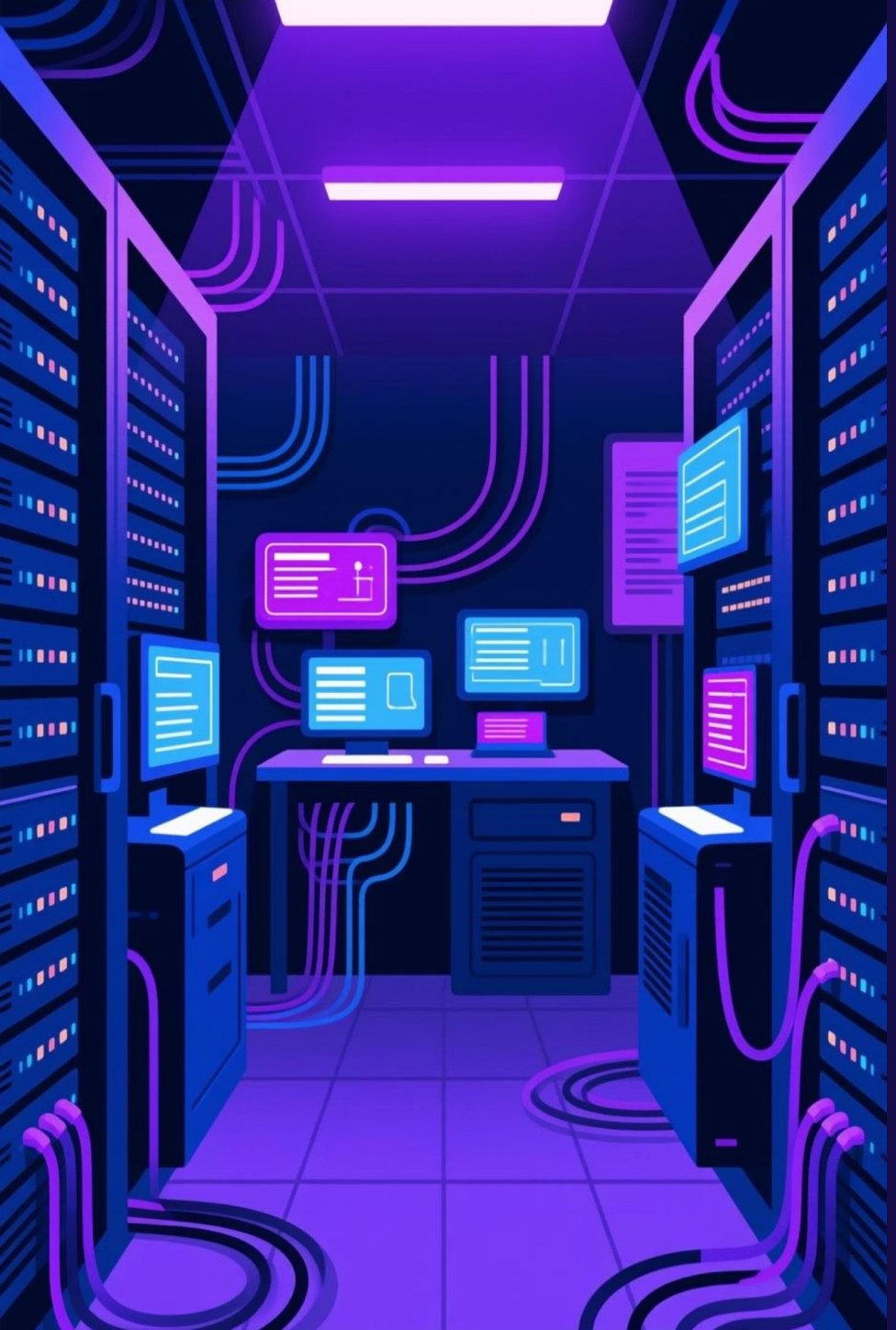


Seguridad en la configuración de sistemas operativos

Braian Flores & Santino Naldini

Arquitectura y Sistemas Operativos

Prof. Roco

Índice

Introducción

La seguridad en la configuración de los sistemas operativos es un pilar de la arquitectura de computadores. Frente a ataques, pérdida de datos y vulnerabilidades frecuentes, proteger el sistema desde su núcleo es esencial para técnicos y programadores.

Objetivo

Reconocer mecanismos de protección del sistema operativo desde la arquitectura hardware hasta la gestión de permisos y fortalecer competencias en prácticas seguras aplicables en entornos personales y profesionales.

Metas clave: comprensión técnica, implementación de políticas y

prácticas preventivas.

Marco Teórico — Conceptos fundamentales

SO y recursos

El sistema operativo coordina procesador, memoria, E/S y aplicaciones; actúa como primera línea de defensa.

Protección del sistema

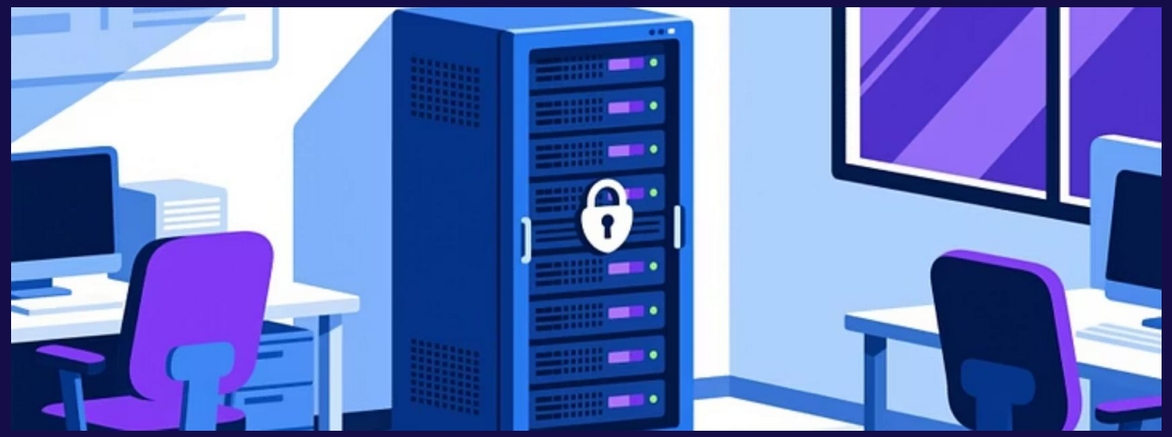
Firewalls, antivirus, cifrado y control de integridad como mecanismos esenciales.

Gestión de permisos

Modelos de control de acceso: usuarios, grupos y políticas; diferencia entre root/administrador y usuarios estándar.

Caso práctico — Escenario

Simulación teórica: pequeña empresa que implementa un servidor para almacenar información de clientes y realizar copias de seguridad, con enfoque en configuración segura del SO (Linux).



Caso práctico — Acciones simuladas

1. Creación de usuarios

Cuentas separadas con permisos mínimos; uso de root solo para tareas administrativas.

2. Permisos de archivos

Principio de menor privilegio: cada usuario accede solo a lo necesario.

3. Firewall y servicios

Activación de cortafuegos y deshabilitación de servicios innecesarios (p. ej. SSH para cuentas no autorizadas).

4. Actualizaciones

Actualizaciones automáticas de seguridad para reducir explotación de vulnerabilidades.

5. Cifrado de datos

Cifrado de directorios sensibles con LUKS o GnuPG.

Metodología

Investigación teórica basada en documentación oficial y bibliografía académica. Etapas: revisión conceptual, identificación de buenas prácticas, simulación teórica y análisis de resultados.

Revisión conceptual

Arquitectura y seguridad en SO.

Identificación de buenas prácticas

Políticas, permisos y servicios.

Simulación

Aplicación teórica de configuraciones en Linux.

Análisis

Evaluación de resultados y conclusiones.

Resultados

La simulación evidenció que la mayoría de vulnerabilidades proceden de configuraciones deficientes o permisos excesivos. Mecanismos integrados (control de acceso, cifrado, auditorías y actualizaciones) son eficaces si se aplican correctamente.

Hallazgo clave

La seguridad depende de una combinación coherente de configuraciones y políticas.

Implicación

Priorizar buenas prácticas desde la instalación del SO.

Conclusiones y bibliografía

Conclusión: la configuración segura del SO es esencial para estabilidad y protección de datos. Valor del principio de menor privilegio y segmentación de tareas. Mejora sugerida: práctica real sobre instalación y configuración segura de Linux o Windows.

Referencias principales

- Red Hat Documentation. Security and Hardening Guide.
- Microsoft Learn. Security best practices for Windows Server (2024).
- INCIBE. Guía de buenas prácticas en sistemas operativos (2023).
- Materiales de Universidad Carlos III y Universidad Nacional del Sur.