Os pilares da segurança de dados são princípios fundamentais que devem ser seguidos para garantir que os dados estejam seguros. Eles são:

Confidencialidade: Garante que as informações não serão divulgadas a indivíduos, grupos, processos ou dispositivos não autorizados. A confidencialidade é sobre proteger os dados de serem acessados por entidades não autorizadas.

Integridade: Assegura que os dados sejam precisos e completos, e que não sejam modificados de maneira não autorizada.

Disponibilidade: Garante que os dados estejam disponíveis quando necessário24. Isso significa que os sistemas devem estar funcionando corretamente e os usuários devem ser capazes de acessar os dados quando precisarem.

Além desses três pilares principais, existem mais três itens que surgiram com o desenvolvimento da tecnologia:

Autenticidade: Garante que as entidades envolvidas em uma comunicação ou transação sejam quem afirmam ser.

Irretratabilidade: Garante que uma entidade não possa negar ter participado de uma transação ou comunicação.

Conformidade: Garante que as políticas de segurança da informação estejam em conformidade com as regulamentações e leis vigentes.

Esses pilares formam a base para o desenvolvimento de um banco de dados seguro. Eles devem ser considerados durante todo o processo de design e implementação do banco de dados para garantir a segurança dos dados.