

A tríade CIA é a combinação de alguns princípios como os fundamentos da segurança. Pode ser referida como tríade AIC ou CID, em português.

## **1.Confidencialidade**

**A confidencialidade impede a divulgação de informações para pessoas, recursos ou processos não autorizados** e garante que as informações apenas sejam acessíveis por pessoas autorizadas, isso significa que os dados não devem ser expostos a pessoas não autorizadas. Empresas restringem o acesso para garantir que apenas os operadores autorizados possam usar os dados ou outros recursos de rede. Os métodos para garantir confidencialidade incluem a criptografia, autenticação e o controle de acesso aos dados.

A maioria dos dados de privacidade são confidenciais, mas nem todos os dados confidenciais são privados. O acesso à informação ocorre após a confirmação de autorização adequada. Criminosos virtuais podem capturar, salvar e roubar dados em trânsito. Profissionais de segurança cibernética devem tomar medidas para combater essas ações.

## **2.Integridade**

**A integridade se refere à precisão, consistência e a confiabilidade dos dados durante seu ciclo de vida** e garante que as informações permaneçam precisas, completas e íntegras, protegendo-as contra alterações não autorizadas. Os dados passam por várias operações, como captura, armazenamento, recuperação, atualização e transferência. Eles devem permanecer inalterados durante todas essas operações por entidades não autorizadas. Os métodos usados para garantir a integridade de dados incluem *hashing*, verificações de validação de dados, verificação de consistência dos dados e controle de acesso.

## **3.Disponibilidade/Avaliabilidade**

**A disponibilidade garante que as informações estejam acessíveis para usuários autorizados quando necessário** e garante que as informações estejam disponíveis quando necessário. Isso implica que sistemas e dados devem estar acessíveis e funcionais, sem interrupções não planejadas. Ataques cibernéticos e falhas do sistema podem impedir o acesso a sistemas e serviços de informação. Os métodos para garantir a disponibilidade incluem a redundância, backups, maior resiliência, manutenção de equipamentos, sistemas operacionais e softwares do sistema, todos atualizados e planos para recuperação rápida de desastres não previsto.