UDS

Mi Universidad

Nombre del Alumno: ***Vania Natali Santizo Morales***

Nombre del tema: ***Trabajo Plataforma 2***

Parcial: ***1° Parcial***

Nombre de la Materia: ***Base de datos 2***

Nombre del profesor: ***Andrés Alejandro Reyes Molina***

Nombre de la Licenciatura: ***Ingeniería en Sistemas Computacionales***

Cuatrimestre: ***8°***

Seguridad en Sistemas de Información

Concepto de Seguridad

- Definición de seguridad en el contexto de sistemas de información
  - La seguridad en el DML implica el uso de comandos de manipulación de datos de manera que se protejan los datos sensibles.
  - Es crucial implementar controles de acceso y auditoría en las operaciones de DML.
- Importancia de la seguridad en la era digital
  - La creciente dependencia de la tecnología ha aumentado la vulnerabilidad de los sistemas a ataques cibernéticos.
  - La protección de datos sensibles es crucial para mantener la confianza de los usuarios y la reputación de las organizaciones.
  - La seguridad adecuada puede prevenir pérdidas financieras significativas y daños a la infraestructura.

Identidad y Autentificación

- Conceptos de identidad y autentificación en sistemas de información
  - La identidad se refiere a la representación de un usuario o entidad en un sistema, mientras que la autentificación es el proceso de verificar esa identidad.
  - Existen varios métodos de autentificación, incluyendo contraseñas, biometría y autenticación de dos factores.
- Métodos de autentificación
  - Contraseñas: Son el método más común, pero pueden ser vulnerables a ataques de fuerza bruta.
  - Biometría: Utiliza características físicas únicas, como huellas dactilares o reconocimiento facial, para autenticar usuarios.
  - Autenticación de dos factores (2FA): Combina dos métodos de autentificación para aumentar la seguridad.

Matriz de Autorización

- Definición y propósito de la matriz de autorización
  - Una matriz de autorización es una herramienta que define qué usuarios tienen acceso a qué recursos dentro de un sistema.
  - Permite gestionar y controlar los permisos de acceso de manera eficiente y clara.
- Componentes de una matriz de autorización
  - Usuarios: Identificación de los individuos o grupos que requieren acceso.
  - Recursos: Especificación de los sistemas, aplicaciones o datos a los que se desea controlar el acceso.
  - Permisos: Definición de las acciones que cada usuario puede realizar sobre los recursos, como leer, escribir o modificar.

Definición de un Esquema de Seguridad

- Elementos clave de un esquema de seguridad
  - Un esquema de seguridad es un conjunto de políticas y procedimientos diseñados para proteger la información.
  - Debe incluir aspectos como la gestión de riesgos, la respuesta a incidentes y la formación de usuarios.
- Implementación de un esquema de seguridad
  - Evaluación de riesgos: Identificación de amenazas y vulnerabilidades en el sistema.
  - Políticas de seguridad: Desarrollo de normas y procedimientos que guíen el comportamiento de los usuarios.
  - Capacitación: Formación continua para los empleados sobre prácticas seguras y concienciación sobre seguridad.

Mecanismos para Implantación de Seguridad

- Herramientas y técnicas para la implementación de seguridad
  - La implementación de seguridad puede incluir tecnologías como firewalls, sistemas de detección de intrusos y software antivirus.
  - Es fundamental realizar auditorías de seguridad periódicas para identificar y corregir vulnerabilidades.
- Estrategias de seguridad
  - Seguridad perimetral: Protección de la red mediante dispositivos de seguridad en los límites.
  - Seguridad en la capa de aplicación: Implementación de medidas de seguridad directamente en las aplicaciones para proteger datos sensibles.
  - Seguridad en la nube: Consideraciones especiales para proteger datos y aplicaciones alojadas en entornos de nube.

Bases de Datos Estadísticas

- Importancia de las bases de datos estadísticas en la seguridad
  - Las bases de datos estadísticas permiten el análisis de patrones de acceso y comportamiento de usuarios, lo que puede ayudar a detectar actividades sospechosas.
  - Proporcionan información valiosa para la toma de decisiones en la gestión de la seguridad.
- Uso de bases de datos para la seguridad
  - Análisis de logs: Revisión de registros de acceso para identificar intentos de acceso no autorizados.
  - Monitoreo de anomalías: Uso de algoritmos para detectar comportamientos inusuales que puedan indicar un ataque.
  - Informes de seguridad: Generación de informes que resuman el estado de la seguridad y las amenazas detectadas.

Encriptamiento de Datos

- Concepto y propósito del encriptamiento
  - El encriptamiento es el proceso de convertir datos en un formato ilegible para proteger su confidencialidad.
  - Se utiliza para proteger información sensible tanto en tránsito como en reposo.
- Tipos de encriptamiento
  - Encriptamiento simétrico: Utiliza la misma clave para encriptar y desencriptar datos, lo que puede ser más rápido pero menos seguro si la clave se ve comprometida.
  - Encriptamiento asimétrico: Utiliza un par de claves (una pública y una privada), lo que proporciona un nivel adicional de seguridad.
  - Protocolos de encriptamiento: Implementación de estándares como SSL/TLS para proteger la comunicación en línea.

Seguridad Empleando un DML con un DBMS Comercial

- Integración de seguridad en el DML (Data Manipulation Language)
  - La seguridad en el DML implica el uso de comandos de manipulación de datos de manera que se protejan los datos sensibles.
  - Es crucial implementar controles de acceso y auditoría en las operaciones de DML.
  - Control de acceso: Definición de roles y permisos para limitar el acceso a datos sensibles.
- Mejores prácticas para la seguridad en DBMS comerciales
  - Auditoría de cambios: Registro de todas las operaciones realizadas en la base de datos para detectar y responder a incidentes.
  - Cifrado de datos: Aplicación de técnicas de encriptación para proteger datos almacenados en la base de datos.