

Segurança da Informação e Segurança em Redes de Computadores

Prof. Dr. Kelton Costa

kelton.costa@gmail.com

kelton.costa@unesp.br

**“O único sistema verdadeiramente seguro é
aquele que está desligado, desplugado,
trancado num cofre de titânio, lacrado,
enterrado em um *bunker de concreto, envolto*
por gás nervoso e vigiado por guardas
armados muito bem pagos. Mesmo assim, eu
não apostaria minha vida nisso.”**

Gene Spafford

Diretor de Operações de Computador, Auditoria e Tecnologia da Segurança
Purdue University, França

Por que preocupar-se com segurança de sistemas de TI?

- Há três razões principais para preocupar-se com segurança de sistemas de TI:
 - **Dependência dos sistemas de informação**
 - **Vulnerabilidade dos sistemas de TI**
 - **Investimento em sistemas de TI**

Dependência dos Sistemas de Informação

- Sistemas que ofereçam serviços adequados e no tempo certo são a chave para a maioria das organizações atuais.
- Sem seus computadores e sistemas de comunicação, as empresas ficariam incapazes de fornecer serviços, processar faturas, contatar clientes e fornecedores ou efetuar pagamentos.
- Os sistemas de informação também armazenam dados sigilosos que, se tornados públicos, causariam embaraço e em alguns casos o fracasso da organização.

Vulnerabilidade dos Sistemas de TI

- Os sistemas exigem um ambiente estável, podendo ser danificados por desastres naturais como fogo, inundação ou terremotos, falhas no controle de temperatura ou do suprimento de energia elétrica, acidentes ou sabotagens.
- Os sistemas de TI são a chave para acesso a vasta quantidade de dados corporativos, tornando-se alvo atraente para hackers e espiões, e podem motivar administradores de sistemas a abusar de seus privilégios, vendendo informações para terceiros.
- A organização depende da exatidão da informação fornecida pelos seus sistemas; se essa confiança for destruída, o impacto para a entidade pode ser comparada a própria destruição do sistema.
- Dessa forma é importante proteger dados tanto de corrupções acidentais quanto propositalis.

Investimento em Sistemas de TI

- Os sistemas de informação são caros tanto no desenvolvimento quanto na manutenção, e a administração deve proteger esse investimento como qualquer outro recurso valioso.
- Bens de TI são particularmente atrativos para ladrões, por serem em alguns casos portáteis, e poderem ser facilmente vendidos.

Objetivos da Segurança

- Os objetivos chaves da segurança são:
 - **Sigilo**

Proteção contra a divulgação indevida de informações
Ex.: criptografia e controle de acesso.
 - **Integridade**

Proteção contra a modificação não autorizada de informações
Ex.: assinaturas digitais.
 - **Disponibilidade**

Proteção contra a interrupção do serviço
Ex.: back-up e duplicação de sistemas.

Que Objetivo é o Mais Importante?

- Em cada caso irá depender da natureza do sistema. Por exemplo, em sistemas da área de desenvolvimento de produtos a ênfase seria em **sigilo** acima de qualquer coisa, enquanto que na maioria das outras aplicações a ênfase maior estaria provavelmente na **disponibilidade**, seguida da **integridade**.
- Os objetivos da segurança de informações se sobrepõem aos da qualidade de serviço. A qualidade do serviço tende a se concentrar em questões de disponibilidade dos serviços no tempo certo, e de informação precisa e exata, deixando de lado a questão de sigilo, mas existem pontos em comum suficientes para que seja útil considerar qualidade de serviço e segurança de forma conjunta.

Qual Informação Deve Ser Protegida ?

A Informação que está:

- Armazenada em computadores;
- Transmitida através de rede;
- Impressa ou escrita em papel;
- Enviada através de fax;
- Armazenada em fitas ou disco.

A Informação que é:

- Falada em conversas ao telefone;
- Enviada por e-mail;
- Armazenada em banco de dados;
- Mantida em filmes e microfilmes;
- Apresentada em projetores;

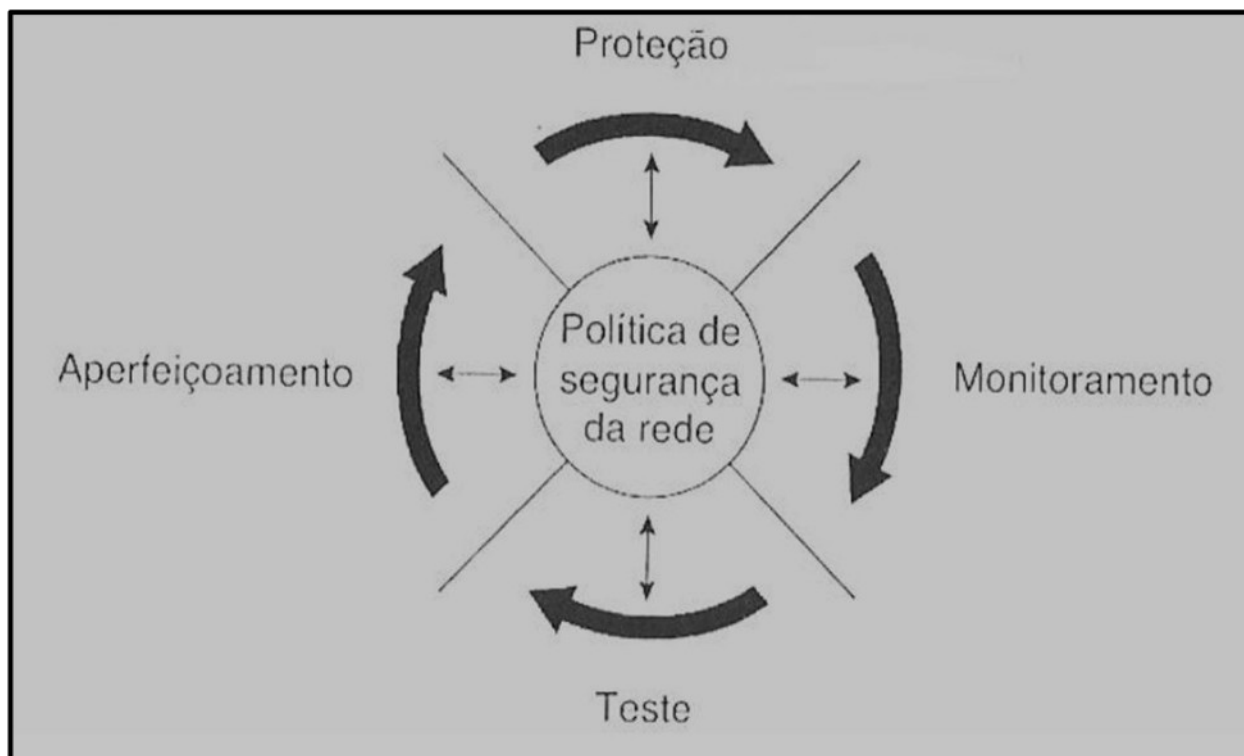
Proteger a Informação De Que ?

- Espionagem industrial;
- Fraude;
- Arrombamento;
- Gravação de comunicação;
- Escuta telefônica;
- Acesso accidental;
- Empregado desleal;
- Crime organizado;
- “*Hacker*” de computador;
- Etc...

Importância de Proteger a Rede

- Ao analisar uma política de segurança deve-se comparar o custo referente aos recursos humanos e de capital para implantar a política, com os custos de exposições a violações de segurança.
- O investimento na segurança da rede deve ser comparado com o possível prejuízo econômico a possíveis violações de segurança.

Processo para Implementar Segurança



Avaliando a Postura de Segurança

- É o esforço contínuo e iterativo da empresa para tentar proteger seus bens mais importantes, da maneira mais econômica, reduzindo o risco a um nível aceitável.
 - Proteção
 - Monitoramento
 - Teste
 - Aperfeiçoamento

Proteção

- Proteger os dados corporativos no nível necessário.
- Tecnologias de segurança são implantadas.
- Firewalls, sistemas de autenticação, proxy Web, sistemas de detecção de intrusão, protocolos criptografados.

Monitoramento

- Observar a atividade em pontos críticos de acesso à rede.
- Monitorar continuamente a rede para verificar intrusões.

Teste

- Certificar-se de que as medidas de segurança sejam suficientes para resistir à sofisticação crescente e frequência de ataques.
- Como as redes mudam com frequência, é necessário testar sua postura de segurança e fazer avaliações das vulnerabilidades.

Aperfeiçoamento

- Atualizar as medidas de segurança conforme necessário.
- Atingir o máximo de eficiência operacional e implementar rapidamente os aperfeiçoamentos.

Chave para Implantar com Êxito a Segurança da Rede

- Equilibrar a facilidade de uso com o nível de segurança apresentado pelas medidas.
- Se os custos de segurança forem desproporcionais em relação aos riscos reais, haverá prejuízo para a empresa.
- Se as medidas forem restritivas demais, os usuários poderão encontrar meios de alterá-las.