# Administrador de Banco de Dados (extra Abril) - Turma 2024A

## 5.19 Auditoria e monitoramento de segurança

A auditoria e o monitoramento de segurança são práticas essenciais para garantir a proteção dos dados armazenados em um banco de dados. Essas práticas ajudam a identificar possíveis ameaças de segurança e garantir que as informações críticas estejam protegidas contra acessos não autorizados.

A auditoria envolve a revisão das atividades do usuário para garantir que os dados sejam acessados e manipulados de maneira adequada e legal. A auditoria pode incluir o registro de todos os acessos ao banco de dados, incluindo o registro de data e hora do acesso, o nome do usuário e o tipo de atividade realizada. Os registros de auditoria podem ser usados para identificar possíveis atividades suspeitas, como tentativas de acesso não autorizado ou alterações indevidas nos dados.

O monitoramento envolve a verificação constante do sistema de banco de dados para detectar atividades suspeitas e vulnerabilidades de segurança. O monitoramento pode incluir o uso de ferramentas de segurança para detectar e relatar atividades suspeitas, como tentativas de acesso não autorizado ou alterações nos dados. O monitoramento constante pode ajudar a identificar problemas de segurança antes que causem danos significativos.

Juntos, a auditoria e o monitoramento são fundamentais para garantir a segurança dos dados armazenados em um banco de dados. Eles ajudam a identificar possíveis vulnerabilidades de segurança e garantem que as políticas e procedimentos de segurança estejam sendo seguidos adequadamente. Além disso, a auditoria e o monitoramento ajudam a garantir a conformidade com regulamentações e políticas de segurança, como a Lei Geral de Proteção de Dados (LGPD) no Brasil.

A auditoria e o monitoramento de segurança devem ser feitos continuamente ao longo do tempo para garantir a segurança do banco de dados. Essas práticas não são eventos únicos, mas sim processos contínuos que ajudam a identificar possíveis ameaças de segurança e garantir que as políticas e procedimentos de segurança estejam sendo seguidos adequadamente.

A auditoria deve ser feita regularmente para garantir que os registros de atividades do usuário estejam sendo coletados e armazenados adequadamente. Os registros de auditoria devem ser analisados regularmente para detectar possíveis atividades suspeitas, como tentativas de acesso não autorizado ou alterações indevidas nos dados. O intervalo de tempo para a auditoria pode variar dependendo do nível de risco do banco de dados e das políticas de segurança da organização.

O monitoramento também deve ser feito regularmente para identificar possíveis vulnerabilidades de segurança e atividades suspeitas. O monitoramento pode incluir o uso de ferramentas de segurança para detectar e relatar atividades suspeitas, como tentativas de acesso não autorizado ou alterações nos dados. O intervalo de tempo para o monitoramento pode variar dependendo do nível de risco do banco de dados e das políticas de segurança da organização.

Além disso, a auditoria e o monitoramento devem ser realizados sempre que houver mudanças no sistema de banco de dados, como atualizações de software ou mudanças na configuração de segurança. Essas mudanças podem afetar a segurança do banco de dados e devem ser cuidadosamente monitoradas e auditadas para garantir que a integridade dos dados seja mantida.

Para realizar a auditoria e monitoramento de um banco de dados, é necessário seguir alguns passos:

1. Definir as políticas de segurança: Antes de começar a auditoria e monitoramento, é importante definir as políticas de segurança que serão seguidas. Essas políticas devem incluir quais atividades serão registradas e monitoradas, como os registros serão armazenados e como as atividades suspeitas serão tratadas.
2. Selecionar as ferramentas de auditoria e monitoramento: Existem várias ferramentas disponíveis para a auditoria e monitoramento de banco de dados, incluindo ferramentas de terceiros e integradas ao próprio banco de dados. As ferramentas selecionadas devem ser compatíveis com o banco de dados e atender aos requisitos das políticas de segurança definidas.
3. Configurar as ferramentas: Depois de selecionar as ferramentas, é necessário configurá-las de acordo com as políticas de segurança definidas. Isso pode incluir a configuração de alertas para atividades suspeitas, a definição de quais atividades serão registradas e a configuração dos registros de auditoria para garantir que eles sejam armazenados de maneira segura.
4. Realizar auditorias regulares: As auditorias devem ser realizadas regularmente para garantir que as políticas de segurança estejam sendo seguidas adequadamente e que não haja atividades suspeitas. É importante revisar regularmente os registros de auditoria para identificar possíveis vulnerabilidades de segurança e atividades suspeitas.
5. Monitorar continuamente: O monitoramento deve ser realizado continuamente para identificar possíveis vulnerabilidades de segurança e atividades suspeitas. As ferramentas de monitoramento devem ser configuradas para alertar a equipe de segurança sobre atividades suspeitas em tempo real.
6. Tomar medidas corretivas: Quando uma atividade suspeita é detectada, é importante tomar medidas corretivas imediatas para proteger o banco de dados. Isso pode incluir a aplicação de patches de segurança, o bloqueio de usuários não autorizados e a alteração de senhas de

acesso.

Última atualização: terça, 21 mar 2023, 13:44

◄ 5.18 Princípios de segurança de banco de dados

Seguir para...

5.20 Proteção de dados e conformidade ►