Para desenvolver um banco de dados seguro, é importante seguir os seguintes pilares da segurança de dados:

1. Autenticação: é necessário garantir que apenas usuários autorizados tenham acesso ao banco de dados. Isso pode ser feito através de mecanismos de autenticação como senhas ou tokens de acesso.
2. Autorização: é necessário garantir que os usuários tenham acesso apenas às informações e operações que eles estão autorizados a acessar. Isso pode ser feito através de mecanismos de autorização como permissões de acesso ou papéis de usuário.
3. Criptografia: é importante criptografar os dados sensíveis armazenados no banco de dados para evitar acesso não autorizado. Isso pode ser feito através de mecanismos de criptografia como criptografia simétrica ou assimétrica.
4. Backup e recuperação: é importante criar cópias de segurança dos dados armazenados no banco de dados para garantir que eles possam ser recuperados em caso de perda ou corrupção.
5. Monitoramento e auditoria: é importante monitorar o acesso e as operações realizadas no banco de dados e realizar auditorias para identificar possíveis vulnerabilidades ou violações de segurança.

Esses são apenas alguns dos principais pilares da segurança de dados que devem ser considerados ao desenvolver um banco de dados. Existem outros fatores importantes a serem considerados, como a proteção contra ataques de negação de serviço (DoS) e a separação de ambientes de produção e desenvolvimento. É importante lembrar que a segurança de dados é um processo contínuo e é necessário implementar medidas de segurança adequadas e atualizá-las regularmente para garantir a proteção dos dados.