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.

**Pilares da segurança**

Ao projetar e desenvolver um novo banco de dados para armazenar informações sensíveis, como detalhes dos clientes, valores faturados e informações de produtos, é de extrema importância adotar uma abordagem robusta de segurança. Os pilares a seguir devem ser seguidos para garantir a segurança;

**Confidencialidade:**

* **Controle de Acesso:** Implementar um sistema de controle de acesso rigoroso, garantindo que apenas usuários autorizados tenham permissão para acessar determinados dados.
* **Criptografia:** Utilizar criptografia para proteger dados em repouso e em trânsito, impedindo que terceiros não autorizados possam interpretar as informações.
* **Máscara de Dados:** Mascare ou oculte informações sensíveis, exibindo apenas uma parte dos dados para usuários sem as permissões adequadas.

**Integridade:**

* **Validação de Dados:** Implementar verificações de integridade para garantir que os dados inseridos no banco de dados sejam válidos e consistentes
* **Assinaturas Digitais:** Utilizar assinaturas digitais para verificar a autenticidade dos dados, evitando modificações não autorizadas.
* **Histórico de Alterações:** Manter um registro de todas as alterações feitas nos dados, possibilitando a auditoria e rastreamento de atividades.

**Disponibilidade:**

* **Backup e Recuperação:** Implementar estratégias de backup regulares e testar procedimentos de recuperação para garantir que os dados possam ser restaurados em caso de falhas.
* **Redundância:** Distribuir os dados em servidores redundantes para evitar interrupções devido a falhas de hardware ou ataques.
* **Monitoramento:** Utilizar ferramentas de monitoramento para identificar rapidamente qualquer problema de disponibilidade e tomar medidas corretivas.

**Autenticidade:**

* **Autenticação de Usuários:** Exigir autenticação forte, como senhas fortes, autenticação de dois fatores ou autenticação biométrica, para garantir que apenas usuários legítimos tenham acesso.
* **Auditoria de Acessos:** Registrar todas as tentativas de acesso e atividades no banco de dados para possibilitar a investigação em caso de incidentes.

**Não Repúdio:**

* **Registros de Transações:** Manter registros detalhados de todas as transações e ações realizadas no banco de dados, incluindo informações sobre quem realizou cada ação.
* **Assinaturas Digitais:** Utilizar assinaturas digitais para garantir que as transações sejam rastreáveis até seus autores.