**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**

Para que o novo banco de dados da empresa de vendas seja bem projetado e funcione corretamente, é importante que ele siga esses pilares, **integridade**, **disponibilidade**e **confiabilidade**.

As recomendações específicas para cada um dos pilares são:

**Integridade**

* Use mecanismos de integridade de dados para garantir que os dados estejam corretos e completos. Isso inclui o uso de validações, checksums e esquemas de controle de versão.
* Implemente políticas de backup e recuperação de desastres para proteger os dados contra perda ou corrupção. Essas políticas devem garantir que os dados possam ser recuperados rapidamente em caso de incidente.

**Disponibilidade**

* Use arquiteturas de alta disponibilidade para garantir que os dados estejam disponíveis mesmo em caso de falhas de hardware ou software. Isso pode incluir o uso de clusters de servidores, replicação de dados ou técnicas de recuperação de desastres.
* Monitore o desempenho do banco de dados para garantir que ele esteja funcionando conforme o esperado. Isso ajudará a identificar problemas potenciais antes que eles causem interrupções no serviço.

**Confidencialidade**

* Adote medidas de autenticação e autorização fortes para restringir o acesso aos dados. Isso inclui o uso de senhas fortes, autenticação multifatorial e controle de acesso baseado em papéis.
* Criptografe os dados em repouso e em trânsito. Isso dificultará que os dados sejam acessados por pessoas não autorizadas.
* Implemente políticas de segurança de dados que definam como os dados devem ser protegidos. Essas políticas devem ser claras e concisas e devem ser comunicadas a todos os funcionários que trabalham com dados.