PROYECTO FINAL CIBERSEGURIDAD

Carlos Vicent Arnau Chuquispuma

spain-cs-pt-11

SEGURIDAD DEL SERVIDOR CRÍTICO CORPORATIVO

AUDITORÍA INTEGRAL DE CIBERSEGURIDAD EMPRESARIAL

INCIDENTE REAL, ANÁLISIS Y REMEDIACIÓN

PLAN ESTRATÉGICO DE PROTECCIÓN CONTINUA

CONTEXTO DEL PROBLEMA

Servidor Debian comprometido

Servicios web y datos expuestos

Riesgo alto para continuidad operativa

OBJETIVO DEL PROYECTO

- Investigar intrusión y evidencias
- Detectar vulnerabilidades críticas
- Fortalecer seguridad y gobernanza

METODOLOGÍA APLICADA

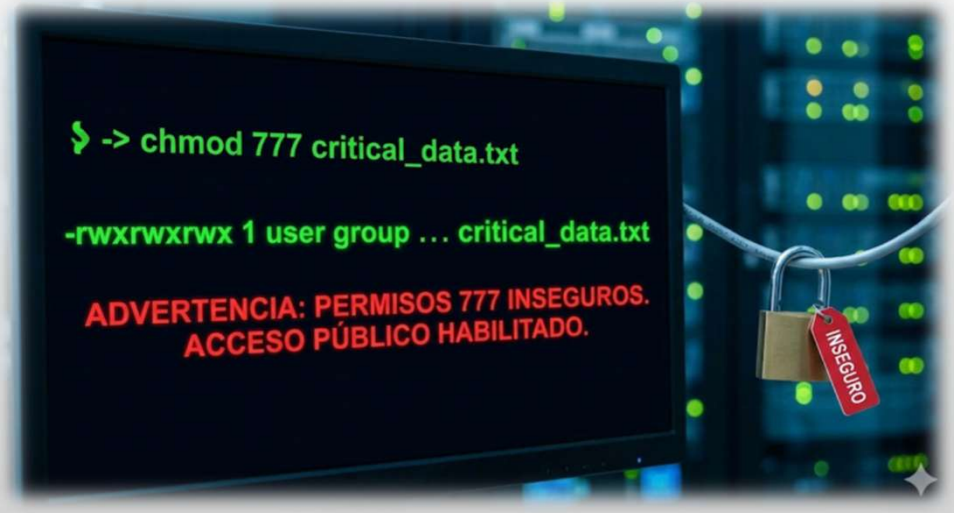
- Análisis forense digital
- Pentesting controlado Red Team
- Remediación defensiva Blue Team

HALLAZGOS FORENSES CLAVE

- Acceso root por fuerza bruta
- Contraseñas débiles expuestas
- Manipulación y borrado de rastros

VULNERABILIDADES DETECTADAS

- SSH root permitido
- Permisos 777 inseguros
- Base de datos expuesta

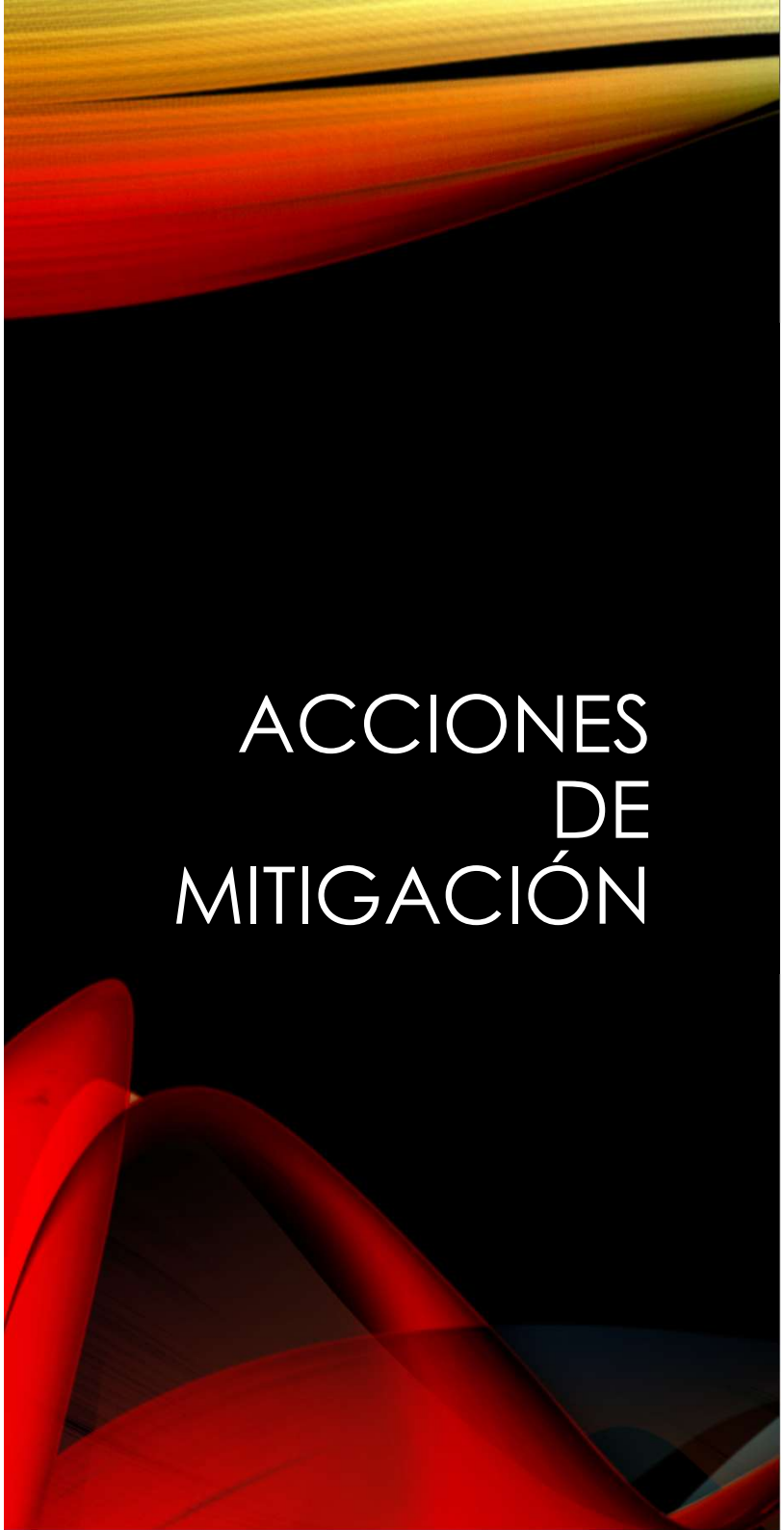


RIESGOS PARA LA EMPRESA

Robo de información sensible

Interrupción de servicios críticos

Daño reputacional y legal

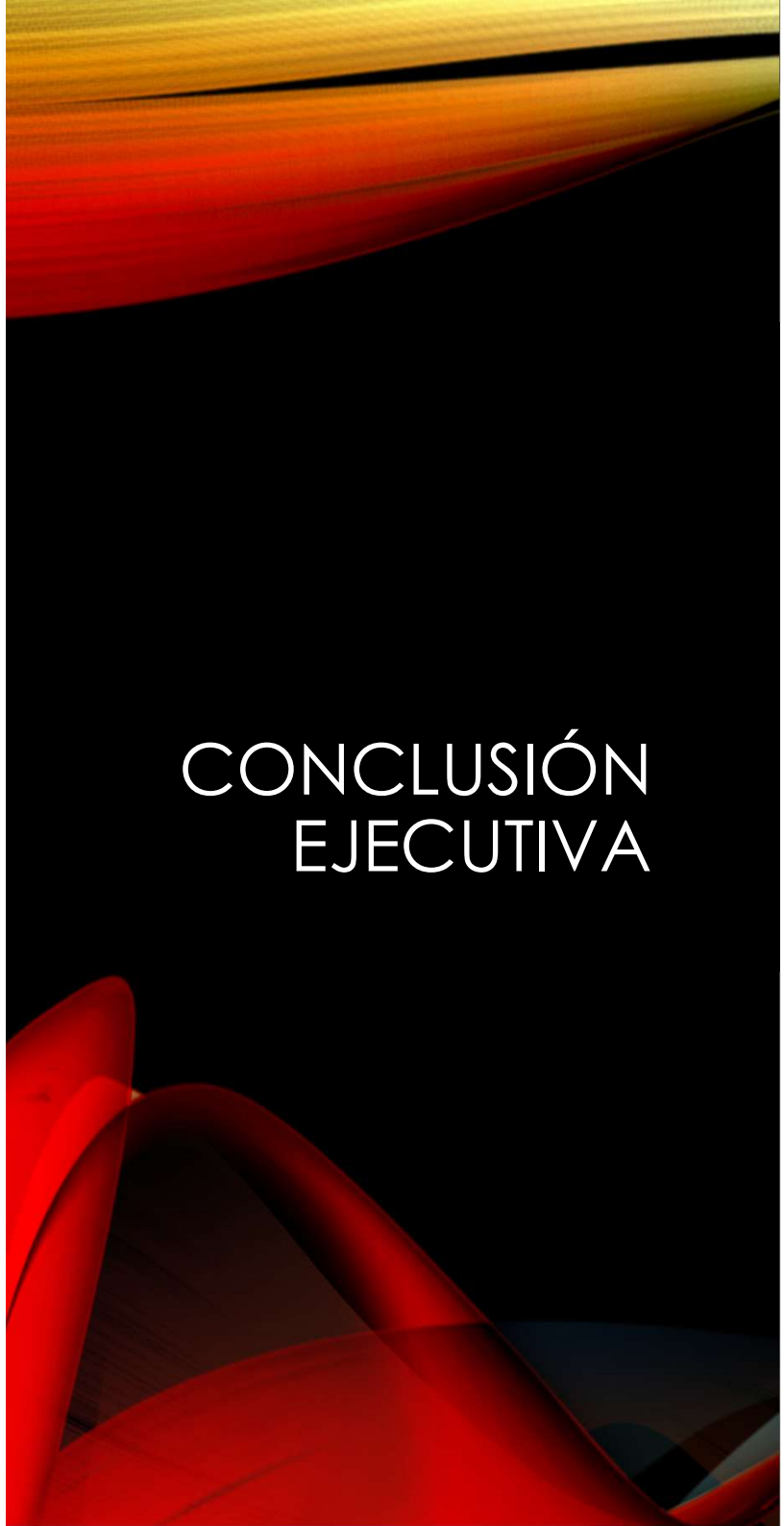


ACCIONES DE MITIGACIÓN

- Hardening completo del sistema
- HTTPS, SFTP y cifrado
- Fail2Ban y políticas fuertes

MEJORAS ESTRATÉGICAS PROPUESTAS

- WAF y monitorización SIEM
- Doble factor en accesos
- Backups automatizados seguros



CONCLUSIÓN EJECUTIVA

Riesgo crítico reducido significativamente

Infraestructura ahora resiliente

Seguridad como proceso continuo