Playbook de respuesta a ransomware

CiberConscientes · Guía paso a paso

1. Detección

Identificar señales: archivos cifrados, notas de rescate, alertas del EDR.

2. Contención

Aislar los equipos afectados de la red. NO apagar (preservar evidencia volátil).

3. Erradicación

Identificar el vector de entrada y eliminar la persistencia del atacante.

4. Recuperación

Restaurar desde backups verificados y offline. Validar integridad antes de reconectar.

5. Lecciones aprendidas

Documentar el incidente y ajustar controles para prevenir recurrencia.