

## Pilares da Segurança da Informação

A segurança da informação está diretamente relacionada a proteção de um conjunto de informações (dados), no sentido de preservar o valor que possuem para um indivíduo ou uma organização.

Hoje, a popularização da Internet a tornou uma das principais ferramentas por onde a informação e os dados são distribuídos, armazenados, analisados e até mesmo comercializados.

Por isso, com tantos dados disponíveis e circulando pela internet, a segurança da informação deixa de ser uma necessidade e passa a ser uma prioridade. Mas afinal, o que é Segurança da Informação e como funciona?

**São propriedades básicas da segurança da informação:**

- Confidencialidade;
- Integridade;
- Disponibilidade;
- Autenticidade;
- Proteção.



## **1. Confidencialidade, integridade e disponibilidade**

Hoje, o maior ativo de pessoas, empresas e até países são seus dados. Se você pensar que todo o seu patrimônio, número do seu CPF, seus investimentos, contagem do tempo de contribuição para aposentadoria, imagens dos seus filhos do nascimento até hoje, são dados armazenados na internet, você começa a entender o tamanho do risco e da responsabilidade que é manter a informação devidamente protegida de indivíduos mal-intencionados.

O primeiro pilar da segurança da informação visa proteger essa representação digital das suas informações e dados que estão armazenados em vários servidores espalhados pelo mundo. A confidencialidade garante que o acesso a informações sensíveis seja feito somente por pessoas autorizadas, ou seja, ninguém a não ser você deve ter acesso a sua vida digital. Ela se materializa quando, por exemplo, uma rede social protege o controle dos seus posts através de um usuário e senha.

A garantia de acesso à informação e aos sistemas é garantida pela disponibilidade, nesse conceito a segurança da informação atua para que servidores que rodam aplicações, bancos de dados que armazenam informações ou links que dão acesso a esses ativos, estejam sempre online e disponíveis para seus usuários.

## **2. Prevenção, Detecção e Resposta**

Nesse pilar encontramos ações desempenhadas pela segurança da informação para garantir a sustentação do primeiro pilar que já foi mencionado nesse artigo. Essas ações evitam que um incidente de segurança ocorra, agindo para percebê-lo no menor tempo possível e evitar ao máximo seus danos.

Para a prevenção dos incidentes se adota medidas de proteção do ambiente, para entender esse conceito precisamos falar sobre superfície de ataque. Qualquer sistema, servidor, aplicação ou ambiente que tenha um acesso remoto, através da web ou outro tipo de conectividade está sujeito a invasões e a superfície de ataque que podem ser comprometidos por um cibercriminoso.

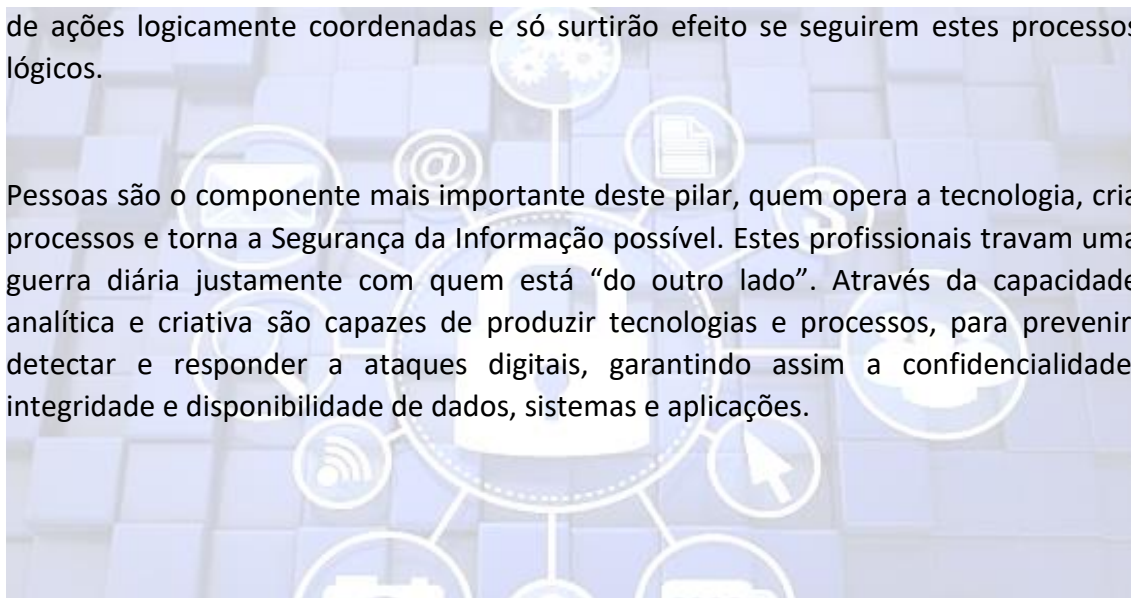
A prevenção atua na proteção desses ativos, evitando que, por exemplo, portas de comunicação estejam abertas, aplicações ou sistemas operacionais estejam desatualizados e assim por diante. Outra parte importante do processo de resposta a incidentes é a investigação para determinar o que aconteceu, porque aconteceu e como evitar que aconteça novamente. A inteligência criada a partir dessa investigação será aplicada às fases de prevenção e detecção para melhorar a resiliência do ambiente.

### 3. Tecnologia, Processos e Pessoas

O último pilar da Segurança da Informação é o que sustenta suas melhores práticas e seus objetivos iniciais. Classificamos como tecnologia todos as ferramentas, sejam elas hardware ou software, que permitem a prevenção, detecção e resposta aos incidentes de segurança, incluímos aqui antivírus, firewalls, IDS, IPS, aplicações de análise forense, SIEMs, etc.

A proteção de ambientes complexos contra ameaças cada vez mais sofisticadas e direcionadas só é possível por meio de processos muito bem definidos que permitem máxima eficiência no uso da tecnologia para sustentar o pilar 2. A documentação extensiva e em profundidade é crucial para permitir que a prevenção, detecção e resposta aos incidentes ocorram de maneira continuada, cada uma delas ocorre através de ações logicamente coordenadas e só surtirão efeito se seguirem estes processos lógicos.

Pessoas são o componente mais importante deste pilar, quem opera a tecnologia, cria processos e torna a Segurança da Informação possível. Estes profissionais travam uma guerra diária justamente com quem está “do outro lado”. Através da capacidade analítica e criativa são capazes de produzir tecnologias e processos, para prevenir, detectar e responder a ataques digitais, garantindo assim a confidencialidade, integridade e disponibilidade de dados, sistemas e aplicações.



## Desafio do Dia

1. Pesquisar sobre um dos pilares da tríade da segurança da informação, traga exemplos de situações reais, problemas causados quando um desses pilares não são respeitados.
2. Quais são os problemas causados, quando não existe autenticidade, compartilhe uma situação “Problema” e comente, como isso poderia ser evitado.
3. O que dizer o Termo **não repudio**, em segurança da informação?

### OBS

- Entrega no formato PDF;
- Tarefa Já está disponível!

