# **5 Pilares da segurança da informação**

Existem 5 pilares de segurança da informação: Confidencialidade, Integridade, Disponibilidade, Autenticidade e Não-repúdio.

**A importância da segurança da informação**

Proteger os dados é o principal objetivo da segurança da informação e, na era digital em que vivemos, a informação ajuda a garantir a vantagem competitiva das empresas. Portanto, é necessário proteger essas informações que geram valor e credibilidade para as organizações.

As ameaças à segurança da informação são inúmeras, como acesso não autorizado, perda de dados, invasões, vazamentos e muitos outros que podem vir de ataques de hackers ou até mesmo erros humanos.

Com a evolução tecnológica, os riscos aumentam e exigem uma gestão de proteção ainda mais eficaz.

Assim, a base de defesa dos sistemas e infraestrutura corporativa são os pilares da segurança da informação que atuam por meio de políticas, senhas, softwares de criptografia e demais processos necessários para esse gerenciamento de riscos.

**Pilares da segurança da informação**

Considerando as muitas ameaças que existem, como as empresas devem se proteger?

1. **Integridade**

O pilar Integridade é responsável por manter as características originais dos dados, tal como foram configuradas na sua criação. Desta forma, as informações não podem ser alteradas sem autorização.

Se houver alteração indevida nos dados, significa que houve perda de integridade, sendo necessário implementar mecanismos de controle para evitar alteração não autorizada de informações.

1. **Confidencialidade**

Este pilar protege as informações de acessos não autorizados, estabelecendo privacidade para os dados da sua empresa, evitando situações de ciberataques ou espionagem.

A base desse pilar é o controle do acesso por meio de autenticação de senha, que também pode ocorrer por meio de varredura biométrica e criptografia, o que vem gerando resultados favoráveis ​​nesse sentido.

1. **Disponibilidade**

O ideal em um sistema de informação é que os dados estejam disponíveis para o que for necessário, garantindo o acesso do usuário em tempo integral. Isso requer estabilidade e acesso permanente aos dados do sistema por meio de manutenção rápida, atualizações constantes e depuração.

É importante lembrar a vulnerabilidade dos sistemas que são suscetíveis a apagões, incêndios, ataques de negação e muitas outras possibilidades de ameaças que existem neste contexto.

1. **Autenticidade**

Confirmação de que os dados possuem legitimidade, ou seja, não haja manipulação ou intervenções externas de terceiros passando-se por colaboradores. Para tal objetivo, é necessário documentar as ações feitas pelos usuários na rede e nos sistemas.

Os dados corporativos devem ter processos para identificar a sua autenticidade e isso é uma das tarefas da equipe de Segurança da Informação. A configuração de um log de acesso ajuda a confirmar a veracidade de um determinado registro.

1. **Legalidade**

Por fim, é necessário ter uma Política de Segurança para assegurar que todos os procedimentos relacionados à informação dentro da empresa sejam feitos de acordo com a lei. Isso evita que ocorram impedimentos operacionais, averiguações e auditorias de órgãos fiscalizadores.

Adequar o conteúdo protegido à legislação é primordial, principalmente porque irá vigorar em agosto de 2020 a nova Lei Geral de Proteção de Dados Pessoais, que exigirá maior rigor de todas as empresas.

**Como fortalecer esses pilares da sua empresa?**

Depois de aprender mais sobre os pilares da segurança da informação, é preciso avaliar se suas práticas seguem esses princípios para ficar longe das infinitas possibilidades de ameaças aos seus dados.

Muitas soluções já são utilizadas por diversas empresas que buscam eliminar riscos aos sistemas de segurança, consolidando os pilares da segurança da informação em sua organização.