Para criar um novo banco de dados bem projetado e seguro, com ênfase na criptografia, é importante seguir os pilares da segurança de dados.

1. Confidencialidade:

- Criptografia de Dados: Utilize a criptografia para proteger os dados confidenciais armazenados no banco de dados. Isso pode incluir a criptografia de campo, onde os dados em si são criptografados, ou criptografia de disco, onde todo o banco de dados é criptografado.

2. Integridade:

- Assinaturas Digitais: Para garantir a integridade dos dados, utilize assinaturas digitais para verificar se os dados não foram modificados durante a transmissão ou armazenamento. Isso ajuda a detectar qualquer alteração não autorizada nos dados.

3. Disponibilidade:

- Gerenciamento de Chaves: Mantenha as chaves de criptografia seguras para garantir a disponibilidade dos dados criptografados. A perda das chaves pode resultar na inacessibilidade dos dados, portanto, é importante gerenciá-las adequadamente.

4. Autenticidade:

- Autenticação de Usuários: Além da criptografia, implemente sistemas de autenticação robustos para garantir que apenas usuários autorizados tenham acesso aos dados criptografados.

5. Não-repúdio:

- Registro de Transações Criptografadas: Ao usar a criptografia, registre as transações de forma criptografada para que não possam ser negadas posteriormente. Isso fornece evidências de quem realizou a ação.

6. Privacidade:

- Criptografia de Dados Pessoais: Em conformidade com regulamentos de privacidade, como o GDPR, certifique-se de criptografar dados pessoais e sensíveis dos clientes para proteger a privacidade.

7. Segurança física:

- Proteção de Chaves de Criptografia: Mantenha as chaves de criptografia seguras e protegidas fisicamente para evitar acesso não autorizado.

8. Segurança de rede:

- Túneis VPN: Para a comunicação segura entre o banco de dados e os sistemas clientes, use túneis VPN com criptografia para proteger os dados durante a transmissão.

9. Segurança de aplicativos:

- Uso de APIs Criptografadas: Se o banco de dados é acessado por meio de APIs, certifique-se de que as comunicações por API estejam criptografadas para evitar vazamentos de dados.

10. Auditoria e monitoramento:

- Registro de Transações Criptografadas: Garanta que os registros de transações e atividades do banco de dados, incluindo tentativas de acesso não autorizado, estejam criptografados para proteger os dados de auditoria.

Lembrando que a criptografia é uma parte importante da segurança de dados, mas não deve ser usada isoladamente. É essencial incorporar outros elementos de segurança, como controle de acesso, políticas de segurança e proteção física, para criar um ambiente de banco de dados seguro e bem projetado.