1. Confiabilidade

A Confiabilidade é o primeiro pilar da Segurança da Informação, pois garante que os dados estejam acessíveis a determinados usuários e protegidos contra pessoas não autorizadas. É um componente essencial da **privacidade**, que se aplica especialmente a dados pessoais, sensíveis, financeiros, psicográficos e outras informações sigilosas.

Para garantir esse pilar nas suas políticas de segurança de TI, você deve incluir medidas de proteção como controle de acesso, criptografia, senhas fortes, entre outras estratégias. Inclusive, a confidencialidade dos dados pessoais de usuários é um dos **requisitos centrais** de conformidade com a GPDR (General Data Protection Regulation) e LGPD (Lei Geral de Proteção de Dados Pessoais).

2. Integridade

A **integridade** na segurança da informação diz respeito à preservação, precisão, consistência e confiabilidade dos dados durante todo o seu ciclo de vida.

Para erguer esse pilar em uma empresa, é preciso implementar [**mecanismos de controle**](https://www.gat.digital/checklists-seguranca-da-informacao/)para evitar que as informações sejam alteradas ou deletadas por pessoas não autorizadas. Frequentemente, a integridade dos dados é afetada por erros humanos, políticas de segurança inadequadas, processos falhos e ciberataques.

3. Disponibilidade

Para que um sistema de informação seja útil, é fundamental que seus dados estejam disponíveis sempre que necessário. Logo, a **disponibilidade** é mais um pilar da segurança da informação, que garante o acesso em tempo integral (24/7) pelos usuários finais.

Para cumprir esse requisito, você precisa garantir a**estabilidade** e acesso permanente às informações dos sistemas, por meio de processos de manutenção rápidos, eliminação de falhas de software, atualizações constantes e planos para administração de crises.