O ano de 2017 ficou marcado como o dos ataques cibernéticos em larga escala, com casos sequenciais de ações que paralisaram serviços variados e ocasionaram prejuízos financeiros e operacionais a empresas e cidadãos em todo o mundo. Sem dúvida, o mais notório foi o do ransomware – tipo de arquivo malicioso que sequestra os dados da vítima em troca de um pagamento de resgate em criptomoedas – Wannacry, que infectou mais de 250 mil computadores em 150 países durante o mês de maio (Prado, 2018).

Em outubro, o vírus Bad Rabbit chegou a causar atrasos em um aeroporto ucraniano porque os funcionários processaram dados manualmente, além de afetar diversos meios de comunicação na Rússia. O Bad Rabbit infectou os computadores por meio de uma falsa instalação do Adobe Flash. Quando a vítima executa o arquivo baixado, o computador passava por um processo de criptografia (Barros, 2018).

# Como evitar os ataques ditais

A gestão de riscos é relevante para a segurança da informação digital e na preservação da segurança. Para garantir que as informações são seguras é preciso levar em consideração esses eixos: confidencialidade, integridade, disponibilidade e autenticidade. Confidencialidade consiste em manter sigilosas as informações; integridade garante que as informações sejam acessadas por pessoas autorizadas; além de serem confidenciais e integras, as informações devem ser disponíveis e enfim a autenticidade permite o não repúdio, assim os usuários se autentificam ao acessar as informações e não podem negar que as acessam. Embora essas medidas evitam alterações e perdas de informações, elas não a totalidade de segurança. (CABRAL e CAPRINO, 2015).

A possibilidade de ataque é alta para os computadores que são conectados na rede mundial de computadores e ela, a Internet (rede mundial de computadores), está cada vez mais indispensável no cotidiano. Existem outras ferramentas e métodos aplicados na SI para amenizar riscos e ataques que são boas práticas para promover a segurança digital. São elas: uso de senhas, criptografia, uso de firewall, backup, etc. A maioria dos sistemas requer um *login* e uma senha ao acessá-lo, o *login* é uma chave público por isso é preciso ter uma senha bem elaborada e mantida sigilosa, pois isso impede que alguém rouba a sua identidade (CERT, 2017).

Os antivírus também são uma ótima ferramenta de segurança cuja instalação e atualização são importante