Os pilares da segurança de dados são um conjunto de princípios fundamentais que são usados para proteger as informações confidenciais contra roubo, acesso não autorizado, uso indevido ou qualquer outra forma de ameaça.
Os principais pilares da segurança de dados são:

1. Confidencialidade: Garantir que as informações confidenciais sejam acessíveis apenas por pessoas autorizadas e que não sejam divulgadas para terceiros sem autorização.

2. Integridade: Garantir que as informações confidenciais sejam precisas, completas e que não tenham sido alteradas ou corrompidas de forma não autorizada.

3. Disponibilidade: Garantir que as informações confidenciais estejam disponíveis sempre que necessário para as pessoas autorizadas a acessá-las, e que o acesso seja possível mesmo em caso de falhas ou interrupções no sistema.

4. Autenticidade: Garantir que as informações sejam autênticas, ou seja, que a fonte seja confiável e que a informação não tenha sido falsificada.

5. Não-repúdio: Garantir que uma pessoa não possa negar ter feito uma determinada ação ou transação, ou seja, garantir que a ação ou transação possa ser rastreada até a pessoa que a realizou.

Esses pilares são essenciais para garantir a segurança de dados em qualquer tipo de sistema ou aplicação, e devem ser levados em consideração em todas as etapas do processo de desenvolvimento, implementação e manutenção de um sistema.