Escenario de ataque Ransomware

Por:

- ★ Brandon Ortegon
- ★ David Hurtado
- ★ Jaime Angulo
- ★ Laura Agudelo

Universidad Nacional de Colombia – Sistemas de Información

Problema

Naturaleza del problema

- Ataque de ransomware con secuestro de datos.
- Fallas técnicas + posible error humano.

información comprometida

- Datos personales, notas y matriculas.
- Alta criticidad y riesgo de filtración.

Implicaciones éticas y legales

- Violación de privacidad (Ley de datos personales).
- Pérdida de confianza institucional.

Procesos de negocio impactados

- Inscripción, consulta de notas, comunicación interna.
- Parálisis operativa y riesgo académico.

Fallas de seguridad

- Sin backups recientes (3 meses)
- Sistema de detección no alertó.
- Posible desactualización y falta de pruebas

Causas raíz

- Gobernanza TI débil.
- Políticas inadecuadas de respaldo y respuesta.
- Falta de capacitación en ciberseguridad

Plan de acción

PASO 1

MITIGACIÓN INMEDIATA

Objetivo: contener el daño, proteger datos y mantener la confianza.

1. Aislar sistemas afectados para detener la propagación del ransomware *(Jefe de S.I.)*
2. Notificar a autoridades y comunidad universitaria, asegurando transparencia y responsabilidad ética *(Asesor Legal y Ético)*
3. Preservar evidencia técnica y legal del incidente *(Jefe de S.I. + Legal)*
4. Activar protocolos de crisis y comunicación para minimizar el caos operativo *(Gerente de Operaciones)*
5. Identificar datos comprometidos y posibles filtraciones *(Asesor Legal y Ético)*

Plan de acción

PASO 2

RECUPERACIÓN Y PREVENCIÓN

Objetivo: restablecer operaciones, evitar futuros ataques y reforzar la cultura de ciberseguridad.

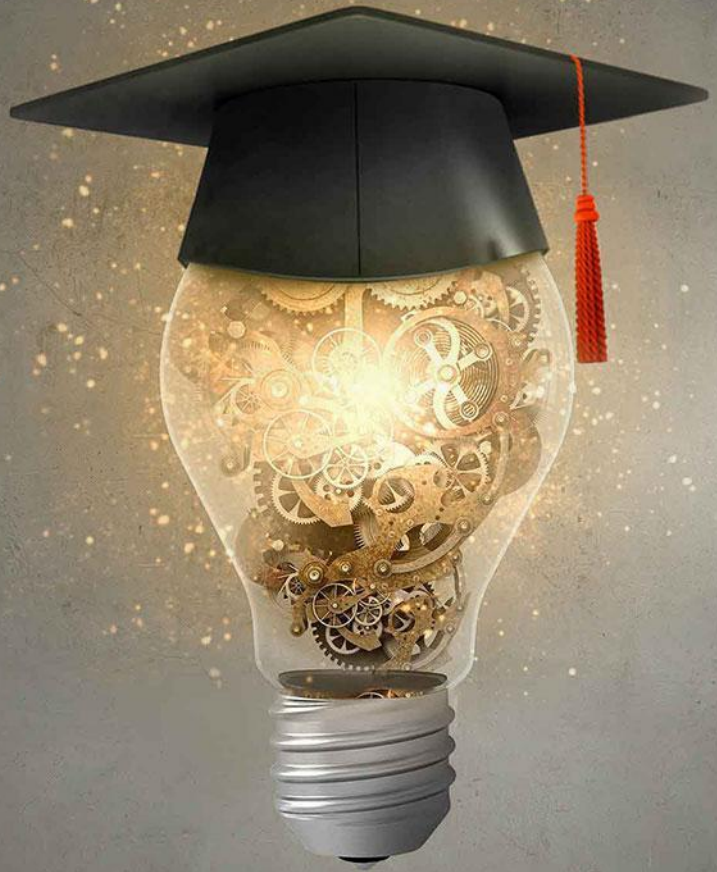
1. Recuperar sistemas desde respaldos válidos (si existen) *(Jefe de S.I.)*
2. Establecer soluciones temporales para la continuidad académica *(Gerente de Operaciones)*
3. Cumplir con obligaciones legales de protección de datos *(Asesor Legal y Ético)*
4. Implementar políticas de backup automático y frecuente *(Jefe de S.I.)*
5. Capacitar a usuarios sobre prevención de ciberataques y ética digital *(Todos los roles)*
6. Fortalecer detección de intrusos y evaluación continua de vulnerabilidades *(Jefe de S.I.)*
7. Auditoría post-incidente y mejora del protocolo de respuesta *(Todos los roles)*

¿Cómo se balancean las necesidades operativas, de seguridad y éticas?

Área	Decisión(Riesgo)
Operativas	Restaurar servicios con urgencia, de forma segura, ética y transparente, cumpliendo la ley.
Seguridad	Investigar el ataque, identificar la vulnerabilidad y aplicar medidas para prevenir futuros incidentes.
Etica/legal	No pagar el rescate. Informar a las partes y cumplir con las obligaciones legales.

¿Cómo son las prioridades más importantes en las crisis?

Prioridades	Descripción
Preparación	Apagar todos servidores y verificar sí algo más fue afectado
Establecer comunicación interna	Habilitar canales alternativos, para informar a la comunidad universitaria
Evaluar Daños	Verificar si existe alguna copia de seguridad así sea antigua
Restaurar servicios críticos	Como notas/matriculas, correos institucionales
Tomar la decisión	En este caso NO pagar el rescate



MUCHAS GRACIAS