**DESEVOLVIMENTO 5 BANCO DE DADOS II**

**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**

**Resposta:**

Ao projetar um novo banco de dados para armazenar informações críticas de uma empresa de vendas, é fundamental seguir os pilares da segurança de dados para garantir a integridade, confidencialidade e disponibilidade das informações. Aqui estão os principais pilares da segurança de dados que devem ser considerados:

**Confidencialidade:** Garantir que apenas usuários autorizados tenham acesso às informações confidenciais. Isso pode ser alcançado por meio de autenticação forte, controle de acesso baseado em função (RBAC), criptografia de dados em repouso e em trânsito, além de auditoria de acesso.

**Integridade:** Assegurar que os dados permaneçam precisos e não sejam modificados ou corrompidos por usuários não autorizados. Isso envolve a implementação de mecanismos de controle de acesso granular, prevenção de ataques de injeção de SQL, uso de chaves estrangeiras e restrições de integridade referencial, bem como a realização de backups regulares e verificação de integridade dos dados.

**Disponibilidade:** Garantir que os dados estejam acessíveis quando necessário, sem interrupções não planejadas. Isso requer a implementação de medidas de redundância e alta disponibilidade, como replicação de banco de dados, balanceamento de carga, backups automáticos e recuperação de desastres.

**Autenticidade:** Verificar a identidade dos usuários e garantir que apenas usuários legítimos tenham acesso ao sistema. Isso pode ser alcançado por meio de autenticação de dois fatores, uso de senhas fortes e complexas, além de políticas de senha robustas e expiração regular de credenciais.

**Auditoria e monitoramento:** Registrar e monitorar atividades de acesso ao banco de dados para identificar atividades suspeitas ou não autorizadas. Isso envolve a implementação de logs de auditoria, monitoramento contínuo de atividades de usuário, alertas de segurança e análise de registros para detecção de anomalias.

**Compliance:** Garantir que o banco de dados esteja em conformidade com regulamentos e padrões de segurança relevantes, como GDPR, HIPAA, PCI-DSS, entre outros. Isso requer a implementação de políticas e procedimentos de segurança adequados, bem como a realização de auditorias regulares para garantir conformidade contínua.

Ao seguir esses pilares da segurança de dados, o novo banco de dados da empresa de vendas estará bem projetado e funcionará corretamente, protegendo efetivamente as informações críticas e garantindo a confiança dos clientes e parceiros comerciais.