Título: Plan de Respuesta ante Incidentes (Basado en NIST SP 800-61)

Contenido:

Fases del Incidente en SI360:

1. **Detección:** El operador nota saturación en las barras del NOC o alertas en la terminal.
2. **Contención:** Acción inmediata de bloqueo para evitar que el ataque DoS tumbe los servicios de la Universidad.
3. **Erradicación:** Identificación del puerto vulnerable (Ej: Puerto 22 detectado con Nmap).
4. **Recuperación:** El sistema vuelve a estado verde ("SISTEMA PROTEGIDO").
5. **Lecciones Aprendidas:** Registro del incidente en la bitácora histórica para auditoría futura.