Plan de Seguridad de la Base de Datos para el Módulo de Radiología e Imagen

Introducción:

El siguiente informe detalla el plan de seguridad propuesto para la base de datos del módulo de radiología e imagen de un hospital, utilizando una combinación de bases de datos relacional MySQL y no relacional MongoDB. La elección de esta combinación de bases de datos se basa en la necesidad de manejar una variedad de datos complejos que van desde registros clínicos detallados. La integración de sistemas relacional y no relacional permite una gestión eficiente y escalable de esta diversidad de datos, garantizando al mismo tiempo su integridad, confidencialidad y disponibilidad de los datos, así como establecer roles, usuarios, privilegios y recomendaciones para el respaldo de la base de datos. Este plan de seguridad busca proporcionar una estructura sólida y adaptable para proteger la información crítica almacenada en la base de datos del módulo de radiología e imagen del hospital, garantizando así la calidad y seguridad de la atención médica ofrecida a los pacientes.

Roles, Usuarios y Privilegios:

Roles radiología e imagen: Se definieron los roles específicos para diferentes usuarios, como Personal Médico, Personal Administrativo y Pacientes, cada uno con acceso y privilegios adecuados según sus responsabilidades y necesidades.

- **Personal Médico**: Acceso a historiales médicos, resultados de radiología, informes de imágenes, etc.
- **Personal Administrativo:** Acceso limitado a información no clínica, como horarios, programación de citas, etc.
- **Paciente**: Acceso a su historial médico y resultados de radiología de manera controlada.

Usuarios en la Base de Datos: Se definieron usuarios con roles definidos para garantizar la seguridad y el acceso controlado a la información. Esto asegura que cada usuario tenga acceso solo a la información relevante para su función dentro del sistema.

- **Usuario Médico**: Acceso completo a las tablas relacionadas con historiales médicos, resultados de radiología, informes de imágenes y otros datos clínicos relevantes.
- **Usuario Administrativo**: Acceso limitado a tablas no clínicas, como horarios, programación de citas, inventario de equipos médicos, etc.
- **Usuario Paciente**: Acceso controlado a su propio historial médico, resultados de radiología y otros datos personales de manera segura y protegida.

Privilegios en la Base de Datos: Los privilegios se asignarán de manera específica para cada tipo de usuario, asegurando un acceso apropiado y seguro a los datos. Lo que significa que se otorgan solo los permisos necesarios para realizar las tareas específicas de cada usuario. Esto minimiza el riesgo de acceso no autorizado a datos sensibles.

- **Privilegios de Usuario Médico**: SELECT, INSERT, UPDATE, DELETE en tablas clínicas, acceso a procedimientos almacenados relacionados con diagnósticos, tratamientos, etc.

- **Privilegios de Usuario Administrativo**: SELECT, INSERT, UPDATE en tablas administrativas, posiblemente con privilegios de creación de informes o consultas ad-hoc.

- **Privilegios de Usuario Paciente**: SELECT en tablas de historial médico personal, acceso limitado a su propia información médica y resultados de radiología.

Recomendaciones para el Respaldo de la Base de Datos:

1. **Frecuencia de Respaldo:**

- Se recomienda realizar respaldos completos de la base de datos relacional (MySQL) al menos una vez al día, preferiblemente fuera del horario de mayor actividad.

- Para la base de datos no relacional (MongoDB), se sugiere un respaldo incremental cada 4 horas y un respaldo completo diario.

2. **Métodos de Respaldo:**

- Para MySQL, se utilizará el comando mysqldump para realizar respaldos completos y el registro binario para respaldos incrementales.

- En MongoDB, se empleará la función de replicación y copias de seguridad automáticas integradas para garantizar la integridad de los datos.

Recomendaciones Adicionales:

- Realizar pruebas regulares de restauración de respaldos para verificar su integridad.

- Mantener actualizados los sistemas de gestión de bases de datos y aplicar parches de seguridad.

- Capacitar al personal en prácticas de seguridad de la información y protocolos de acceso seguro a la base de datos.