Nome: Bruno Soares dos Santos
E-mail: brunobsds8@hotmail.com

Os pilares da segurança de dados são fundamentais para garantir a proteção e a confidencialidade dos dados em um banco de dados. Aqui estão alguns dos principais pilares que devem ser seguidos:

1. Confidencialidade: Garantir que apenas pessoas autorizadas tenham acesso aos dados. Isso pode ser alcançado por meio de autenticação de usuários, criptografia de dados e controle de acesso baseado em funções.
2. Integridade: Proteger os dados contra alterações não autorizadas ou corrupção. Isso inclui a implementação de medidas de verificação de integridade, como hash de dados e assinaturas digitais.
3. Disponibilidade: Assegurar que os dados estejam disponíveis e acessíveis para as pessoas que precisam delas, quando precisarem. Isso inclui a implementação de medidas de alta disponibilidade, como redundância de dados e backups.
4. Auditoria: Rastrear e registrar as atividades de acesso aos dados, para fins de auditoria e conformidade. Isso inclui o registro de eventos de acesso, modificações e tentativas de acesso não autorizadas.
5. Privacidade: Respeitar as preferências dos usuários em relação à coleta, armazenamento e uso de seus dados pessoais. Isso inclui a implantação de políticas de privacidade claras e a observância de regulamentos de privacidade, como o RGPD na Europa.

É importante seguir estes pilares da segurança de dados ao desenvolver um novo banco de dados para garantir a proteção dos dados armazenados e a confiança dos usuários em sua empresa.