

# Solución 3.1: Configuración de ACLs en Linux

## Descripción de la tarea

Esta documentación detalla la configuración de listas de control de acceso (ACLs) en un sistema Linux para gestionar los permisos de acceso a archivos y directorios dentro de un entorno empresarial.

## Esquema de Usuarios y Grupos

Cuenta	Grupo Principal	Grupos Secundarios	Shell
sis	sistemas	sudo	bash
des	desarrollo	sudo	bash
exp	explotacion	sudo	bash

Cada usuario tendrá su carpeta personal en `/home` y una contraseña por defecto `abc123...`

## Permisos por Grupo

- A. Grupo `sistemas`** Deben tener permisos de lectura, escritura y ejecución en los directorios y subdirectorios. Permisos de lectura y escritura en todos los archivos existentes en el árbol. Pero lo que NO tendrán es permisos de ejecución en los ficheros existentes dentro del subdirectorio binarios.
- B. Grupo `desarrollo`** Deben tener acceso de lectura, escritura y ejecución en todos los directorios del árbol. En los ficheros del directorio raíz y del directorio fuentes sólo de lectura y escritura. Y en los ficheros del directorio binarios tendrán permisos de lectura, escritura y ejecución.
- C. Grupo `explotacion`** Este grupo debe tener acceso en modo lectura y ejecución sobre los ficheros del directorio binarios. Para poder ver lo que hay y navegar por los directorios, tendrán sobre ellos permisos de lectura y ejecución. Eso sí, NO podrán ni acceder al directorio fuentes.
- D. Otros usuarios** El resto de los usuarios del sistema no deben tener ningún tipo de acceso a ninguno de los ficheros o subdirectorios.
- E. ACLs por defecto** Los archivos nuevos que se vayan creando en esos directorios deben tener los mismos permisos que tienen en este momento los archivos existentes.

## Estructura de Directorios

```
datosEmpresa/  
|-- fichero1  
|-- fichero2  
|-- fuentes/  
|   |-- fichero3  
|   |-- fichero4  
|-- binarios/
```

```
|-- fichero5  
|-- fichero6
```