Projetar um banco de dados seguro envolve considerar vários aspectos para garantir a integridade, confidencialidade e disponibilidade dos dados. Aqui estão alguns pilares importantes da segurança de dados que devem ser considerados ao projetar um novo banco de dados:

Controle de Acesso:
Autenticação e Autorização: Implementar um sistema robusto de autenticação para garantir que apenas usuários autorizados tenham acesso ao banco de dados. A autorização deve ser granular, concedendo permissões mínimas necessárias para cada usuário ou papel.

Criptografia:
Dados em Repouso: Utilizar criptografia para proteger dados armazenados no banco de dados, garantindo que, mesmo que alguém tenha acesso físico ao servidor, os dados não possam ser lidos sem a chave apropriada.
Dados em Trânsito: Utilizar protocolos seguros (por exemplo, SSL/TLS) para criptografar a comunicação entre o aplicativo e o banco de dados.

Auditoria e Monitoramento:
Registros de Auditoria: Manter registros de auditoria para rastrear quem acessou o banco de dados, quando e quais operações foram realizadas. Esses registros podem ser vitais para a detecção de atividades suspeitas.
Alertas e Notificações: Configurar alertas para atividades incomuns ou potencialmente maliciosas, como tentativas de login fracassadas ou acessos fora do horário comercial.
Backup e Recuperação:

Backup Regular:
Implementar um plano de backup regular para garantir a recuperação eficiente dos dados em caso de falha, corrupção ou ataques cibernéticos.
Testes de Recuperação: Periodicamente, testar a recuperação dos dados para garantir que o processo seja eficaz.

Padrões de Codificação Segura:
Prevenção contra Injeção SQL: Utilizar consultas parametrizadas ou instruções preparadas para evitar ataques de injeção SQL.
Validação de Dados: Validar e sanitizar todos os dados de entrada para prevenir ataques de Cross-Site Scripting (XSS) e outros ataques de injeção.

Gestão de Identidade:
Políticas de Senhas Fortes: Implementar políticas que exijam senhas fortes e oportuna troca de senhas para prevenir acessos não autorizados.
Gestão de Ciclo de Vida de Contas: Desativar contas de usuários que não são mais necessárias e monitorar as mudanças nos privilégios de acesso.
Segurança Física:

Local Seguro:
Garantir que o servidor do banco de dados esteja em um local físico seguro, com controle de acesso restrito.

Atualizações e Patches:
Manutenção Regular: Aplicar regularmente atualizações e patches de segurança fornecidos pelos fornecedores do banco de dados e do sistema operacional.
Conformidade com Regulamentações:

Leis e Regulamentações:
Garantir que o banco de dados esteja em conformidade com leis e regulamentações relevantes, como o Regulamento Geral de Proteção de Dados (GDPR) ou normas da indústria.

Treinamento e Conscientização:
Treinamento dos Usuários:
Educar os usuários sobre as práticas de segurança, incluindo a importância de senhas fortes, reconhecimento de ameaças e relatórios de atividades suspeitas.