1. **Confidencialidade:**

- Garantir que apenas usuários autorizados tenham acesso aos dados sensíveis.
- Usar técnicas de criptografia para proteger os dados em repouso e em trânsito.
- Implementar controles de acesso granulares para restringir o acesso apenas ao necessário.

2. **Integridade:**

- Certificar-se de que os dados são precisos, consistentes e confiáveis.
- Utilizar mecanismos de verificação de integridade, como checksums e hashes, para detectar alterações não autorizadas nos dados.
- Implementar restrições de integridade nos bancos de dados para garantir que apenas dados válidos sejam inseridos.

3. **Disponibilidade:**

- Assegurar que os dados estejam disponíveis quando necessário para os usuários autorizados.
- Implementar estratégias de backup e recuperação para proteger os dados contra falhas de hardware, desastres naturais ou ataques cibernéticos.
- Utilizar técnicas de redundância para garantir a disponibilidade contínua dos dados.

4. **Autenticidade:**

- Verificar a identidade dos usuários antes de conceder acesso aos dados.
- Utilizar métodos de autenticação forte, como senhas seguras, autenticação multifator e biometria.
- Registrar e auditar as atividades dos usuários para detectar e responder a atividades suspeitas.

5. **Autorização:**

- Definir e aplicar políticas de controle de acesso para determinar quais usuários têm permissão para acessar quais dados.
- Implementar o princípio do menor privilégio, concedendo aos usuários apenas as permissões necessárias para realizar suas tarefas.
- Regularmente revisar e atualizar as permissões de acesso para garantir que permaneçam alinhadas com as necessidades do negócio.

6. **Auditoria:**

- Registrar todas as atividades realizadas no banco de dados, incluindo acessos, modificações e tentativas de acesso não autorizadas.
- Analisar regularmente os registros de auditoria para identificar possíveis ameaças à segurança e garantir a conformidade com regulamentos de privacidade e segurança de dados.