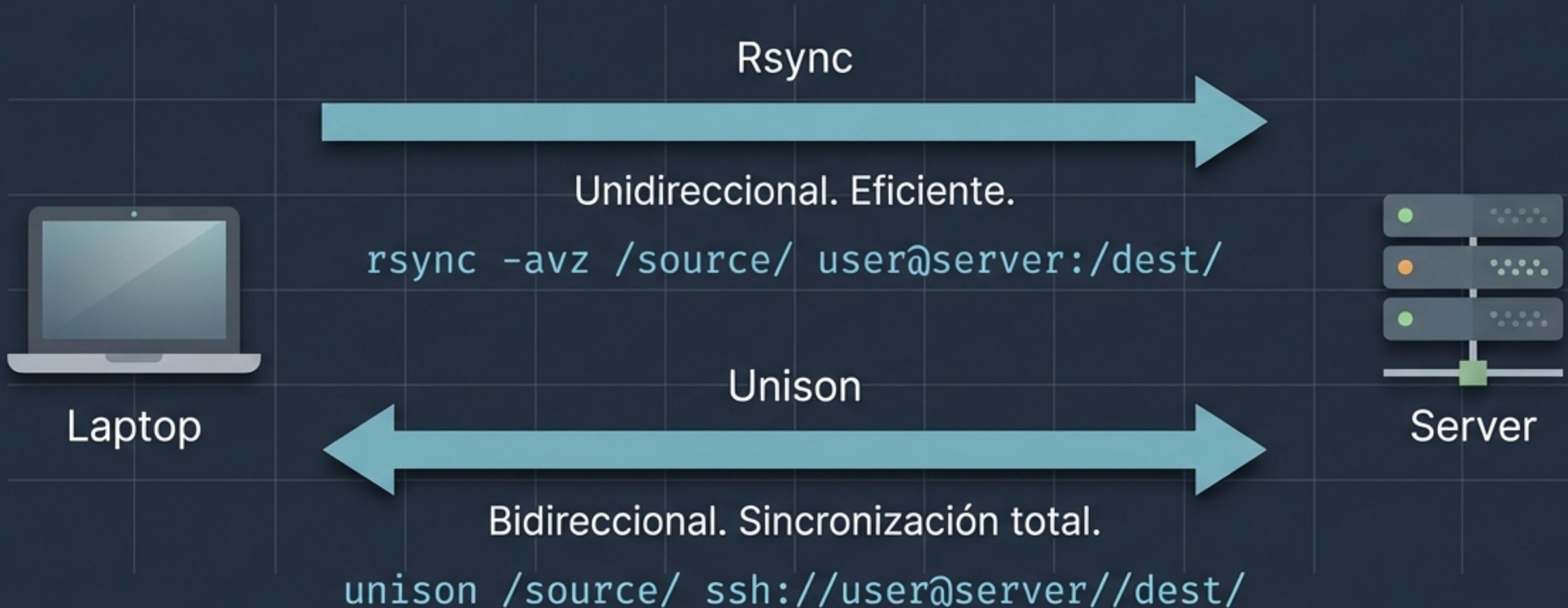
2. Powertop (Diagnóstico)

- Función: Identificar procesos de alto consumo.

- Comando: 'sudo powertop'

Objetivo: Maximizar vida de batería y reducir temperatura.

Conectividad y Datos Offline



Solución para mantener la productividad sin conexión permanente.

El Piloto Automático: Cron y Systemd

Cron (Programación Clásica)



Systemd Timers (La Alternativa Moderna)

- Mayor flexibilidad y control que Cron.
- Integrado en el proceso de inicio del sistema (init).

Gestión Avanzada e Infraestructura

Infraestructura como Código

Ansible:

- Agente: No ([Agentless](#)).
- Lenguaje: [YAML](#) Playbooks.
- Uso: Despliegue rápido.

Puppet:

- Lenguaje: Declarativo (Estado).
- Uso: Gestión de estados complejos y escalables.

Control de Acceso (ACLs)

Listas de Control de Acceso:

Permisos granulares que extienden el modelo básico Propietario/Grupo/Otros.

Continuidad: Actualizaciones y Respaldo

Copias de Seguridad (Backups)

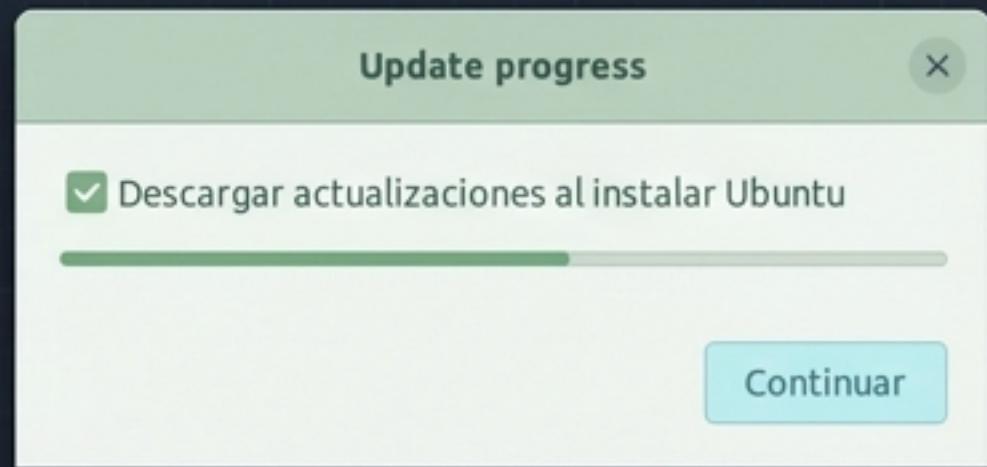
- rsnapshot: Copias incrementales vía CLI (basado en rsync).
- Deja Dup: Interfaz gráfica, integración con la nube.

Gestión de Paquetes (Updates)

Debian/Ubuntu:
`sudo apt-get update → upgrade`

Fedora/RHEL:
`sudo dnf install [paquete]`

SUSE:
`sudo zypper update`



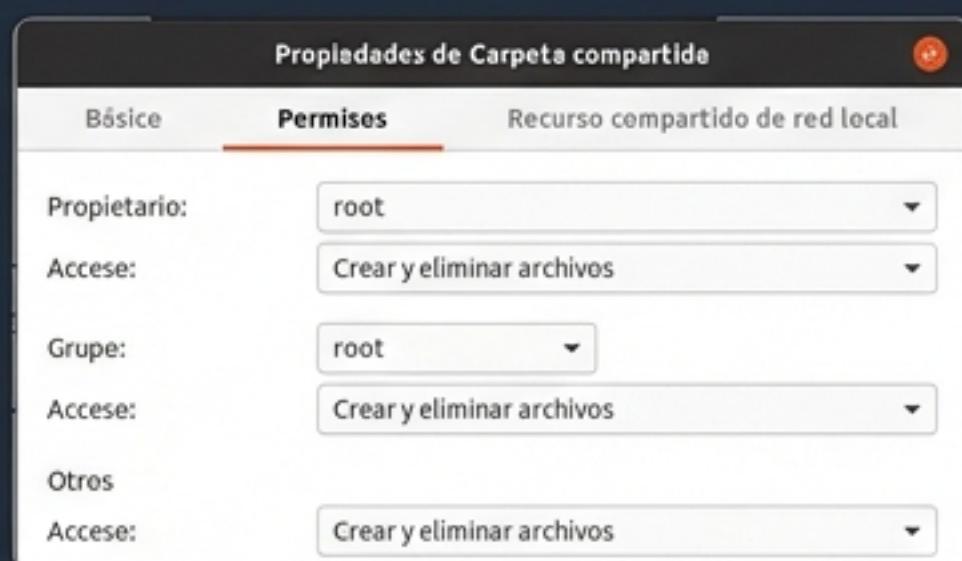
Casos Prácticos: Teoría en Acción

Caso A: La Carpeta Compartida (Sergio)

Problema: Directorio común R/W.

Solución:

1. Ejecutar 'sudo nautilus'.
2. Crear carpeta en /home.
3. Configurar permisos: 'Crear y eliminar archivos' para el Grupo.



Caso B: Actualización Crítica (Juan)

Problema: Parches de seguridad necesarios.

Workflow:

1. sudo apt-get update
2. sudo apt-get dist-upgrade
3. sudo apt-get autoremove
4. Documentar el proceso.

Checklist del Administrador de Sistemas

-  Identidad: Usuarios creados y asignados a grupos correctos (`useradd`, `usermod`).
-  Energía: TLP activado para portátiles (`systemctl start tlp`).
-  Seguridad: Permisos revisados y auditoría activa (`chmod`, `auditd`).
-  Mantenimiento: Cron jobs programados y backups verificados.

La documentación rigurosa y el mantenimiento preventivo son la diferencia entre un sistema que funciona y uno que sobrevive.