ESCUELA MILITAR DE INGENIERIA
Mcal. ANTONIO JOSÉ DE SUCRE
BOLIVIA

ACTIVIDAD 5

CIBERCRIMEN Y CIBERTERRORISMO

Informática Forense

Ing. Yoelma Melendres Flores

Estudiante:

Sofia Guadalupe Alejo García	S9077-8
Cesar Tintaya Ruiz	S9117-0
Gustavo Andrés Arequipa Gonzales	S9170-7

SEMESTRE:

Octavo

CARRERA:

Sistemas

SANTA CRUZ DE LA SIERRA, 2025

ACTIVIDAD ACADÉMICA: CIBERCRIMEN Y CIBERTERRORISMO

Descripción del caso:

“El sistema de gestión académica de una universidad ha sido comprometido. Los atacantes exigen dinero y amenazan con filtrar datos personales de los estudiantes. Se sospecha de un grupo con motivaciones ideológicas”.

Realizar:

1. **Identificar el tipo de ataque.**

Cibercrimen: Los atacantes buscan obtener una ganancia económica directa mediante la amenaza de divulgar datos; su motivación instrumental (dinero) domina sobre cualquier retórica ideológica.

Motivos que sustentan la clasificación como cibercrimen

- **Motivación económica predominante**

Demanda de pago: La exigencia explícita de dinero es el indicador más directo de cibercrimen. En la mayoría de los casos legales y forenses, la presencia de extorsión económica sitúa el incidente dentro del ámbito de la delincuencia financiera cibernética.

- **Tácticas comunes de cibercrimen presentes**

Extorsión por divulgación de datos (double extortion): Combinación de cifrado o secuestro de sistemas + exfiltración y amenaza de divulgación — táctica típica de grupos criminales orientados a lucro.

Ransomware: Aunque no se informa explícitamente de cifrado, la exigencia de pago es congruente con ataques de ransomware o ataques de filtración condicionada al pago.

Impacto probable

Privacidad: Exposición de datos personales de estudiantes (Nombres, CI, correos, calificaciones, direcciones, teléfono, historial académico).

Reputacional: Perjuicio a la confianza de la comunidad universitaria y posibles demandas.

Operativo: Interrupción temporal de servicios académicos.

Legal/Regulatorio: Posibles sanciones por protección de datos personales (leyes locales/internacionales) y obligación de notificar a afectados.

2. **Analizar los vectores de ataque.**

La intrusión en el sistema de gestión académica de la universidad pudo haberse producido a través de varios vectores de ataque comunes en incidentes de cibercrimen orientados a extorsión, como el descrito:

Phishing y Ingeniería Social:

- Correos electrónicos maliciosos dirigidos a empleados o administradores con enlaces o archivos infectados, logrando que otorguen acceso o entreguen credenciales.
- Manipulación de personal para obtener acceso a sistemas críticos.

Explotación de Vulnerabilidades Técnicas:

- Aprovechamiento de fallos sin parchear en el software del sistema académico o en servicios relacionados (web, base de datos, servidores).
- Uso de exploits conocidos o herramientas automatizadas para comprometer sistemas.

Uso de Credenciales Robadas o Débiles:

- Acceso con usuarios y contraseñas obtenidas antes por filtraciones o fuerza bruta.
- Reutilización de contraseñas o falta de autenticación multifactor para proteger accesos.

Movimientos Laterales Internos:

- Una vez dentro de la red, el atacante podría haber escalado privilegios y accedido a bases de datos con información personal.
- Uso de malware o backdoors para mantener persistencia y moverse sin ser detectado.

Tácticas de Ransomware y Extorsión:

- Cifrado de datos o secuestro de sistemas para condicionar su recuperación al pago.
- Exfiltración de datos para aplicar la doble extorsión, amenazando con divulgar información personal sensibles en caso de impago.

3. **Proponer un plan de respuesta.**

Medidas Técnicas (Respuesta y Mitigación)

Fase inmediata (contención y análisis)

1. **Aislamiento de los sistemas comprometidos:** Desconectar del entorno de red todos los servidores y equipos afectados para evitar propagación del ataque o filtración adicional.
2. **Preservación de evidencias digitales:** Resguardar copias forenses de logs, discos y memoria RAM antes de realizar cualquier limpieza.
3. **Activación del protocolo de respuesta a incidentes:** Convocar al equipo CERT/CSIRT institucional o equivalente, y establecer comunicación con proveedores de ciberseguridad externos si es necesario.

4. **Identificación del vector de entrada:** Revisar logs de autenticación, accesos remotos, correos de phishing y vulnerabilidades conocidas en los sistemas (Moodle, SAGA, etc.).
5. **Cambio forzado de credenciales:** Restablecer contraseñas de todos los usuarios, especialmente administradores y personal TI.
6. **Revisión de copias de seguridad:** Validar integridad y disponibilidad de respaldos previos al ataque para restauración segura.

Fase de recuperación

1. **Restaurar los sistemas desde copias seguras y limpias.**
2. **Aplicar actualizaciones de seguridad y parches críticos.**
3. **Implementar controles reforzados:** Autenticación multifactor (MFA), segmentación de red, listas de control de acceso (ACLs) y cifrado de bases de datos.
4. **Monitoreo continuo y auditoría post-incidente:** Emplear herramientas de detección de intrusos (IDS/IPS) y SIEM para vigilancia continua.

Fase de prevención futura

- **Capacitación en ciberseguridad** para todo el personal administrativo y docente (reconocimiento de phishing, buenas prácticas de contraseñas, uso de canales seguros).
- **Evaluaciones periódicas de vulnerabilidades** y pruebas de penetración.
- **Política de gestión de incidentes documentada** y simulacros regulares de respuesta ante ciberataques.

Medidas Legales

1. **Notificación a las autoridades competentes:** Comunicar el incidente al **Ministerio Público** (Unidad de Delitos Informáticos) y a la **Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT)**, en cumplimiento de normativas bolivianas.
2. **Asesoría legal especializada:** Activar el comité jurídico institucional para evaluar responsabilidades y pasos legales a seguir.

- **Ley 1080 – Ley de Ciudadanía Digital** Artículo 12: ***Protección de datos personales y seguridad informática***. Establece que los servidores y funcionarios del Estado deben usar los datos personales solo para los fines permitidos por la normativa vigente, y obliga responsabilidad si se incumple.
- **Artículo 227 – Extorsión**: amenaza, intimidación con fines de obtener beneficio económico. En este caso, exigencia de dinero más amenaza de divulgar datos

personales podría encajar aquí. Sanciones de prisión de 2 a 4 años, o de 4 a 8 años si es caso especialmente grave.

- **Art. 363 bis / Art. 363 ter** – Disposiciones vinculadas a delitos informáticos / manipulación informática, alteración, acceso y uso indebido de datos informáticos. Estas normas sancionan, entre otras conductas, el acceso no autorizado a datos, su alteración o uso indebido.
- **Constitución Política del Estado (CPE), Bolivia:** Derecho a la privacidad e intimidad. Este fondo constitucional refuerza las obligaciones legales de organismos públicos/privados. (Referencias a habeas data, intimidad, etc.)

3. **Protección de datos personales:** Cumplir con la normativa nacional e internacional (por ejemplo, principios del RGPD o leyes locales de privacidad).
4. **Conservación de evidencias:** Mantener todos los registros técnicos y comunicaciones relacionados con el ataque bajo cadena de custodia.
5. **Notificación a las personas afectadas:** Comunicar formalmente a los estudiantes sobre la posibilidad de exposición de sus datos personales y orientar sobre medidas preventivas (cambio de contraseñas, vigilancia de cuentas, etc.).
6. **No negociación ni pago del rescate:** Evitar cualquier pago a los atacantes, dado que no garantiza la recuperación segura y podría constituir financiamiento indirecto de actividades ilícitas.

Medidas Comunicacionales

1. **Activación de un Comité de Crisis:** Integrado por Rectorado, Dirección de Comunicación, Asesoría Legal y Departamento de TI, encargado de centralizar todas las decisiones y mensajes públicos.
2. **Comunicación interna controlada:** Informar a docentes, estudiantes y personal administrativo sobre el incidente, los pasos de mitigación y la continuidad académica, evitando generar alarma innecesaria.
3. **Comunicación externa y pública:** Emitir un comunicado institucional oficial, con un lenguaje transparente pero prudente, destacando las medidas adoptadas y la cooperación con las autoridades.
4. **Gestión de reputación:** Reforzar la confianza de la comunidad universitaria mediante campañas de transparencia y de mejora de la ciberseguridad institucional.
5. **Relación con medios de comunicación:** Nombrar un único vocero autorizado y evitar declaraciones no coordinadas que puedan afectar la investigación.
6. **Seguimiento y actualización pública:** Proporcionar información progresiva a medida que se avance en la contención y la investigación.

Conclusiones

El incidente analizado se clasifica como **cibercrimen**, ya que la motivación principal de los atacantes es **económica**, evidenciada por la exigencia de dinero a cambio de no divulgar información sensible.

La intrusión probablemente se produjo mediante **phishing, vulnerabilidades técnicas o contraseñas débiles**, lo que resalta la necesidad de fortalecer la seguridad interna y la capacitación del personal.

El **plan de respuesta** combina acciones **técnicas**, **legales** y **comunicacionales**: aislar y restaurar sistemas, aplicar la **Ley 1080**, los **artículos 227 y 363 bis/ter del Código Penal**, y comunicar de forma transparente a la comunidad universitaria.