

# Segurança da informação

---

## Conceitos iniciais

---

A segurança da informação se refere a proteção dos dados existentes de pessoas e empresas, a informação é qualquer conteúdo que tenha valor pessoal ou empresarial e dentro da segurança da informação nós possuímos alguns pilares que definem algumas características para que essas informações tenham uma boa segurança, eles são:

- **Confidencialidade**

A confidencialidade é o pilar que garante que ninguém além do dono da informação e as pessoas autorizadas irão ter acesso a tal conteúdo, como por exemplo, o whatsapp, note que quando você inicia uma nova conversa o whatsapp exibe uma mensagem falando que a conversa é protegida por criptografia ponto-a-ponto, ou seja, apenas você e a pessoa que você está conversando podem ler a mensagem. (pelo menos é o que eles dizem KK)

- **Integridade**

O pilar da integridade é referente a característica de os dados não serem alterados de forma ilegal, ele garante a autenticidade dos dados e isso inclui também futuras mudanças sofridas por esse dado, esse pilar garante que mensagens trocadas por pessoas não sejam alteradas no meio do caminho por exemplo, novamente usando o whatsapp, se você manda "oi, tudo bem?" para alguém, essa pessoa deve receber "oi, tudo bem?", exatamente da forma que foi enviada a mensagem.

- **Disponibilidade**

A disponibilidade é o pilar que como o próprio nome sugere, garante que a informação esteja sempre disponível para acesso legítimo pelo dono da informação, um bom exemplo para esse pilar são aplicativos de banco, nesses aplicativos é importante que os seus dados estejam sempre disponíveis para o seu uso.

## Malware

---

Um bom conceito inicial são o que são malwares e quais os tipos existentes, os malwares são softwares que se infiltram em um computador de maneira ilícita sem que o usuário saiba e temos vários tipos de malwares, eles são:

- **Vírus**

O vírus depende da execução de um programa ou arquivo, quando dentro de um arquivo ele começa a se multiplicar inserindo cópias de si mesmo em outros locais, o vírus infecta somente PROGRAMAS ou ARQUIVOS, ele não infecta seu computador, logo a expressão "meu computador está com vírus" não está correta. Um vírus de computador não afeta o celular e vice e versa, pois possuem instruções físicas diferentes, o único objetivo do vírus é atrapalhar sua vida, eles são feitos na maioria dos casos para prejudicar o desempenho do seu computador.

- **Trojan**

Programa que além de executar as funções que foi projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário. O trojan pode ser instalado pelo próprio usuário ou por atacantes, após invadir o computador eles podem alterar programas já existentes para executarem ações maliciosas como: acesso remoto,

capturar informações, destruir aplicativos e etc.

- **Rootkit**

É um conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido, ele pode ser usado para remover evidências de arquivos de logs, instalar outros códigos maliciosos, esconder informações e atividades, capturar informações da rede e mapear potenciais vulnerabilidades em outros computadores, é de longe o malware mais ameaçador na minha opinião e o que eu mais te aconselho a estudar.

- **Spyware**

São softwares responsáveis por ações como: publicidade, coleta de informações pessoais ou alterações da configuração do computador sem o consentimento do usuário. Existe o spyware do tipo Keylogger que é capaz de capturar e armazenar as teclas digitadas pelo usuário do teclado do computador e tem o Adware que se instala secretamente no computador e verifica os hábitos de navegação do usuário e armazenando nos cookies do navegador de internet, um bom exemplo de Spyware é o Baidu.



 [jcesar\\_n](#)

 [JulioCesarNSM](#)

Obrigado!