Módulo 8: Práctica

Trabajo Práctico: Fundamentos y Desafíos Emergentes en la Seguridad de Bases de Datos

Introducción: En el panorama digital actual, los datos se han convertido en uno de los activos más valiosos para organizaciones de todos los tamaños. Las bases de datos, que almacenan información crítica para operaciones comerciales, detalles personales y propiedad intelectual, son, por lo tanto, blancos frecuentes de ataques. Las consecuencias de una violación de datos pueden ir mucho más allá de las pérdidas financieras inmediatas, incluyendo daño a la reputación, pérdida de confianza del cliente, sanciones legales y regulatorias, interrupción operativa y desventaja competitiva. De hecho, el costo promedio de una violación de datos alcanzó los $4.45 millones en 2023. Proteger estos activos es fundamental, y requiere un enfoque multifacético que combine controles técnicos, políticas administrativas y concienciación sobre seguridad. La seguridad efectiva de las bases de datos no es solo una necesidad técnica, sino también un requisito legal y una obligación ética.

Objetivos de Aprendizaje: Al completar este trabajo práctico, los estudiantes deberán ser capaces de:

- Comprender la importancia crítica de la seguridad de las bases de datos en el contexto actual.
- Investigar y comprender los principios de tecnologías de cifrado avanzadas como el cifrado homomórfico.
- Identificar y describir las técnicas de auditoría y monitoreo esenciales para la seguridad de bases de datos relacionales.
- Comprender y aplicar los principios de las estrategias de respaldo y recuperación para garantizar la resiliencia y disponibilidad de los datos.
- Reconocer la relevancia de la legislación en materia de privacidad de datos.

Preguntas de Investigación:

1. **Explorando el Cifrado Homomórfico para la Protección de Datos en Uso:** Los textos indican que el cifrado es una medida de protección crucial para los datos, ya sea en reposo *(almacenados en disco*), en tránsito (*viajando por la red*) o **en uso (***mientras se procesan en la memoria***)**. Específicamente, se menciona el **cifrado homomórfico** como una tecnología emergente para proteger los datos mientras se procesan en la memoria.

Basándose en la importancia de proteger la información confidencial, desarrolle una investigación sobre el cifrado homomórfico que incluya:

- **¿Qué es el cifrado homomórfico?** (Definición y concepto básico).
- **¿Cuál es su principio fundamental y cómo se diferencia de otras técnicas de cifrado más tradicionales** (como el cifrado en reposo o en tránsito) **en términos de su aplicación a los datos en uso?**

- **Identifique al menos dos ventajas clave y dos desafíos o limitaciones** para su implementación en sistemas de bases de datos a gran escala.
- **Mencione al menos dos ejemplos concretos de aplicaciones potenciales** donde el cifrado homomórfico podría ser particularmente útil para garantizar la privacidad y seguridad de los datos en bases de datos.

Nota para el estudiante: Los textos proporcionados mencionan el cifrado homomórfico como una tecnología emergente para proteger datos en uso. Para responder a esta pregunta en profundidad, necesitará **investigar en fuentes externas**, ya que las ofrecidas no detallan sus principios o funcionamiento específico.

2. **Técnicas de Auditoría y Monitoreo en Bases de Datos Relacionales:** La auditoría y el monitoreo en tiempo real de la actividad de las bases de datos son herramientas esenciales para detectar actividades sospechosas y proporcionar un registro forense para análisis posteriores. La auditoría de la base de datos puede ayudar a identificar cambios no autorizados en registros críticos.

Investigue y describa las técnicas de auditoría y monitoreo más relevantes aplicables a las bases de datos relacionales. Su investigación debe cubrir:

- **¿Cuál es el propósito principal de la auditoría y el monitoreo** en la seguridad de bases de datos?
- **Describa al menos tres tipos de actividades o eventos específicos que deben ser monitoreados** en una base de datos para detectar posibles incidentes de seguridad (por ejemplo, seguimiento de inicios de sesión, cambios de esquema, ejecución de consultas).
- **Explique cómo las herramientas de Gestión de Eventos e Información de Seguridad (SIEM)** pueden mejorar la detección de incidentes al analizar registros de auditoría de bases de datos.
- **Argumente la importancia de la auditoría y el monitoreo para el cumplimiento legal y normativo**, haciendo referencia a la necesidad de proteger la información personal del cliente y cumplir con regulaciones como la Ley 25.326 en Argentina o el RGPD en la UE, que exigen medidas de seguridad de datos.

3. **Estrategias de Respaldo y Recuperación para la Resiliencia de Bases de Datos:** La pérdida y corrupción de datos debido a diversas causas, desde fallas de hardware hasta ataques maliciosos, pueden tener consecuencias devastadoras para las organizaciones, incluyendo interrupciones operativas, pérdidas financieras y daño a la reputación. Las estrategias de respaldo y recuperación son componentes críticos de la seguridad de las bases de datos para mitigar estos riesgos y garantizar la continuidad del negocio.

Basándose en la importancia de proteger la información y asegurar la disponibilidad de los datos, desarrolle una investigación que abarque:

- **Defina la importancia fundamental de las estrategias de respaldo y recuperación** en el contexto de la seguridad y disponibilidad de las bases de datos.
- **Describa detalladamente los siguientes tipos de respaldo**, explicando cuándo se aplica cada uno y sus implicaciones para la recuperación:
  - **Respaldo completo**: Consiste en una copia completa de toda la base de datos.
  - **Respaldo diferencial**: Guarda solo los cambios que se han producido desde el último respaldo completo.
  - **Respaldo incremental**: Registra los cambios desde el último respaldo de cualquier tipo (*completo, diferencial o incremental*).
  - **Respaldo de registro de transacciones**: Consiste en un registro de todas las transacciones que se han realizado en la base de datos, crucial para la recuperación puntual.
- **Explique la "Regla 3-2-1" para respaldos** y justifique por qué cada uno de sus componentes es vital para una estrategia de protección de datos robusta. Esta regla establece que se deben mantener al menos **tres (3) copias** de los datos, almacenar estas copias en **dos (2) tipos de almacenamiento diferentes**, y tener **una (1) copia almacenada fuera del sitio o en la nube**.
- **Discuta la relación entre las estrategias de respaldo y la definición del Objetivo de Punto de Recuperación (RPO) y el Objetivo de Tiempo de Recuperación (RTO)**, así como la importancia de probar y documentar los procedimientos de recuperación.

Recursos Sugeridos:

Para la investigación de las preguntas, puede consultar los siguientes sitios web. **Tener en cuenta que esta información proviene de fuentes externas y puede que necesite verificarla de forma independiente.**

- **Para Cifrado Homomórfico:**
  - **Microsoft Research - Criptografía Homomórfica:** https://www.microsoft.com/en-us/research/project/homomorphic-encryption/ (sitio en inglés, busca versiones en español o utiliza herramientas de traducción)
  - **IBM Research - Fully Homomorphic Encryption:** https://www.ibm.com/blogs/research/2021/04/08/fully-homomorphic-encryption-is-more-real-than-you-think/ (sitio en inglés, busca versiones en español o utiliza herramientas de traducción)
  - **OpenFHE:** https://www.openfhe.org/ (Comunidad y recursos sobre cifrado homomórfico. Sitios con recursos técnicos y académicos).
- **Para Auditoría, Monitoreo y Estrategias de Respaldo y Recuperación de Bases de Datos Relacionales:**

- **Documentación oficial de proveedores de bases de datos** (ejemplo, busca "auditoría Oracle Database", "SQL Server Audit", "PostgreSQL audit logging", "backup and restore Oracle", "SQL Server backup strategies", "PostgreSQL backup"):
  - **Oracle:** https://docs.oracle.com/en/database/oracle/oracle-database/index.html (Navega a la sección de seguridad, auditoría, administración o respaldo y recuperación)
  - **Microsoft SQL Server:** https://learn.microsoft.com/es-es/sql/relational-databases/security/auditing/sql-server-audit-database-engine?view=sql-server-ver16 y https://learn.microsoft.com/es-es/sql/relational-databases/backup-restore/backup-overview-sql-server?view=sql-server-ver16
  - **PostgreSQL:** https://www.postgresql.org/docs/ (Navega a la sección de logging, seguridad o backup y restore)
- **Sitios de ciberseguridad y blogs especializados:** Busca "auditoría bases de datos", "monitoreo seguridad bases de datos", "SIEM database security", "estrategias de backup bases de datos", "plan de recuperación de desastres".
  - **Ejemplo general:** https://www.incibe.es/ (Instituto Nacional de Ciberseguridad de España - busca recursos sobre seguridad de bases de datos, incluyendo respaldo).

Formato y Entrega:

- El trabajo debe presentarse en formato digital (PDF).
- Extensión sugerida: entre 3 y 5 páginas (*sin contar portada y bibliografía*).
- Incluir una portada con los datos del alumno *(nombre, apellido, nro de legajo, carrera, asignatura, fecha*).
- Citar todas las fuentes utilizadas (*incluyendo las proporcionadas y las investigadas*) en formato APA o similar. Ver https://normas-apa.org/
- Se valorará la claridad en la exposición, la coherencia de las ideas, el uso de terminología técnica apropiada y la capacidad de síntesis.