Integridade, Confidencialidade e Disponibilidade

DANILLO ARAÚJO DE PAIVA

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:

Integridade, Confidencialidade e disponibilidade são três pilares fundamentais da segurança da informação. Esses princípios formam a base para garantir a segurança e proteção dos dados em sistemas e ambientes computacionais. Vamos explorar cada um deles:

1. Integridade:

- **Definição:** A integridade refere-se à precisão e confiabilidade dos dados. Em um sistema ou conjunto de dados íntegros, as informações não são alteradas de maneira não autorizada ou inadvertida.

- **Importância:** Garante que os dados permaneçam consistentes e confiáveis ao longo do tempo, preservando sua precisão e evitando modificações não autorizadas.

2. Confidencialidade:
- **Definição:** A confidencialidade diz respeito à proteção e restrição do acesso a informações sensíveis apenas para usuários autorizados.

- **Importância:** Assegura que as informações críticas e privadas sejam acessíveis apenas por indivíduos ou sistemas autorizados, evitando divulgação não autorizada.

3. Disponibilidade:

- **Definição:** A disponibilidade envolve garantir que os sistemas e dados estejam acessíveis quando necessário, sem interrupções não planejadas.

- **Importância:** Assegura que os usuários autorizados possam acessar os recursos necessários quando precisarem, promovendo a continuidade operacional e evitando interrupções prejudiciais.

Esses três princípios, muitas vezes referenciados como o triângulo da segurança da informação, são interdependentes. Uma violação de qualquer um desses princípios pode comprometer a segurança global dos dados. As práticas de segurança, como criptografia, controle de acesso, backups regulares e monitoramento contínuo, são implementadas para garantir a aplicação efetiva desses princípios. A segurança da informação busca equilibrar esses três aspectos, proporcionando um ambiente seguro e confiável para dados e sistemas.