Pilares da segurança de dados que devem ser seguidos para que o novo banco seja bem projetado e funcione corretamente

Copilot

A segurança de dados é fundamental para proteger informações sensíveis e garantir que o banco de dados funcione corretamente. Existem três pilares principais da segurança de dados que devem ser seguidos:

1. Integridade:
   * A integridade dos dados refere-se à garantia de que as informações armazenadas são **verdadeiras, precisas e confiáveis**.
   * Para manter a integridade, é importante implementar mecanismos que evitem alterações não autorizadas nos dados, como restrições de chave primária, validações e auditorias.
   * Isso ajuda a evitar erros, corrupção e inconsistências nos dados.
2. Disponibilidade:
   * A disponibilidade diz respeito a assegurar que as informações estejam **acessíveis sempre que necessário**.
   * Para garantir a disponibilidade, é essencial ter backups regulares, redundância de servidores e planos de recuperação de desastres.
   * Evitar interrupções no acesso aos dados é crucial para o funcionamento contínuo do sistema.
3. Confidencialidade:
   * A confidencialidade visa proteger as informações contra **exposições não autorizadas**.
   * Isso envolve a aplicação de controles de acesso, criptografia e autenticação.
   * Apenas usuários autorizados devem ter acesso aos dados sensíveis.

Outros aspectos importantes da segurança de dados:

* Auditoria e Monitoramento:
  + Registre atividades no banco de dados para rastrear quem acessou, modificou ou visualizou os dados.
  + Monitore continuamente o sistema em busca de atividades suspeitas.
* Controle de Acesso:
  + Defina permissões de acesso com base em funções e responsabilidades.
  + Restrinja o acesso a dados confidenciais apenas aos usuários necessários.
* Criptografia:
  + Proteja os dados em trânsito e em repouso usando técnicas de criptografia.
  + Isso inclui criptografar conexões de rede (SSL/TLS) e dados armazenados no banco de dados.
* Atualizações e Patches:
  + Mantenha o sistema atualizado com as últimas correções de segurança.
  + Corrija vulnerabilidades conhecidas para evitar explorações maliciosas.