Laboratorio 4

Activos críticos

Bases de datos, sitio web, plataforma de correo electrónico

Análisis y amenazas

Phishing, Ransomware, DDOS

Formación de equipo

Responsable de comunicaciones, técnico en sistemas, responsable legal

Respuestas

Monitoreo de logs, alertas en tiempo real, revisión tráfico web

Plan contención

Aislar sistema comprometido, cambiar credenciales, notificación interna

Plan de recuperación

Restauración de copias de seguridad, pruebas de funcionalidad, notificación a clientes