Caso 5: Gestion de Vulnerabilidades

Nota: Documento demostrativo (caso hipotetico/anonimizado)
No contiene datos reales de clientes.

RESUMEN EJECUTIVO
Implementacion de programa estructurado de gestion de vulnerabilidades incluyendo escaneo automatizado y hardening de sistemas criticos.

ALCANCE
- Escaneo de vulnerabilidades en 45 servidores
- Hardening de sistemas Windows Server y Linux
- Revision de configuraciones de red \(firewalls, routers\)
- Evaluacion de aplicaciones web \(OWASP Top 10\)
- Validacion de parches criticos aplicados

HALLAZGOS PRINCIPALES
ALTA: 15 servidores con parches criticos faltantes
ALTA: SSH con autenticacion por contrasena habilitada
MEDIA: Servicios innecesarios ejecutandose
MEDIA: Cifrados debiles en TLS \(RC4, 3DES\)

ENTREGABLES
- Reporte de vulnerabilidades inicial \(2,400 hallazgos\)
- Reporte post-remediacion \(reduccion 89%\)
- Scripts de hardening automatizados
- Baseline de configuraciones seguras \(CIS Level 1\)

RESULTADOS
Remediacion del 89% de vulnerabilidades en 90 dias.
Reduccion de tiempo de remediacion de 45 a 12 dias.