

## 1. Autenticação

**A autenticação verifica a identidade de um usuário para evitar acesso não autorizado.** Os usuários provam sua identidade com um nome de usuário ou ID. Eles também podem precisar verificar sua identidade proporcionando uma das seguintes opções: Algo que saibam (senha), algo que tenham (token/cartão) ou algo que sejam (impressão digital). Em comunicações de rede, a autenticação pode ser realizada usando métodos criptográficos. Isso é especialmente importante para aplicativos ou protocolos, como e-mail ou IP, que não possuem mecanismos internos para evitar falsificação da fonte.

## 2. Autorização

**Os serviços de autorização determinam quais recursos os usuários podem acessar,** juntamente com as operações que os usuários podem executar. Alguns sistemas conseguem isso através de uma ACL. Autorização também pode controlar quando um usuário tem acesso a um recurso específico.

## 3. Accounting

**Accounting representa o controle sobre o que os usuários fazem,** desde o que acessam até a quantidade de tempo que acessam os recursos disponíveis, observando as alterações feitas. Serviços de accounting de segurança cibernética funcionam da mesma maneira, com o sistema controlando cada transação de dados e fornecendo os resultados da auditoria.

