Caso 6: Respuesta a Incidentes

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

RESUMEN EJECUTIVO
Desarrollo de plan de respuesta a incidentes y ejecucion de simulacros tabletop para validar procedimientos y entrenar al equipo.

ALCANCE
- Desarrollo de plan de respuesta a incidentes
- Definicion de roles y responsabilidades \(RACI\)
- Diseno de 3 escenarios de simulacro realistas
- Ejecucion de ejercicios tabletop
- Evaluacion de tiempos de respuesta y decisiones

HALLAZGOS PRINCIPALES
ALTA: Sin procedimiento documentado de IR
ALTA: Cadena de escalamiento poco clara
MEDIA: Sin herramientas de analisis forense
MEDIA: Backup sin probar en 18 meses

ENTREGABLES
- Plan de respuesta a incidentes \(IRP\) completo
- Playbooks por tipo \(ransomware, DDoS, breach\)
- Matriz de clasificacion de incidentes
- Arbol de decision de escalamiento
- Reporte de simulacros ejecutados \(3 escenarios\)

RESULTADOS
Tiempo promedio de deteccion reducido de 4 horas a 45 minutos.
Capacitacion de 25 miembros del equipo.