

Aula 8 – Auditoria de Banco de Dados

Objetivos da Aula:

- Entender a importância da auditoria em bancos de dados.
- Explorar técnicas e ferramentas para auditoria de logs e atividades.
- Detectar acessos não autorizados e anomalias em bancos de dados.

Introdução à Auditoria de Banco de Dados

- A auditoria monitora e revisa atividades no banco, como consultas, alterações, criação de usuários e permissões.
- Objetivo: Garantir integridade, segurança e conformidade.
Exemplo: Um auditor pode verificar logs de acesso para detectar invasões ou uso indevido do sistema.

Motivações para Auditoria de Banco de Dados

- Segurança: Garante que apenas usuários autorizados accessem os dados.
- Conformidade: Assegura operações em conformidade com LGPD e GDPR.
- Desempenho: Avalia consultas e operações para otimização.
- Integridade: Detecta alterações ou corrupções indevidas.

Ferramentas e Técnicas de Auditoria

- Logs de Auditoria: MySQL, PostgreSQL e Oracle registram atividades detalhadas.
- Triggers: Executam ações automáticas em eventos (INSERT, UPDATE, DELETE).
- Consultas SQL: Revisam histórico de alterações e permissões.

Exemplo SQL:

```
SELECT * FROM audit_log WHERE user = 'admin';
```

Atividades Comuns de Auditoria

- Acompanhamento de Acessos: Quem acessou e quando.
- Auditoria de Consultas: Detectar abusos de acesso.
- Auditoria de Alterações: Quem alterou o quê e quando.
- Auditoria de Permissões: Garantir privilégios corretos.

Auditoria de Logs

- Logs mostram todas as atividades do banco.
- Ajudam a detectar ações suspeitas e falhas de segurança.
- São importantes para investigações e conformidade legal.

Exemplo: Tentativas de login sem sucesso, exclusões indevidas, alterações não autorizadas.

Conclusão

- Auditoria é essencial para segurança e confiabilidade dos dados.
- Combina ferramentas automáticas e revisões periódicas.
- Garante conformidade com LGPD e protege contra invasões.