Após uma varredura rápida no sistema de banco de dados de uma empresa de vendas, identificamos a necessidade de melhorar a segurança dessas informações. Por isso, será necessário desenvolver um novo banco para armazenar os dados mais importantes, como detalhes dos clientes, valores faturados diariamente e informações sobre os produtos, além de outros. Sendo assim, explique quais são os pilares da segurança de dados que devem ser seguidos para que o novo banco seja bem projetado e funcione corretamente

1. Autenticação e Controle de Acesso: Implementar um sistema robusto de autenticação para garantir que apenas usuários autorizados tenham acesso ao banco de dados. Isso inclui o uso de senhas fortes, autenticação de dois fatores e a aplicação de políticas de acesso baseadas em funções para restringir o acesso apenas ao necessário para cada usuário.
2. Criptografia de Dados: Utilizar técnicas de criptografia para proteger os dados armazenados no banco. Isso inclui a criptografia de dados em repouso (armazenados) e em trânsito (durante a transmissão entre sistemas). Métodos como SSL/TLS para comunicação segura e algoritmos de criptografia adequados são essenciais.
3. Integridade dos Dados: Implementar mecanismos para garantir a integridade dos dados, assegurando que eles não sejam alterados indevidamente. Isso pode ser feito por meio de assinaturas digitais, controle de versão e auditorias regulares.
4. Auditoria e Monitoramento: Estabelecer procedimentos para monitorar e auditar o acesso ao banco de dados. Isso envolve a implementação de logs de acesso, análise de logs para identificar atividades suspeitas e ações corretivas em caso de detecção de violações.
5. Backup e Recuperação: Desenvolver um plano de backup regular para garantir que os dados estejam protegidos contra perda ou corrupção. Além disso, é fundamental testar regularmente a capacidade de recuperação para garantir que os backups sejam eficazes em caso de necessidade.